



User Guide



Rev 1.8

This document and any files transmitted with it contain information which is privileged and/or confidential. This document is not to be released in the public domain and is for use by authorized users of the CFID product only. If you have received this document in error or you are not the intended recipient, you may not use, copy, disseminate or distribute it. If this document has been downloaded or distributed in error, please contact support@scgcanada.com.

1	Introduction.....	1
2	Hardware Overview	4
3	Configuration.....	5
4	Operation.....	10
5	DJI UAV Extraction & Processing.....	17
6	CFID Android Based UAV Viewing Application	18
7	REMOTE VPN Connectivity	19
8	SIM Card - Extracting & Viewing	20
9	Accessing the CFID.....	21
10	PC/Laptop/Tablet Imaging.....	24
11	Password Recovery	27
12	Firmware Update Procedure	27
13	CFID Equipment Best Practices	28
14	Glossary of Terms	29
15	Appendix A – BIOS Hot Keys	30
16	Appendix B – Smart Copy Rules	31
17	Appendix C – Working With Image Files	32
18	Appendix D – Managing Watch-Lists	33
19	Appendix E – CFID Default Transfer Settings	34
20	Appendix F – CFID Accessories.....	35

Thank you for your purchase of the CFID.

This guide will provide a basic understanding of the CFID interfaces and functionality. Following examination of this guide the user will be able to properly use the CFID as intended by the manufacturer. Further information (including in person training) beyond this guide is available directly from the manufacturer or your distributor.

Please contact support@scgcanada.com for more information or help.

1 Introduction

1.1 About The CFID

The Covert Forensic Imaging Device (**CFID**) is a device designed for SOF units, intelligence operators, site exploitation operations personnel and forensic collection users. We have succeeded in significantly reducing the delay associated with in-field forensic data reconnaissance. Prior to CFID, acquisition by an operator of actionable time sensitive data in real time was difficult given equipment constraints. CFID allows its users to retrieve and retain forensically sound data in seconds and minutes on a target or objective of interest.

1.2 What is the CFID and what can it do?

The CFID is a small, battery powered, hand held device with upgradeable firmware and an expanding suite of features. The primary purpose of our device is the rapid, in field extraction of data from SIM cards, mass storage devices (USB sticks, SD cards) and Smartphones such as iOS and Android devices. The CFID also provides the ability to forensically image or copy hard drives of devices such as desktop PCs, laptops or tablets. CFID includes powerful functions such as watch-list searching for SIM cards and web based remote connectivity

1.3 Important Notice

1.3.1 CFID is now an exFAT Licensed Device

CFID firmware 5.12.017 and greater is now licensed by Microsoft to support the exFAT filesystem. Previous to this and due to licensing restrictions, the filesystem type was limited to FAT32. Once a secure wipe is performed on the CFID with this latest firmware (or anything in the future), the CFID's internal drive will be re-formatted as exFAT. So if your CFID has been updated, but a secure wipe has not been performed, it is suggested to do so at least once. This process only needs to occur once.

One of the key benefits of this is that the MAX file size is now > 4GB making dealing with disk images less cumbersome since they do not have to be split into smaller chunks.

1.4 What Supporting Equipment Comes With CFID?



CFID is shipped with the following equipment. Kits shipped prior to 2019 may not have included all of the following accessories.

- Multi-Pouch Soft Case for Entire Kit
- CFID Device
- Small CFID Pouch
- Power Adapter
- Plug for power adapter for US,UK and EU
- Ethernet cable
- USB 3.0 Type A to Gigabit Female
- Sim Adapter Set x2 per kit
- Type C to USB3.0 A Female
- USB2.0 Micro B to A Female
- USB 3.0 Card Reader
- USB3.0 Type A to Micro Type B
- Type C to micro type B
- 3 in 1 USB Micro Lightning + C Cable

See appendix F for individual description and photos of equipment.

1.5 How do I get support for CFID?

Additional training and support is available for CFID. If you experience any issues with your device or you would like to update to the latest software, contact support@scgcanada.com.

1.6 Feature Summary

- Forensic Imaging, Copying, Cloning & Wiping
- Configurable Smart Copying
- Smartphone Data Extraction
- SIM Card Extraction, Live Preview & Watch-list
- PC, Laptop and Tablet Imaging & Copying
- Network Connectivity
- Browser based access to data
- Easily field firmware upgradeable
- Remote VPN Client
- DJI UAV Acquisition

The CFID is a light-weight hand-held device with a built in solid state hard drive, hardened glass capacitive touch screen and high resolution display.

1.7 Specifications

Dimensions (L x W x H)

108mm x 67mm x 23mm (4.25" x 2.64" x 0.91")

Weight

250 grams (8.8 oz)

Power

Battery: 6000mAH 3.7V LiPoly

Battery Life: 6 Hours (Operating)

External Source: 3A 9V Power Supply

Charge time (Vendor Provided Source): 4 hours

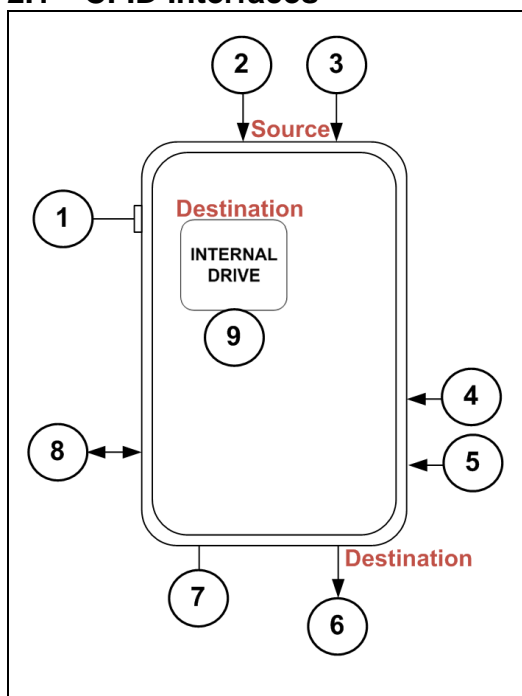
Charge time (USB Device port): 14 hours

Storage

128 GB Solid State Drive

2 Hardware Overview

2.1 CFID Interfaces



1	Power On <ul style="list-style-type: none"> Hold for 5 Seconds or until SEG logo appears Normal Power Off <ul style="list-style-type: none"> Click once to access the CFID SYSTEM CONTROL screen and then press 'SHUT DOWN NOW' on the screen. Force Power Off <ul style="list-style-type: none"> Hold for 10 Seconds
2	SD Card Slot Read Only Source for Imaging <ul style="list-style-type: none"> Supports standard SD cards and supports micro SD adapters.
3	USB 3.0 Host Port Read Only Source for Imaging <ul style="list-style-type: none"> Any USB Mass Storage Device Connect iOS or Android Smartphones Connect USB Ethernet adapter to image
4	Micro SIM Slot
5	Full Size SIM Slot
6	USB 3.0 Host Port Read/Write Destination Drive <ul style="list-style-type: none"> Imaging, Cloning or Wiping Output Connect USB Ethernet adapter to connect the CFID to your network as a shared drive.
7	Power & Charging Port <ul style="list-style-type: none"> Use vendor provided power supply to charge.
8	USB 3.0 Device Port <p>When the CFID is Powered OFF</p> <ul style="list-style-type: none"> Connect port to computer using USB 3.0 device cable (included). CFID will be detected by computer as external hard drive. Copy files to and from the CFID such as SIM card watch-list, image files, SIM Card files etc. Charge the CFID. Note charging from this port is considerably slower than from the power port (7), but it is useful if other power is not available. <p>When the CFID is Powered ON</p> <ul style="list-style-type: none"> This port is not in active for data transfer.
9	Internal Storage Drive (Destination Drive) <ul style="list-style-type: none"> Internal 64 GB Solid State Drive

3 Configuration

TRANSFER SETTINGS	DATE-TIME LANGUAGE	WATCHLIST	ERASE INTERNAL
	SET PASSWORD OR SET ID	SYSTEM INFO	CFID REMOTE TOOLS

3.1 Transfer Settings

Image Type RAW (dd) ENCASE6 FTK ENCASE 5 ENCASE 4	Block Size 1M
Compression None Low(fast) High(slow)	Hash Type None MD5 SHA1 SHA256
Format Type NTFS exFAT FAT32	Wipe Method Zero RANDOM
Notifications None END START START END START WARN END	SD Mode READ ONLY READ+WRITE
AutoStart Mode DISABLED AUTO IMAGE AUTO COPY AUTO SMARTCOPY	Image Split Size MAX 3GB 1GB

Default Transfer Settings are highlighted in Yellow.

3.1.1 Image Type

There are several file types that the CFID can store images in. 'dd' is the standard industry raw format. Encase and FTK are formats recognized by popular forensic analysis tools. We recommend 'dd' unless an analyst has requested otherwise.

3.1.2 Compression

Compression options can be used to reduce the size of image files stored on destination devices. The open-source software LZOP can be used to uncompress images once removed from CFID. Compression will slow down the imaging process and only applies to disk imaging, not copying, cloning, formatting, or wiping.

3.1.3 Format Type

CFID provides the ability to format destination devices using one of three file system types, FAT32, exFAT and NTFS.

3.1.4 Notifications

The CFID can be configured to warn users of the Start and/or End of a process with a vibration

3.1.5 AutoStart Mode

This configuration option is used to automatically start a process as soon as a device is detected.

3.1.6 Block Size

A Block is the minimum amount of data transferred at once from a source device during Cloning or Imaging. CFID is currently fixed at an optimized 1M. This is where a custom block size could be implemented.

3.1.7 Hash Type

This option is used for imaging and allows the user to choose the type of checksum. This feature will slow down the imaging process.

3.1.8 Wipe Method

When wiping destination devices the user has the option to write zeros to every byte of a device or write random data to a device. The generation of random data takes more time.

3.1.9 SD Mode

Devices connected to the source port on CFID are Read Only by default. The user can bypass this setting using the SD Mode option. Warning: This will make the source SD card slot writeable for wiping. This is an advanced feature that will revert back to read-only after a reboot.

