

Issue 3/2012 (10) ISSN 1733-7186

# HARDWARE HACKING DATA RECOVERY



DATA RETENTION FOR SMARTPHONES RECOVERING USB DATA

CONTENT-AWARE E-MAIL RECOVERY

S

DO IT YOURSELF DATA RECOVERY

## SeagateDataRecovery.com

# Bad things can happen to your laptop They don't have to happen to your data.

#### Seagate Data Recovery Services work on any disk drive.

Seagate takes the dread out of data mishaps. From accidental file deletions to physical hard disk damage-from any brand-we make it easy to get your files back. With our No Data-No Recovery Charge Guarantee, our skilled professional data recovery technicians use cutting-edge technology to retrieve your data. And for your peace of mind, we also recover data from server applications and virtual technologies. Learn more at www.seagatedatarecovery.com.



© 2012 Seagate Technology LLC. All rights reserved. Seagate, Seagate Technology and the Wave logo are registered trademarks of Seagate Technology LLC in the United States and/or other countries. Seagate reserves the right to change, without notice, product offerings or specifications.

# he Industry's commerci testing

Printer PSU

less

**Air Freshener?** 

ATURES: E

Covert tunneling SSH access over 3G/GSM cell networks NAC/802.1x bypass and more!

> Discover the glory of Universal Plug & Pwn

# @ pwnieexpress.com

e) info@pwnieexpress.com <a>P</a>) 802.227.2PWN

THE



t) @pwnieexpress



Managing: Michał Wiśniewski m.wisniewski@software.com.pl

Senior Consultant/Publisher: Paweł Marciniak

Editor in Chief: Grzegorz Tabaka grzegorz.tabaka@hakin9.org

Art Director: Marcin Ziółkowski

**DTP:** Marcin Ziółkowski www.gdstudio.pl

**Production Director:** Andrzej Kuca andrzej.kuca@hakin9.org

Marketing Director: Grzegorz Tabaka grzegorz.tabaka@hakin9.org

**Proofreadres:** Dan Dieterle, Michał Wiśniewski

#### **Top Betatesters:**

Venay Bhana, Daniel Sligar, Scott Paddock, Graham Hili, Bert White, Joseph Werns, David von Vistauxx, Kashif Aftab, Nana Onumah, Amit Chugh, Rissone Ruggero

**Publisher:** Software Media Sp. z o.o. SK 02-682 Warszawa, ul. Bokserska 1 www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage. All trade marks presented in the magazine were used only for informative purposes. All rights to trade marks presented in the magazine are reserved by the companies which own them.

To create graphs and diagrams we used program by Mathematical formulas created by Design Science MathType<sup>™</sup> DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

