

Acquiring and Encrypting Evidence Data in the Field

Easy Key Management

Manage your keys by plugging the KeyLoader via USB connection to your Forensic Workstation. Create, erase, duplicate and transfer Key code(s) to your Key dongle(s) or CF card(s) utilizing the Keyloader Utility Software.

KeyLoader Utility Software

Key Dongle

CF Card

Key Dongle Option

Step 1
Prior to going into the field, prepare the key dongle(s) you will use to encrypt the Evidence Drive(s) utilizing a PC, a KeyLoader and the KeyLoader Utility Software

Step 2
Connect the DiskCypher(s) with the key dongle(s) to the Evidence Drive(s) and then plug the DiskCypher into the Solo-3 unit using the provided SATA cable. You can make up to two Evidence copies simultaneously, but you must have a DiskCypher (and key dongle) for each drive. Begin the acquisition process.

Step 3
Remove your Encrypted Evidence Drive and transport or ship it to your Forensic Lab with confidence the data is secured in the event drive is lost or stolen

Compact Flash Option

Step 1
Prior to go to the field, prepare the CF Card with the key Code you will use to encrypt the Evidence Drive(s) utilizing a PC and the KeyLoader Software

Step 2
Connect the DiskCypher(s) to the Evidence Drive(s) and then plug the DiskCypher into the Solo-3 unit using the provided SATA cable(s). You can make up to two copies simultaneously, but you must have a DiskCypher for each drive. Insert the CF card into the Solo-3 Unit. Begin the acquisition process. Solo-3 will prompt you to select which encryption key code you would like to use. You can choose the key code from the prepared CF card or you can enter a passphrase directly on the Solo-3 keyboard to generate an encryption key without the CF card or a Key Dongle.

Step 3
Remove your Encrypted Evidence Drive and transport or ship it to your Forensic Lab with confidence the data is secured in the event drive is lost or stolen

Decrypting and Analyzing Evidence Data in the Forensic Lab

Option 1 Decrypting "on the fly"

Only one step!
Simply connect the DiskCypher with its key dongle to the Encrypted Evidence Drive and then plug the DiskCypher into your Forensics WorkStation via SATA cable. You can now work with the data on the drive, it will appear as a new drive letter on your WorkStation.

CAUTION! if you made a 100% copy (as opposed to a forensic DD image) of the Suspect Drive using Solo-3, you will need to utilize a Write Protection device such as the Super DriveLock between the DiskCypher and your WorkStation.

Recommended

Option 2 Decrypting with Solo-3

Step 1
Connect the DiskCypher to the Encrypted Evidence drive and then plug the DiskCypher into the Solo-3 unit in the **SUSPECT POSITION** using the provided SATA cable.

Step 2
Plug the key dongle into the DiskCypher

Step 3
Make a 100% copy of the Encrypted Evidence drive and the data will be decrypted as the copy is made.

Step 4
Connect the Decrypted Evidence drive to your WorkStation.

Option 3 Decrypting with ICS Utility Software

Step 1
Connect the Encrypted Evidence drive and another sanitized hard drive to your PC using eSATA cables.

Step 2
Use the ICS Utility Software to decrypt the Encrypted Evidence drive data and save it to the other drive as decrypted data