Intelligent Computer Solutions

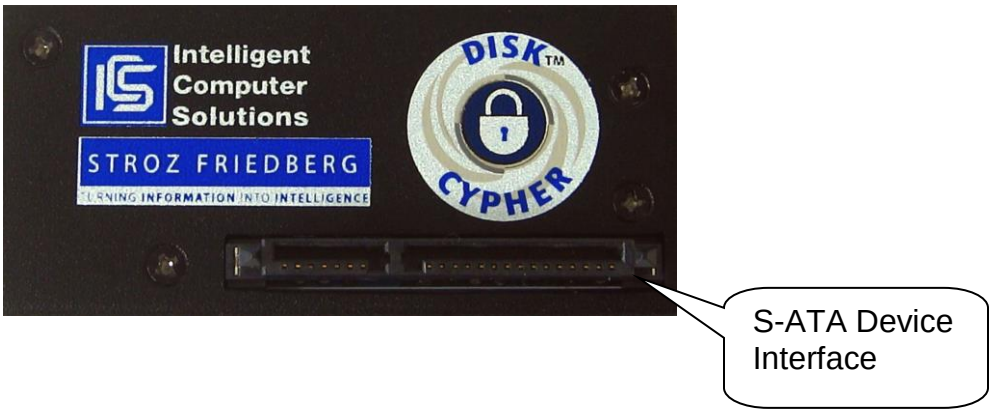
Disk Cypher Quick Start Setup Instructions

Disk Cypher Setup Instructions

The following instructions describe the basic procedure to setup and start using the Disk Cypher with the IM-Solo.

1. Verify that IMSolo-III Forensic Software version 2.0.10.4.f or newer is installed. The IMSolo-III Forensic v20104f.zip Compact Flash upgrade file is available on the supplied Disk Cypher Utility CD. The file can also be downloaded from the ICS FTP site DiskCypher.
2. Verify that a folder named "CFUSER" and subfolder named "CFUSER\CORPKEY" exists on the ICS supplied CF Card. If one does not exist, create a folder named "CFUSER" in the root directory of the IMSolo-III CF Card and a subfolder named "CFUSER\CORPKEY".
3. Erase (WipeOut) the Evidence drive(s) prior to capturing data with Disk Cypher.
4. Connect the Suspect's (Source) P-ATA or S-ATA drive to the IMSolo-III Suspect (Source) position.
5. Connect the Disk Cypher to the Evidence (Target) S-ATA drive(s).

   NOTE: The capture operation supports using a second Evidence drive without a Disk Cypher attached. The second Evidence drive will not be encrypted.



6. Connect the Evidence (Target) S-ATA drive(s), with the Disk Cypher attached, to the IMSolo-III S-ATA Evidence (Target) position(s) using the standard IMSolo-III S-ATA cables.

   NOTE: Do not use LinuxDD Evidence drives which contain previously captured cases, not encrypted using Disk Cypher.

7. If purchased, enter the ICS supplied Disk Cypher Corporate Key and the Disk Cypher ICS Default Key Option Codes using the IMSolo-III Tools\Options\Add Option function. Refer to the section titled "OPERATIONAL MODE INSTRUCTIONS" for additional instructions.

Operational Mode Instructions

Capture and Encrypt Data from Removed Drives using the IMSolo-III *Single Capture* or *LinuxDD Capture* Mode of Operation

The following section describes the procedure to use the Disk Cypher with the IMSolo-III *Single Capture* or *LinuxDD Capture* mode for Capturing and Encrypting the Suspect's data from the drive that has been removed from its PC or Notebook.

Requirements:
- IMSolo-III
- Disk Cypher
- IMSolo-III CF Card

1. Connect and configure the drives as outlined in the "IMSolo-III Disk Cypher Quick Start Setup Instructions".
2. Insert the IMSolo-III Compact Flash Card containing the "CFUSER" folder.
3. Select **Settings** from the **Main** Menu.
4. Select **Operational Modes** from the **Settings** Menu.
5. Select **Single Capture** or **LinuxDD Capture** from the **Operational Mode** Menu.