3.1.10 Image Split Size

Images can be split into multiple files of 1GB, 3GB, or the MAX that the file system on that destination drive will support. FAT32 is limited to a max of 4GB whereas NTFS and exFAT do not have this limitation. We suggest leaving this on MAX unless you have a specific requirement for smaller files. Newer CFID firmware 5.12.017 and greater support internal filesystem of exFAT on the CFID itself.

TRANSFER SETTINGS

3.2 Date-Time Language




3.2.1 Set Date and Time

Use the up-down arrows to modify the values.

We recommend that the date and time be set and confirmed prior to any usage. Although very minimal, CFID time can drift over long periods. The date time is important because folders are created based on date-time stamps and is a simple way to differentiate between multiple extractions.

3.2.2 Language Options

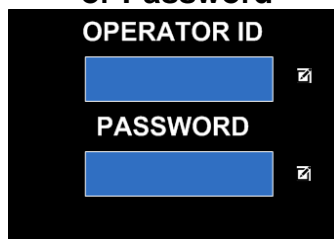
CFID supports foreign languages. Custom languages are enabled as a custom request. Please contact Teel Technologies if you have a specific language request.

3.2.3 Set Time to UTM

When CFID is connected to a network which has internet connectivity the user can sync system date and time to UTM.

DATE-TIME
LANGUAGE

3.3 Set Operator ID or Password



3.3.1 Set Operator ID

The ID could represent a case number, an operation number or your identification number for example. The operator ID is only used to tag all of your extractions with an ID.

3.3.2 Set Password

If set, a user will be prompted for a password upon initial boot up or if the CFID is manually locked.

SET PASSWORD
OR SET ID

3.4 Watch-List

Currently: # of watchlist(s) on this unit.

Watchlist_Name.cfidwl ▼

Add New Record To Watchlist

1234567

7654321

WATCHLIST

3.4.1 Total Watch-List(s)

The top of the watch-list display shows the total number of watch-lists stored on the CFID. Watch-lists can be created manually and loaded onto the CFID via the device port, or via the network connection. Refer to **Appendix D for instructions on managing and creating watch-lists.**

3.4.2 Select Watch-List

Select the watch-list filename from this dropdown menu.

3.4.3 Add New Record

Enter the last 7 digits of the IMSI you wish to add to the watch-list. Your entry does not have to be an IMSI, it can be any 7 digits contained within any number or entry on the SIM card. The entries must be 7 digits in length.

3.4.4 Current Record List

Once a watch-list is selected, It's contents will be displayed in the Record List at the bottom of this screen.

3.5 System Info

Storage Remaining	#####. # MB
CPU Frequency	396 MHz
CPU Temperature	40.0 Degrees Celcius
Battery Voltage	3.578V 2.84 Watts
Battery Current	Discharging at - 784mA
Battery Life	99% 579 minutes
Battery Temperature	40.0 Degrees Celcius

SYSTEM INFO

3.5.1 Storage Remaining

The System Info screen displays the amount of storage remaining on the Internal Drive. **#####. # MB** from image to the left will be replaced with the space remaining on the CFID.

3.5.2 CPU

The speed at which the CFID processor is operating is displayed in real time. It will vary between 336 and 996MHZ based on temperature, usage and required performance.

3.5.3 Battery

Various metrics related to the battery are displayed. This can be used for real time status of the CFID while in operation.

3.6 Erase Internal



ERASE INTERNAL

3.6.1 Make Space

The Make Space option will remove all files excluding watch-lists, SIM Card data and custom copyrules.txt entries. The CFID will restart after this operation.

3.6.2 Delete All Files

This option will remove all files on the CFID and format the internal drive. The CFID will restart after this operation.

3.6.3 Secure Wipe

CFID will perform a full secure erase the internal storage drive. This option will remove ALL DATA the user has collected on Internal Drive.

CFID Firmware will remain intact. Upon completion, the CFID will shut down. When a user powers the CFID up again, the CFID will prompt the user to format it with a simple dialog (since it has been wiped). The CFID will restart after this.

3.7 CFID Remote Tools



CFID REMOTE TOOLS

3.7.1 Create Bootable USB

In instances where a device to be imaged does not have the ability in BIOS to boot from network or it is not working, CFID can be used to create a Bootable USB stick which can be used to USB boot a source computer into the CFID operating system

3.7.2 Tag a Drive As Writeable

When a device is booted via CFID the custom CFID operating system will not allow an operator to write to an external device that is not Tagged as Writeable by the CFID Remote. This feature ensures that an operator is not able to unintentionally overwrite data on the source computer or any disks attached to it..

3.7.3 Remove a Writeable Tag

The opposite of the Tag drive function, an operator can remove a Tag from their drive once operation is completed. Re-formatting will also remove this.

3.8 System Control



3.9 Access the setting Menu

Click the Configuration button or press and release the power button to access system settings

3.10 Lock Screen

Set a password for the device under the settings menu. Use the Lock Screen option to stop unauthorized access to CFID.

3.11 Normal Power Down

Use the SHUT DOWN NOW button to perform a normal shutdown of the CFID.

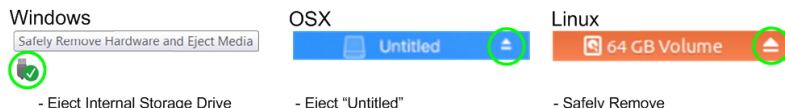
3.12 Force Power Down

To force a power down press and hold the power button for 10 seconds.

4 Operation

4.1 Safely Eject Media and Remove Hardware

While the CFID is powered off and connected to a user computer it will appear as a USB mass storage device. Users should always eject the CFID properly using the options provided in their operating system.



4.2 Device Preparation Prior to Usage

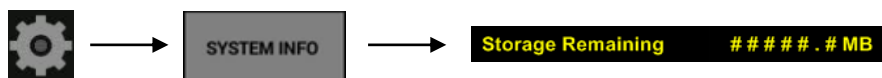
We recommend that you become familiar with the available device and preparation procedures prior to using the CFID.

4.2.1.1 Internal Drive Space

If we intend to use the internal Drive to store data as a **Destination**, we need to ensure there is enough free space.

(Examples: 'Copy' or 'Image' modes)

1. Click the Settings Icon
2. Press the 'SYSTEM INFO' button
3. Confirm there is adequate free space.
4. If more space is required refer to the 'Erase Internal' Section 3.6 of this guide.



4.2.1.2 Format or Wipe External Drives

The CFID is capable of utilizing and/or formatting the following file system types.

- NTFS
- exFAT
- FAT32

If we intend to use an external drive to store data as a **Destination**, we need to ensure that the drive is formatted with one of the recognized file system types. FAT32 is the most compatible. A laptop or computer can be used to format drives for use with the CFID or the CFID can be used to format drives. (If data on the **Destination** needs to be deleted securely, we recommend that the 'Wipe' mode be used, followed by format). The time it takes to wipe a device is proportional to maximum write speed of the device (USB2 vs USB3 for example). Also device size should be considered.

1. Select Format (or Wipe if required).
2. Connect your External device.
3. Select USB as **Destination**.
4. If 'Wiping', the CFID will automatically prompt with an On/Off switch for the 'Format After Wipe' option.
 - a. Set Format After Wipe to 'ON'
5. CFID will provide a final warning that the previous contents of the drive will be destroyed.
6. The 'Wipe' operation by default will write zero to every Byte on the drive.



Check Settings  to pre-configure available 'Wipe Method' and 'Format Type'

4.3 Modes









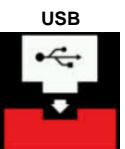


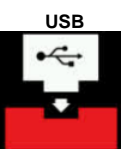



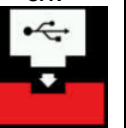











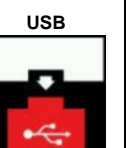
4.3.1 Mode Usage

We recommend that the following workflow be used when selecting a Mode of operation:

1. Optionally restart the CFID if time permits. This will clear all previous RAM and ensure best performance.
2. Disconnect all devices and peripherals from the CFID.
3. Select a Mode and then connect your device(s) one at a time verifying that the appropriate icons appear individually.

4.3.2 CFID Mode Functionality

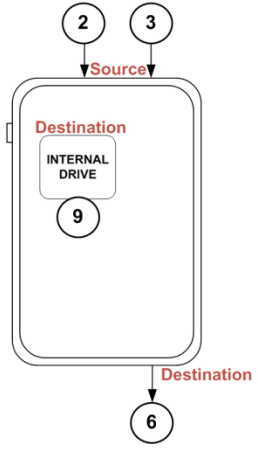
The Main CFID screen provides the following Modes (See UAV Instructions below if looking for the UAV Mode) :

	Image	Copy	Mobile	Format	Wipe	Clone	Uav
Mode							
Source	SD  OR USB 	Internal Drive  OR SD  OR USB 	iOS Device  OR Android Device 			USB 	UAV  See section below on specific UAV details. Mode is only available if licensed.
Destination	Internal Drive  OR USB 	Internal Drive  OR USB 	Internal Drive  OR USB 	USB 	USB  OR 	USB 	Internal Drive  OR USB 

4.3.3 CFID Ease of Use

CFID is designed with operator efficiency in mind. Upon recognition of media installed into **Source** SD or USB slot, CFID can prompt a user with the logical operation based on the **Destination** devices available.

