



SalvationDATA

Forensic Data Recovery Solution

Grow Your Business with SalvationDATA's Overall Data Protection Service



Index

■ **Background of Current Computer Forensics**

- [Computer Forensics: Data caging, retrieving and recovering do great help](#)
- [Essential reminding before obtaining evidence from computer](#)

■ **We Provide Solutions & Tools to Meet the Various Demands on the Current Market**

- [Forensic Data Recovery Solution: Data Compass, HD Doctor and HPE Pro](#)
- [Flash Memory Basic Forensics: Flash Doctor](#)
- [On-The-Spot Investigation and Fast Forensics: Data Copy King](#)
- [Protection Of Evidence: USB Blocker](#)

■ **Why Choose Us**

■ **Appendix**

- [Appendix I](#)
- [Appendix II](#)

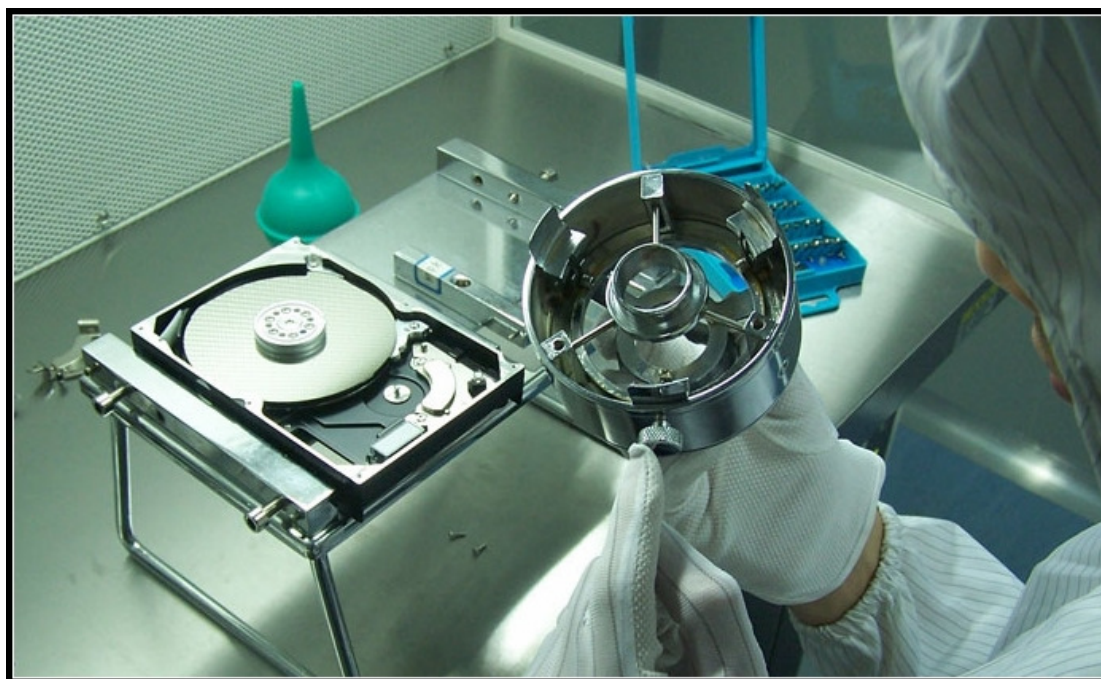
■ Background of Current Computer Forensics

● Computer Forensics: Data caging, retrieving and recovering do great help

Electronic information always includes fatal resources of enterprises and government agencies. For the enterprises, it usually represents the lifeline for keeping their competitive force in the battle field.

Along with fast development of information technology and a huge population of computer users, it is more and more difficult for the computer forensic inspector to collect useful evidence from highly skilled and experienced suspicious bodies. The suspicious media containing criminal evidence has a higher possibility of being damaged or destroyed deliberately, rather than being performed a deletion, a format or an encryption. It becomes more and more difficult and complicated during the exploration of the criminal evidence.

Therefore, computer forensic institutions are desperate for constructing one advanced data recovery lab to obtain evidence more effective and optimized via the utilization of professional data recovery platforms which combines mobile data with fixed data.



● Essential reminding before obtaining evidence from computer

As forensic data recovery professionals, we need to:

1. Make sure the whole forensic data recovery process measures up the forensic requirement, that is write protection to the source drive;
2. Prevent secondary damage to the source drive during the data recovery process;
3. Retrieve every single byte of data possible from each hard drive because each of them is vital which will lead to complete different judgments since the data is being used as evidence for court cases. And because of the sensitivity of the data and the strict legislation

to the “evidence acquiring”, we are required to perform all of our data recovery operations in a controlled environment by authorized personnel.