   NOTE: Sanitize (WipeOut) the Evidence drive(s) prior to capturing data with Disk Cypher. Do not use LinuxDD Evidence drives which contain previously captured cases which were not encrypted using Disk Cypher.
6. Select **Case Info** from the **Settings** Menu and enter required information.
7. Verify the remaining Settings (Refer to Table 1).
8. Select **Run** from the **Main** menu or from the **Settings** menu.
9. Select **Run** from the **Run** Screen. The "Select Encryption Key" menu is displayed.
10. Select **Enter Pass Code** to generate a new User Key. Enter a "Pass Code" containing 8 or more characters. To use a previously generated User Key, which is stored on the CF card, select the existing User Key from the list provided then select **CONTINUE**.

    NOTE: If two Evidence drives are connected with a Disk Cypher attached to both, the same Pass Code and generated User Key will be used for both drives.

    Document the Pass Code entered for future reference.

11. Verify the “Pass Code” by entering the “Pass Code” a second time.
12. Enter a name for the “User Key” which will be generated using the entered “Pass Code”. The ”User Key” will be required to decrypt the data on the Evidence drive when required. The “User Key” file will be stored in the CFUSER folder of the CF card.

    NOTE: Selecting **ENTER** will result in using a default User Key name.
13. The “Select Corporate Key” menu is displayed if the Corporate Key Option is enabled. If the Corporate Key Option is not enabled, continue with step 16.
14. Select **Type in Key**. Enter a password for the Corporate Key containing 8 or more characters.
15. Enter a name for the “Corporate Key” which will be generated using the entered “Corporate Password”. The ”Corporate Key” will be required to decrypt the data on the Evidence drive, if the “User Key” is lost.

    NOTE: Selecting **ENTER** will result in using a default Corporate Key name.
16. Select **OK** to begin the capture operation using the selected Pass Code and User Key. The Disk Cypher will encrypt the data transferred to the Evidence drive(s) “on-the-fly”.

    NOTE: The resulting hash values for the Suspect and Evidence drive(s) are generated using the decrypted data.
17. Refer to the section titled **Decryption Operational Mode Instructions** for instructions to decrypt the encrypted Evidence drive.

Capture Settings
(Table 1)

Menu Item	Setting
Operational Modes	Single Capture/ LinuxDD Capture
Hashing	MD5+
Verify	Disabled (Optional)
Suspect’s Position	Direct
Drive Mode	AUTO
PIO Mode	AUTO
UDMA Mode	AUTO
Wipe Remainder	Disabled (Optional)
Bad Sectors	Prompt
Case Info	Optional
Printer Type	None (Optional)
Printer Port	AUTO

Encrypt Data using a PC

The following section describes the procedure to use the Disk Cypher with a PC to Encrypt data.

Requirements:

- PC
- Unformatted S-ATA Drive.
- ICS Decryption and Key Management Application
- Disk Cypher
- Key Dongle
- Key Loader
- User Key

NOTE: The procedure requires programming a Key Dongle with a User Key generated using the Key Management application. The Key Loader is required to program a Key Dongle.

1. Install the Key Management application and Key Loader using the instructions described in the section titled **Decryption Operational Mode Instructions**.
2. Connect the Key Dongle to the Key Loader's External Key port.
3. Connect the Key Loader to the PC using the supplied USB cable. The Key Loader is power through the USB interface.
4. Run the Key Management application.
5. Select the **RESCAN** function. The Key Loader icon should indicate "Key Loader found".
6. Select **User Key: Create New Key** from the Operational menu.
7. Enter a Password for the User Key using 8 or more characters in the "*Create New Key*" field.
8. Retype the Password in the "*Verify Password*" field.
9. Enter a name for the User Key in the "*Enter Key Name*" field.
10. Enter the path "C:\DiskCypher\CFUSER" in the "*Save Key to Drive*" field.
11. Select the "Send Final Key to Dongle" check box.
12. Select **EXECUTE** to program the Key Dongle with the selected User Key.
13. Disconnect the Key Loader from the PC.
14. Connect the programmed Key Dongle the Disk Cypher. The Key Dongle will be used to encrypt the data written to the drive.

