




A User Guide for the FRED Family of Forensic Systems



Thank you for your recent order. We hope you like your new FRED!

Please do not hesitate to contact us if you have any questions or require any additional information. The best method of contact is via our website www.digitalintelligence.com. The sales and technical support ticketing system is easy to use and allows us to track all requests and responses. It also increases the number of team members that can view your requests and decrease your wait time for an answer. You can also call us at our toll free number if you prefer.

To create your user account click on the User Icon  on the top right of the web page banner and click on Sign Up. Here you can register your FRED system as well as track your web order history and support tickets. Please note your system serial number is the unique identifier for your system and typically located on the back of your FRED near the power supply. It is helpful if you use the system serial number in your correspondence.

If you have a sales related question or technical support issue, simply navigate to www.digitalintelligence.com/support. A searchable knowledge base, links to other help or informational topics as well as an "Open A Ticket" button link can be found near the bottom of the page. You can often find the answers to your technical questions in our existing knowledge base.

We want to remind you, regardless of your warranty status, we will always be willing to assist with any technical questions you have regarding any Digital Intelligence product.

***** Read me first *****

Forensic Recovery of Evidence Device

This document contains important information about the configuration and operation of your FRED system. **FAILURE TO FOLLOW THESE GUIDELINES MAY RESULT IN PHYSICAL DAMAGE TO YOUR EQUIPMENT WHICH IS NOT COVERED UNDER WARRANTY.** Do not attempt to operate your equipment prior to reading and understanding this document. Please call Digital Intelligence if you have any questions regarding this information: (866) DIGINTEL

Before starting the system for the first time, all Drive Trays that do not contain hard drives should be unlocked and slid out of the rack far enough to disengage the connector on the back of the tray to avoid confusion with Windows during the initial setup.

SYSTEM IDENTIFICATION	1
QUICK SETUP	2
UNPACKING YOUR FRED	2
PHYSICAL SET UP	2
REMOVABLE DRIVE TRAYS	2
MONITOR(S)	2
KEYBOARD/MOUSE	2
POWER AND ENVIRONMENT	3
SECURITY “DONGLES”	3
INITIAL SYSTEM START-UP	3
SYSTEM COMPONENTS	4
USB HUB	4
ULTRABAY 4D™ AND ULTRABAY 4™ HARDWARE WRITE BLOCKERS	4
RETRACTABLE VENTILATED IMAGING SHELF	5
USB 3.0 FORENSIC CARD READER	7
BLURAY-DVD DRIVE	8
REMOVABLE DRIVE BAYS	8
SATA REMOVABLE DRIVE BAYS	9
HOT SWAP REMOVABLE DRIVE BAYS	9
MOTHERBOARD USB PORTS	10
RAID ARRAY(S)	10
POWER SUPPLY	11
INSTALLED/INCLUDED SOFTWARE	13
OPERATING SYSTEM INFORMATION	13
TABLEAU IMAGER (TIM)	13
TABLEAU FIRMWARE UPDATE (TFU)	13
SYMANTEC GHOST	14
FACTORY IMAGE RESTORATION MEDIA	14
TOOLBOX	14
PROCEDURES	15
OPERATING PROCEDURES	15
<i>Working with “Hot Swap” Removable Drive Bays:</i>	15
<i>Working with SATA Removable Drive Bays (without HotSwap label)</i>	15
<i>Notes about “Dongles”</i>	15
ETHERNET CONNECTIONS	15
ULTRABAY USE	16
CARD READER USE	17

BEST PRACTICES	18
STORAGE CONFIGURATION	18
IMAGING AND COMPRESSED IMAGES.....	18
PERIODIC/MAINTENANCE PROCEDURES	19
OPENING YOUR COMPUTER’S CASE.....	19
ULTRABAY FIRMWARE UPDATES.....	19
WINDOWS UPDATE.....	19
TROUBLESHOOTING	19
CONTACTING TECHNICAL SUPPORT - THE DIGITAL INTELLIGENCE HELPDESK WEBSITE.....	20
RESTORE “FACTORY” IMAGE.....	3
RAID DRIVE FAILURE	3
POWER SUPPLY FAILURE	3
LIMITED WARRANTY AND RETURN POLICY Q&A	4
NO QUESTIONS ASKED RETURN POLICY (CONTINENTAL U.S. ONLY)	5
EXTENDED MAINTENANCE OPTIONS	6
SYSTEM LIFE-CYCLE PLANNING	7
APPENDIX A – USING THE FACTORY IMAGE RESTORATION MEDIA	8
RESTORE FACTORY IMAGE (DIWIMS)	9
CREATE/RESTORE YOUR OWN IMAGE (GHOST)	14
VIEW DISK PARTITION INFO (GDISK)	16
CREATE FORENSIC IMAGE (TIM).....	16
APPENDIX B – USING GHOST EXPLORER	16
APPENDIX C – USING YOUR WORKSTATION WITH THE FREDC FORENSIC DATACENTER.....	20
FCCINSTALL – FREDC CLIENT INSTALLER	20
NETLOGON – FREDC DRIVE AUTO MAPPER	20
MAPSTER – ONE-CLICK DRIVE MAPPING.....	21
WINMENU – USER-CONFIGURABLE PROGRAM EXECUTION	21
DIWIMS – IN THE FREDC ENVIRONMENT	21
<i>Overview</i>	<i>21</i>
<i>Preparation</i>	<i>23</i>
<i>Booting your System</i>	<i>24</i>
<i>Creating Menus.....</i>	<i>26</i>
<i>Creating Images</i>	<i>26</i>
<i>Restoring Images</i>	<i>27</i>

<i>Maintenance Options: Edit/Delete/ReImage/Do Nothing</i>	28
<i>DIWIMS Summary</i>	29
INDEX	30

System Identification



Several areas of this documentation provide information or guidelines that are specific to a particular FRED configuration. It is important that you identify your particular FRED Configuration to interpret this document properly:

μFRED: (Micro FRED) The small, portable 6-bay case FRED configuration

FRED: The standard “single-wide” tower FRED Configuration with an i9 motherboard

FRED X: The standard “single-wide” tower FRED Configuration with a Xeon motherboard

FRED AMD: The standard “single-wide” tower FRED Configuration with an AMD motherboard

FRED-SR: The larger “double-wide” tower FRED Configuration with a Xeon motherboard

FRED-RM: The rack mount version of a FRED system

FRED-L: The FRED Laptop computer with up to 3 drives and an i9 motherboard. It also includes our UltraKit - the preferred mobile forensic acquisition solution

Quick Setup

Unpacking your FRED

Please note the condition of your packaging when your system arrives and note any evidence of mishandling. Digital Intelligence systems ship fully assembled - and can be very heavy - sometimes exceeding 100 pounds (45 kg). **If feasible, please keep the original packaging for possible future FRED shipping needs.**

Physical Set Up

Prior to operation, the unit requires several cables and adapters to be connected. Here are some items that may require special attention:

Removable Drive Trays

Before starting the system for the first time, all Drive Trays that do not contain hard drives should be unlocked and slid out of the rack far enough to disengage the connector on the back of the tray. This ensures that Windows doesn't have any issues during the initial setup.

Monitor(s)

Depending on the specific FRED model options selected, up to 4 monitors may be attached to the system. All graphics card options have only digital signal outputs. If you wish to connect an analog (VGA) monitor, an adapter is required. HDMI to VGA adapters are available for purchase. There are graphics card options that do not have a DVI connector. DisplayPort to DVI and HDMI to DVI adapters are available for purchase.

Keyboard/Mouse

A wireless USB keyboard and mouse are included with your system. Note that they require batteries and are included. Digital Intelligence recommends that these peripherals connect to a USB2 port (black insert) on the rear of the unit. If your wireless keyboard and mouse are not in

close proximity to the wireless signal dongle, reduced performance may result. A USB extension cable is a good solution for moving the wireless signal dongle closer to the keyboard and mouse.

Power and Environment

If you decide to utilize an uninterruptable power supply (UPS) with your FRED, we recommend sizing equal to the capacity of the power supply. Although, your system will not (typically) draw power at the full rating of the power supply, it is good to have a margin of safety with the UPS capacity.

Fred Model	Power Supply Rating
µFRED	650 Watts
Desktop FREDs and FRED-SR	1200 Watts

From an environment/temperature standpoint, your FRED will be comfortable if you are.

Security “Dongles”

Digital Intelligence recommends that any security device, such as a license dongle, connect via USB2.

Initial System Start-Up

The installed Windows Operating System will require a license or product key. Most systems have the OEM Windows License key label applied to the back of the chassis. This key is also included in your welcome letter in the FRED packaging. FRED-L systems have the License key label applied to the bottom of the chassis. FRED-RM rack mount systems have the License key label applied to the left or right side of the unit (you will have to open the side panel door if installed in a rack mount cabinet).

Workstations ship with Windows pre-installed. The first time the system is started, you will be asked a series of questions as part of the Windows “Out of Box Experience”.

OoBE no longer automatically prompts for a Windows License Key. You will need to navigate to the Activation Screen by typing “Activation” in the search box on the toolbar and choose “Change Product Key” to enter your Windows License Key.

The password for the Administrator account, if required, is: secret

An OpenSUSE Linux environment is included with your system. See the “Backing up and Restoring Your System...” sections later in this document for installation instructions.

System Components

USB Hub

Your system will have front-accessible USB ports. These ports are NOT write-blocked! USB 3.0 / 3.1 ports typically have BLUE inserts visible. USB 3.1 Gen2 often have TEAL inserts and USB 2.0 ports have BLACK inserts. Depending on the system there will also be additional USB ports on the rear of the system (Motherboard ports).

We recommend that peripherals (mice and keyboards) and license “dongles” connect to USB 2.0 ports whenever possible for reliable performance.

UltraBay 4d™ and UltraBay 4™ Hardware Write Blockers

UltraBay 4d™ comes standard in FRED, FRED X, FRED AMD, FRED-SR, and FRED-RM systems.

UltraBay 4™ comes standard in μFRED systems.

The UltraBay 4d™ and UltraBay 4™ are hardware based write blockers with the following features and capabilities:

Integrated Write Blocked (Read-Only) Ports

- SATA/SAS
- SATA Gen3
- IDE
- PCIe – with an appropriate adapter
- FireWire 800 / 400
- USB 3.x / 2.0 / 1.1

The UltraBay 4d™ also comes with these additional features:

- Integrated touch screen with a graphical user interface (GUI) for acquisition process monitoring when using Tableau Imager.
- A “Write Enable” button available on the front panel – the device must be power cycled to take effect.
- Connecting 2 devices simultaneously.

Full multi-LUN FireWire acquisition support is provided for Write Protected imaging of Apple Mac systems booted to FireWire device mode (Target Disk Mode).

Note: UltraBay devices require periodic firmware updates. Please see the “Periodic/Maintenance Procedures” section of this document for details.



Retractable Ventilated Imaging Shelf (FRED, FRED X, FRED AMD, FRED Sr, & FRED-RM)

The custom retractable imaging work shelf provided with the unit is designed to support and cool the drive as it is being imaged. The shelf is located immediately below the UltraBay. When deployed, the integrated cooling fans switch on automatically. The material is non-slip and anti-static

The UltraBay 4d™

Incorporates a touch screen with a graphical user interface (GUI) for acquisition process monitoring when using Tableau Imager.