## TO HACK OR NOT TO HACK – THAT IS THE QUESTION

OU NEVER MISS THE WATER TILL THE WELL RUNS DRY, YOU NEVER MISS THE SUN TILL IT LEAVES THE SKY" - WORDS FROM THE SONG "UNEASY" BY LAIKA PERFECTLY PORTRAY ONE'S RELATION WITH HIS/HER DATA. WE ONLY REALIZE ITS IMPORTANCE ONCE IT IS LOST. SUCH LOSS MAY BE CAUSED BY THE VARIETY OF REASONS: HDD ERRORS, VIRUSES, USER'S IGNORANCE AND LACK OF KNOWLED-GE ETC. THIS MONTH, WE DECIDED TO PREPARE AN IS-SUE ON DATA RECOVERY TO SHOW YOU, DEAR READERS, MULTIPLE WAYS IN RECOVERING YOUR LOST DATA. WE GENUINELY HOPE THAT THE SELECTION OF TOPICS WILL BROADEN YOUR THEORETICAL KNOWLEDGE AND HOW-TO SECTIONS WILL MASTER YOUR PRACTICAL SKILLS. FIRST, WE HAVE AN ARTICLE BY FRANK MEINCKE, WHICH WILL. STEP BY STEP, SHOW YOU HOW TO SAFELY PERFORM DO--IT-YOURSELF DATA RECOVERY. MIKE PAINTER WILL GU-IDE YOU THROUGH MORE SOFTWARE-ORIENTED PROCESS AND WILL ALSO SHOW YOU WHAT TO DO WHEN YOUR USB STICK IS DOWN. MICHAEL SPREITZENBARTH AND SVEN SCHMITT WILL PRESENT YOU HOW SMARTPHONES PERFORM DATA RETENTION AND SHOW YOU WHERE SUCH DATA IS STORED AND FOR WHAT PURPOSE. ENOUGH? WELL, WE ARE JUST GETTING STARTED, DMITRY SOLOP IS GOING TO PRESENT YOU THE MYSTERIES BEHIND CON-TENT-AWARE E-MAIL DATABASE RECOVERY. THIS MIGHT BE PRETTY USEFUL WHEN YOU REALIZE THAT YOUR BU-SINESS E-CORRESPONDENCE HAS BEEN LOST. IT IS AL-WAYS IMPORTANT TO HAVE YOUR FEET ON THE GROUND, BUT. ON SOME OCCASIONS - YOU MIGHT FIND IT ENJOY-ABLE TO HAVE YOUR HEAD IN THE CLOUDS. ARIEL BERK-MAN AND DANIEL KARIO ARE GOING TO DISCUSS THE ADVANTAGES AND DISADVANTAGES OF DATA BACKUP FOR THOSE WHO DECIDED TO MOVE THEIR SERVICES TO THE CLOUD. KEN KRAUSS WILL HELP YOU TO DIAGNOSE WHAT WENT POSSIBLY WRONG WITH YOUR DRIVE. IF YOU DECIDE TO USE THE SERVICES PROVIDED BY THE DATA RECOVERY COMPANY - GORDON BELL WILL EXPOSE THE TRICKS AND SCAMS USED BY SUCH COMPANIES. WE DO NOT LET THEM CHARGE YOU FOR NOTHING! AS USUAL, AT THE FINAL PAGES OF OUR HAKIN9 EXTRA MAGAZINE WE PREPARED AN INTERVIEW WITH DMITRY L. KISSELEV - A LEADING FIGURE IN SEAGATE'S DATA RECOVERY SECTION. LAST BUT NOT LEAST, WE WOULD NOT BE HAKIN9 EXTRA IF WE HAD NO BONUSES FOR YOU DEAR SUBSCRIBERS. FIRST 15 PEOPLE WHO SUBSCRIBE TO HAKIN9 EXTRA WILL GET FREE DATA RESCUE PC3 LICENSES FROM PROSOFT. IN ADDITION, OUR READERS HAVE 10% DISCOUNT AT SE-AGATE'S DATA RECOVERY LAB.

STAY TUNED!!!

# Need to recover deleted files? Hard drive crashed? Virus taken over?



PROSOFT Engineering, Incorporated

## System Requirements

Data Rescue PC3 requires no Operating System or installation.

Data Rescue PC3 is provided on a self-booting CD containing a special Operating System & user-friendly GUI-based Data Rescue PC3 software.

## Award-winning technology, works when other software fails

- Recovers all types of files from your hard drive.
- Works if the drive fails to mount or only partially operates.
- Recovers deleted, lost and damaged files.
- Recovers digital pictures from your camera media even after it has been erased or reformatted.
- Recover your whole drive or just the files you need.
- Recovers pictures, movies and music from PC drives and any type of digital camera media.

### Two ways to use this software!

#### Application within Windows™

Windows<sup>™</sup> 2000, Windows<sup>™</sup> XP, Windows<sup>™</sup> Vista or Windows<sup>™</sup> 7. Firewire, USB 2.0 or a second hard drive (external or internal) to recover to.

#### Using included emergency boot CD

PC with CD-ROM Drive, 64MB of RAM, Intel or AMD Processor 300MHz or greater. Firewire, USB 2.0 or a second internal drive to recover to.







