



A Total Forensic Solution

Addressing the Challenges to Quickly, Securely and Accurately Capture, Store and Connect Digital Forensic Evidence

Advances in digital technology, and in particular the expanding capacities of data storage media, have given users the flexibility to create and store almost unlimited amounts of data. Criminal investigations encounter a wide variety of sophisticated digital devices that can contain hundreds or even thousands of gigabytes of data to analyze from a single case. Digital evidence has become prevalent in the majority of criminal cases. This backlog of evidential data needs to be moved quickly into the hands of forensic analysts to drive the judicial process to conclusion.

The combination of explosive data growth and rising crime statistics provide several challenges to forensic investigators. The amount of time it takes to capture evidence data has increased. This in turn delays how quickly the evidence data can get into the hands of the analyst. In addition, investigators must be prepared with large quantities of bulky hard disk drives on scene and in the lab to effectively store the large amounts of evidence data routinely seen in criminal investigations today. The current economic climate has put further pressure on investigative organizations to process cases quickly with limited resources both in personnel and budgets.

Logicube has developed three modular forensic products that when used together provide a **Total Forensic Solution** to quickly capture, store and connect evidence data. The Forensic Dossier®, MPFS™ (Massive Portable Forensic Storage) and NETConnect™ are designed specifically to meet the challenges that high volumes of evidence data and limited timelines create for forensic investigators.

How can these solutions work for you? Each forensic investigation provides its own unique set of circumstances and challenges. Whether you are the sole investigator or one of many on a large team, the common goal is to quickly acquire evidence data and get it to the investigations' analysis phase without compromising security or accuracy.

CAPTURE**The Forensic Dossier®**

The centerpiece to Logicube's Total Forensic Solution is the [Forensic Dossier®](#). A feature-rich, multi-source, multi-target data capture solution, the Dossier can capture from 1 or 2 suspect drives to 1 or 2 evidence drives at transfer speeds over 7GB/min. The Dossier provides capture in dd images or in E01 file format as well as native copy. The Dossier is a sophisticated but easy to use solution that even non-technical personnel can use for forensic data capture.

- Supports a broad array of hard drive interfaces including IDE, SATA, SCSI, SAS, eSATA, microSATA and laptop drives
- Supports RAID drive pairs, solid state drives, flash media
- Provides write-protected source drives; use Dossier as an external write-blocker
- Evidence drives fully protected and secured inside Dossier
- Proprietary O/S provides a stable platform that virtually eliminates virus vulnerability
- Use with MPFS™ to capture up to 8TB of evidence data

STORE**MPFS™ (Massive Portable Forensic Storage)**

Hard disk drive capacities are growing exponentially. It is not unusual to encounter desktop and laptop PCs with 500GB or larger hard drives. Investigators are tasked with capturing potential suspect data quickly from multiple computers and multiple crime scenes that can amount to hundreds or thousands of gigabytes of data. When faced with large amounts of data and/or multiple scenes, investigators may need to replace evidence hard drives for each capture session or even several times during a single capture session. This can mean managing and transporting bulky sets of evidence drives and a greater chance of compromising the chain of custody.

The [MPFS™](#) allows the user to capture and store up to 8TB of suspect data in one convenient, secure and portable device. The large storage capacity of MPFS reduces the need for large quantities of hard disk drives on-scene or in the lab for data capture and ultimately reduces the financial investment for storage media. The data capture process is further streamlined by eliminating the necessity of swapping out hard disk drives when faced with capturing large amounts of evidence data.

Investigators can also use the MPFS to archive evidence data. The MPFS features an “always-on” display that allows users to identify contents by case/file names at a glance. Multiple MPFS units can easily fit neatly into a rack to archive evidence data during or at the completion of an investigation.