■ We Provide Solutions & Tools to Meet the Various Demands on the Current Market

- Forensic Data Recovery Solution: Data Compass, HD Doctor and HPE Pro



Hard disk drive is one of the most common storage systems that may be used to contain the computer criminal evidence. In order to gain access to the data on the hard disk drive through one of the operation systems (e.g. Windows, MAC, Linus), the quality and status of the hard disk drive needs to be in a very good standard. For further analysis and investigation of the data on the media, some special and authorized forensic software tools are also needed.

SalvationDATA has a team who has been working as a contractor of Chinese military and government public security agencies in providing data security management and forensic technologies. With their years of experience and outstanding achievements in R&D for the specific needs of forensic data recovery field, they provide a comprehensive idea for Forensic Data Recovery Solution for forensics services– from drive-level cases to data-level cases – in a conformable, resource respected environment under strict control.

- ✓ **Extract, analyze and validate the data on a working hard disk drive.**

There is a couple of computer forensic software available in the market, such as Encase, X-Ways, FinalForensic, F-Response and so on. These software are designed to achieve a high performance in data restoration, data analysis, generation of auto-report and data archive.

When the forensic investigation comes to a situation where the computer hard disk drive is malfunctioning, none of the forensic software will be able to access the data. The malfunctioning hard disk drives may behave like having severe bad tracks, corrupted Master Boot Record (MBR), or being recognized by its ‘Alias’ in BIOS.

Data Compass is designed to resolve the problems mentioned above. It can be used to extract the data from a defective drive while maintaining 100% integrity of the original data. This is one of the most significant breakthroughs in the computer forensic and data recovery industry.

✓ **Fully and effectively recover data from instable and bad sectors defective hard disk drive**

As far as you know, it is not suggested to recover and analyze data on instable or defective hard disk drives. It is not able extract the data from this kind of hard disk drives due to the instability of the read write head and the likelihood to damage platter. Furthermore, it may also cause a further damage to the whole hard disk drive, which makes the data irrecoverable forever. The most efficient and common approach is to image the data onto a stable donor media, and then proceed to recover and analyze data from the donor.

The technology and algorithm that used to deal with the bad sectors is a crucial and critical part of a cloning tool/procedure. The bad sectors cause system to crash or freeze, making the hard disk drive irresponsive or even being damaged. Data Compass possesses a superb solution for this problem. As you may be aware of, the existing image/cloning tools skips the bad sectors and results in data loss, which corrupt the integrity of the files. The intelligent 'Bad Sector Leap Function' and 'Dynamic Balanced Enhanced Reading Technology' help the users obtain 30% more data than the other image tools. The 'High Efficiency Power Supply System' function is also introduced and integrated into the Data Compass, which is used to resolve the problem of hard disk drive being irresponsive. A multiple of parameters of the reading algorithm are also set to be configurable by users, e.g. the Retry time, Readiness Time, Reset Time, which enable an optimized data recovery.

Obviously, to ensure the security of the original hard disk drive is also important. This has been addressed during our research process. The new technology of 'ShadowDisk' has been developed and introduced in Data Compass after a few years hard research. This technology is also be classified as the 4th generation of image technology. The 'ShadowDisk' minimizes the reading times towards the source drive and protect the further damage to the source drive.

The hard disk drive Bitmap can be also be analyzed by the Data Compass. Different Operation System (OS) will have different bitmap to record the cluster and sector information. In order to find the location of specific file for cloning, the bitmap information is needed. This information are contained in FAT table in FAT system, BT table in NTFS and Block Allocation table in Linux system.

Along with the development of the hard disk drive technology, higher capacity and higher density, the traditional image tools will not be able to resolve all the problems mentioned above. The Data Compass will be a leading technology in the data recovery industry.