#### 8. Do It Yourself Data Recovery

#### **By Frank Meincke**

In this article we will cover the basics of what failures one may experience with their hard drives and data, the start-up procedure for the hard drives to better determine what type of failure was experienced, some simple fixes one may do to gain access to their data as well as how to look for a professional Data Recovery Company when needed.

#### **16.** The Mysteries Behind Data Recovery

#### **By Mike Painter**

In this article we will cover the basics of what failures one may experience with their hard drives and data, the start-up procedure for the hard drives to better determine what type of failure was experienced, some simple fixes one may do to gain access to their data as well as how to look for a professional Data Recovery Company when needed.

#### 20. Is Data Retention Still Necessary in the Age of Smartphones?

#### By Michael Spreitzenbarth and Sven Schmitt

It is well known that smartphone operating systems persistently store location information in their local storage for various reasons. However, less well known is probably the fact that also various applications do this, too. In this article we will give you some hints where you can find this data on Android smartphones as well as we will present a system with which all this information can be extracted and visualized at the same time. We will also provide you with a comparison of the quality and quantity of location data gathered through data retention in contrast to the data gathered by forensic acquisition.

#### 26. Content-Aware Recovery of Email Messages and Databases

#### **By Dmitry Solop**

This article reveals the internals of one of such algorithms in application to recovering email databases and individual email messages in RFC -822 format, discussing quirks and issues the developers faced when implementing content-aware recovery of users' emails. The article comes from the developers of numerous data recovery tools employing signature-search algorithms in their products. Expertise shared by the developers will help computer users better understand strengths and weaknesses of much-touted contentaware algorithms.

#### **32.** Head in the Cloud – Feet on the Ground

#### by Daniel Kario and Ariel Berkman

In the last couple of years we have been witnessing a trend of moving internal IT systems to the «cloud». The delivery of computing as a service rather than a product, whereby shared resources, software, information and systems are provided as a utility over the internet. The main motivations for this process are to increase the efficiency of the IT department with cost savings and improved management. The typical and reasonable assumption is that the availability of the data in the cloud will be as good as the availability of the systems of the company before the move to the cloud. Indeed, cloud service providers are carefully defining the SLA for the availability of the cloud based service in their offering, but what about the availability of the data and the its backup (and restore) policy?

#### 36. What's Wrong With My Drive?!?

#### **By Ken Krauss**

Although the computer world is moving towards solid state technology in hard drives, a majority of the hard drives in use today have moving parts, and where there are moving parts, there are increased chances for failure. The parts inside your hard drive are moving at amazing speeds within microscopic tolerances of one another and your data is saved in a few grams or at most a few ounces of metal and ceramics. Most of us really take for granted the miracle of technology....

#### **46.** Computer Hard Drive Recovery: Tips, Tricks and Scams

#### **By Gordon Bell**

This article will give you information of what to do in case you have a computer emergency as well as details on some of the scams and dirty tricks that are out there in the wild. For the sake of this article, I will concentrate on two distinct, common computer problems: Logical and Physical hard drive failures.

#### 50. An Interview with Dmitry L. Kisselev

#### **By Nick Baronian**

One observation is that we haven't seen a significant difference in the size of the data set stored in the cloud from an enterprise level. On the other hand, as one would suspect, consumers tend to store less data in the cloud, because most consumers just don't have the same amount of data as a business entity would. Unrelated to the size of the data set, the value attached to the data is what dictates whether a customer wants our services or not.

# DO IT YOURSELF DATA RECOVERY

#### FRANK MEINCKE

Electronic data and information has become a crucial portion of one's life. Data is important whether it is your Business' Operations Data, Secret product development research, Master's Thesis, pictures of your baby's first steps or loves first kiss one needs access to it. When your data is no longer accessible and/or your hard drive dies there are a few first steps one may do to regain access.

an data recovery actually be Do It Yourself? The answer which is sometimes used in Germany is Jein (a combination of Ja [Yes] and Nein [No]). In this article we will cover the basics of what failures one may experience with their hard drives and data, the start-up procedure for the hard drives to better determine what type of failure was experienced, some simple fixes one may do to gain access to their data as well as how to look for a professional Data Recovery Company when needed. One should note that when a drive is brought to a data recovery company they will inspect the drive for signs of tampering. If they detect that the drive has been worked on previously by someone, they will most likely charge a high analysis or recovery fee, regardless if the data is recovered or not. Data recovery is a field which requires specialized training, background and equipment to move from software only recoveries to the teardown and reassembly of the hard drives to make it function to the point of recovering the data. This background becomes critical when working on Electronic and Physical failures.