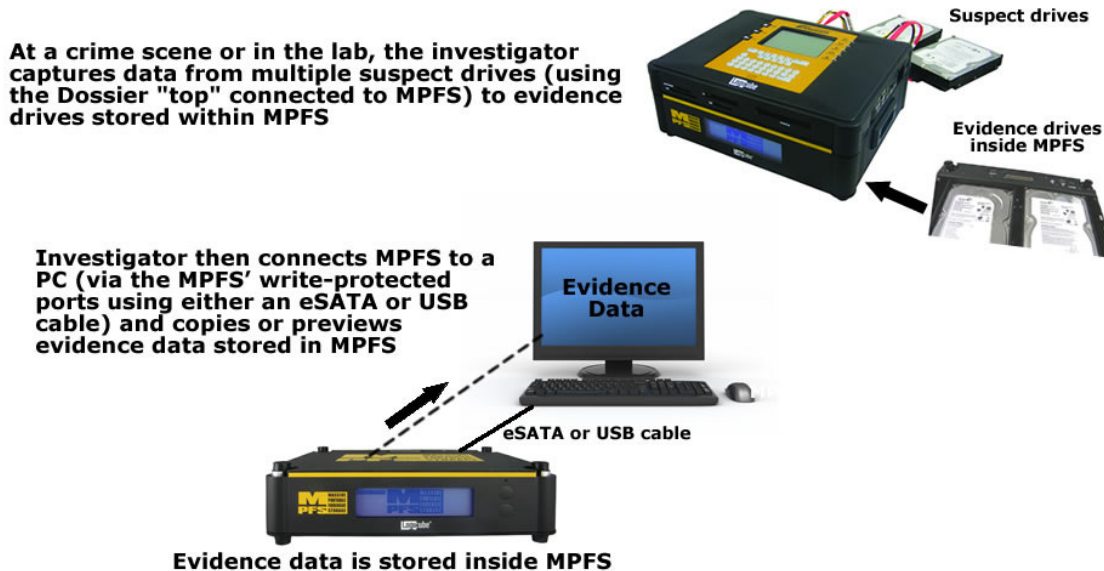
The MPFS works seamlessly with the Dossier and NETConnect. Attach the Dossier “top” to the MPFS and proceed with capturing to evidence hard drives installed within MPFS. MPFS features a four drive JBOD (Just a Bunch of Disks) configuration (all drives in the configuration appear as one large logical volume or drive). Evidence data can be previewed or transferred post-capture using the write-protected eSATA or USB ports connected directly to a PC or attached to NETConnect for fast transfer to a network location.

- Direct connection (write-protected ports) to a PC for preview or transfer using eSATA with transfer speeds over 4GB/min, or use USB.
- Supports both dd image and E01 file format
- Store multiple evidence capture sessions in one convenient portable device
- Use NETConnect™ to preview or “push” data to a network location, or configure as a NAS (Network Attached Storage) device to provide immediate access to data
- Use MPFS (or multiple MPFS units) to archive evidence data; battery-powered “always-on” display shows case/file names for easy identification

Figure 1: Using MPFS

USING MPFS™

Capture-Transfer-Preview/Copy Direct to a PC



CONNECT**NETConnect™**

Capturing forensic data is only one step in the investigation process. Once the evidence data has been captured investigators need to make the data available on their workstations for analysis. Investigations may require that digital evidence be examined by multiple investigators in parallel, each investigator tackling different files or working on the same file and performing different analysis processes. This may require the primary investigator to copy the file to his local drive, make duplicate copies of evidence hard drives for each team member working the case (requiring a significant investment in storage media) or ship/transport the drives to remote offices, which can jeopardize the chain of custody protocol. As the amount of data increases in size these can be cumbersome and time-consuming tasks. Additionally, some computers' processing power may not be sufficient to effectively and quickly copy and store large data volumes or perform multiple, simultaneous analyses.

NETConnect™ provides automated high speed access to evidence data for any size organization. Used in conjunction with the Dossier tray or with MPFS, NETConnect automates the transfer/copy process to provide fast, secure access to evidence data. NETConnect uses a Gigabit Ethernet connection (with transfer speeds approaching 7GB/min depending on your network infrastructure performance). The centralized access control facilitated with NETConnect allows administrators to configure users, assign levels of access to users and establish unique user names and passwords providing increased security and control over sensitive evidence data.

The NETConnect can be configured as a NAS (Network Attached Storage) so that computers on the same network can connect to the NETConnect and copy evidence data from the hard drives stored in MPFS or Dossier tray. Multiple users can mount the drives to their workstation to immediately start working with the data or copy files to any location including their local drive, CD, DVD, USB drive, a shared directory or another network drive location. A single investigator could use NETConnect as a NAS and perform multiple processes in parallel on several PCs or workstations on the same network – essentially creating a multi-processor, multi-tasking forensic lab.