Accessory Cables



SAS



SATA Power



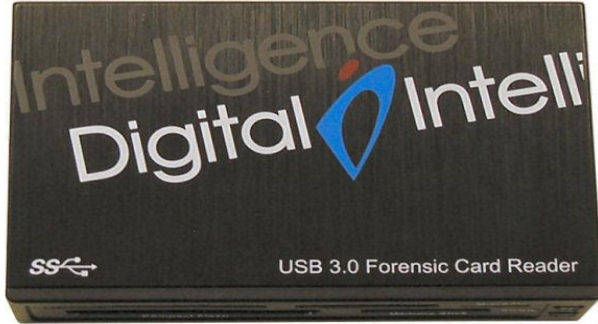
SATA



IDE



Molex Power



SB 3.0 Forensic Card Reader

- Switchable between Read-Only and Read-Write operation
- SDHC and SDXC compatible
- The USB 3.0 forensic card reader is included in the toolbox or accessory bag depending on the type of FRED purchased.

Supported multimedia card formats:

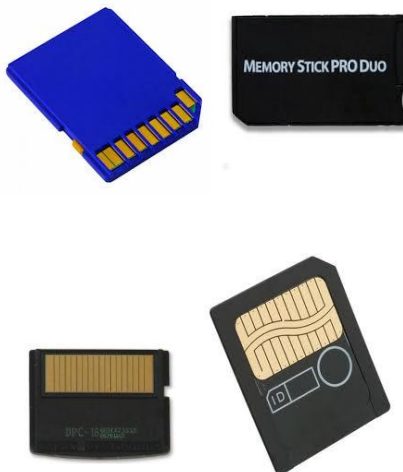
- Compact Flash Card (CFC)
- Memory Stick Card (MSC)
- MicroDrive (MD)
- Memory Stick Pro (MSP)
- Memory Stick Pro Duo (MSPD)
- Secure Digital Card (SDC, SDHC, and SDXC)
- MicroSD
- MultiMedia Card (MMC)



For FREDs with the USB 3.0 FCR included in the toolbox: In order to change the status from read/only to read/write, the device must be disconnected from the computer. Changing the switch while the UltraBlock 3.0 FCR is connected to a powered up computer WILL NOT change its operating state.

For FREDs with a HotSwap tray integrated FCR, the tray must be powered OFF when the switch is moved, then powered on in order to change the functionality.

The FCR does NOT require firmware updates.



System Drives (Operating System, Data Drives, CD/DVD Drive)

The default location for the OS drive is an M.2 slot (PCIe based) directly mounted to the motherboard.

The default system configurations include two additional drives for use as a database/temp location and an evidence/case storage location.

BluRay-DVD Drive

All systems, except FRED-L and the μ FRED, include a SATA connected optical read/write disk drive bay that supports dual and single layer BluRay, DVD, and CD discs. An external USB3.0 BluRay drive is optional on FRED-L and the μ FRED.

Removable Drive Bays (SATA/HOTSWAP)

“Drive Bays” are the positions in the chassis provided to facilitate insertion, removal, and reconfiguration of hard drives. A Drive Bay consists of two pieces, the Drive Tray and the Drive Rack.

“Drive Trays” are the removable portion of the drive bay which holds the hard drive.

“Drive Racks” are the part of the drive bay that mounts permanently inside the system chassis.

There are two system interface types for the drive bays.

- SATA Interface - connected directly to an onboard disk controller (SATA)
- USB 3.1 Interface - connected to a USB 3.1 controller

Drive Racks without the “Hot Swap” label utilize a SATA interface to connect to the motherboard.

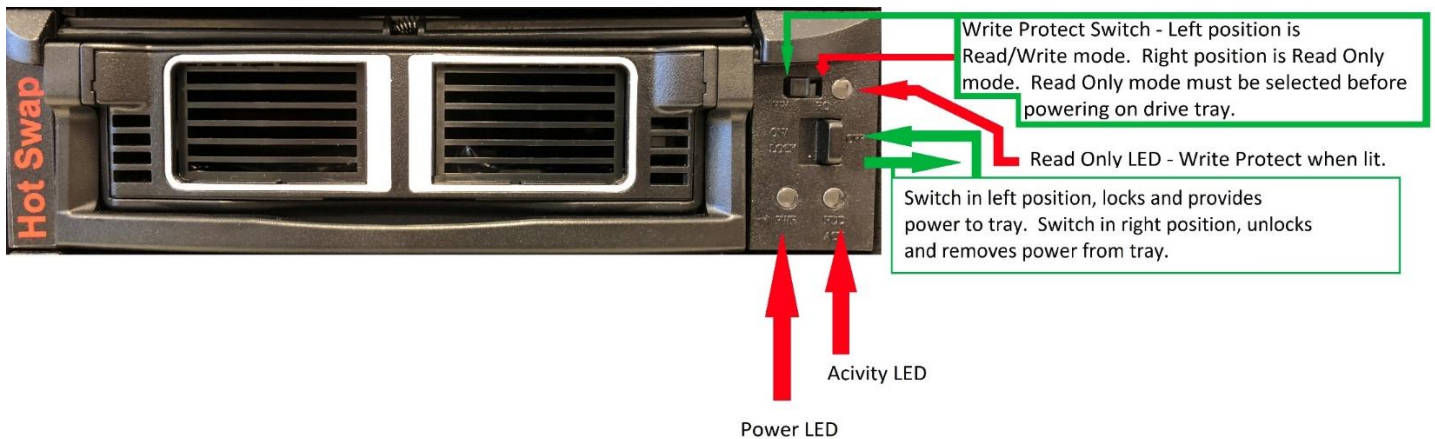
Drive Racks labeled as “Hot Swap” utilize a USB3.1 interface to connect to the motherboard. These are typically located below the BluRay drive.

SATA Removable Drive Bays




Removable Drive Trays allow convenient access to storage drives. The slide switch functions as a power switch and lock for the drive tray. An LED will illuminate when a drive bay is locked and powered on. **NOTE: Drive Trays/Racks with the slide switch are NOT compatible with the previous generation of Digital Intelligence Drive Trays/Racks with the key lock.**

Hot Swap Removable Drive Bays



ONLY DRIVE BAYS SPECIFICALLY LABELED AS "HOT SWAP" SHOULD BE POWERED OFF AND ON WHEN THE SYSTEM IS RUNNING!

Hot Swap bays allow convenient access to storage drives for evidence or images. The slide switch functions as a power switch and lock for the drive tray. An LED will illuminate when a drive bay is locked and powered on. Please observe the following limitations:

- Hot Swap bays are only write protected when the **red** LED is lit
- Drives in Hot Swap bays **MUST** be ejected via the operating system “add / remove” feature before physical removal 
- Hot Swap bays should always be powered off when not in use

Motherboard USB ports

On the rear of most FRED workstations, you will find an array of USB ports. Generally, USB 3.1/3.2 ports will have teal inserts, USB3 ports will have blue inserts and USB2 ports will have black inserts.

You may find USB ports with white inserts (or white highlighting). These are used for BIOS recovery as well as “normal” USB2 ports.

RAID Array(s)

The FRED-1R, FRED-2R, and FRED-Sr have one (or more) RAID arrays. Each array consists of five(5) hot swap bays. The bays can either house rotational media or Solid State Drives (SSD’s). These drives can be grouped into one or more volumes.

The array is pre-configured as a RAID5. This storage can be viewed in Disk Management (formatted or unformatted) or Windows Explorer (formatted only). When initializing, select “GPT format” if the volume is to be over 2TB . Status checks of the array or configuration changes are made via the RAID utility. There are multiple ways to enter into the RAID utility. Either go into the BIOS and change the boot order to the “Areca UEFI” option, or bring up the Boot Menu by pressing F8 while the system is booting.



A browser based GUI (graphical user interface) can be accessed by either installing the Areca ArchHTTP utility in the Windows environment or connecting a network cable to the RAID controller card and browsing to the configured IP address.

For more information regarding RAID configuration, please consult the included controller manual or contact Digital Intelligence. The password for the controller card has been set to "secret". The manufacturer default password for the controller card is "0000".

A RAID5 array can tolerate the failure of a **single drive only**. If a drive fails, as indicated by an alarm sound as well as an indication light on the failed drive bay, please contact our technical support for assistance.

REMOVING AN INCORRECT DRIVE CAN RESULT IN A TOTAL LOSS OF DATA!

Power Supply

All FRED systems come standard with an auto-switching power supply unit (PSU) that supports a wide range of voltages, making them viable almost anywhere in the world.

The power supply for all FRED systems is also fully modular. Replacing the PSU (should it become necessary) is easily done in the field saving down time and costs.



Installed/Included Software

Operating System Information

Your system includes a pre-installed Windows Operating System.

The default password for the Administrator account is: secret

A fully configured OpenSUSE Linux image (complete with NTFS read-only mount support) is also provided which may be installed from a bootable DVD (BluRay). It should be noted that any installation (or reinstallation) using the Bootable Restoration DVD's (Linux or Windows) will completely overwrite the contents of the target drive.

The default username/password for the Linux image is: root/secret

Tableau Imager (TIM)

Tableau Imager is optimized for use on all Tableau hardware devices. It is proven to be significantly faster than other imaging products. Tableau Imager supports a number of industry standard formats such as E01, DD and DMG. The user can also select from various compression levels. MD5 and SHA-1 hashing is also supported, however, auto verification is not available.

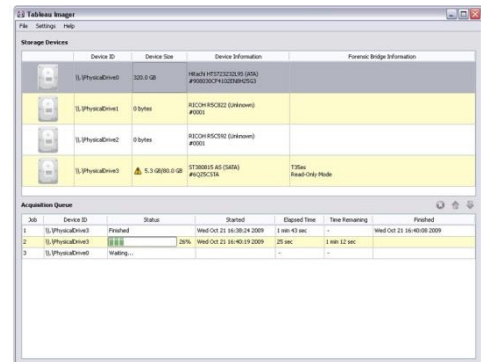


Tableau Firmware Update (TFU) Download

Tableau devices require periodic updates to ensure compatibility with ever-changing hardware platforms. The utility can be downloaded from the Opentext™ website. The download contains the latest firmware for all supported Tableau devices. It is not necessary to connect to the internet to run the utility. Please see "Ultrabay Use" for instructions on updating the Ultrabay write-blocker.

Symantec Ghost

Your FRED purchase includes a license of Ghost from Symantec. Though this tool can create forensic images, it is generally used to create *functional* images for backing up and restoring the contents of the disk volumes in your workstation. By default, Ghost ignores unused space on the drive (including deleted files). Please see Appendix A or Appendix C for more information about this powerful utility.

Factory Image Restoration Media

Each system includes “Factory Image Restoration” media which can be used to put the Operating System volume back as it was when the system shipped. Included is the DIWIMS (Digital Intelligence Windows Image Management System) program which guides the user through the creation and maintenance of Symantec Ghost images. This media contains Ghost images of the Windows Operating System volume and an OpenSUSE Linux image pre-configured for your system. See the Appendix A – Using the Factory Image Restoration Media – for further details.

Toolbox

Each FRED desktop comes with a toolbox containing:

- System Restore Media
- System Keys: Front case bezel key, and if equipped, keys for 4 bay chassis (2.5)
- Adapters and Cables: Including SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air Blade Type SSDs, PCIe based SSDs.
- Security Screwdriver Set: A varied assortment of popular security bits for opening computer enclosures
- OEM Media and licenses
- Forensic Card Reader



Procedures

Operating Procedures

NOTE: Removable drive bays are NOT write-protected unless red LED is lit!