Before we get out the screwdrivers and disassemble our hard drive, we should address a few points.

A proper diagnosis of the patient hard drive's failure can help ensure we cause no further damage to the drive or most importantly the data contained on the hard drive.

#### **Hard Drive Start Process**

How does a hard drive start? The startup procedure for a hard drive begins with applying power to the hard drive. Microcode is loaded from ROM to the drives RAM and the magnetic heads are polled. The drive then begins to spin the platters and when the nominal rotational speed is met, the heads unpark and fly above the platters to read additional microcode from the service area. Lastly the magnetic heads are calibrated then the translator is initialized. When these steps are accomplished successfully, the hard drive will return its correct information (Make, model name and capacity) and the hard drive is ready for use.

#### **Read/Write Head Floats on an Air Bearing**

When the hard drive is started, the platters should spin up and stabilize at its nominal speed. When this occurs, the read/write heads will unpark from their storage position and float over the platters on what is called the Air Bearing. The heads fly over the platters as would an airplane fly over the Earth. The distance between the heads and the platters is measured in nanometers. The heads float approximately 76 nanometers above the platters. Looking at table 1 one can see a comparison of common objects we are familiar with and their size in comparison to the Air Bearing distance.

#### Table 1. Relational Sizes Compared to an Air Bearing

Approximate Size	Object
1 nanometer	Size of a water molecule
76 nanometers	Distance the hard drive head flo- ats above the platter
500 nanometers	Size of a particle of dust
1,000 nanometers	Size of a typical germ
8,000 nanometers	Diameter of a Red Blood Cell
100,000 nanometers	Width of a human hair

Hard drives are pretty robust; however, when looking at how close the tolerances are, one can see why a hard bump while the drive is on could be damaging to the drive.

#### **Hard Drive Failures**

Hard drive failures can be broken down into the following three categories:

- Logical: Logical damage to the hard drive's data may occur by system failure, data corruption or deletion of data. There are many forms of damage that may be experienced i.e. Master Boot Record damage, drive formatted, new operating system installed over needed data, when there are bad sectors on the hard drive (unreadable areas) and the application appears to freeze while attempting to access data on the drive, or the intentional or unintentional deletion of data through personnel actions or malware.
- Electronic: The Printed Circuit Board (PCB) or one of its components may be damaged. This problem can occur if the voltage is not stable and a spike occurs damaging the electronic parts on the board. This problem occurs when the code in the ROM is corrupted or the System Area data is damaged. The firmware and system area contain code that instructs the various components of the hard drive on where to locate the requested data. If the electronics or microcode is damaged, then the hard drive cannot function.
- Physical: This damage may occur through various means. Whether the heads have landed on the platters and do not allow them to turn (Sticktion), the spindle bearing is frozen which also prevents the platters from rotating, or the worst case if the hard drive suffers a head crash (dropped hard drive). With head crashes the read/write head can be damaged to the point it will no longer function (hard drive makes clicking noise) or they have been partially or fully dislodged from the arm assembly scraping the magnetic coating from the platters.

#### **Preparing the Workstation**

Searching the internet for software to use for data recovery can present the requester with an abundance of choices. Looking through the returned search engine list, you may ask yourself, which one is the best one for me? The answer sounds simple "the one that works for the situation you have been presented!" Remember, software is developed by people who were faced with a task and either there was no software available or if available, it could not handle the task that was to be accomplished. Most software is try before you buy.