4.3.4 Image



Users can select SD card or USB drive (2) (3) as **Source**

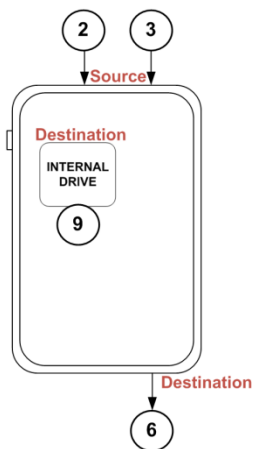
1. Select 'Image' Mode
2. Insert SD card or USB drive into CFID.
3. CFID Ease of use (refer to 4.3.3) applies its logic if applicable, select 'Yes' to begin imaging the connected device(s) or select 'No' and choose alternate options.
4. Once the **Source** and **Destination** devices are connected and available select them.
5. User is prompted to continue.
6. Imaging begins.
7. The CFID will create a new folder on the **Destination** device. The file will be named with the following format:

 'DiskImage-YYYY-MM-DDTHH-MM-SS'.
 Where **YYYY** = Year; **MM** = Month; **DD** = Date;
 'T' = Start of the Time Stamp (time is in universal format, 24 hour clock)
HH = Hour; **MM** = Minutes; **SS** = Seconds

 serials.txt, checksums.txt and metadata.txt will contain the device metadata such as serial number, make, model and manufacturer. If specified, the checksums will exist here as well.

The Destination device must be equal to or greater in capacity to the Source device in order to be able to store the source device image.

4.3.5 Copy – All Files



Users can select SD card, USB drive or Internal Drive. (2) (3) (9) as **Source**.

1. Select 'Copy' Mode
2. Insert SD card or USB drive or select Internal Drive as **Source**.
3. Select CFID Internal drive as **Destination** (9) or Insert USB Drive (6) and select it as **Destination**.
4. User will be prompted with an 'Optional Copy Settings' screen.
5. Turn on '**Copy ALL Files**', Turn off '**Smart Copy**'
6. The user can choose to ignore files greater than 50MB (On/Off) when copying ALL files.
7. Click 'Continue' button.
8. CFID will prompt the user to confirm their selected **Source**
9. Click 'Yes' to continue. The copy function will create a folder on the **Destination** device and copy files there.
10. The CFID will create a new folder on the **Destination** device. The folder will be named with the following format:

 'DiskImage-YYYY-MM-DDTHH-MM-SS'.
 Where **YYYY** = Year; **MM** = Month; **DD** = Date;
 'T' = Start of the Time Stamp (time is in universal format, 24 hour clock)
HH = Hour; **MM** = Minutes; **SS** = Seconds

4.3.6 Copy - Smart Copy

4.3.6.1 Windows Operating Systems Defaults

When using CFID Smart Copy with Windows files system, a special set of files is copied. Typical system files and unnecessary C:\ drive files are not copied. A non standard folder, for example "C:\ImportantDocs" would be copied. Windows Registry files are copied regardless of size, Windows Home Folders (My Documents and Desktop, App Data etc) will be copied. **See** Appendix B **for full details** of what is copied and what is ignored with default rules.

4.3.6.2 Non-Windows Operating Systems Defaults

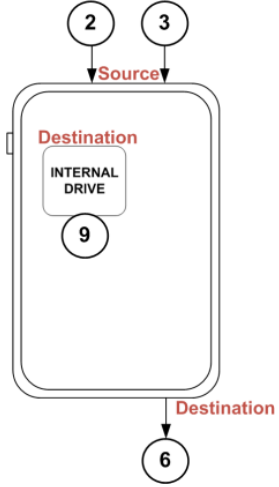
With the exception of the files listed in Appendix B (mp3, video, system drivers), Smart Copy on Mac, Linux and Flash drives will copy all files from the **Source** to **Destination**.

For All Cases (Windows, Mac, Linux, or External drives): If you have a specific set of files that you need or are requested to obtain, we strongly suggest creating a custom copyrules.txt file and testing it on a test system prior to usage. This will optimize time on target and ensure that the right data is collected.

4.3.6.3 Copyrules

The user can customize the Smart Copy operation. To manually specify which files to copy a custom rules file called copyrules.txt is utilized. This set of rules is applied for a Smart Copy regardless of the OS type or device type and overrides all copy settings. copyrules.txt applies to any **Source** drive contents. See Appendix B for full details.

Note: The default rules and copyrules.txt apply to all source types.. including when connecting to PC & Laptops using an external connection. Also, the 'Ignore Large Files' option does not take effect if using copyrules.txt.



The diagram shows a device with a large rounded rectangle labeled 'Destination' in red. Inside this rectangle is a smaller rectangle labeled 'INTERNAL DRIVE' with a circle '9' below it. Above the main rectangle, two circles '2' and '3' have arrows pointing down to a label 'Source' in red. Below the main rectangle, a circle '6' has an arrow pointing down from a label 'Destination' in red.

Users can select SD card, USB drive or Internal Drive (2) (3) (9) as **Source**.

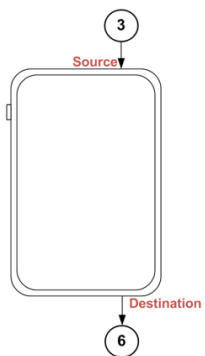
1. Select 'Copy' Mode
2. Insert SD card or USB drive or select Internal Drive as **Source**
3. Select CFID Internal (9) as **Destination** or Insert USB Drive (6) and select it as **Destination**
4. User will be prompted with an 'Optional Copy Settings' screen.
5. Turn on '**Smart Copy**', Turn off '**Copy All Files**'
6. The user can choose to ignore files greater than 50MB (On/Off)
7. Click 'Continue' button.
8. CFID will prompt the user to confirm their selected **Source**
9. The copy function will create a folder on the **Destination** device to copy files into. Click 'Yes' to continue.

4.3.7 Clone

4.3.7.1 About Cloning

Clone will create an exact bit for bit clone of a **Source** device to a **Destination** device assuming the drives are the same size and have the same number of bytes. If the destination device is larger the remaining destination space will not be zeroed. If the destination is smaller than the amount of data clone is limited to the size of the destination device. Cloning has a slight speed advantage over copying since there is no file system overhead but data must be re-imaged before it can be processed

This feature supports disk to disk cloning so the user can clone any source to any destination with the exception of the internal drive. External USB to External USB is typical use case.

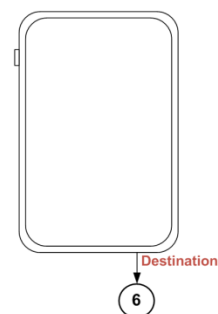


1. Select Clone mode
2. Connect **Source** device being cloned (3)
3. Connect **Destination** device (6)
4. User will be prompted that the **Destination** device will be over written. Do you want to continue (Y/N).
5. Clone begins.

If the progress bar is Yellow the CFID is still working. Make sure that the CFID says complete when it shows 100%. The CFID will pause for a moment while completing the clone process data synchronization which must occur.



4.3.8 Format

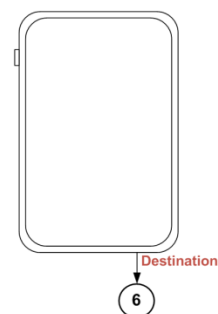


The Format mode allows the CFID user to prepare a source device for use by formatting it. The CFID is capable of formatting **Destination** devices in following file system types:

- NTFS
- FAT32
- exFAT

1. Select Format Mode
2. Connect **Destination** device (6) and select it.
3. User will be prompted that the **Destination** device will be over or re-written. Do you want to continue (Yes/No).
4. Note: That a disk does not need to be formatted by the CFID prior to use, this is only necessary if the disk does not contain a valid file system, or if it needs to be emptied prior to use.

4.3.9 Wipe



The Wipe operation will write zero to every Byte on the drive. Wipe time is proportional to device size.

1. Select 'Wipe' option.
2. Connect your External device
3. Select USB as **Destination**
4. CFID will automatically prompt with an On/Off switch for the 'Format After Wipe' option.
5. Set Format After Wipe to 'ON'
6. CFID will provide a final warning that the previous contents of the drive will be destroyed.
7. In settings, users can also choose to wipe random data as opposed to zeros.

4.3.10 Mobile – Apple

4.3.10.1 iOS Backup

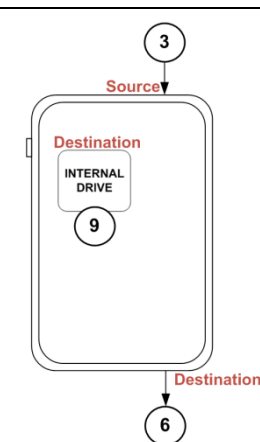
iOS backup is the method Apple uses to create a backups of an iOS device. The contents of backups can be viewed using a third party tool. The CFID is an excellent tool to extract iOS backup files from devices for future analysis.

4.3.10.2 View iOS Backup Contents

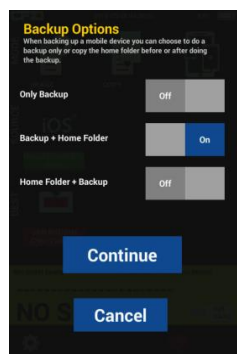
To view the contents of the iOS backup, including but not limited to SMS messages, contacts and photos we recommend an application called 'iPhone Backup Extractor' (<http://www.iphonebackupextractor.com/>) If the iOS backup is encrypted, this program will allow you to enter a password to extract the contents (professional version). The tool can export content in multiple formats and is a low cost option for quickly viewing the contents of a backup. Software retails for approximately \$69 USD. Other options to view iOS backup content include Cellebrite Physical Analyzer.

4.3.10.3 OEM Cable Compatibility

We highly recommend using OEM cables for iPhones or any mobile devices. Many non-OEM cables will cause issues with CFID connection.



Backup Options Confirmation Screen



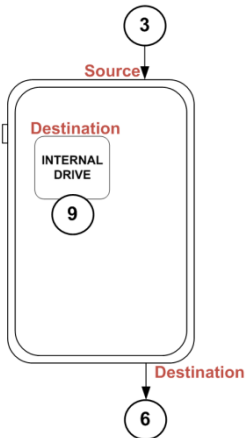
1. Select 'MOBILE' from the main menu.
2. Unlock the iOS device if it is locked and open it to the home screen.
3. Disable Personal Hotspot and Ensure the Screen is set to never auto lock. The phone must stay unlocked during this process.
4. Connect an iOS device to the **Source** (3) of the CFID using a standard Apple USB cable.
5. The iOS device will prompt you to 'Pair' or 'Trust This Device' select 'YES'.
6. If the iOS device connects successfully, you will see an iOS icon **iOS** appear as the **Source** device.
7. If the iOS icon does not appear as a **Source** device, then unplug it, wait 3 seconds and plug it back in. It may take 1-2 tries.
8. Select CFID Internal (9) as **Destination** or insert USB Drive (6) and select it as **Destination**.
9. Click on the **Source** iOS icon and an available **Destination**.
10. The Backup Options screen will be displayed
 - a. Only Backup – Perform iOS backup.
 - b. Backup + Home Folder
 - c. Home Folder + Backup
11. The Backup Options confirmation screen will display: "The following iOS device: (Phone Name) will be copied to <The **Destination** device user selected in Step 7>. Click Yes
12. Backup will begin after a few moments.