NETConnect can also be configured to push or transfer data stored on MPFS or Dossier to specified network locations using FTP, CIFS or NFS file protocols (these protocols allow a user on a client computer to access files over a network). Administrators can configure NETConnect using a Telnet client (a network protocol available built-in to most Windows O/S). The evidence data can be pushed or transferred to any workstation or network storage device on the network. Data can be viewed from any workstation on the network, copied from the network to the workstation's local drive or to any other directory on the same network. A convenient "Macro" can be set up by the administrator to initiate preconfigured commands and automate the transfer and validation. The Macro feature can also be set up, upon completion of the push/transfer process and successful

validation of the transfer, to wipe and format. This streamlines the entire process and quickly makes the drives available for the next data capture session using Dossier.

NETConnect allows users to easily connect to their network. Using a standard CAT-6 type Ethernet cable (included with NETConnect) and a PC on the network you are connecting to, users can easily locate NETConnect on their network by using Apple’s Bonjour (Zero Configuration Networking) or by viewing your network’s workgroups. Once logged in, all of the drives and their contents (contained in MPFS or the Dossier tray) are viewable. Administrators can set up multiple NETConnects (attached to either MPFS or Dossier trays) to transfer evidence data quickly and efficiently for investigator analysis.

- NETConnect works seamlessly with the Forensic Dossier and MPFS
- Configure as a NAS or use CIFS, NFS or FTP protocols to push data to a PC or network location
- Provides automated, fast and secure network access to forensic data to multiple investigators
- Administrative controls allows you to limit data access, set up user logins and passwords and create a macro to automate the entire process

Figure 2: Modular Design

A sleek, modular design allows NETConnect to attach easily to the Dossier Tray or MPFS

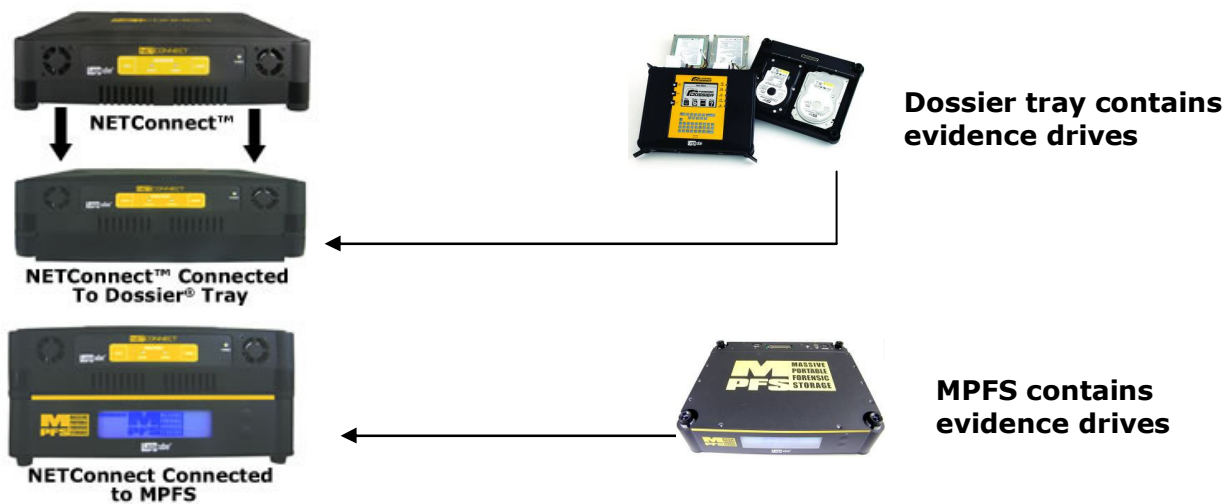


Figure 3: Using NETConnect

Using NETConnect™ with Forensic Dossier® or MPFS™

At the crime scene or lab, investigator captures data from multiple suspect drives using the Forensic Dossier alone or attached to MPFS



OR



Attach NETConnect to the MPFS or the Dossier Tray



OR



Connect NETConnect to the Network

Use as a NAS (Network Attached Storage) and preview data or copy to a PC on the network

OR

Preview or push/transfer data to a network location or any PC on the network using CIFS, NFS or FTP protocols