#### **Write Protection**

Write protection for the patient is of utmost importance. If one overwrites the data on the patient it cannot be recovered following the guidelines in this article. To protect the hard drive from being written to, one must either use a software or hardware write blocker. Software write blockers can be accomplished with a registry edit, or one can purchase hardware write blockers from Tableau like those used by computer forensic examiners.

#### **Imaging Software**

Imaging software can be found in a variety of forms and prices. At the beginning of my journey into data recovery I used a variety of software but eventually I selected the following software to use.

- Forensic Toolkit (FTK) Imager (Accessdata). This tool is used by computer forensic examiners to make forensic images of hard drives. FTK Imager is available from Access-Data as a free download.
- Disk Recoup (QueTek Consulting). This tool is useful if the drive you are trying to image has bad sectors or other problems which hang up the imaging process. At times when one is imaging a problematic drive, the workstation

must be rebooted due to the system hanging. With Disk Recoup when you restart the program, it will remember where it left off, jump over that area and continue imaging the patient hard drive. This tool is available from QueTek Consulting Corporation as a try before your buy.

- *R-Studio* (R-Tools Technology). This is a more advanced tool which can be used to image patient hard drives. R-Studio then can be used to scan the image and attempt to recover the file structure and files as originally found. This tool is available from R-Tools Technology as a try before you buy.
- Data Recovery Software
- Data Recovery Software can also be found in a variety of forms and prices. The data recovery software is used to scan through the images which were created with the Imaging Software. During the scan the software searches for files and folders using various algorithms and scanning from the first sector to the last. The following is a small sample of available software:
- Forensic Toolkit (FTK) Imager (Accessdata). This tool can be also used to export files and directories out of the image. FTK Imager is available from AccessData as a free download.
- File Scavenger (QueTek Consulting). This tool is useful for carving data from images which were created from patients using MicroSoft Windows as its operating system. This tool is available from QueTek Consulting Corporation as a try before your buy.
- *R-Studio* (R-Tools Technology). This is a more advanced tool which can be used to recover files from images whose operating system was originally FAT 12/16 to Linux. This tool is available from R-Tools Technology as a try before you buy.

#### **Recovering the Data**

There are three types of failures which can occur to a hard drive Logical, Electronic and Physical. We will explore the different failures and some do it yourself tips to recover the data. When working on a hard drive that failed, regardless of the failure one must remember the following:

- Purchase a couple of identical drives and practice on them. Learn how the make and model of hard drive sounds as power is applied to it.
- Once the patient hard drive is running and access to the data is gained, do not turn it off, for one may never gain access to the data again.
- Create an image of the patient hard drive and then work from the image.
- The hard drive failed once, it can and most likely will fail again.

#### **Logical Failures**

This failure can occur at most anytime. This can be presented to us when a novice computer friend decides that they want to clean up their hard drive. They begin deleting files and directories they deem unimportant or the hard drive develops bad sectors in critical areas (Master Boot Record, Master File Table) and the data is no longer accessible.

Rectifying this failure is not so problematic and can be done rather quickly (depending upon the size of the patient hard drive).

Before we begin a logical recovery we should have the following items available.

- External USB hard drive enclosure to place the patient hard drive into. Use your own known good enclosure.
- Target hard drive which is larger than the patient hard drive.
- Software to image the patient hard drive.
- Software to recover or carve the data from the image.
- Software or hardware write-blocker.

#### **Quick and easy software blocker**

Creating the software write blocker can be done by registry entry modifications. This can be accomplished quickly by creating two files to modify the registry for the system.

*Disablewrite.reg* will be used to disable the writing to external USB drives. Open a text editor like notepad and place the following entries into it:

Windows Registry Editor Version 5.00 [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ StorageDevicePolicies] "WriteProtect"=dword:00000001

#### Save this to your Desktop, naming it Disablewrite.reg

*Enablewrite.reg* will be used to enable writing to an external USB drive. Open a text editor like notepad and place the following entries into it:

Windows Registry Editor Version 5.00 [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ StorageDevicePolicies] "WriteProtect"=dword:00000000

#### Save this to your Desktop, naming it Enablewrite.reg

To activate or deactivate the write-blocker either right-click the *Disablewrite.reg* or *Enablewrite.reg* and select Install or Modify depending upon your version of windows. Reboot the computer so that it loads the registry entry.