If the progress bar is Yellow the CFID is still working. Make sure that the CFID says complete when it shows 100%. The CFID will pause for a moment while completing the clone process data synchronization which must occur.




The CFID will create a new folder on the **Destination** and save the iOS backup in the new folder. The folder name is a long string of characters representing the device ID.

4.3.11 Mobile – Android



The diagram shows a CFID device with a 'Source' port (3) at the top and a 'Destination' port (6) at the bottom. An 'INTERNAL DRIVE' (9) is located in the center. Arrows indicate data flow from Source to Internal Drive and from Internal Drive to Destination.

1. Select 'MOBILE' from the main menu.
2. Unlock the Android device and open it to the home screen.
3. Ensure that USB Debugging is enabled on the phone.
4. Connect an Android device to the **Source** (3) port of the CFID using a standard mobile USB cable.
5. When connected the Android device the user will see "USB Connected".
6. If the Android device connects successfully to the CFID, the Android icon will appear as a **Source** device. 
7. If the Android icon does not appear as a **Source** device, then unplug it, wait 3 seconds and plug it back in.
8. Select CFID Internal (9) as **Destination** or insert USB Drive (6) and select it as **Destination**.
9. Click on the **Source** Android icon and an available **Destination**.
10. The Backup Options screen will be displayed
 - a. Only Backup – Perform Android backup.
 - b. Backup + Home Folder
 - c. Home Folder + Backup
11. The Backup Options confirmation screen will display: "The following Android device: (Phone Name) will be copied to <The **Destination** device user selected in Step 7>. Click Yes.
12. Backup begins.

If the progress bar is Yellow the CFID is still working. Make sure that the CFID says complete when it shows 100%. The CFID will pause for a moment while completing the clone process data synchronization which must occur.

In Progress

100%

COMPLETE

100%

The CFID will create a new folder on the **Destination** and save the Android content into the new folder.

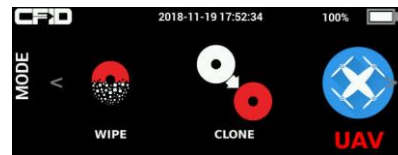
Once the Android is plugged in, wait until you see USB connected before trying to plug in the device again.

The user can view the backup folders using 3rd party extraction software or file viewer.

5 DJI UAV Extraction & Processing

The CFID can collect data from many DJI UAV Devices. It will support all models from the Phantom 3 Series onwards.

The CFID can extract data directly from the internal micro SD card, or via direct connection to the UAV in most cases. Once data is extracted, the CFID will generate KML and CSV files with the flight logs on them. General guidelines are below



An additional mode is available on CFID devices which have been activated for UAV Support. The blue icon above will appear and be selected automatically if a supported model is attached to the CFID.

5.1 Guidelines for UAV Extraction

5.1.1 Image or Copy the Internal Micro-SD from the UAV

If the UAV is damaged, you can extract the micro sd card from the logic board (this is not the same as the card that is externally accessible and contains the photos/video) and image it with the CFID. Once a memory card from a UAV is inserted into the CFID, it will be detected as a UAV device and processed. The CFID will process this like any other media device, but will automatically generate the DAT, KML, and CSV files for you once it detects UAV data on the card.

5.1.2 Connect the UAV directly to the CFID

Once the CFID is connected to the UAV, it will be detected as such and the mode will switch to UAV mode.

It is suggested to optimally process the UAV by allowing the CFID to detect the model, and exploiting it using the build-in UAV processing system within the UAV Mode of the CFID.

Once automatic processing is complete, we suggest removing the external sd card which contains photos and videos, and processing that separately like you would process any regular micro sd card separate from a drone completely.

5.2 Power status

In both cases, whether direct connect or by imaging the internal sd card manually, no special options are required to be selected, the CFID will automatically sense that the content is from a UAV and generate the KML and CSV files for you.

5.3 Special Cases

5.3.1 DJI Inspire

The DJI Inspire requires a Type A to Type A cable for extraction.

5.3.2 Mavic Pro Controller

The CFID supports extracting hidden photos from the Mavic Pro controller. In this case, please ensure that the CFID is connected to the controller when the controller is turned off, and then the controller is turned on while already connected to the CFID. Please also ensure that the CFID is FULLY charged before attempting this extraction due to the large current draws from the controller. If the CFID is not fully charged, it may reset. This extraction may require multiple attempts due to the precise timing required for the attack.

6 CFID Android Based UAV Viewing Application

The CFID now comes with a free APK which can be used for viewing flight logs extracted from UAV Devices. The application includes support for offline mapping in case there is no data connectivity on the android device being used to view the logs.

6.1 Installation & Operation

6.1.1 Please contact support@scgcanada.com for more information.

7 REMOTE VPN Connectivity

The CFID will connect to an OPENVPN server upon sensing any network connectivity given that the following configuration options are set:

7.1 Steps To Configure Built In VPN

7.1.1 Create a folder

Folder called 'vpn' is put in the root of the internal storage on the CFID.

7.1.2 Copy configuration file to the CFID

A configuration file named '**vpn.ovpn**' should be placed in the vpn folder and must contain the complete connection profile for your vpn. This includes the certificates and optionally the private key to connect to the VPN.

7.1.3 Authentication

If an auth file is present called '**auth.txt**' next to the configuration file, the CFID will attempt to authenticate using the auth.txt file. If **auth.txt** is not present, the CFID will attempt to authenticate using the private key stored within the **vpn.ovpn** file. The format of the **auth.txt** file is a username on the first line and a password on the second line, plain text. Do not include the word 'username or password' in the file, only their values, one per line.

7.1.4 Mobile Access (GSM/LTE)

If a file called apn.txt is included, this will enable a mobile apn to ensure connectivity while using a cellular connection. The CFID will support connections from most Huawei data sticks. For specific device support please send us the model number of your connection device and we will work together to ensure the drivers are available on the CFID.

7.1.5 Requirement

VPN connectivity requires the date/time to be set properly on the CFID prior to connecting. This is a common issue.

VPN connectivity generally requires that you connect from outside of the lan which the VPN server resides on. This depends on your setup, but is also a common issue while testing.

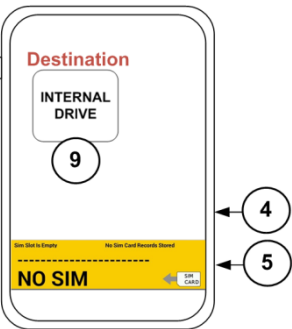









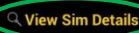


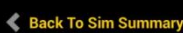

A log file will exist in the vpn folder if connectivity issues are present.

7.1.6 VPN Status

VPN connectivity status is available on the network info page including the LAN IP, and the VPN IP. The VPN IP is what someone within your network requires to access the CFID remotely

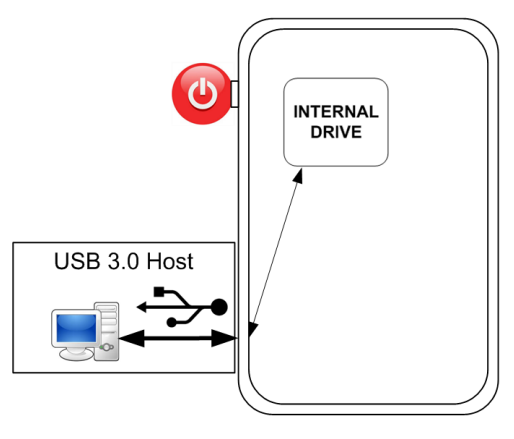
8 SIM Card - Extracting & Viewing

SIM Card data which has been extracted is stored on the CFID's internal drive. Consult the 'Retrieving Data From Internal Drive' for details on how to view this data.