15. Connect the Disk Cypher to an **unformatted** S-ATA drive.

NOTE: Do not use a drive with previously un-encrypted stored data. This will result in loss of data.

16. Connect the drive with the Disk Cypher attached to a PC.
17. Format the drive using the PC's O/S with the Disk Cypher attached. The drive's format will be encrypted.
18. Transfer files as needed to the Disk Cypher attached drive. All transferred data will be encrypted. The drive's contents will only be accessible if the drive is connected using the Disk Cypher with the programmed Key Dongle attached.

Decryption Operational Mode Instructions

The following section describes the procedures to use the ICS supplied “Decryption and Key Management” application and the Key Loader to Manage Keys and Decrypt data, using a PC. The Key Loader is used to program a User Key into the Key Dongle using the Key Management application.

Decryption and Key Management Application Install Instructions

1. Extract the file “DC Key Management.exe”, located on the ICS supplied CF card or the supplied Disk Cypher Utility CD, to a folder on the PC’s local HDD called “C:\DiskCypher”. The file can also be downloaded from the ICS FTP site DiskCypher.

2. Create a Desktop Shortcut for the “C:\DiskCypher\ DC Key Management.exe” application.

3. To run the Decryption and Key Management application, select the “DC Key Management” Desktop Shortcut. The Decryption and Key Management Console will be displayed.

4. If the Key Loader is available, follow the “Key Loader Install Instructions” to configure and connect the Key Loader.

Key Loader Install Instructions

1. Extract the Key Loader driver files from the “Key Loader Driver.zip” file, located on the ICS supplied CF card or the supplied Disk Cypher Utility CD, to the PC’s “C:\DiskCypher” folder. The file can be can be downloaded from the ICS FTP site DiskCypher.

2. Install the Key Loader driver by running the “Key Loader Driver.exe” install application located in the “C:\DiskCypher\Key Loader Driver” folder. A DOS window will open temporarily indicating “Installing Driver” and will close when the driver has been installed.

3. Connect the Key Loader to the PC using the supplied USB cable. The Key Loader is power through the USB interface.

Decrypt Data on a PC, Using the Disk Cypher with an Un-Programmed Key Dongle

The following section describes the procedure to use the Disk Cypher with an Un-Programmed Key Dongle to Decrypt Data from a drive previously encrypted using the IMSolo-III.

Requirements:

- PC
- Encrypted Drive
- Disk Cypher
- ICS Decryption and Key Management Application
- Key Dongle
- Key Loader
- User Key File

NOTE: The procedure requires programming a Key Dongle with the User Key generated during the IMSolo-III capture and encryption operation. Once programmed the Key Dongle can be used along with the Disk Cypher to decrypt the drive for analysis.

1. Connect the Key Dongle (Fig. 2) to the Key Loader's External Key port.
2. Connect the Key Loader (Fig. 3) to the PC using the supplied USB cable. The Key Loader is power through the USB interface.
3. Copy the User Key file generated for the encrypted drive and stored in the IMSolo-III CF Card's CFUSER folder, to a folder on the PC called C:\DiskCypher\CFUSER.
4. Run the Key Management application (Fig. 4).
5. Select the **RESCAN** function. The Key Loader icon should indicate "Key Loader found".
6. Select **User Key: Read an Existing Key** from the Operational menu.
7. Enter the path "C:\DiskCypher\CFUSER" in the "Select Key From Drive" field.
8. Select the "Send Final Key to Dongle" check box.
9. Select **EXECUTE** to program the Key Dongle with the selected User Key.
10. Disconnect the Key Loader from the PC.

11. Connect the programmed Key Dongle the Disk Cypher. The Key Dongle will be used to “unlock” the encrypted drive’s contents.
12. Connect the Disk Cypher to the encrypted drive.
13. Connect the encrypted drive to a PC. The drive’s volume will be accessible for viewing or analysis.