Working with “Hot Swap” Removable Drive Bays:

Only those drive bays specifically labeled as “HOT SWAP” drive bays can be treated as such. Hot Swap bays are particularly useful to mount hard drives which are intended to receive evidence or images. Using a Hot Swap drive bay to mount your evidence or casework drive allows these drives to be changed without turning off the system. Drives must be locked into the bays for proper operation. An LED will illuminate when the drive is locked into place and power is being provided to the unit. The Operating System will physically detect the drive once it is locked into the “Hot Swap” drive bay. If the OS does not detect the drive, use the “Rescan Disks” command from the Actions Menu in Disk Management or the “Scan for Hardware Changes” in Device Manager.

Always notify the Operating System before unlocking a “Hot Swap” drive bay. This will give the O/S a chance to flush any pending disk writes in the cache before the drive is removed. This can be done using the “Safely Remove” Icon on the taskbar in the Windows Operating System. Failure to “Safely Remove” or “Stop” the drive before it is removed from the system can lead to data loss and file system corruption. After a drive tray is unlocked, slide the tray out to disengage the internal connector or completely remove tray from the drive rack.

Working with SATA Removable Drive Bays (without HotSwap label)

Drives must be locked into the bays in order for proper operation. An LED will illuminate when the drive is locked into place and power is being provided to the unit.

Notes about “Dongles”

Digital Intelligence recommends that security devices and other peripherals (keyboards, mice, etc.) be plugged into USB 2.0 ports (identified with a BLACK insert), when possible.

Ethernet connections

The system is prepared for use on a TCP/IP network. The network adapter is configured to retrieve its TCP/IP address from a DHCP server on the local network. If the machine is connected to a TCP/IP network without DHCP services, the system may take a longer time to boot (as it looks for DHCP services). If you find this unacceptable in your environment, simply assign a static IP address to the network card or disable TCP/IP services altogether.

Some FRED systems have 2 Ethernet ports on the motherboard. If you need to connect to a second network (typically called “dual homing”) be especially careful as the typical forensic network environment should be isolated. Digital Intelligence recommends disconnecting your system from the forensic network and then connecting it to another network when performing Windows or software updates..

UltraBay Use

1. Two devices may be plugged into the UltraBay 4d™ at a time. The UltraBay 4™ only supports a single device at a time.

2. The power should always be OFF (no LED indicator light) Before connecting any device

3. Full multi-LUN FireWire acquisition support is provided for Write Protected imaging of Apple Mac system booted to FireWire Target Disk Mode

4. To update the firmware on the UltraBay, run the Tableau TFU utility. Please follow all on-screen instructions closely and ensure nothing is connected to the UltraBay at the time. Firmware updates are periodically released and can be found at:

OpenText.com/products/tableau-download-center



Connecting Drives to the UltraBay 4d™ or UltraBay 4™

- Connect SATA, SAS, and IDE hard drives to the UltraBay using the appropriate Power and Data cables included with the system.
- For SAS drives, use the unified SAS/SATA Data and Power cable ONLY
- IDE drives MUST be configured (via jumper) as a Master Device or a Single Master Device. The orientation of the IDE Data cable is important. The BLUE end of the IDE cable should be plugged into the UltraBay, and the BLACK end into the Hard Drive.

Connecting a USB 3.0 / 2.0 / 1.1 Device: USB flash drives may be plugged directly into the USB port. Removable USB devices (typically “thumb drives”) may require that the UltraBay is powered on before plugging them in. USB enclosures containing a hard drive may also be connected to this port using a USB cable. Improved imaging speeds may be achieved by removing the hard drive from the enclosure and imaged using the hard drive's "native" interface. A USB 3.0 cable is provided with your system.

Connecting a FireWire 800 /400 Device: FireWire enclosures may be connected to this port, as well as devices designed to operate in "Target Mode" (i.e. some Apple devices). Improved imaging speeds may be achieved by removing the hard drive from the enclosure and imaged using the hard drive's "native" interface. FireWire adapters and cable are provided with your system.

Digital Intelligence provides many kinds of adapters for a wide variety of disk drives allowing you to attach nearly any kind of drive in a forensically sound environment!



Card Reader Use

The USB 3.0 Forensic Card Reader (FCR) can accommodate a wide variety of removable media. When the RED LED is illuminated, the device is in write-protect mode. A small switch allows the device to be placed in Read/Write mode—you must cycle the power on the unit in order for the switch change to take effect.

Inserting any valid media into the reader will mount the device in read-only mode (depending on the switch setting). There needs to be a valid partition on the device in order to mount it.

Best Practices

Storage Configuration

There are some general concepts which will aid in determining the best storage locations when installing software. Here are some guidelines you should consider:

1. Application software should be installed to the O/S drive – generally, the O/S drive is not significantly burdened and having the applications installed there aids in workstation imaging. Evidence and case folders should not be put on the O/S drive.
2. Temporary workspaces benefit from being located on an SSD – these drives are optimal for IOPS (essentially large numbers of small random transactions). The standard FRED configurations include an additional NVMe that can be used for databases, case folders or temp locations. Maximum IOPS will be achieved with this connection versus a USB connected “Hot Swap” bay.
3. Case files can reside in a “Hot Swap” bay location when an additional NVMe is not an option. The actual case data (not the evidence) is very small and does not impact performance, unless the forensic program utilizes a database in the case folder.
4. Evidence files should reside on fault-tolerant storage, if possible. RAID arrays are optimal for throughput (in our default RAID-5 configuration). If this is not available, the next best location is in a “Hot Swap” bay location. The “Hot Swap” bay facilitates the removal of the evidence (and likely case files) for storage. Mechanical drives often work best for evidence as they offer large capacities at reasonable price points.
5. Databases/Caches typically require IOPS capacity so they should be located on an NVMe or SSD if possible. A RAID would be a good second choice as this would offer some degree of fault-tolerance.

Imaging and Compressed Images

Testing has confirmed that compressed (typically E01) images are optimal for forensic use. Not only are overall storage capacity requirements reduced, but processing times are improved as well. This is primarily due to the fact that the compression/decompression overhead is easily

offset by the reduced file I/O requirements. This is also true in an FREDC Datacenter environment when forensic images are stored on the network server.

Users are encouraged to utilize MD5 and/or SHA1 hashing as part of their imaging procedures to ensure validation of the process.

Periodic/Maintenance Procedures

Opening your FRED Desktop Case

Tower Case: There is a lock at the base of the front of the unit. The front piece is referred to as the bezel. You should have a key (in the toolbox) which fits this lock. Turn it counter-clockwise to the “open” position. Then pull out at the bottom of the case, gently and slowly, only far enough for the base to disconnect. You may have to press down at the top of the bezel in order to disengage the metal tab on the bezel from the rest of the unit. Once the front bezel is disconnected, you can loosen the screws (they don’t have to be completely removed) and then swing the sides of the case open.

When the case is open approximately 45 degrees, you can lift the side up to disconnect the rear tabs from the rest of the case. Make sure to disconnect the fan power cable if it is present.

uFred Case: Each side panel is secured by 2 screws on the back. Remove the 4 screws and slide each panel towards the back of the case.

Fred-SR Case: Loosen the 3 screws per side on the back of the case and pull the outer sides backward.

UltraBay Firmware Updates

With the constantly changing equipment in the field, the Ultrabay needs a method to stay current with these changes. This is accomplished via a firmware update. The Tableau Firmware Update (TFU) program can be periodically downloaded from the Tableau web site below and includes the latest firmware for all supported Tableau devices.

<https://www.opentext.com/products/tableau-download-center>

Windows Update

In a normal Forensic environment, your workstation will likely not have access to the Internet. Even if your environment does have Internet access, it is recommended that you not allow

Windows Update to run automatically. Instead, we suggest you backup your system prior to manually running Windows Update.

Be especially careful of updating drivers (or the system BIOS). Digital Intelligence has invested significant time in testing our systems and making sure that they are reliable and perform well with the preconfigured components.

Troubleshooting

We hope you have years of reliable service from your FRED workstation, however, in the event you do experience issues we encourage our customers to contact us. *Regardless of your warranty status, you have "lifetime" technical support on any Digital Intelligence branded equipment.* Often, we may be aware of the issue you may be facing, so check our online knowledge base or contact us.

Contacting Technical Support - The Digital Intelligence Helpdesk website:

The first step when you have an issue is to go to our support website:

How can we help?

Enter a keyword, topic, or question

Featured Topics

- Flashing Cursor During Bootup
- When Will my Order Ship?
- Constant Beeping or Alarm Sound From the Inside of a FRED System
- Forensic Bridge Dip Switch Settings
- Areca RAID Controller Administrator Password
- How to Remove the Side Panel From a FRED or FRED DX
- Blue Screen When Windows Loads
- How to Open a FRED System Without a Case Key
- Enabling AHCI Mode in Windows 7
- TXI Instructional Videos are Available in our Video Library
- FRED Manual
- EnCase Locks up During Device Detection

Browse Knowledgebase



FRED Systems

FRED systems and related hardware



UltraBlock, UltraBay & Write Blockers

Working with write blockers



Duplicators

Dedicated imaging solutions



Setup & Troubleshooting

Up and running



Training

Training options and course availability

Still Need Help?

Open a ticket

<http://www.digitalintelligence.com/support>

Here you can search our Knowledge Base or open a Support Ticket to get assistance with your issue.

Depending on the type of issue, it may be important to determine if the issue is hardware or software related. This is most easily done by restoring your “factory image” (see instructions to follow). Once you have backed up the current state of your system, you can quickly restore the original factory image to your hard drive. Though it is possible to substitute another drive (especially with our removable drive bays), that might remove the source of the problem.

Once you have a “fresh install”, if your system is still having issues, it would be likely that the issue is hardware related.

<http://www.digitalintelligence.com/support>

Here you can search our Knowledge Base or open a Support Ticket to get assistance with your issue.

Depending on the type of issue, it may be important to determine if the issue is hardware or software related. This is most easily done by restoring your “factory image” (see instructions to follow). If you have backed up your system, you can quickly restore the factory image to your hard drive. Though it is possible to substitute another drive (especially with our removable drive bays), that might remove the source of the problem.

Once you have a “fresh install”, if your system is still having issues, it would be likely that the issue is hardware related.

Restore “Factory” Image

Your system includes bootable media allowing you to restore the original factory Windows system image or the included Linux operating system. The operating system may be reinstalled to the factory baseline by booting to the “Factory Image Restoration Disc.” Please see Appendix A – Using the Factory Image Restoration Media for further details.

RAID Drive Failure

Some of the most active devices in your system are your hard drives. Unfortunately, even with the high-quality components we utilize in every system, a drive may fail at some point. One method to mitigate this failure is to use RAID (Redundant Array of Inexpensive Disks) which can tolerate a drive failure without a loss of data. FRED 1R and 2R systems have RAID5 volumes precisely designed to preserve your storage volume if a drive failure occurs.

If a drive does fail, there may be a physical indication -typically a red LED and/or an audible alarm.

It is EXTREMELY important that you address a drive failure as soon as possible and NOT rely on the fault-tolerance of the RAID array. With a five drive RAID5 array, a single drive can fail with no data loss.