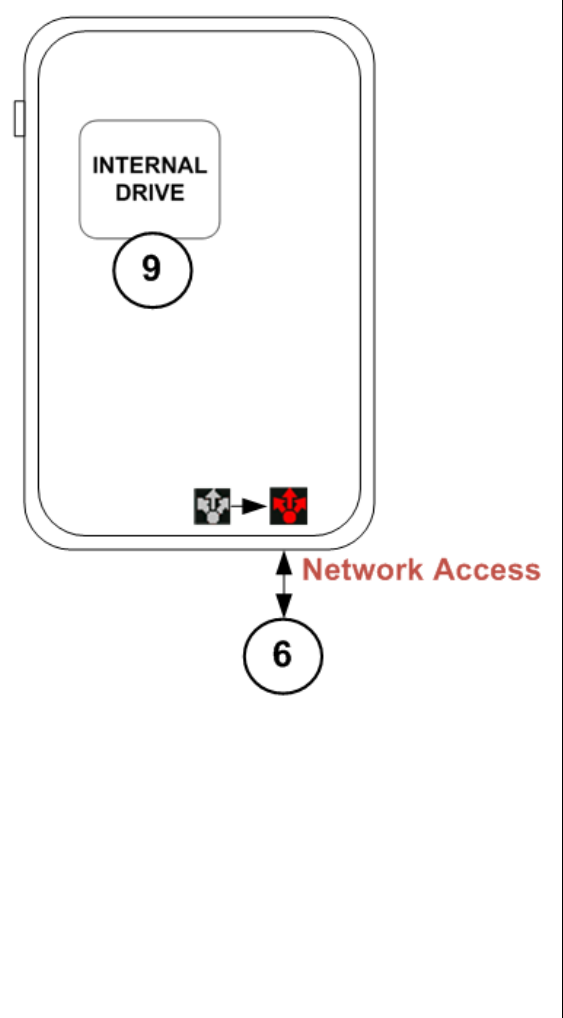
<div></div> <div>Watch-list On / Off Buttons</div> <div></div>	<div><div>1. To extract SIM card data, simply insert it into full size ⁵ or micro ⁴ slot</div><div>2. The ICCID will be displayed and if found the IMSI of the current SIM. Clicking on the yellow box will open the main SIM Card list.</div><div>3. The current SIM card is highlighted in red. Clicking the arrow to the right of the SIM card in the list will open the summary page.</div><div>4. Summary page allows you to add notes and view basic SIM details.<div><div>a. Watch-list On / Off buttons (left) can be used to quickly add the last 7 digits of this SIM card to your internal watch-list. This is not often used, but can be useful in certain occasions.</div></div></div><div>5. Clicking on the magnifying glass icon on the SIM summary page will allow you to view:<div><div>a. Contact List</div><div>b. Last Dialed Numbers</div><div>c. SMS Messages</div></div></div></div>		
Install SIM CARD, Automatically starts reading SIM shows ICCID and then IMSI.	Read Complete IMSI is also displayed	SIM Card List. Current card highlighted in Red. Watch-list match icon on cards below it.	
<div>1.<div><div>ICCID of Current SIM</div><div>7 Sim Cards On Disk >>> Details</div><div>8970199070529628471</div><div>READING</div><div></div></div></div>	<div>2.<div><div>IMSI of Current SIM</div><div>7 Sim Cards On Disk >>> Details</div><div>250993140814057</div><div>100%</div><div></div></div></div>	<div>3.<div><div>Sim Card List: 7 Records</div><div>8970199070529628471</div><div>SMS: 18 CONTACTS: 0 - 2016-03-17 07:41:53</div><div>8970199070529628471</div><div>SMS: 18 CONTACTS: 0 - 2016-03-17 07:41:10</div><div>8970199050608615276</div><div>SMS: 13 CONTACTS: 34 - 2016-03-09 20:26:10</div><div></div></div></div>	
Summary Page allows you to add notes.	SIM Card Details Example 1	SIM Card Details Example 2	
<div>4.<div><div>Sim Card Details</div><div>ICCID 89014103211887275182</div><div>IMSI 310410188727518</div><div>MSISDN</div><div>SMS 0</div><div>CONTACTS 0</div><div>NO MATCHES</div><div>Add or update user notes for this sim card:</div><div></div><div></div><div></div><div>Back To Media View</div></div></div>	<div>5.<div><div>Sim Card Details</div><div>-----PROVIDER INFO-----</div><div>NETWORK: Beeline</div><div>NETWORK: Beeline</div><div>COUNTRY: Russian Federation</div><div>-----MESSAGES-----</div><div>Ваша просьба перезвонить получена</div><div>DATE: 2007-12-27 18:12:02+03:00</div><div>TYPE: SMS-DELIVER</div><div>NUMBER: +79085235429</div><div>Ваша просьба перезвонить получена</div><div>DATE: 2007-12-27 19:45:59+03:00</div><div>TYPE: SMS-DELIVER</div><div>NUMBER: +79273818126</div><div></div><div>Back To Media View</div></div></div>	<div>5.<div><div>CFD</div><div>2016-04-11 05:23:50 47%</div><div>Sim Card Details</div><div>COUNTRY: Russian Federation</div><div>-----CONTACTS-----</div><div>Еленка 79270998861</div><div>-----LAST DIALED-----</div><div>@@@@ @@@@</div></div></div>	

9 Accessing the CFID


9.1 USB 3.0 Host

	<p>The CFID Internal Drive can be accessed as a mounted USB drive. The firmware upgrade process is also performed in this mode by uploading the latest file on to Internal Drive. Watch-list(s) can be manually updated in this mode.</p> <p>When connecting the CFID to a USB port on a PC or laptop you may be prompted to scan / fix the drive. Select 'Continue without scanning.'</p>
---	--

9.2 Network

	<p>The CFID facilitates access to its internal drive via a network. It also provides network access to devices connected to its Source and Destination ports. Once connected to a network it will initiate a DHCP request for an IP address.</p> <p>9.2.1.1 Available Data</p> <ul style="list-style-type: none"> • Download data • Update watch-list(s) and copyrules.txt files. • Upload new firmware so that it is applied on the next reboot. • Source and Destination Drive content. <p>9.2.1.2 Requirements</p> <ul style="list-style-type: none"> • DHCP enabled network • Gigabit Ethernet to USB 3.0 <p>We recommended that only the model of Ethernet adapters which are provided with the CFID be used however other common (apple, startech) may work as well</p> <p>9.2.1.3 Security Guidelines</p> <ol style="list-style-type: none"> 1. Always ensure that your CFID is connected to a secure network if you have any sensitive data on it. 2. Do not plug it into an unknown internet connection.
--	--



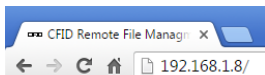
1. Power on the CFID.
2. Connect the USB-Ethernet Adapter to your network.
3. Connect the USB-Ethernet Adapter into the **Destination** USB port.
4. You will then see a Network icon appear in the bottom left corner. It will initially be GREY. Once an IP address is obtained (DHCP required), the Network icon will turn RED.
 1. If you do not see the GREY icon, disconnect the USB Ethernet adapter and re-connect it.
 2. If you see the GREY icon, but it does not turn RED, then you should confirm that your network can provide ip addresses via DHCP.
5. Click the icon to see what the ip address the CFID had obtained.
 1. This is the IP address that a remote user can connect to.
6. The remote user can connect using most commonly available Web browser. 
7. Enter the IP address found in step 5. <http://xxx.xxx.xxx.xxx> (where CFID IP address is xxx.xxx.xxx.xxx).
8. The default username and password are cfid

At this point, the connected remote user will see the contents of the CFID which contains the following folders \\simcards, \\simreports, and \\watch-lists the contents of each can be downloaded.

The **Source** drive ² ³ can be browsed as well. The **Source** drive will be read-only.

9.3 Browser Interface

Web Address



User Login



Username

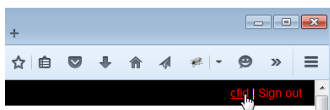
cfid

Password

••••

Sign in

Change Password



Change password

New password:

Confirm password:

Change

Brows Connected Devices



Add Files...

Home » USB_SOURCE » System

Go Back

ntuser.dat

9.4 Typical Network IP address

CFID will acquire an IP address via DHCP as indicated in the preceding section, enter this address into the browser of your choice (CFID has been tested with all major browser types).

9.5 Default Username and Password

Log on using the default username: cfid and password: cfid

9.6 Change Password

Click the CFID hyperlink in the top right corner of the browser window to bring up the Change password option.

9.7 Settings

Clicking the Gear Icons will bring up the configuration page with options based on your selection.

9.8 Device Folders

The names are hyperlinks to folder locations on the device, in this example to access the CFID Internal storage click the name 'INTERNAL'.

INTERNAL

9.9 Adding Files or Folders

Users can upload files from local PC to CFID Internal by clicking the 'Add Files' button. To create a new folder on CFID Internal Drive enter the name of the folder in the field provided and click 'New Folder' Button. This is a great place to add a new watchlist or copyrules.txt file

Add Files...

My_New_Folder

New Folder

9.10 Menu Navigation

The current directory path will be displayed on the left corner of the folder view, use the provided navigation buttons on the web page rather than the web browser buttons for best results.

Home » INTERNAL

Go Back

9.11 Download or Edit Internal Drive Files

CFID configuration files can be edited directly here (you can edit a watchlist or copyrules this way).

copyrules.txt

Download Link:

<http://192.168.1.8/media/INTERNAL/copyrules.txt>

Download

Edit

Rename

Close



10 PC/Laptop/Tablet Imaging

10.1 Booting Custom CFID Remote Operating System

The CFID provides a custom remote operating system which we can boot into via Network Boot (PXE Boot). Alternatively, if a network port is not available the CFID can create a bootable USB stick (see below). Once the source has booted into the custom CFID Remote operating system, it can send data to the CFID over a network cable or write images to a directly connected storage device.

10.2 Image Destination

10.2.1 Internal Drive (Optional, slower)

Ensure that the CFID internal drive has enough free space remaining to image the source device. To check drive space select configuration and 'System Info'. Refer to section 4.2.1.1 for details on checking remaining drive space.

10.2.2 External Drive Connected to CFID (Optional, slower)

An external drive can be connected to the CFID's **Destination** port, this method allows the user monitor the progress of imaging using the CFID device.

10.2.3 External Drive Connected Directly to Source Computer (**fastest option**)

An external drive can be connected directly to the source device to be imaged. We recommend the external drive method as it offers the highest data transfer performance.

10.2.4 Tagging External Drives

If an external drive will be used as the destination device it must first be 'tagged' as writeable by the CFID. This process is used to ensure that any drives already connected to the source computer can never be accidentally overwritten. Tagging is accomplished via the CFID configuration menu under the 'CFID Remote Tools' option. Refer to section 3.7.2 for further information.

10.3 BIOS Access

Typically, you can access the BIOS, or Boot Selection Menu using F12, F10, F8, F2 or ESC or DEL. Depending on the model of the source computer you will need to research this first. Refer to 15.1 for a comprehensive list of commands to access system BIOS by PC, Laptop or BIOS vendor Access to the BIOS is required to instruct a source computer to boot from a location other than it's internal hard drive (network or USB).

10.4 Custom Operating System Options

The following options are available once the CFID Custom Operating System has booted.

F8 - Refresh the drive list on the source PC (**Important!**).

- If you connect an external drive to the source computer (a **Source**, or a **Destination**). You may need to press F8 once or twice to refresh drives when you start or when new drives are inserted. After each press, please wait a few seconds for the system to synchronize.