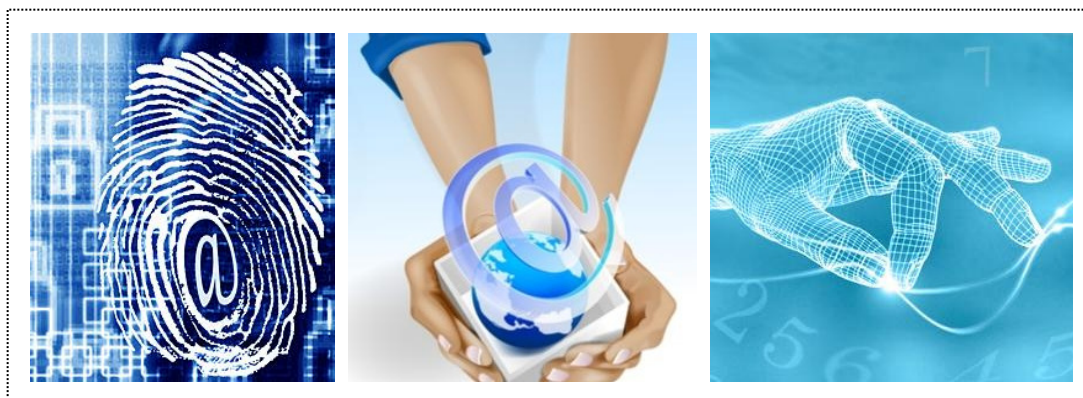
ATA password protection is also one of the problems that need to be addressed during the evidence collection procedure. The decryption software and the forensic software support up to 70% hard disk drives. This is extremely not good enough for the fast developing hard disk drive models. The Data Compass 'Password Filter' function can thoroughly and effectively resolve this problem. Data Compass detects hard disk drive through integrated virtual background files, bypassing the original password protected firmware. It establishes the corresponding firmware modules and then retrieve and recover data directly. This technology is achieved independent from any other decryption software. It will not damage the original password module and

support up to 95% of the drive models available in market, include all the Hitachi hard disk drives. Along with the rapid manufacturing of new hard disk drive, Data Compass will be constantly updated and supported the new models. For example, Data Compass has already supported Hitachi 5432 which was manufactured in June 2008.

The function is very easy to use. It is achieved by selecting a corresponding hard disk drive model from the menu. The Data Compass will automatically start the emulation of the firmware. The tips message will also guide the users step by step to complete the restoration of data.

Obviously, the evidence is not only the completed set of data, but also 100% compare to the original data. During the forensic investigation process, the content and the last modified time should be maintained and imaged to a donor copy. No additional data will be introduced during the whole process.

The 'SWPS Technology' is used to maintain the original copy and avoids the affection by virus and Trojan. This is another leading technology developed by SalvationDATA which satisfy the requirement of forensic investigation procedure where the 100% original data is compulsory.



✓ **Access and analyze data from unrecognized hard disk drives.**

The reasons why the hard disk drive is not able to be recognized by BIOS can be categorize into two types:

1. Physical damage. The HPE Pro will be helpful in this case where the read write head or platter needs to be swapped. For more details about HPE Pro, please refer to our website.
2. Firmware corruption, which is quite common. For example, if a certain amount of modules of the firmware are corrupted, then the hard drive may not be recognized by BIOS correctly. HD Doctor Suite is a professional hardware-software integrated system that fixes and recovers HDD firmware problems from drives of all the major manufacturers and popular drive families. Then you repeat the procedures of Data Compass

Nowadays, the capacity of hard disk drive is increasing dramatically, as well as the density. Hard disk drives have a higher possibility of being corrupted or damaged than before. Thus an efficient way to access data independent on local/native firmware is undoubtedly a big advantage.

✓ **Recover data at any time, any place, and any environment from any manufacturer of hard**

disk drives.

In terms of computer forensic, evidence should be collected as soon as possible and securely protected. Therefore, ensure the data is being recovered/imaged without external influence is a crucial thing during the forensic evidence collection procedure. The portability of Data Compass is designed to allow you to provide an on-site evidence collection through the USB interface. The Data Compass can be used by connecting with anyone of the laptops at any time, any place and any environment to recover data from any manufacturer of hard disk drives.

Data Compass supports a physical or logical data recovery from PATA or SATA hard disk drives, including IDE, SATA, 3.5", 2.5", 1.8" and 1.0" of different manufacturers. Also it can be used for the logical data recovery from the FLASH storage media such as USB pen drive, SD, MMC and FDD.

Data Compass supports more partition formats than the other similar tools, includes FAT16, FAT32, NTFS, Linux Native, Linux Swap, HFS+, and other peculiar partition formats used on special equipment.

The Data Compass adopts the 'Open-source' design on high level recovery/image software. Thus, users are free to use any one of the logical data recovery programs they are familiar with to work with the Data Compass, such as ENCASE, X-WAYS, FianlForensic, F-Response and so on. Data Compass eases the limitation of high level software programs to be used. This is also one of the significant breakthroughs in this industry.