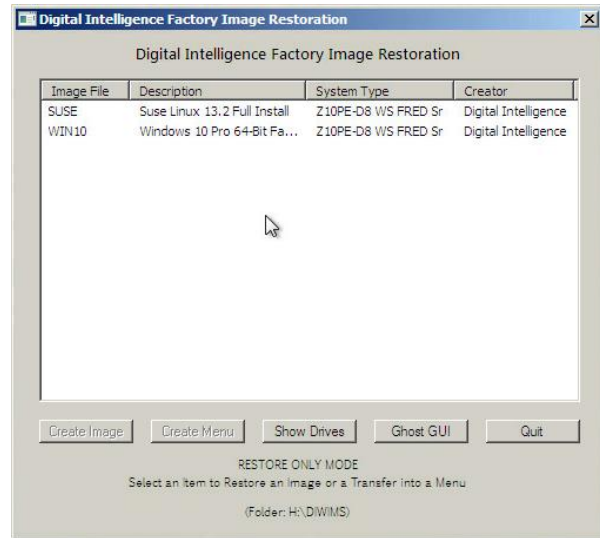
You can access the RAID controller most easily during system boot. Press <F8> when the system is POSTing to enter the Boot Menu, then select the Areca UEFI option to boot directly into the utility. The password should be “secret”. Your drive trays should be labeled to match the naming convention in the controller utility to aid in identifying the failed drive. With RAID5, it is necessary to tell the controller to make use of the replaced drive.

Please contact technical support for assistance with RAID related issues to ensure no data is lost.

Power Supply Failure

Digital Intelligence recommends that you utilize power conditioning equipment with your FRED workstation. See the “Power and Environment” section for sizing guidelines.

If your power supply has failed it is, fortunately, “modular” which means that the interior cabling does not need to be removed to replace the power supply. Before disconnecting cables, please note their locations. Many of the connectors are physically similar but their locations DO matter. See the “Periodic Maintenance” section for instructions on opening the workstation’s case.



As always, please contact technical support for assistance!

Limited Warranty and Return Policy Q&A

Regardless of your warranty status, you have “lifetime” technical support on any Digital Intelligence branded product.

“What is covered by this limited warranty?”

This limited warranty covers defects in materials and workmanship in your Digital Intelligence branded hardware products, including Digital Intelligence branded peripheral products. The following sections describe the limited warranties and return policy for the U.S.

“How long does this limited warranty last?”

Digital Intelligence branded FRED systems purchased in the U.S. include a 3 year/36-month warranty unless your packing slip or invoice indicates a different limited warranty term. To determine which warranty came with your hardware product(s), see your packing slip or invoice. The limited warranty on all Digital Intelligence-branded products begins on the date of the packing slip or invoice. The warranty period is not extended if we repair or replace a warranted product or any parts. Digital Intelligence may change the availability of limited warranties, at its discretion, but any changes will not be retroactive. In the event a component manufacturer has a warranty period that extends beyond your limited warranty from Digital Intelligence, we may use reasonable efforts to assist you in obtaining service through the original manufacturer’s warranty.

“What is not covered by this limited warranty?”

This limited warranty does not cover software, including the operating system and software added to the Digital Intelligence branded hardware products. All software terms are covered in their respective software licenses.

“What will Digital Intelligence do?”

During the limited warranty period we will repair any Digital Intelligence branded hardware products returned to us that we deem to be defective in materials and/or workmanship. If we are not able to repair the product, we will replace it with a comparable product that is new or refurbished. If we determine that the problem is not covered under this warranty, we will notify you and inform you of service alternatives that are available to you on a fee basis.

If we determine that an item needs to be returned to us, we will issue a Return Material Authorization number for you to include with your return. You must return the products to us in their original or equivalent packaging, prepay shipping charges, and insure the shipment or accept the risk if the product is lost or damaged during shipment. We will return the repaired or

replacement products to you via pre-paid shipping if your address is in the continental United States. For international customers we may ship the product to you freight collect.

We use new and refurbished parts made by various manufacturers in performing warranty repairs and in building replacement parts and systems. Refurbished parts and systems are parts or systems that have been returned to Digital Intelligence, some of which were never used by a customer. All parts and systems are inspected and tested for quality. Replacement parts and systems are covered for the remaining period of the limited warranty for the product you bought. Digital Intelligence owns all parts removed from repaired products.

Cross shipment: At our discretion, we may cross-ship replacement components rather than wait for the defective components to be returned to us first. We will require a valid credit card, but we will not charge you for the replacements as long as you return them to us within 30 days. If we do not receive the requested components within 30 days, we will charge to your credit card the then-current standard price for those components.

NOTE: Before you ship any product(s) to us, make sure to back up the data on the hard drive(s) and any other storage device(s). Remove any confidential, proprietary, or personal information and disconnect removable media such as floppy disks, CDs etc. We are not responsible for any of your confidential, proprietary, or personal information, lost or corrupted data, or damaged or lost removable media.

“What if I purchased an Extended Maintenance Contract?”

Service will be provided to you under the terms of the Extended Maintenance Contract. Please refer to that contract for details on how to obtain service. Typically, the Extended Maintenance Contract keeps the new product warranty in effect for the duration of the contract.

“May I transfer the limited warranty?”

Limited warranties on systems may be transferred if the current owner transfers ownership of the system and records the transfer with us.

No Questions Asked Return Policy (Continental U.S. Only)

We value our relationship with you and want to make sure that you're satisfied with your purchases. That's why we offer a 30-day No Questions Asked return policy for most products that you, the end-user customer, purchase directly from Digital Intelligence. Under this policy, you may return to Digital Intelligence any non-customized products and any unopened software that you purchased directly from Digital Intelligence for a credit or a refund of the purchase price paid, less shipping and handling and a 15% restocking fee. We may choose to waive the restocking fee if the products are returned to us unopened or in their original condition. All

returns must be received within 30 days after the product ships to you. When you contact us, we will issue a Return Material Authorization Number for you to include with your return.

THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE (OR JURISDICTION TO JURISDICTION). DIGITAL INTELLIGENCE'S RESPONSIBILITY FOR MALFUNCTIONS AND DEFECTS IN HARDWARE IS LIMITED TO REPAIR AND REPLACEMENT AS SET FORTH IN THIS WARRANTY STATEMENT. ALL EXPRESS AND IMPLIED WARRANTIES FOR THE PRODUCT, INCLUDING BUT NOT LIMITED IN TIME TO THE TERM OF THE LIMITED WARRANTY PERIOD REFLECTED ON YOUR PACKING SLIP OR INVOICE NO WARRANTIES, WHETHER EXPRESSED OR IMPLIED, WILL APPLY AFTER THE LIMITED WARRANTY PERIOD HAS EXPIRED. SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THIS LIMITATION MAY NOT APPLY TO YOU. WE DO NOT ACCEPT LIABILITY BEYOND THE REMEDIES PROVIDED FOR IN THIS LIMITED WARRANTY OR FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, ANY LIABILITY FOR THIRD-PARTY CLAIMS AGAINST YOU FOR DAMAGES, FOR PRODUCTS NOT BEING AVAILABLE FOR USE, OR FOR LOST DATA OR LOST SOFTWARE. OUR LIABILITY WILL BE NO MORE THAN THE AMOUNT YOU PAID FOR THE PRODUCT THAT IS THE SUBJECT OF A CLAIM. THIS IS THE MAXIMUM AMOUNT FOR WHICH WE ARE RESPONSIBLE. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

Extended Maintenance Options

Prior to the expiration of your Limited Warranty, you should receive a proposal to purchase Extended Maintenance. These plans are quoted for each system serial number and are typically one-year agreements. Multiple systems can be included on a single agreement however. Extended Maintenance has the effect of extending all aspects of the original Digital Intelligence warranty.

Extended Maintenance is offered for up to 2 years after the original 3 year warranty expires. Please remember, you have "unlimited" technical support regardless of your warranty/maintenance status.

If you have a FREDC Datacenter, you will receive a proposal for extended maintenance about 3 months prior to the expiration of your original 1 year warranty. There are 2 levels of Extended Maintenance for a FREDC: Extended Support and Premium Support. Extended Support includes the extension of all aspects of the original Digital Intelligence warranty. Premium Support is Extended Support with the addition of an annual one day on-site visit.

Extended Maintenance is offered for up to 4 years after the original 1 year warranty expires. Please remember, you have “unlimited” technical support regardless of your warranty/maintenance status.

System Life-Cycle Planning

The purchase price of your computer is not the total cost of ownership. If you do not have a computer systems background, you may not be aware of the other costs of a system. You will need to consider:

- Software licensing and maintenance
- Periodic subscriptions like anti-virus
- Power usage and cooling requirements
- Hardware warranty and extended support
- Administrative costs
- Downtime costs
- Repairs and Upgrade costs

Depending on your specific situation, these costs can be substantial. It is important to be aware of these costs as, typically over time, many of them will increase. This information is an important input to the decision-making process regarding system replacement.

Especially for “non-systems” people, life-cycle planning is often not considered. It is important to realize that many factors will contribute to the decision-making process. System reliability, support availability, and system performance must all be included in the “total cost of ownership”. Once this cost is determined, a plan can be formulated based on the factors which apply to your organization.

With an approved plan in place, expectations can be set appropriately and budget planning can include manageable life-cycle system replacement and upgrades. Only then can total cost of ownership be minimized, reliability be maximized, and the best utility of the computer system be obtained.

Appendix A – Using the Factory Image Restoration Media

Your workstation comes with “bootable” media containing both a Windows Ghost image of the Operating System volume and a fully configured OpenSUSE Linux image.

The factory image allows you to restore your operating system volume to its factory delivered state.

NOTE: THIS WILL OVERWRITE THE CONTENTS OF THE TARGET DRIVE IMMEDIATELY RENDERING THE PREVIOUS CONTENTS LIKELY UN-RECOVERABLE!

Reasons to perform this task would be:

- Periodic planned re-install of the system
- Diagnosing system stability issues
- Replacement or upgrade of hardware components

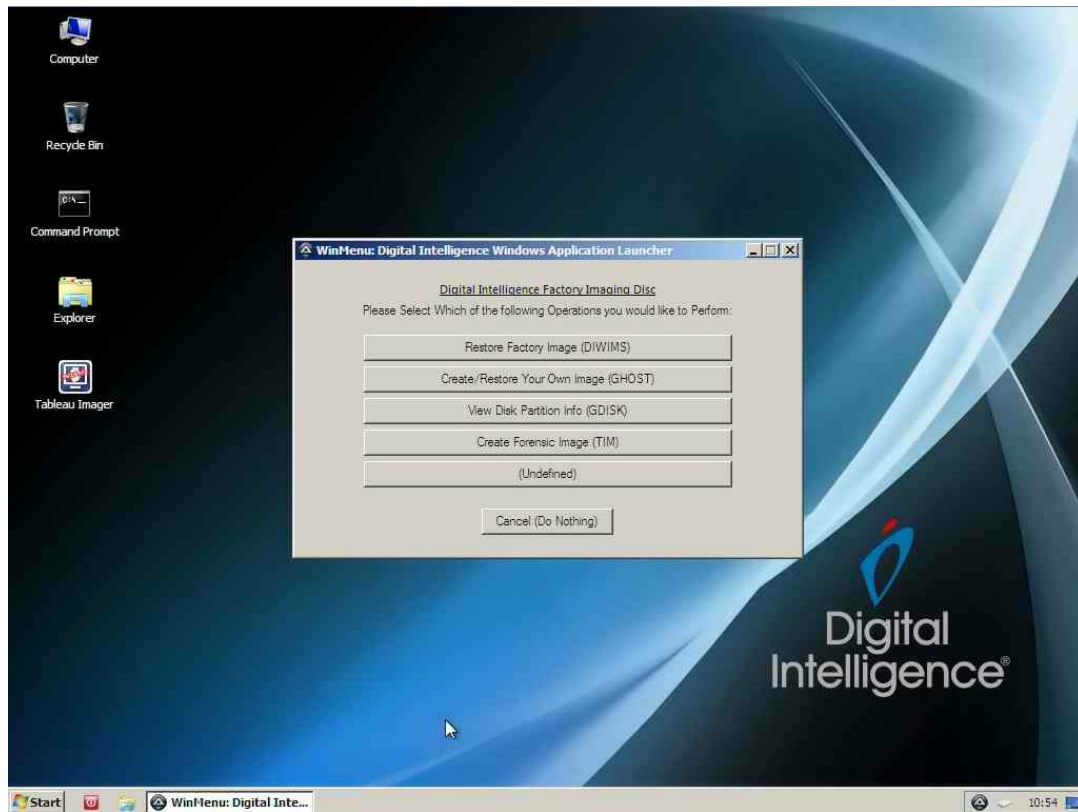
Also note that any licensing information (typically for the Windows Operating System and application software) will have to be re-entered and activation may be required.