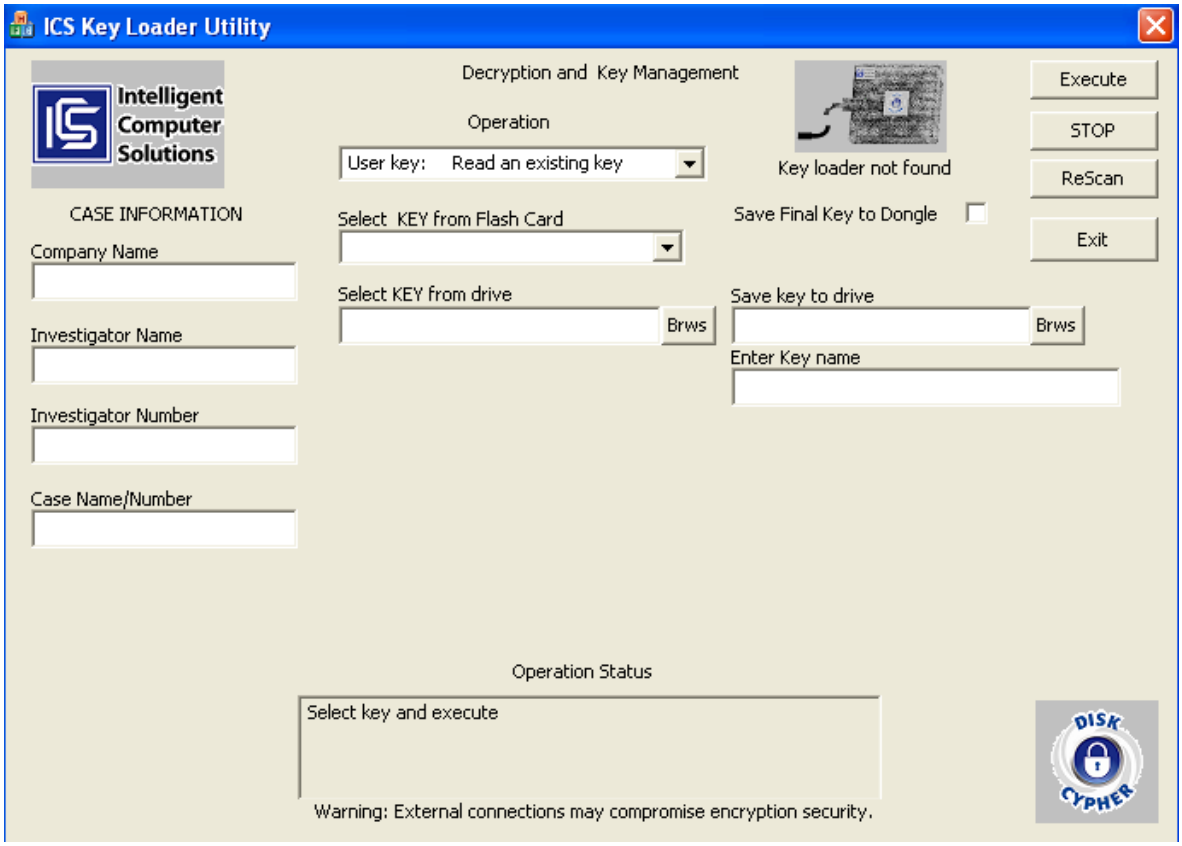
The Key Dongle is used to “unlock” an encrypted drive attached to the Disk Cypher to allow viewing or analyzing the encrypted drive’s data. The Key Dongle can be programmed with a User Key using the Key Loader and Key Management application. The Key Dongle is attached to the Key Loader during programming.

Key Dongle
(Figure 2)

The Key Loader is used to program a User Key into the Key Dongle using the Key Management application (Fig. 4).