CTRL Q - Quit,

- Hold down the power button on the source computer if CTRL Q key combination doesn't shut down the source computer. This option only works on some PCs.

F12 - Quit the CFID client and drop to linux shell.

- User can run manual commands

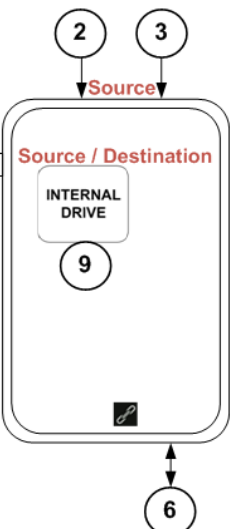

F10 - Disconnect the CFID if a remote process has started.

- User can disconnect and shut the CFID down after F10 is pressed and save battery life while the remote process continues.

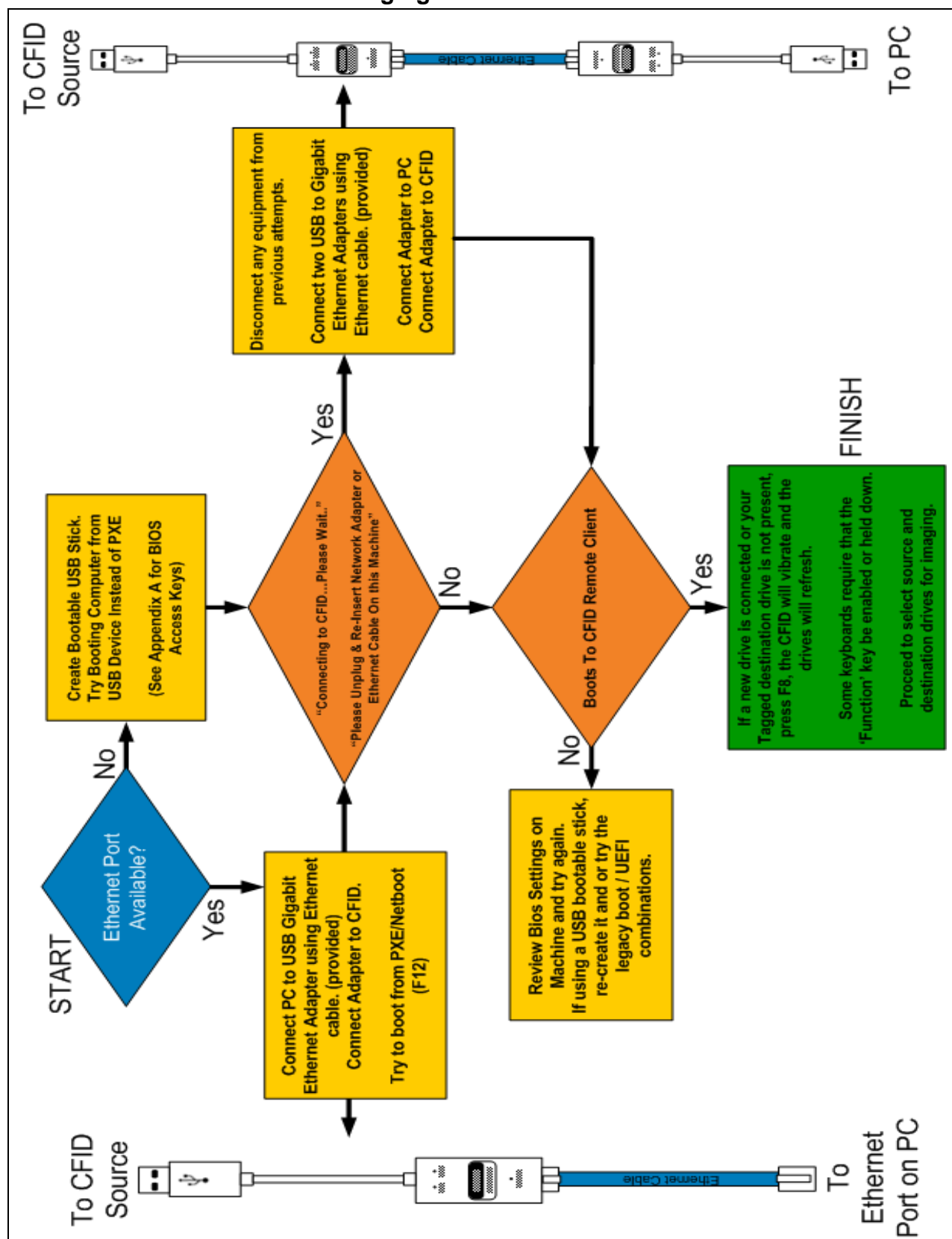
10.5 Devices without Network Adapters

The CFID comes with two Gigabit Ethernet Adapters. In the event of a source computer system not having a functional Ethernet port or not supporting PXE boot, the 2nd adapter can be used along with the USB Bootable Method (see 8.5.1.2 below).



	<ol style="list-style-type: none"> 1. Reboot the CFID if it has not been started specifically for this task. Wait until completely booted. 2. Connect a USB3.0 to Ethernet adapter to the Source port on the CFID and using the short Ethernet cable provided. 3. Connect the other end of the Ethernet adapter to the source computer. 4. The 'Link' icon will appear.  <ol style="list-style-type: none"> a. If the icon does not appear, unplug and try again. b. If still unsuccessful, return to Step 1. c. Once successful, you will feel the CFID vibrate with a heartbeat. 5. Power up the source computer and attempt to PXE or Network boot. <ol style="list-style-type: none"> a. If the source computer gets past the initial boot, but continues to suggest inserting and removing the network cable try using the second USB to Ethernet adapters provided with the CFID. 6. Once you have booted the machine into the CFID Remote environment, you can select the Source and Destination devices, image, or copy as indicated above in this quick start guide. Press F8 to refresh this information after each device is added or removed. <p>10.5.1.1 Image or Copy a Source Computer to External Remote Destination Drive</p> <ol style="list-style-type: none"> 1. In order to safely ensure that the source computer's hard drive is not modified we must tag any of our own destination drives as writeable with the CFID before we can image to them using the remote process. 2. Format your external hard drive using the CFID, or ensure that it is pre-formatted with a valid NTFS filesystem. The system will work with FAT32 or exFAT, but NTFS provides the best performance and stability for this function. 3. Plug the newly formatted drive into the Destination port on the CFID and choose options/cfid-remote-tools/"tag as writeable by cfid remote". This will tag the drive as a possible destination for the remote process when connected directly to the source computer 4. Plug drive into a spare USB port on the source computer and then press F8 one or two times until you see the drive appear on the source computer's screen. This may take a few seconds. The drive should now also show up as a Destination drive now on the CFID and on the source computer. If you select it using the CFID, you will then start a direct process which will image the source computer, to the destination drive directly. Once this has started, you can disconnect the CFID (press F10 then remove the network connection) and the process will continue without the CFID. <p>10.5.1.2 USB Bootable Method</p> <p>If the source computer does not have an Ethernet port and cannot network boot, or is a Macintosh, you must create a bootable USB stick by connecting a new USB stick (this will overwrite existing data on the stick) into the Destination port of the CFID and using options/cfid-remote-tools/"create bootable USB". Certain USB sticks do not write as well as others, so this step should be performed twice to ensure that the bootable stick is created properly. Once your USB stick has been created you can insert it into the source computer and boot from it. This is under Settings – Create Bootable USB. You will still need to connect the CFID to the source computer however. For this, both USB-to-Ethernet adapters are required. The connection in this case would be CFID Source USB port, to Ethernet Cable (via USB Adapter) to source computer via second Ethernet adapter.</p>
---	--

10.6 Flow Chart for Remote Imaging



11 Password Recovery

11.1 Added Security

The only way to restore access to a CFID if the password has been lost is to restore the device to factory defaults by re-loading a firmware image. This is an intended security measure which ensures that only people who have access to the encrypted firmware will be able to re-enable a locked CFID. This only protects access to the CFID functionality itself as **the password does not encrypt the contents of the internal storage**.

To reset the password, perform a firmware update procedure as outlined below.

12 Firmware Update Procedure

12.1 Before you Begin

Connect the vendor provided external DC power adapter.

If your initial SCG boot logo is Blue, please contact the manufacturer or distributor for specific firmware update instructions.

12.1.1 Disconnect Input and Output Devices

Before performing a firmware update it is important to ensure that no devices are plugged into the system.

12.2 Retention of Configuration Options and User Data

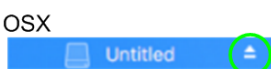
Your configuration options will be reset to default values. Any user data (sim cards and disk images) which may be stored on the internal drive are NOT be affected by this procedure. This procedure does not wipe the internal storage.

12.3 Update Procedure

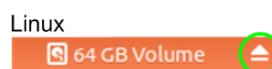
1. Turn off the CFID
2. Plug in the USB 3.0 Device cable into the left hand side of the CFID ⁸
 - a. Plug the other end of the cable into a device hosting the firmware (PC or Laptop)
 - b. Any previously installed firmware could be on the Internal Drive labeled installed_firmware.aes
3. Copy the new x.x.firmware.aes file (link provided to customers via email) onto the CFID and ensure it is re-named firmware.aes (For example, if you downloaded 3.9.9.1.firmware.aes, you would rename it to firmware.aes).
4. Eject the CFID - Users should always eject the CFID as if it was a USB Mass Storage device using the options provided in their operating system.



- Eject Internal Storage Drive



- Eject "Untitled"



- Safely Remove

5. Power on the CFID and wait a few moments for the firmware update to take place. You will see 'NEW FIRMWARE FOUND – PLEASE WAIT' as the process occurs. It takes a few minutes.
6. Upon completion CFID will reboot 2-3 times. Once the CFID is finished a few reboot cycles, it will settle on the home screen.
7. Firmware version can then be confirmed on the System Info screen under settings.

13 CFID Equipment Best Practices

13.1 Use Factory Provide Charger for Best Results

Do not attempt to charge the CFID with anything other than the included DC power adapter that came with your CFID or a standard USB 3.0 device cable. Replacements are available.