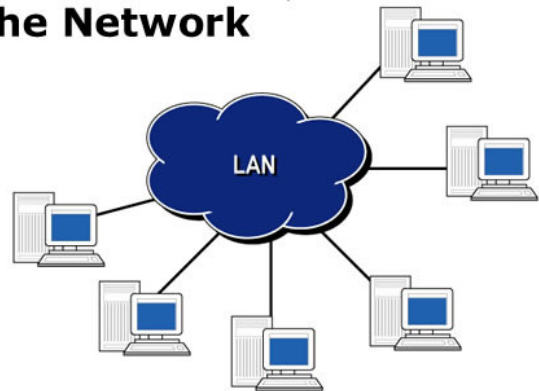


Figure 4: NETConnect as a NAS

CONFIGURE NETCONNECT AS A NAS (NETWORK ATTACHED STORAGE)

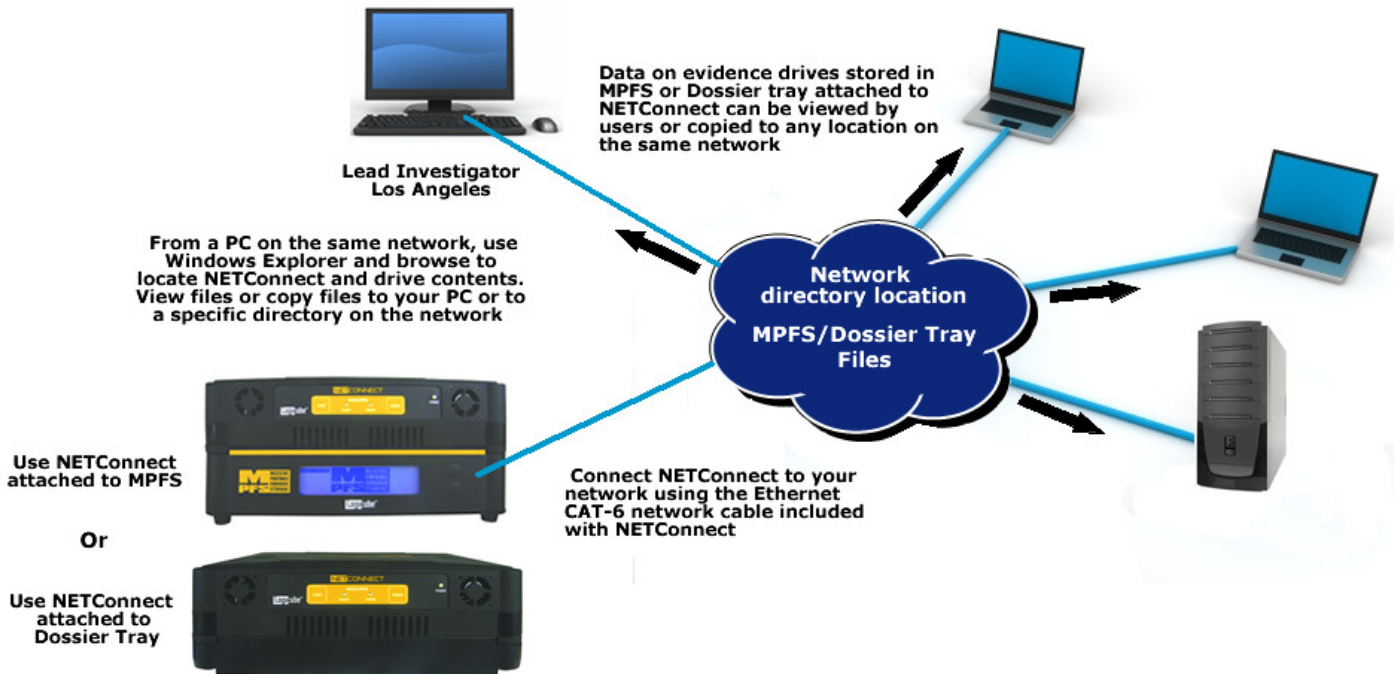
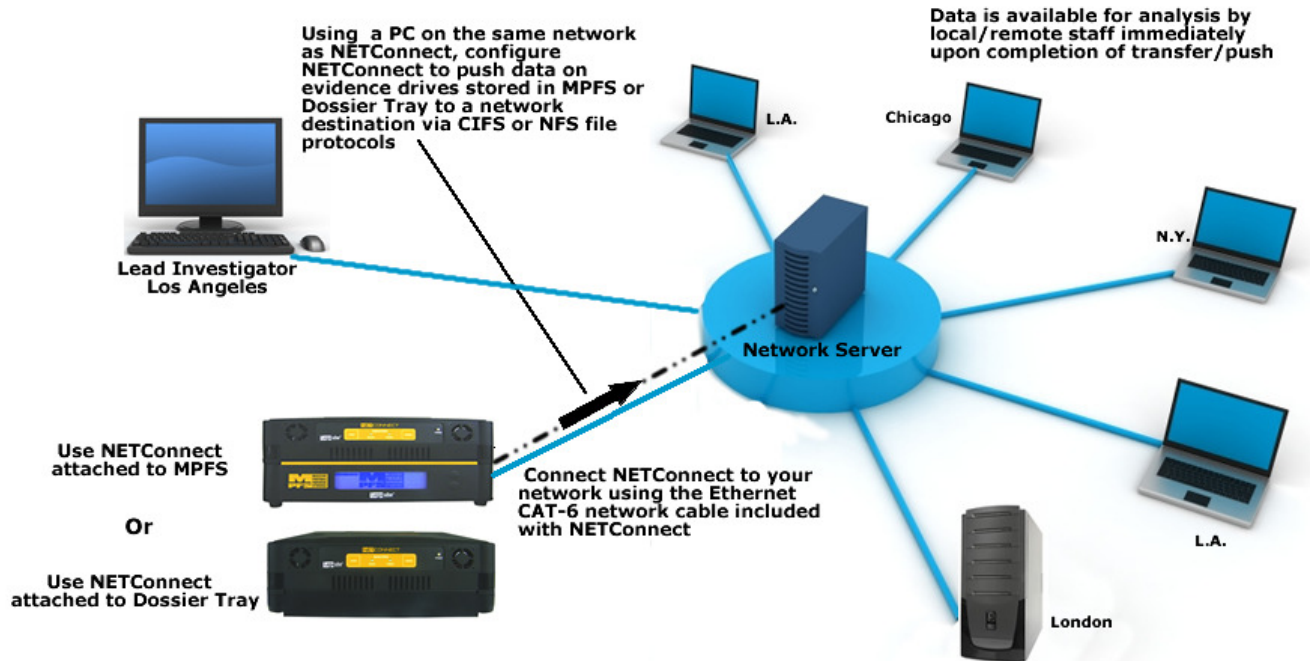