Key Loader
(Figure 3)

Key Management
(Figure 4)



Decrypt Data on a PC, Using the Disk Cypher with a Programmed Key Dongle

The following section describes the procedure to use the Disk Cypher with a Programmed Key Dongle to Decrypt Data from a drive previously encrypted using the IMSolo-III.

Requirements:
- PC
- Encrypted Drive
- Disk Cypher
- Programmed Key Dongle

NOTE: The procedure requires a Key Dongle programmed with the User Key which was generated during the IMSolo-III capture and encryption operation. The Key Loader is required to program a Key Dongle.

1. Connect the programmed Key Dongle the Disk Cypher. The Key Dongle will be used to “unlock” the encrypted drive’s contents.
2. Connect the Disk Cypher to the encrypted drive.
3. Connect the encrypted drive to a PC. The drive’s volume will be accessible for viewing or analysis.

Decrypt Data on a PC, without the Disk Cypher

The following section describes the procedure to Decrypt Data from a drive previously encrypted using the IMSolo-III, without the Disk Cypher.

Requirements:
- PC with a blank target drive.
- Encrypted Drive
- User Key File

NOTE: The procedure requires transferring data from the encrypted drive to a blank destination drive. The encrypted data will be decrypted during the transfer operation.

1. Connect a blank target drive to the PC. The drive should be the same size or larger than the encrypted source drive.
2. Copy the User Key file generated for the encrypted drive and stored in the IMSolo-III CF Card's CFUSER folder, to a folder on the PC called C:\DiskCypher\CFUSER.
3. Run the Key Management application.
4. Select **S/W Decrypt** from the Operational menu.
5. Enter the path "C:\DiskCypher\CFUSER" in the "Select Key From Drive" field.
6. Select the "Send Final Key to Dongle" check box.
7. Select the encrypted Source Drive from the *SOURCE DRIVE* pull down menu.
8. Select the Destination Drive from the *DESTINATION DRIVE* pull down menu.
9. Select **EXECUTE** to begin the S/W Decrypt operation.
10. After the operation completes, the Destination drive's decrypted data will be accessible for viewing or analysis.

Decrypt Data using the IMSolo-III, with the Disk Cypher and Programmed Key Dongle

The following section describes the procedure to Decrypt Data using the using the IMSolo-III with the Disk Cypher and Programmed Key Dongle.

Requirements:
- IMSolo-III
- Encrypted Drive
- Disk Cypher
- Programmed User Key

1. Connect the Key Dongle, programmed with the Encrypted drive's corresponding User Key, to the Disk Cypher.
2. Connect the Disk Cypher with the programmed Key Dongle to the Encrypted drive.
3. Connect the Encrypted drive to the IMSolo-III Suspect's S-ATA connector.
4. Connect the Evidence drive(s) to the IMSolo-III Evidence position(s).
5. Select **Settings** from the **Main** Menu.
6. Select **Operational Modes** from the **Settings** Menu.
7. From the **Operational Mode** Menu select **Single Capture** if the Encrypted drive was encrypted originally using the Single Capture mode or select **LinuxDD Restore** if the Encrypted drive was encrypted originally using the LinuxDD Capture mode.
8. Select **Case Info** from the **Settings** Menu and enter required information.
9. Verify the remaining Settings (Refer to Table 2).
10. Select **Run** from the **Main** menu or from the **Settings** menu.
11. Select **Run** from the **Run** Screen to begin the capture operation. The Disk Cypher will decrypt the data transferred to the Evidence drive(s) "on-the-fly".

    NOTE: The resulting hash values for the Suspect and Evidence drive(s) are generated using the decrypted data.

Capture Settings
(Table 2)

Menu Item	Setting
Operational Modes	Single Capture/ LinuxDD Restore
Hashing	MD5+
Verify	Disabled (Optional)
Suspect's Position	Direct
Drive Mode	AUTO
PIO Mode	AUTO
UDMA Mode	AUTO
Wipe Remainder	Disabled (Optional)
Bad Sectors	Prompt
Case Info	Optional
Printer Type	None (Optional)
Printer Port	AUTO