Another function of this media is to allow you to utilize Symantec Ghost to create or restore Ghost images of your hard disk volumes. Please see the section “Create/Restore Your Own Image (GHOST)” in this appendix.

Any USB storage devices should be removed before booting the Image Restoration DVD. The NVMe drive or Drive Bay containing the hard drive to receive the Restore Image should be the ONLY Drive Bay turned on or connected.

All other Drive Bays should be turned OFF. On systems with RAID arrays, hard drives should also be removed from the RAID chassis. This prevents restoring the image to the wrong location.

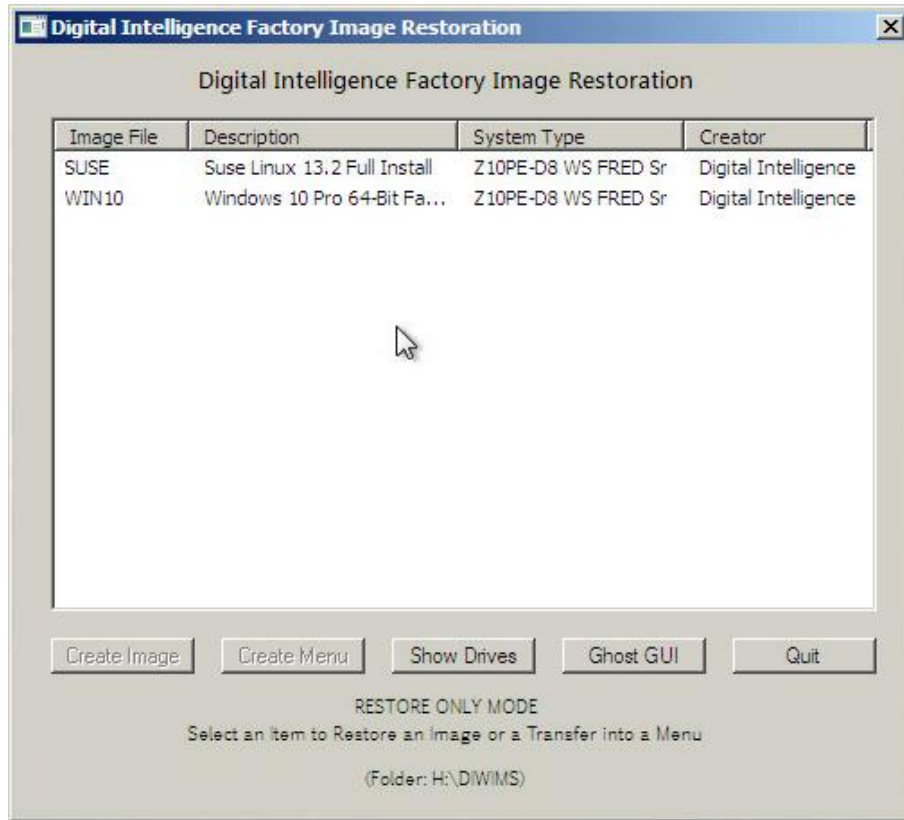
Booting to the restore media: you can either press the F8 Key when the initial POST screen is displayed and select the BluRay Drive, OR enter the bios and switch the BluRay drive to the number one position in the boot order. You will eventually see the following WINMENU screen:



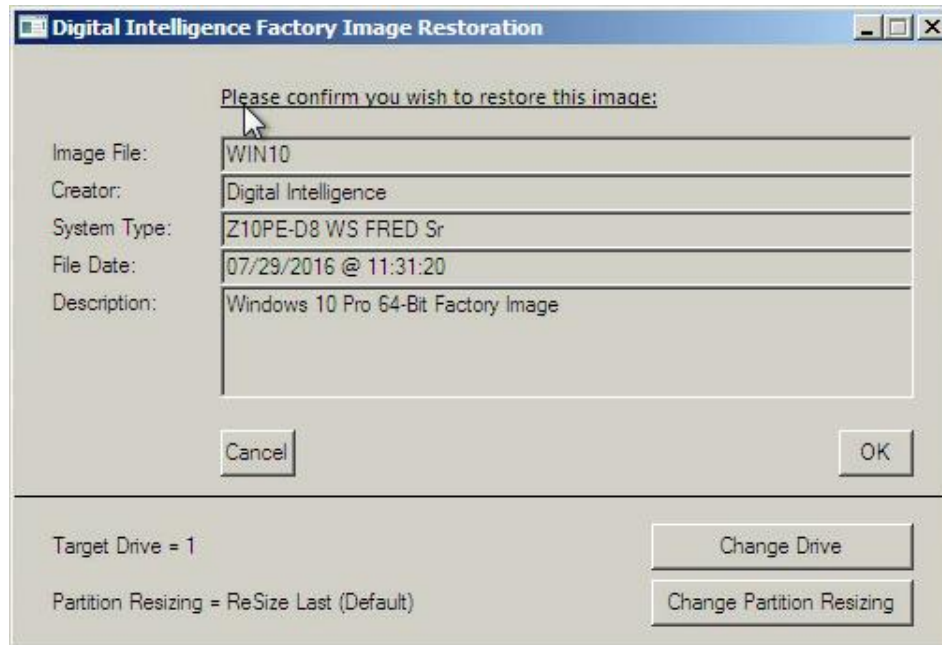
Restore Factory Image (DIWIMS)

Selecting this option will launch the DIWIMS (Digital Intelligence Workstation Imaging Management System) program. This program prompts the user for information and then launches Symantec Ghost to create/restore “ghost” images.

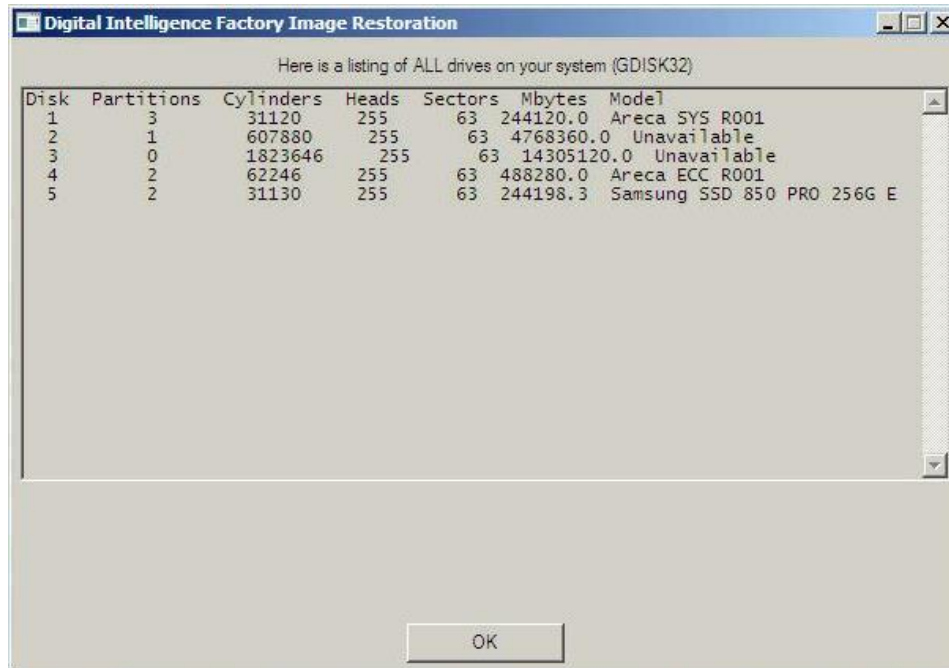
The user is presented with a list of available images to restore. Information about each image will be displayed. You can also “Show Drives” or run the Ghost program by clicking on those buttons.



Select an image by clicking on it and the following image file information will be displayed:

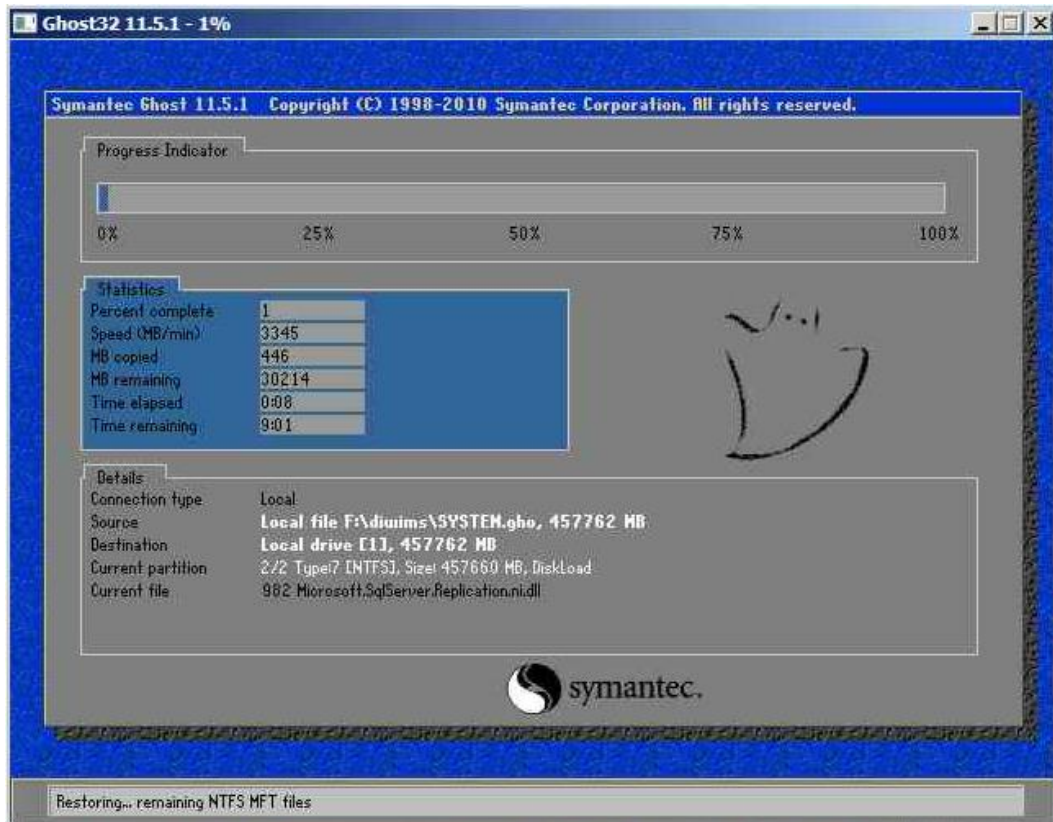


Make SURE to note the “Target Drive” number. They are enumerated as Ghost “sees” them and might not be intuitive. Select the “Change Drive” button (or “Show Drives” on the main menu) to display the drives and confirm the correct disk is targeted. Use the Mbytes, Model, and/or the Partitions information to determine which disk to image or restore to.



The correct disk for the Operating System for your FRED workstation by default has 2 partitions. In this case, Disk #5 is the correct disk for the Operating System.