● Flash Memory Basic Forensics: Flash Doctor

The evolution in consumer electronics has caused a Texponential growth in the amount of mobile digital data. The majority of mobile phones nowadays has a build in camera and is able to record, store, play and forward picture, audio, and video data. Some countries probably have more memory sticks than inhabitants. A lot of this data is related to human behavior and might become subject of a forensic investigation.

Flash memory is currently the most dominant non-volatile solid-state storage technology in consumer electronic products. An increasing number of embedded systems use high level file systems comparable to the file systems used on personal computers. Current forensic tools for examination of embedded systems like mobile phones or PDAs mostly perform logical data acquisition. With logical data acquisition it's often not possible to recover all data from a storage medium. Deleted data for example, but sometimes also other data which is not directly relevant from a user standpoint, can not be acquired and potentially interesting information might be missed. For this reason data acquisition is wanted at the lowest layer where evidence can be expected. For hard disk based storage media it's common to copy all bytes from the original storage device to a destination storage device and then do the analysis on this copy. The same procedure is desired for embedded systems with solid-state storage media.

Flash memory is a type of non-volatile memory that can be electrically erased and reprogrammed. Flash memory comes in two flavors, NOR flash and NAND flash, named after the basic logical

structures of these chips. Contrary to NAND flash, NOR flash can be read byte by byte in constant time which is the reason why it is often used when the primary goal of the flash memory is to hold and execute firmware, while parts of NOR flash that are not occupied by firmware can be used for user data storage. Most mobile media, like USB flash disks, or multimedia centered devices like digital camera's and camera phones, use NAND flash memory to create compact mobile data storage.

Flash Doctor is professional tool designed for recovering data from damaged flash devices (both physical and logical problems). It is an advanced stand-alone kit contains hardware and software featuring unique built-in universal algorithm that supports all NAND flash without need to compare the controller types. It supports all NAND-based flash storage devices (SD, SM, MMC, XD, USB Pendrive, Memory Stick, Compact Flash etc.) It is equipped with built-in intelligent Flash Data Rebuilder software providing ultimate opportunities for manual file structure analysis and rebuilding that helps forensic data recovery from flash memory much easier and direct.

- **On-The-Spot Investigation and Fast Forensics: Data Copy King**

During the investigation, administration of justice usually extract all suspicious data from the computer or other mobile HDD then and there aiming to find the vigorous evidence for the crime via strict analysis to that amount of disordered potential information.

Professional data copy-backup device utilized to collect potential evidence requires functions of read-only and selfscan to ensure the originality, authenticity and legality of information collection.

Evidence is often collected through 2 ways of printing and copying. Under most circumstances, we apply the way of printing, or both ways simultaneously. Copying can be applied only when it's inconvenient to carry out all files that need printing on the spot.

Copying is to obtain evidence via the way of copying files to soft disk or CD. After finishing the copying process, it's necessary to insert the soft disk or CD into computer for virus detection. Do not proceed on opening files if virus has been found. Clear it first.

For the on-the-spot investigation, time is justice, reputation, hope, money and even life to be rescued. Here is the problem that damaged data or information destroyed deliberately will consume a long exporting time even the original data can be extracted by forensic devices. Data Copy King is designed to help solve this tough trouble. Fast forensic speed lights up the whole solution. Its data cloning speed up to 7GB/min, for a 120GB hard drive, it takes 20 minutes at most.

Data Copy King (DCK) is a newly designed hard drive duplicator from SalvationDATA top technology in the industry, with color touch screen and build-in SATA/IDE support, USB support with adapters. It's the only hard drive duplicator with "UNIC" disk imaging solution which is able to copy data from good drives or damaged drives with severe bad sectors or unstable heads but still detected in the bios.



Latest Fastest HDD Duplicator, Forensics Friendly

**Disk Image @ 6 GB/min
Disk Wipe @ 6.6 GB/min**

Data Copy King

Highly Successful Disk Image Machine, Copy and restore from 160GB
all of volume from scratch in just 15-20 minutes. Original and
Highly Successful Disk Image Machine, Copy and restore from 160GB
all of volume from scratch in just 15-20 minutes. Original and
Highly Successful Disk Image Machine, Copy and restore from 160GB
all of volume from scratch in just 15-20 minutes.



- ◆ Copy Fast, Copy Must!
- ◆ Bad sector is a big loser here!