Figure 5: Transfer Data

Transfer Data to a PC or Server Using FTP, CIFS or NFS File Protocols



A "Macro" can be set up in NETConnect to automatically transfer, verify and then wipe and/or format evidence drives so they are ready for the next data capture session using Dossier

Summary

Logicube's Total Forensic Solution has been designed specifically for forensic investigations. Each of the products included in this solution leverages the latest technological advances to insure that users have cutting-edge tools. Users can utilize all three products together or in any combination to suit their specific situations. Whether for a small or large organization these cost-effective products will maximize your return on investment and reduce the amount of time (that for most investigators is in short supply) it takes to capture and access evidence data and to optimize the analysis phase of the investigation.

CAPTURE

Forensic Dossier

- Fast data capture exceeding 7GB/min
- Multi-source, multi-target data capture
- Multiple image formats including dd image and E01 file format
- Broad support for the vast array of hard drive interfaces on the market including IDE, SATA, SAS, SCSI, laptop, eSATA, microSATA

STORE

MPFS

- Maximizes the amount of evidence data storage with up to 8TB capacity
- Minimizes storage media investment
- Improves on-scene storage media handling
- Works seamlessly with the Forensic Dossier and NETConnect

CONNECT

NETConnect

- Network evidence data to provide access to multiple investigators locally or remotely
- Enables multi-tasking to speed the analysis processes
- Uses high-speed gigabit Ethernet data transfer
- Automates the transfer process so administrators can quickly move to the next capture session

Automating and expediting the capture, store and connect process, Logicube's Total Forensic Solution is the only solution on the market today that provides fast evidence capture, expanded storage capability and fast, broad access to evidence data. This approach addresses the complexities and challenges digital forensic professionals face in processing massive amounts of evidence data and helps forensic investigators swiftly build the criminal case. Logicube is committed to building solutions that are designed specifically for the digital forensic community.