The DIWIMS program launches Ghost and displays a screen similar to the following during its operation:



Upon completion, an "Imaging Completed" message will be displayed. If prompted, you may either "Reset Computer" or exit from Ghost.

To exit the DIWIMS application, keep pressing the "Back" button until the "Quit" button is displayed. To restart the system, press the small **RED** button in the taskbar.



You may either “Shutdown” or “Restart” the system. After a new image is freshly installed, it may be required to enter into the BIOS and put the O/S drive (Windows Boot Manager) back into the number one position in the boot order.

Create/Restore Your Own Image (GHOST)

The Symantec Ghost program will allow you to do a “bare-metal” restore of your system. This means you can recover your system to an empty hard disk. Of course, in order to do this you need a good image of your system. Digital Intelligence has included an option to make it simple to backup or restore one or more volumes using Ghost.

Bootable media is required because Ghost needs exclusive access to the volume for imaging. The volume must also be quiescent so that the image represents an exact snapshot of the entire drive – the drive contents cannot change during the imaging process.

Please note that the Ghost images (.gho files) need to be copied to some alternate location as the whole point is to be able to recover from a failed or corrupted device. Make sure to copy the files, preferably to network storage, as soon as practical after creating the images locally.

Before you create your image you should:

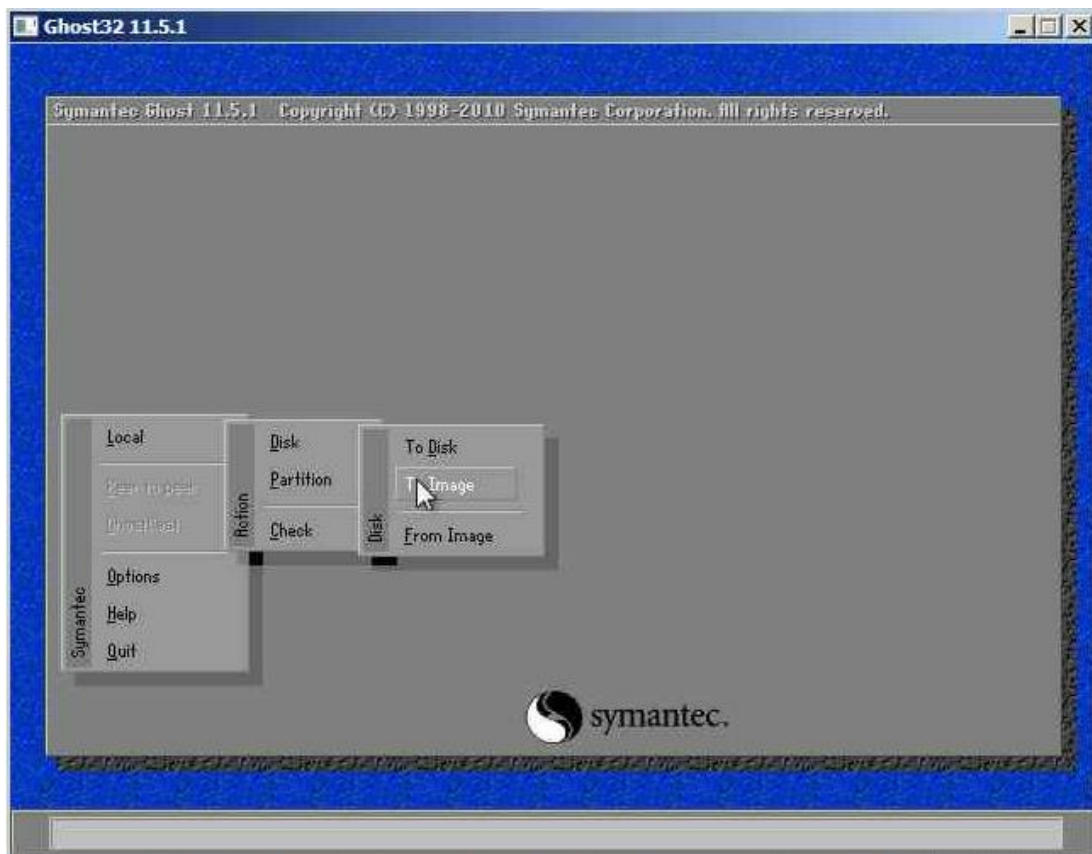
- Remove any temporary files and clean up any work areas
- Run Disk Cleanup
- Verify that “System Protect” is turned off – this Windows function creates “restore points” and, by default, uses 10% of your disk space. By using Ghost, restore points and the disk space they consume are not necessary
- Note the size of the disk volumes to aid in identification of the source/target drives in Ghost (GDISK).

Selecting the “Create/Restore your own image” option runs the Symantec ghost program with the following command line options pre-selected:

-cns – number ghost image file extensions – eg. .001 .002 .etc

-split = 2000 – create 2GB image files

-z2 – use high compression



To create a Ghost image, select the options, Local, Disk, To Image. Select the volume to be imaged and then select “OK”. On the “File name to copy image to” screen, specify a target drive with enough capacity to store the images. Remember to copy or move those files to another location so that they are available in the event of a failure!

Once you accept the options, the Ghost program will be called. Once completed, you may wish to run the “Check” option to verify your image.

The restoration process is similar – Local, Disk, From Image. Note that the Ghost images must be available on local storage media in order for Ghost to restore them.

View Disk Partition Info (GDISK)

This option runs the GDISK program which displays the drives as Ghost “sees” them. In addition to the Disk [Number], the Partitions, Mbytes, and Model are also displayed. If you have 2 physically identical disks, the # of Partitions should allow you to determine which drive has your Operating System.

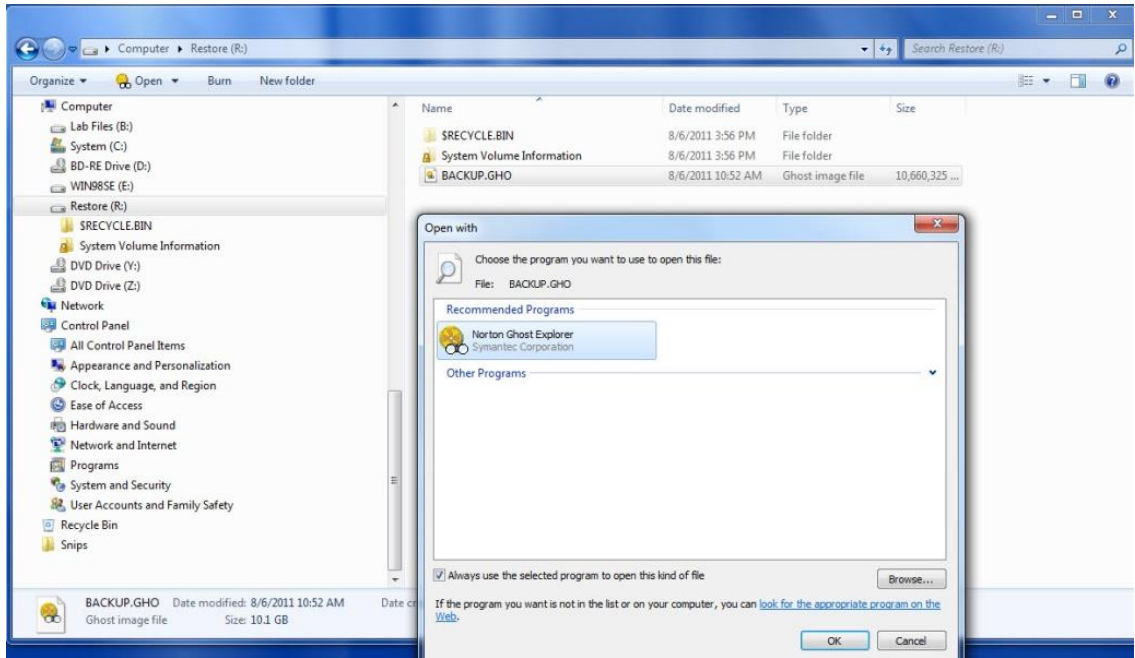
Create Forensic Image (TIM)

This option runs the Tableau Imager software as a “diskless” imaging workstation. This would be a benefit if your system was in an unknown or non-functional state and you needed to acquire forensic images. There is no reliance on any of the internal volumes as you can see network resources in this environment.

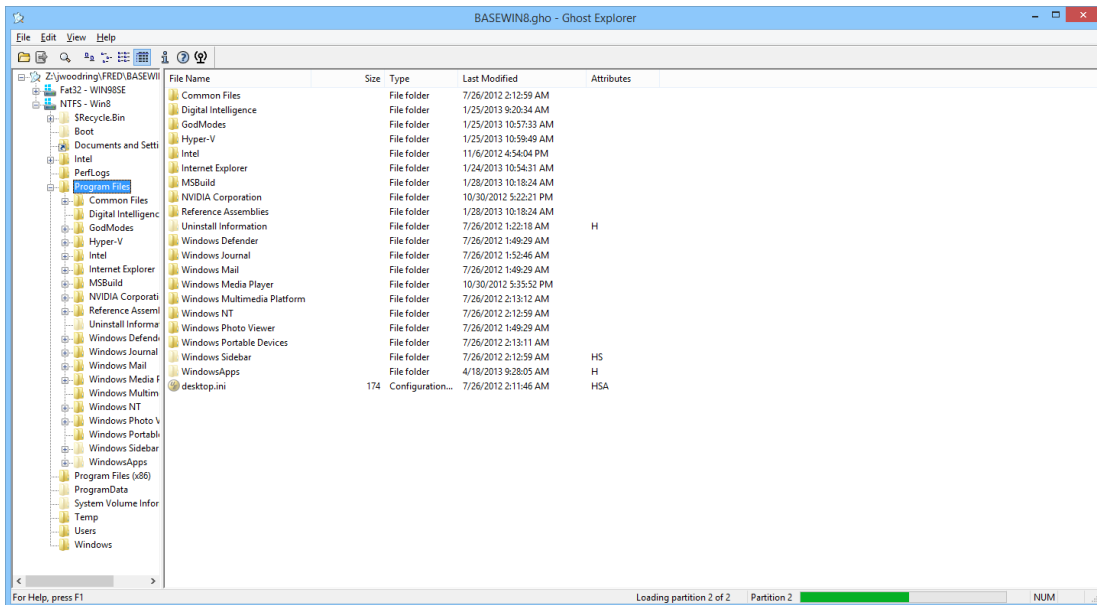
Appendix B – Using Ghost Explorer

Ghost Explorer is a tool for viewing and manipulating Ghost images. You can add to, delete from, and extract from images. Digital Intelligence does not recommend altering Ghost images. Instead it is better to restore the image, manipulate it, and then re-create the Ghost image.

However, there might be occasions where it is desirable to extract files or folders from a ghost image. Use Windows Explorer to browse to the .GHO file you are interested in. Use the “Open with” option to associate .GHO files with the Ghost Explorer application. It is not necessary to install the application; just make sure you know where on your system the GhostExp.exe application is located.



The Ghost Explorer interface is very similar to Windows Explorer. Start by clicking on the disk partition (if it is an entire disk image) and then browse as you would normally. Be extremely careful as, if you delete something, it is IMMEDIATELY removed from the image – there is no undo option or “quit without saving”.



Appendix C – Using your workstation with the FREDC Forensic Datacenter

The FREDC is a fully configured private cloud for Forensic Storage. It includes centralized storage, centralized administration, centralized security, and centralized backup! All the things that made REAL file servers great - all in a platform fast enough to make it worthwhile!