13.2 CFID Settings & Internal Storage

If you perform a firmware update on the CFID, your custom settings will go back to factory default (including a blank password) but your user data (sim cards and images) which are stored on the internal drive will not be affected.

If performing a secure erase; your configuration options will not be affected but the internal storage will be securely erased. Refer to 'Upgrade Procedure' Section 12 and Erasing Internal Storage Section 3.6 in this user guide for more information.

13.3 Freeing Space

If the internal storage of the CFID is full, you will not be able to extract SIM cards until space is made for them. See 'Erasing Internal Storage' section of the CFID Manual for options to make space. If require more space on the internal drive, we recommend just deleting the files manually or using the 'Make Space' button. Using the Secure erase of Internal storage option will cause the system to perform a full secure erase of the internal storage drive and then restart itself. It will remove all data that you have collected including SIM cards, disk images, and watch-list(s).

13.4 Default Filesystem

If you choose to format the CFID manually via a pc, you should ensure that the internal drive is formatted FAT32. It can also be formatted as NTFS or exFAT for regular operations, BUT it must be FAT32 for the firmware update system to work. ***In other words, if you format the CFID's internal drive to anything other than FAT32 and forget, the next time you go to do a firmware update, it will not work until it is re-formatted as standard MBR Fat32.***

13.5 Adapter Compatibility

A USB device with an SD socket is a valid Destination. External Hard drives can also be connected to USB ports to be imaged, copied or cloned.

13.6 External Drive Power

If you are using an external USB to SATA adapter to connect to larger hard drives, please ensure they have their own power source. The CFID can provide up to 900mA of current to each USB port but some drives draw considerably more than this when they get older. If the option is available, ensure external hard drives are powered.

If one of the USB ports on the CFID exceeds its 900mA max current rating, it will temporarily shut down that port and no USB devices will be able to be connected to that port until the CFID is shut down and rebooted. This is a safety current limiting feature that will protect the CFID and non-standard drives from an overcurrent state.

13.7 Password Lock

The password lock will deter any unauthorized users from being able to ascertain the type of device or the purpose of the CFID. The contents of the internal drive are not encrypted.

13.8 Powering off or Ejecting the CFID

Do not switch CFID power on while you are copying files to and from it.

Ensure that you safely eject the CFID3 from your computer prior to disconnecting it when using the USB 3.0 DEVICE PORT on the left hand side of the CFID.



14 Glossary of Terms

AES

The Advanced Encryption Standard is a symmetric block cipher implemented in software and hardware to encrypt and protect information.

ANDROID

An open-source operating system typically used for smartphones and tablet computers.

BIOS

Basic Input Output System – A program / set of computer instructions that control input and output operations.

BLOCK

In CFID a Block is the minimum amount of data transferred at once from a source device during Cloning or Imaging.

CFID

Covert Forensic Imaging Device

CLONE

In the CFID Context, drive Cloning is a sector by sector copy of one drive to another facilitated by the CFID.

DD

dd is a command-line utility for Unix and Unix-like operating systems whose primary purpose is to convert and copy files.

DHCP

Dynamic Host Configuration Protocol – A network protocol for automatically assigning IP addresses from servers to clients.

ENCASE

Referenced in CFID as an optional file type to store disk images as.

exFAT

Extended File Allocation Table, compatible with Mac and Windows operating systems.

FAT32

32 Bit File Allocation Table, widely used for compatibility on all platforms. Max file size is 4GB.

FIRMWARE

Software program installed on a hardware device

FORMAT

The act of formatting a drive is the preparation for use. The format function allows the user to specify the type of File Allocation table and the amount of a drive to be used for storage.

FTK

Forensic Toolkit, referenced in CFID as an optional file type to store disk images as.

HASH

Also referred to as a cryptographic fingerprint, the process of converting data into a non-reversible alphanumeric string. Also known as a checksum. Typically MD5, or SHA1, SHA256.

HDD

Hard Disk Drive

HFS

Apple File System

ICCID

Integrated Circuit Card ID – A unique number assigned to a SIM Card. Typically visible on the sim card itself.

IMAGE

Drive imaging is a byte by byte copy of a drive which is stored into a file

IMSI

International Mobile Subscriber Identity is a unique subscriber identification number. Important for SIGINT and a key piece of information extracted from unlocked SIM Cards.

IOS

Operating system used for mobile devices manufactured by Apple

LAN

Local Area Network

LZOP

Open-Source Compression/Decompression program available online. (<http://www.lzop.org/>)

MAC

MAC is a hardware address that uniquely identifies each node of a network.

NTFS

NT File System also known as New Technology Files System used for Windows.

PAIRING

The act of establishing a connection between two devices. Also described as establishing "Trust" between devices. Connecting CFID to a Mobile Phone can require this activity.

PXE

Pronounced pixie, Pre-Boot Execution Environment. Industry standard network boot environment preceding internal operating system.

OS

Operating System

SATA

Serial Advanced Technology Attachment

Secure ATA Erase

A method for completely irrevocably erasing all traces of previous data on an Advanced Technology Attachment (ATA) drive. Generally not recoverable using forensic methods.

SD Card

Secure Digital Card

SIM

Subscriber Identity Module

SSD1 – Internal Drive

Solid State Drive internal to the CFID.

TAG

In CFID context, tagging a drive is adding a digital marking which CFID will recognize. When using the remote process to image a PC or laptop, the CFID will not write to an external drive which is plugged into that source computer unless it has been tagged first by the CFID.

UEFI

Unified Extensible Firmware Interface – Specification for a software program that connects a computer's firmware to its operating system.

USB

Universal Serial Bus

Watch-List

In the CFID context, watch-list is a list of numbers (typically the last 7 of an IMSI) designated by the operator. CFID will alert the user if a SIM card being analyzed is on the pre loaded watch-list.

WiFi

Wireless Fidelity – a facility allowing computers, Smartphones or other devices to connect to the internet or communicate with one another wirelessly

15 Appendix A – BIOS Hot Keys

15.1 BIOS HOT-KEYS

Unless otherwise stated, to access BIOS, power on the device and press the following hot keys once per second. This list contains computer manufacturers as well as specific BIOS makes.

Brand	BIOS Key
Acer	F1, F2, CTRL+ALT+ESC
ALR Advanced Logic Research, Inc. PC / PCI	F2
ALR PC non / PCI	CTRL+ALT+ESC
AMD (Advanced Micro Devices, Inc.) BIOS	F1
AMI (American Megatrends, Inc.) BIOS	DEL
ARI	CTRL+ALT+ESC, CTRL+ALT+DEL
AST	CTRL+ALT+ESC, CTRL+ALT+DEL
Award™ BIOS	CTRL+ALT+ESC, DEL
Cannon	F1
Castex	DEL
Compaq (Red Compaq Logo Screen)	F10
CompUSA	DEL
Cybermax	ESC
Dell	F1, F2, F12, Del or Fn+F1
Digital	F2
DTK (Datatech Enterprises Co.) BIOS	ESC
eMachine	DEL, F2
Enpower (laptop)	Ctrl+alt+s
Fujitsu (Once the Fujitsu logo apears)	F2
Gateway 1440, 2000, 2000 Solo	F1,F2
HP (Hewlett-Packard)	F1, F2, Del or F1 (at blue screen) Esc or F10
Hewlett Packard (Pavillion Notebook)	F2 (Insyde BIOS) or F10
IBM	F1
IBM E-Pro Laptop	F2
IBM PS/2	CTRL+ALT+INS after CTRL+ALT+DEL
Intel Tangent	DEL
Leading Edge	Ctrl+alt+s
Lenovo	F1 or F2
Lenovo Older Products may use	CTRL+ALT+F3, CTRL+ALT+INS or Fn+F1
Micron	F1, F2, or DEL
NEC	F1 or F2
Packard Bell	F1, F2, Del or after Packard Bell start up screen - F1 or F2
Phoenix™ BIOS	CTRL+ALT+ESC or CTRL+ALT+S or CTRL+ALT+INS
Quantex	DEL
Samsung	F2
Seanix	DEL
Sony VIAO (After Sony Start up screen)	F2 then hit F1 or F3
Sharp (Some Very old Sharp require setup Diagnostics Disk)	F2
Shuttle	F2 or DEL on Startup
Tiger	DEL
Toshiba	F1, F2 or ESC

15.2 BIOS Boot Device Settings

CFID requires that the source computer boots UEFI USB, UEFI Network, Legacy Network Boot (PXE BOOT) or USB Boot.

User may need to adjust BIOS settings to Net Boot or USB boot. This typically will require going to “Onboard NIC” at the main BIOS screen. You may need to hit ‘enter’ on the PC during the boot phase if it hangs at the word ‘boot’.

16 Appendix B – Smart Copy Rules

16.1 Smart Copy – Default Settings

In **all cases**, by default the following file types are ignored when smart-copy is used and copyrules.txt is not employed (Windows, OSX, Linux and External Drives):

```
*.mp3
*.m4a
*.sys
*.so
*.dll
*.m4v
*.avi
*.wmv
```

16.1.1 Windows Only Settings

The following directories and files will be copied from a system running a Windows operating system:

"Windows/System32/config/SAM" folders

"Windows/System32/config/SYSTEM" "Windows/System32/config/SECURITY" folder

"Windows/System32/config/SOFTWARE" "Windows/System32/config/DEFAULT" folder

All copies of Users/*/*ntuser.dat files

All users home folders (desktop, documents etc)

16.2 Smart Copy – Options (copyrules.txt)

16.2.1 About copyrules.txt

The **copyrules.txt** file is placed in the root directory of the CFID Internal Drive. If the file is not present the user simply adds an empty file named copyrules.txt and uses it. The file contains specific folders or files they wish to have copied off of the source device in the form of rules. The file copyrules.txt must be spelled exactly as such and the filename must be lowercase. The rules themselves are INCLUSIVE, that is you add content that you would like to include, everything else is ignored.

The user can add a copyrules.txt file to the CFID Internal Drive by:

- 1) Powering the device off, connecting the USB 3.0 Host Cable and uploading copyrules.txt directly.
- 2) Connecting the **Destination** port via provided Gigabit Ethernet adapter to local network and accessing the tool via the web interface.