SalvationDATA Technology LLC. Tel: 0086-28-68107757 [Http://www.salvationdata.com](http://www.salvationdata.com)

It integrates the latest bad sector repair and bypassing technology as used in Data Compass which is able to retrieve up to 95 percent of bad sectors that are partially corrupted and cannot be cloned by any other tools. Data Copy King reduces the time to image one hard drive with bad sectors, processing the image within several hours while the traditional tools use several days or are impossible to image.

After finishing data copy, DCK will wipe the original information at a fast seed to make sure

investigation is under safety and private condition. Industry's highest data erasing speed up to 8 GB/min, Data Copy King follows the strict DoD (Department of Defense) standard which requires seven passes and is able to provide 999 passes of 0 fill or F fill or random data strings fill to the hard drive for complete data erasing.

Data Copy King supports CRC32, MD5 and SHA-256 checking modes to make sure the integrity of the data from the source drive to the target drive. It has double build-in IDE/SATA ports which are physical read only, this guarantees no data in the source drive will be changed.



- **Protection Of Evidence: USB Blocker**

USB Blocker is designed for write-blocked data acquisitions of any USB Devices, with portable design and data transfer rate at 1.8GB/min. It is one anti-virus device aiming to protect original data from being affected by virus when connecting USB to computer.

■ Why choose us

It is no doubt that numerous outstanding technologies are being researched and developed in different sectors, SalvationDATA are always engaged in research on leading high technology of data recovery and computer forensic.

Since 2001, SalvationDATA initiated into data recovery industry, continuously making technical development and achievements in high-level data recovery products. Now 2/3 of data recovery companies are using SalvationDATA products as facilities to provide real-time and qualified service to customers, to win a value of one hundred million dollars per year, and that means ten billion dollars more save from loss.

In 2005, SalvationDATA entered into forensic field, since then, we focus on forensic technology research. It's being a pioneer that you can see any forensic software in the world is totally compatible with our products.

In fact, SalvationDATA never look back on achievements in the past; instead, facing up to the future development of technology. It's always a technology ensures end user with the best benefits.

We not only can manufacture superior judicial forensic products, but also help to develop OEM products which also satisfy the customer's needs. We highly respect every one of our customers.

We are not aiming at selling. We are looking forward to developing high performance and

easy-to-use products, to benefit our customers.

■ Appendix

● Appendix I

Intelligent bad sector leap function

After implementation of the bad sectors attempts according to the value which is pre-set on the device, the software will try to leap from the sector skipped and read backward until bad sectors found again, rather than reading directly forward from identified bad sector. Through this technique, you can get more user data than other general bad sectors leaping technologies.

Automatic monitor

Automatic monitor function of DC can realize auto soft reset, auto hard reset and power reset, total three kinds of methods to automatically reset/reboot drives that become unresponsive because of media scratch, to continue imaging process and make the program continue the data read operation automatically. As a result, you don't need to stand around watching and waiting for the entire system to be rebooted. Save your valuable time and labor cost!

HEPSS--High efficiency power supply system

When the head reads the bad sector areas, the hard disk's control section will automatically increase the electric output of the head power supply, Thus it can enhance the head's read and write ability to the utmost limit of the design, in order to prevent the endless clicking caused by the head read failure in the original standard working mode.

ShadowDisk technology

DC can image sectors which have been read to an external shadow disk. Therefore the future read operation request will be sent to corresponding sectors of the shadow disk. That means the sectors in source disk which are read many times in the traditional data recovery process will be read only one time now

SWPS - safe write-protect system

It is a great risk of accessing customer's HDD directly through OS. That is because when the OS is reading the sectors, it will automatically write administrative data into the sectors, which provides convenience to the system resource management. Unfortunately, this operation will cause the source HDD corruption and data loss, when this configuration runs on some extremely unstable HDD. DC has a built-in technology which can block the accessing command beyond this rule via base monitoring to prevent all the accidental damage. Finally, "SWPS" it ensures the 100% intactness of the data on the source HDD when doing data recovery.

"SA Analog" technology

DC directly generates key information for booting drive in RAM; therefore, users can directly access data area in hard drive without initializing the SA. No need to find suitable firmware donor or do hot swap, especially problems like multiple bad sectors in SA.

● Appendix II

Computer /network intrusion potential evidence

The following outline should help investigators identify the common findings of a forensic review as they relate to specific categories. This may also help define the scope of the examination to be performed.

Address books

configuration files

email/notes/letters

executable programs

IDS logs

Internet activity logs

IP address and user name

IRC logs

source code

text files (user names and passwords)