Unlike other generic "IT-Centric" network solutions, the FREDC has been designed from the ground up to be fast and reliable for direct forensic imaging and processing to/from the server itself. While other solutions require secondary copies to network storage, the FREDC systems have been designed for the direct ingest and processing of data. No need for closets full of old hard drives or massive amounts of local workstation storage!

More info on the FREDC can be found here:

https://digitalintelligence.com/products/fred_c

The FREDC includes a number of tools for integrating your FRED workstation into the network environment and managing your FRED as well. A brief description of each utility:

FCCInstall – FREDC Client Installer

There are a number of updates necessary to allow a new FRED workstation to use resources on the FREDC network. This utility makes those updates and guides the user through the installation of optional application software beneficial in a FREDC environment. Another major function of FCCInstall is to install the NetLogon program. This program runs at user login and maps network drives.

Note that FCCInstall makes "user-based" changes and thus needs to be run for each user on the system.

FCCInstall uses a configuration file FCCInstall.ini located in the same folder as the FCCInstall program (typically in the FCCInstall folder under APPS). Please see the FCCInstall section of the FREDC Documentation for more information.

NetLogon – FREDC Drive Auto Mapper

Since the FREDC environment does not utilize an Active Directory Domain Controller, there are no policies available to automatically map network drives upon logon. The FCC Install program

(mentioned above) installs NetLogon which is run when a user logs into the workstation. NetLogon also synchronizes the workstation clock to the server's clock.

NetLogon uses a number of NetLogon.ini configuration files. The first is located in the NetLogon share on the FREDC server. This file contains drive mapping for the user's "home" folder and other application volumes.

Next the NetLogon.ini file located in the user's "home" folder is consulted. Here is where, if the user is in the "Examiners" group, mapping to evidence volumes is configured. Other user-specific drive mapping can be configured here as well.

Mapster – One-click Drive Mapping

This utility allows you to quickly map a drive to a particular volume share. This is normally used if you have multiple evidence volumes and want to switch quickly between them. However, this can also be used for other drive mapping purposes. The utility is configured with the Mapster.ini file located in the APPS\Mapster folder.

WinMenu – User-configurable Program Execution

The WinMenu utility allows the user to configure a menu with pre-defined selections. These menu selections are defined in the WinMenu.ini file located in the APPS\WinMenu folder. This utility is pre-configured for the DIWIMS imaging environment described in the next section.

DIWIMS – In the FREDC Environment

Overview

DIWIMS is designed to make it easy for any user to use Symantec Ghost to make *functional* images of any of their system drives. It is important to stress that these are NOT forensic images. These images only include valid files and other necessary objects for the operating system. This document will discuss all the necessary procedures in order to fully utilize DIWIMS.

DIWIMS images are stored on the Server-RM's internal (INTRAID) RAID array. At the time of this writing, there is approximately 72TB of fault-tolerant storage available on a new FREDC INTRAID. A fresh installation of Windows results in an image which is approximately 12GB meaning almost 6,000 images could be stored on the INTRAID. Typically, a special DIWIMS backup will be configured as part of your FREDC Orientation (given when the system was installed). It is important to note, after creating DIWIMS images, the DIWIMS backup should be scheduled to be run to preserve that data.

There are a number of compelling reasons to make workstation images. In the FREDC environment all evidence and other important information should be stored on the network.

Since the network storage is fault-tolerant, the risk of loss due to equipment failure is greatly reduced. This DOES NOT mean that there still isn't a risk of accidental modification or erasure however! Ideally only the operating system and application programs should be installed on your local workstation. The following is an incomplete list of good reasons to image.

1. Disaster Recovery – Even with the Digital Intelligence provided “Factory Installation” media, the recovery of your workstation from a disk failure or misconfiguration can be quite time-consuming. Re-installing all programs (if you can locate the media and licensing info) and configuring your system could take a day or more. Instead, the restoration of a typical Windows Ghost image can take less than 15 minutes. To recover, you replace the failed drive, boot to DIWIMS (see below) and recover your system EXACTLY as it was when the image was created.
2. Consistency – Each Ghost image is specific to the system hardware. It is not recommended that you restore an image created on one system to another. If you have systems which are identical, you can use a “master baseline” to configure all of the systems identically. However, depending on your Windows Licensing, you will have to re-activate each system with its unique product code to be in compliance with Microsoft’s License Agreement. Also, it is recommended that you periodically restore your system baseline to ensure that you have a consistent platform for repeatable case processing.
3. Reliability and Performance—The Windows “Recycle Bin” might seem like a likely place for garbage to collect. Over time, however, updates to the registry as well as file-system fragmentation can severely impact the reliability and performance of your system. Newer versions of Windows have “defragmentation” services or utilities for disk and registry maintenance. None of these can match the benefit of periodically restoring your system from a known good image.
4. Viruses – For most circumstances, Digital Intelligence strongly recommends against anti-virus software as it can impact system processing speeds and network performance. Even with AV software installed, the detection and removal of a known threat cannot give you 100% confidence that your system is clean; only restoring a known good image can give you absolute certainty.
5. Multiple Configurations and Upgrades—Digital Intelligence workstations feature Removable Drive Bays, however, more and more systems have the Operating System installed on an NVMe drive which is affixed to the motherboard and is not easily accessible. It is very reasonable to create an image of a custom installation for one task – maybe cellphone work, and others for different sets of requirements. If you wish to upgrade your operating system drive (maybe to a larger drive or SSD), the new drive can be installed, and the existing baseline image can be deployed. Our pre-configured defaults specify the option of “resize last” which will expand the final (or only) partition to use the entire target drive.

6. Testing—if you want to install a new version of a program or are concerned about compatibility it is simple to make an image prior to the installation or upgrade. When you are finished, or if issues arise, it is quick and simple to restore the system to a previous known good state.
7. Problem Determination – Sometimes it is difficult to determine “what changed” when you have problems with your system. By performing a DI factory installation to your system, hardware versus software problems can be more efficiently diagnosed.

If your FRED is new, we recommend that you make a “baseline” image after you have installed the programs you will be using on a daily basis. Over time, as you apply program updates, Windows updates, and other “tweaks” to the system, a new baseline should be created once you know your system is functional.

A typical “best practice” should be to install patches and test. When you are satisfied that the patches/updates are sound, restore your baseline (which puts your system in a known good clean state), then re-apply the tested patches and create a new baseline.

Please note that in addition to making an image of the Operating System drive (typically the C: drive), you can make an image of any other drives such as a database drive. If you are running a product which uses a dedicated database drive, making an image after a new installation can be a great way to be able to start over with a “clean” database.

If your system has been in place for some time, Digital Intelligence still recommends you make an image as soon as practical so that you are protected in the event of a disk failure, infection from a virus, or other unforeseen event.

Preparation

Prior to the creation of a disk image, a few steps are necessary:

- Clean up your drive. Remove any temporary files (try looking in C:\Temp and C:\Windows\Temp), run “Disk Cleanup”, or even use a commercially available utility like CC Cleaner.
- Confirm that “System Protect” is turned off for the drive. This Windows utility makes “Restore Points” which can be used to return to a known good clean state. By default, your system may allow up to 10% of the total physical volume for storage of this information. By utilizing Ghost, the restore points and their accompanying data is not necessary.
- Make sure you can identify the drive you want to image. Ghost sometimes enumerates drives differently than you might expect. This is especially important if you have 2 or more identical drives in your system. Typically, the Operating system drive can be

identified as it will have more than one partition (our default configuration). Running DIWIMS and selecting the “Show Drives” option will display the drive information as Ghost “sees” it. Ghost is smart enough to recognize certain Windows “sparse” files such as the pagefile.sys and hiberfil.sys which can be quite large, and will not back them up in their entirety. This won’t affect the ability to restore the image.

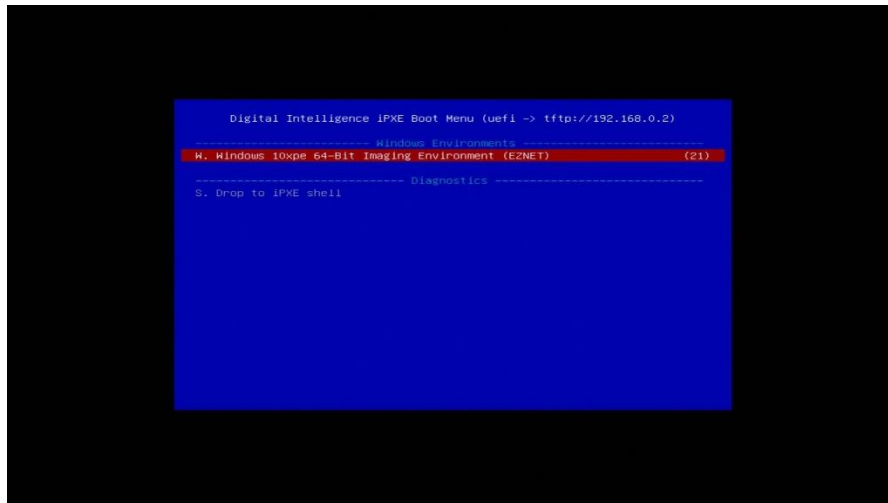
Booting your System

In order to image a volume it must be quiescent (not active) so that Ghost can have exclusive access. Your O/S drive (typically Windows) is ALWAYS active so there is no way to image this drive when it is the boot drive. Digital Intelligence has created a bootable CD (or PXE Network Boot method) which allows the system to boot into the WinPE environment. This is essentially Windows 10 running in memory. Once booted, the physical hard drives can be accessed exclusively by Ghost and a consistent image can be created.

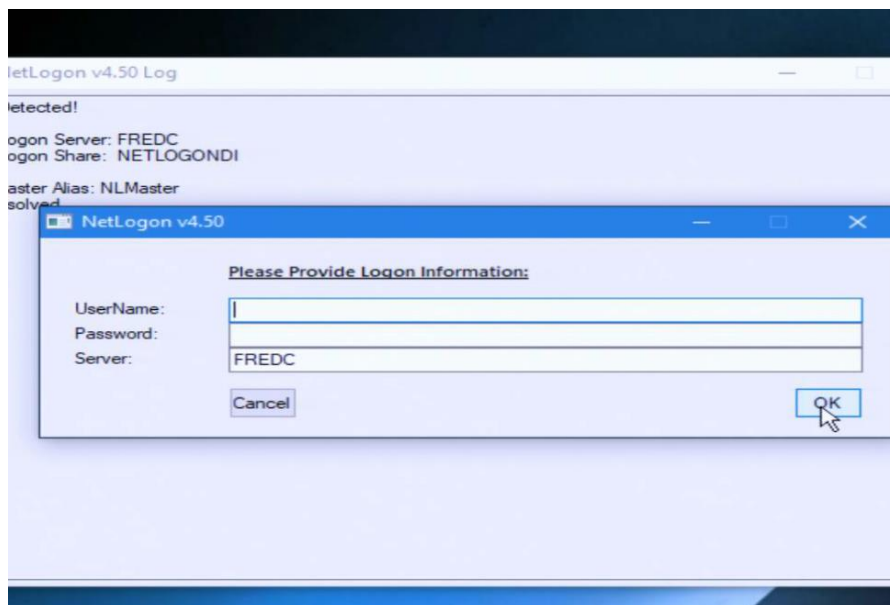
Either use the EZ-Net CD (provided in your disk pack) or enable the “boot menu” (by pressing F8 on Digital Intelligence workstations during system POST) and select the appropriate network boot device. Your system BIOS settings may need to be updated in order to enable the PXE boot option.