The % symbol can be used as a wild card prefix or suffix.

'd:' Informs Smart Copy that it should copy a directory

'f:' Informs Smart Copy that it should copy a file

The following examples illustrate how the smartcopy filtering works

Copy the /system/config directory regardless of the preceding directory location

d:%/system/config

Copy any file regardless of location matching the name SystemVersion.plist

f:%/SystemVersion.plist

For directories, it is important to start with d:%/ and if you want a wildcard start of directory name, use

d:%/%partialmatch%

17 Appendix C – Working With Image Files

The 'Image' mode will separate images into separate files based on your 'Image Split Size' setting. In order to analyze the images they must be re-assembled into their original single file.

If compression is enabled, the files are compressed and then split up by the CFID. You must re-join the parts using a file-joiner such as CAT in linux, Copy in windows, or a third part tool prior to decompressing them using the open source LZOP decompression tool.

The following are tools which can be used to perform the assemble image files:

17.1 Linux CAT (to join files)

```
cat device.img.0001 device.img.0001 (etc) > fulldevice.img
```

17.2 Windows File-Joiner (Third Party Application)

A program called File-Joiner (<http://www.igorware.com/file-joiner>) does a great job at joining up file parts.

17.3 Windows COPY (CAT for windows)

On Windows the following command can be used.

```
Copy /b device.img.0001+device.img.0002 (etc) fulldevice.img
```

17.4 Linux LZOP (to decompress files)

If the image is compressed, you must concatenate the individual files (using CAT, or COPY or other tools in windows) before the decompression takes place.

```
STEP 1: cat device.img.lz00 device.img.lz01 etc > fulldevice.img.lzo
```

Lzop is an open-source compression / decompression program. LZOP uses the LZO compression algorithm.

```
STEP 2: lzop -d fulldevice.img.lzo
```

18 Appendix D – Managing Watch-Lists

18.1 Proper Watch-List usage

Watch-list entries must be 7 characters in length. The match system works on matching 7 digits so it is important to use the last 7 digits of the number you are trying to match on. You can utilize multiple watch-lists.

For phone numbers, you should choose the last 7 digits of the phone number not including area codes. For example: 1-613-555-5555 would be entered as 5555555 and +70(1)234-5525-623 would be entered as 5525623.

For IMSI or ICCID identifiers, it is important to choose the last 7 digits of the identifier also. If you enter the entire IMSI, or the entire ICCID, you are likely to get matches on all of the cards from that provider.

When a watch-list match occurs, you will see a flashing red icon in the lower right of the CFID. By clicking on this you can see the details of what matched on which watch-list. Each SIM card record is flagged with the match information if a match was made at the time of extraction.

Records which have previously been collected prior to a watch-list being created are not retroactively scanned.

The watch-list system in the CFID will ignore all non numeric characters and is designed to provide a robust matching system that will search all data on the SIM card including but not limited to the contact numbers, last numbers dialled, SMS content (including text). For this to work properly, it is imperative to ensure that the proper watch-list format is adhered to. Remember: 7 digits/characters max.

18.2 Adding Entries to the Watch-List (4 ways to add)

1. By using the CFID while powered off and by appending a line to a simple text file with the extension `.cfidwl` to the watch-lists folder on the CFID. For example: `highvalue.cfidwl` could contain a line with the number 1234567 and 8945334. The watch-list would then have two entries representing those 7 digit numbers.
2. By using the CFID while powered on and selecting watch-list under settings, you can add a new entry to an existing watch-list directly from the CFID. If there is no existing watch-list, a default one called `watchlist.cfidwl` is created.
3. By appending an existing SIM card to the watch-list from any collected SIM card's details page. This works by selecting the last 7 digits of this SIM card's IMSI and storing it in the watch-list for future encounters.
4. By connecting the CFID over a network and creating a new file with the extension of `cfidwl` in the watch-lists folder.

You can have as many watch-lists as you like.

The system can handle hundreds of thousands of watch-list entries but the larger the watch-list is, the slower the scanning process will be. We suggest keeping the watch-list size small and specific to a particular use.

19 Appendix E – CFID Default Transfer Settings







TRANSFER SETTINGS	DATE-TIME LANGUAGE	WATCHLIST	ERASE INTERNAL
	SET PASSWORD OR SET ID	SYSTEM INFO	CFID REMOTE TOOLS



<h3>19.1 Transfer Settings</h3> <table> <tr> <td> Image Type RAW (dd) ENCASE6 FTK ENCASE 5 ENCASE 4 </td> <td> Block Size 1M </td> </tr> <tr> <td> Compression None Low(fast) High(slow) </td> <td> Hash Type None MD5 SHA1 SHA256 </td> </tr> <tr> <td> Format Type NTFS exFAT FAT32 </td> <td> Wipe Method ZERO RANDOM </td> </tr> <tr> <td> Notifications None END START START END START WARN END </td> <td> SD Mode READ ONLY READ+WRITE </td> </tr> <tr> <td> AutoStart Mode DISABLED AUTO IMAGE AUTO COPY AUTO SMARTCOPY </td> <td> Image Split Size MAX 3GB 1GB </td> </tr> </table> <p>Default Transfer Settings are highlighted in Yellow.</p>	Image Type RAW (dd) ENCASE6 FTK ENCASE 5 ENCASE 4	Block Size 1M	Compression None Low(fast) High(slow)	Hash Type None MD5 SHA1 SHA256	Format Type NTFS exFAT FAT32	Wipe Method ZERO RANDOM	Notifications None END START START END START WARN END	SD Mode READ ONLY READ+WRITE	AutoStart Mode DISABLED AUTO IMAGE AUTO COPY AUTO SMARTCOPY	Image Split Size MAX 3GB 1GB	<h3>19.1.1 Image Type</h3> <p>There are several file types that the CFID can store images in. 'dd' is the standard industry raw format. Encase and FTK are formats recognized by popular forensic analysis tools. We recommend 'dd' unless an analyst has requested otherwise.</p> <h3>19.1.2 Compression</h3> <p>Compression options can be used to reduce the size of image files stored on destination devices. The open-source software LZOP can be used to uncompress images once removed from CFID. Compression will slow down the imaging process and only applies to disk imaging, not copying, cloning, formatting, or wiping.</p> <h3>19.1.3 Format Type</h3> <p>CFID provides the ability to format destination devices using one of three file system types, FAT32, exFAT and NTFS.</p> <h3>19.1.4 Notifications</h3> <p>The CFID can be configured to warn users of the Start and/or End of a process with a vibration</p> <h3>19.1.5 AutoStart Mode</h3> <p>This configuration option is used to automatically start a process as soon as a device is detected.</p> <h3>19.1.6 Block Size</h3> <p>A Block is the minimum amount of data transferred at once from a source device during Cloning or Imaging. CFID is currently fixed at an optimized 1M. This is where a custom block size could be implemented.</p> <h3>19.1.7 Hash Type</h3> <p>This option is used for imaging and allows the user to choose the type of checksum. This feature will slow down the imaging process.</p> <h3>19.1.8 Wipe Method</h3> <p>When wiping destination devices the user has the option to write zeros to every byte of a device or write random data to a device. The generation of random data takes more time.</p> <h3>19.1.9 SD Mode</h3> <p>Devices connected to the source port on CFID are Read Only by default. The user can bypass this setting using the SD Mode option. Warning: This will make the source SD card slot writeable for wiping. This is an advanced feature that will revert back to read-only after a reboot.</p> <h3>19.1.10 Image Split Size</h3> <p>Images can be split into multiple files of 1GB, 3GB, or the MAX that the file system on that destination drive will support. FAT32 is limited to a max of 4GB whereas NTFS and exFAT do not have this limitation. We suggest leaving this on MAX unless you have a specific requirement for smaller files.</p>
Image Type RAW (dd) ENCASE6 FTK ENCASE 5 ENCASE 4	Block Size 1M										
Compression None Low(fast) High(slow)	Hash Type None MD5 SHA1 SHA256										
Format Type NTFS exFAT FAT32	Wipe Method ZERO RANDOM										
Notifications None END START START END START WARN END	SD Mode READ ONLY READ+WRITE										
AutoStart Mode DISABLED AUTO IMAGE AUTO COPY AUTO SMARTCOPY	Image Split Size MAX 3GB 1GB										

TRANSFER
SETTINGS

20 Appendix F – CFID Accessories

Complete Kit Packaged in Soft Case		
CFID Device In Soft Inner Pouch		
Power Adapter	This is a custom power adapter which produces 9V @ 3A. Only provided adapter should ever be used.	
Included are EU UK US Adapters. Australian and others are available upon request.		

Ethernet cable	Used for connecting to the gigabit adapter when performing PXE Boot imaging of laptops.	
USB 3.0 Type A to Gigabit Female	Used for connecting the CFID to any ethernet network,	
SIM Card Adapter Set - x2 per kit	For converting between full size and micro or nano SIM cards. It is recommended to use the nano to full size adapter rather than the nano slot on the CFID.	
Type C to USB3.0 A Female	Useful for connecting the CFID to mobile devices running the CFID Viewing Application in conjunction with the Type A to Micro Type B cable.	
USB2.0 Micro B to A Female	Useful for connecting the CFID to mobile devices running the CFID Viewing Application in conjunction with the Type A to Micro Type B cable.	
USB 3.0 Card Reader	Useful for reading memory cards with the CFID.	

<p>USB3.0 Type A to Micro Type B</p>	<p>Standard cable for accessing data on the CFID with a computer or laptop.</p>	
<p>Type C to micro type B</p>	<p>Standard cable for accessing data on the CFID using a computer, or laptop that has a type C connector.</p> <p>This cable is also used to directly read data from the CFID on Android devices with type C ports.</p>	
<p>3 in 1 USB Micro Lightning + C Cable (Braided)</p>	<p>Multi Cable for a variety of uses including reading data from DJI UAV devices, iPhones, and Androids.</p>	