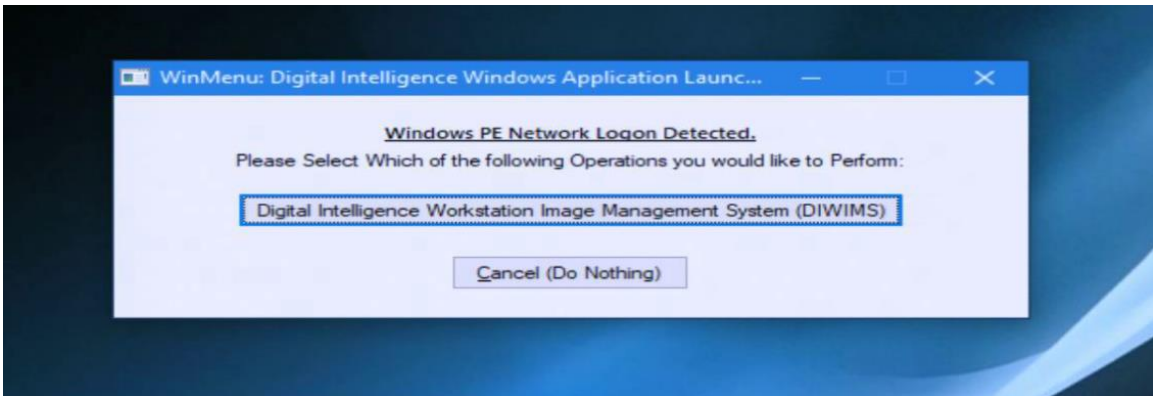
If you are using the PXE boot, you may (depending on your FREDC release) then see a screen similar to the following. Please select the PXENET option and press <ENTER> – there is no timeout.



With either boot method, you will see a screen indicating that the environment is loading.



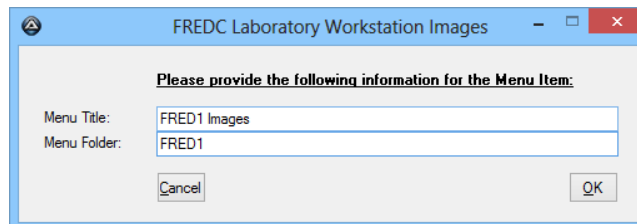
Shortly, the system will boot and the “NetLogon” screen will be displayed and can be used if you have a FRED-C environment. When making workstation images, you can use any valid user login or you can use the “root” login. NetLogon will map up your network drives (just as when you are booting normally) and will run “WINMENU”. The WINMENU utility can give the user easily selectable options – but, by default, there is only the option to run DIWIMS.



Select that option and, after a “terms of use” message is displayed, the DIWIMS utility will run. Navigation is intuitive – just click on the menu, image, or button of interest.

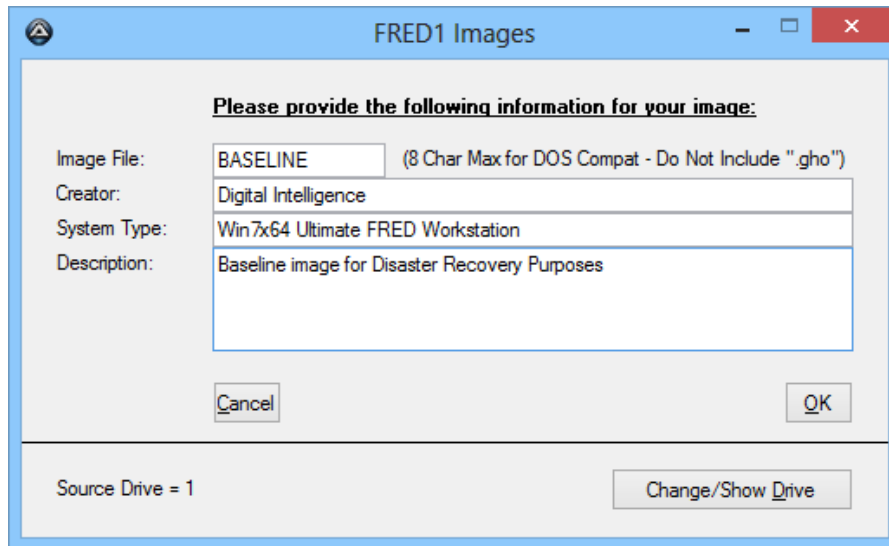
Creating Menus

Workstation images are specific to the exact hardware configuration of the system. Digital Intelligence recommends that you make separate images for each workstation. A convenient way to organize these images is to create a “menu” for each system. You can create sub-menus if you need to separate images further. When creating a menu, you can use a descriptive text string in the “Menu Title:” field. The “Menu Folder:” should conform to reasonable folder naming conventions and should not contain spaces, punctuation, or special characters.



Creating Images

Once you have created the appropriate “menu” you can create your image. Clicking on “Create Image” displays the following screen. The user is prompted for information which makes the image easy to identify later.



Other than the “Image File” field, which should be 8 characters or less and “DOS” compatible, the other fields are a free format. Note the “Change/Show Drive” button which will allow you to verify the enumeration of the source drive. Make sure to confirm the Source Drive number so that you know you will be imaging the correct drive!

Once you click “OK”, DIWIMS runs Symantec Ghost for you with our recommended options while saving the image to the network storage. If you need to run Ghost manually, you may run use the “Ghost GUI” button on the main menu.

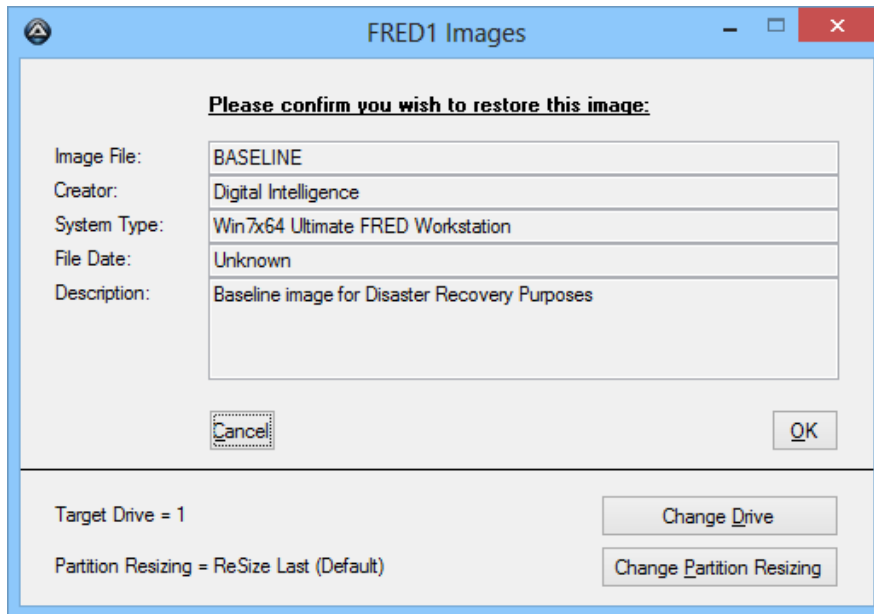
The default options for image creation are stored in the DIWIMS.ini file in the DIWIMS home folder. A brief description of the recommended options:

- cns – use older Ghost file naming convention.
- split=2000 – create extension files 2GB in size
- sure – displays the “Reset or Continue” dialog after Ghost completes
- z2 – use High Compression

Restoring Images

As with image creation, Ghost must have exclusive access to the target drive in order to restore an image onto it. If you wish to restore an image to an inactive drive, it is possible to run DIWIMS without re-booting your system. Typically though, you will be restoring your Operating System drive so you will either have to boot from the Factory Image Restore Disc, or using the PXE Network Boot as described in the Image Creation section of this document.

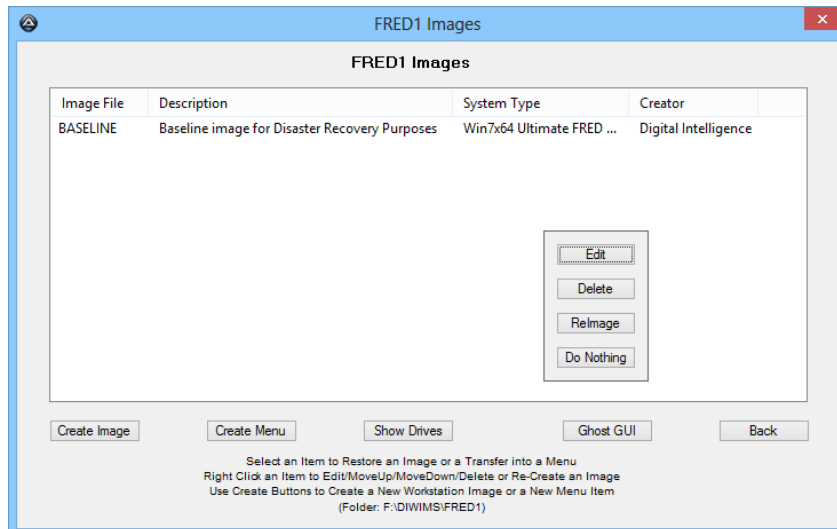
We highly recommend that you disconnect any other drives prior to attempting to restore an image. Once in DIWIMS, you can navigate to the desired image by clicking on the appropriate menu. Clicking on the image will bring you to the “Restore Image” screen.



CAUTION: Clicking “OK” will start the restore process and will IMMEDIATELY destroy the existing contents of the Target Drive! Make sure to confirm the Target Drive number BEFORE continuing!

Maintenance Options: Edit/Delete/ReImage/Do Nothing

If you “right-click” on an image or menu, you will be presented with additional set of Maintenance Options.



You may:

- Edit the information which was entered when the image or menu was created
- Delete the image or menu
- Re-Image – overwriting that image with the same image name leaving the user supplied information unchanged (disabled in Menu Maintenance)
- Do Nothing – just close the Maintenance Options menu

DIWIMS Summary

Symantec Ghost is a great tool for managing your Forensic Lab workstations. Our DIWIMS utility makes creating, deploying, and managing Ghost images easy. The ability to quickly recover a system means that your workstations are available and that case processing is the focus of the users. With the ability to boot from CD or from a PXE Network Boot, all Digital Intelligence systems (and some non-Digital Intelligence systems) can be protected from many common problems.

Index

Case

Bezel, 19

Lock, 14, 19

Opening, 19

DIWIMS, 14, 21, 27, 37, 44

Dongles, 3, 4

Drive Bays

Hot Swap, 10, 15

RAID, 10

DVI Adapter, 2

Factory Image Restore, 21, 26, 38

FireWire, 16

Forensic Card Reader, 7, 17

FREDC Datacenter, 18, 19, 24, 36

GDISK, 29, 31, 33, 39

Ghost, 26, 29, 31, 32, 39, 42

Ghost Explorer, 34

Keyboard, 3

Network Adapter, 15

OpenSUSE Linux, 13

Passwords

Linux root, 13

RAID Controller, 11, 21

Windows Administrator, 4, 13

Power Supply, 12, 21

PXE Boot, 40, 43, 44

Software

DIWIMS, 14

Factory Image, 20

FCCInstall, 36

GDISK, 33

Ghost, 13

Ghost Explorer, 34

Mapster, 37

NetLogon, 36

Tableau Firmware Update, 13, 19

Tableau Imager, 5, 13, 18

Windows Update, 19

WinMenu, 37

UltraBay, 16

Firmware Update, 5

Warranty

Coverage, 22

Duration, 22

Extended Maintenance, 23, 24

Return Policy, 23

Shipping, 23

Windows License, 3, 26

WinMenu, 26, 37