#### **Logical Failure Recovery Process**

The processes used for the logical failure recovery process will be used for imaging and recovering the data regardless of which type of failure you're presented. The only difference is the other failure types require one to get the hard drive functional so that it may be imaged and the data recovered.

Imaging the patient hard drive:

- Remove the patient hard drive from its original computer or external hard drive enclosure.
- Attach a target hard drive to the workstation. The target drive must be larger than the patient hard drive we are going to work with. The target drive will be used to receive the bit-by-bit image of the patient hard drive. Connect this to the appropriate port (IDE or SATA) on the mainboard.
- Disable the write feature to external USB drives. Test this to ensure it is functional, by trying to write to an external device i.e. USB thumb drive. If it is functional one should see the pop-up stating that the drive is write protected.
- Install the patient hard drive into the external USB enclosure, power it on and listen to the sounds it makes. Ideally the drive will spin up, the heads will leave the park ramp and read the Service Area. When the USB cable is connected to the computer, Windows should then recognize the hard drive and provide the correct identification of the drive. It may even ask to format the drive, but cancel this.

- To image the drive in this example we will use FTK Imager.
- Open FTK Imager and select File/Add Evidence Item...
- Select Physical Drive. One will be offered a selection menu to connect to the appropriate drive. Physical drive is the best choice since the entire drive will be imaged regardless of the partition it is located in.
  - Select the appropriate drive which will be listed similarly to \\PHYSICALDRIVE0-Make and model (Size)
  - Select Finish
- In the window Evidence Tree, clicking on the + will expand the file folders. For this guide we will assume that the software could not recognize a partition.
- Right click the top of the tree \\PHYSICALDRIVE0 and then select Export Disk Image.
- The Create Image window will appear. Under Image Destination(s) select Add...
- Select Image Type, accept the default Raw (dd) selecting Next.
- Evidence Item Information may be left blank, select Next.
- Select Image Destination window will appear.
  - Click on Browse; expand the folders until you see the target drive which is connected to your workstation.
  - Select the drive and click OK.
  - Give the image a useful name i.e. Frank\_Notebook\_ Drive Use a useful name so that when you do more recoveries, you can tell whose data belongs to who.
  - Set Image Fragment Size to 0 (zero) for we want only one image file for this drive.
  - Select finish
- We are now in the Create Image window. Select the following check boxes: Verify images after they are created and Precalculate Progress Statistics. These two selections will ensure that the image we create is identical to the one we are imaging and also let us know how long the imaging process will take.
- Creating Image window will appear and show us the progress of this procedure. When it is completed we will be back in the original window of FTK Imager.
- Close FTK Imager and remove the patient hard drive from the computer. Disable the software write blocker and reboot the system.

#### **Recovering data from the image**

With the drive imaged and safely put away, it is now time to recover the data from the hard drive image. Working with the image is the most recommended way of conducting data recovery since one can always come back and look for data that was not recovered during the initial recovery.

In this example we will be using File Scavenger to search for the lost data.

Opening File Scavenger the first thing to do is to mount the image as if it is a drive.

- Select File/Disk Image/Load...
  - The window Open will be displayed
  - Navigate to where your image is located.
  - If the image is not visible, change the Files of type: to All Files (\*.\*)
  - Click on Frank\_Notebook\_Drive.001 (if FTK Imager and the setting Raw DD were used) and select Open.
  - A popup will inform you when the image is added.
- Under the field Step 1: Search
  - Click on the grey bar next to Look in:

- The Drive/directory/image.001 should be displayed.
- Click on this and the program will load the image.
- In the field Search for: The default search will include every file. If one is only looking for documents and pictures, click the down arrow on the far side of the Search for: field and select the files of interest.
- In Search mode there are two choices
- Quick-This is best used when files were accidently deleted. This will use the Windows file system structure and is very fast.
- Long- This is best used when the directory structure or file system has been damaged. This scan can take a long time depending upon the size of the patient hard drive. This setting scans the entire image looking for files.
- Click on the button Search and the scan will commence.
- At the completion of the scan, a list of files and their directory will be returned. The program will provide an indication if the file is Good or Not. Even if the program says it is good, manually sampling the data is required to see if it is in fact usable.
- One can click on the Tree View on the task bar. This will present the data in a Windows Explorer view if possible.
- If the file system is corrupt, then the most likely recovery will be a RAW recovery and the only folder will be labeled Unknown.
- Exporting the data to the target drive
  - On the right side of the program there is a *Browse* button. Click it and navigate to the external drive where the data will be placed on.
  - Select Recover
  - Volume or Partition Affiliation will pop up, select the default, clicking on OK.
  - The data will begin transferring onto the location specified in the previous step.
  - When finished another pop-up will display the results of the recovery.
  - Exit the program and go to the directory where the data was recovered to.
  - Open a few of the files which were recovered to see if useable data has been recovered.
- Return the data to the owner

#### **Electronic Failure**

Electronic failures can be quickly recognized. The two most prominent signs of an electronic failure are when power is applied to the hard drive and it does not show any sign of functionality (no platter spin-up or sounds coming from the drive) or a puff of smoke appears from the hard drive; however, no Genie appears granting you three wishes.

#### **Electronic Failure Recovery Process**

Resolving the electronic failure can be as simple as exchanging the Printed Circuit Board (PCB) to complex operations of reprogramming the firmware/micro-code with Ace Laboratory's PC-3000 UDMA. For this guide we will explore how to find a suitable donor PCB to moving the patient's ROM to a donor PCB. Now comes the warnings, if the data contained on the patient hard drive has a value far exceeding the cost of a professional data recovery company's prices, then take it to a professional straight away. Note: The data recovery company will inspect the drive for signs of tampering. If they detect that the drive has been worked on previously by someone, they will most likely charge a high analysis or recovery fee, regardless if the data is recovered or not.

During the lifetime of one's hard drive there are many changes that are not obvious to us, but the hard drive keeps track of them when they occur. These changes are called the adaptive data of a hard drive and are stored and maintained by the hard drive. When a drive is initialized in a factory it is tested for functionality. For instance, when bad sectors are found on the platters they are marked as bad and their location is annotated in the P-List. When the hard drive leaves the factory and is in use by the customer any bad sectors identified by the hard drive are marked as bad and an entry is placed in the G-List so that no data will be placed in the bad sector. Adaptive data lists are kept in the Service Area of the hard drive as well as in the ROM chip on the PCB. When you move the PCB of the donor drive to the patient drive, and start it up, the patient drive will read the adaptive data from ROM and apply it to the drive it is on. The hard drive may not function i.e. it may start knocking or not start at all. Some hard drives can be fixed by just moving the PCB over to the patient and it will start up without a problem which is an exception not the rule.

When presented with a hard drive which has an electronic failure we must take into consideration what may have caused the failure, what component was damaged and do we have the correct tools to fix the problem.

The following items are needed when you begin trouble shooting an electronic failure:

- Torx screw driver set- from size 4 to size 9 (different manufacturers use different sized screws). This will be used to remove the PCB from the hard drive.
- Multi-Meter check the impedance of some electronic components.
- Donor hard drive PCB- This is a tested PCB which is fully functional. Never use a PCB from a hard drive containing your data as a donor. A quick PCB change may leave one with two non-operational hard drives.
- Hot Air Rework Station or Soldering Iron

#### **Identify Electronic Errors**

The easiest symptom of a damaged PCB is, when attached to a power supply the hard drive remains unresponsive. If there is no sound from the hard drive, this could indicate that component(s) may be damaged on the PCB. The second test one should do is hold the hard drive up to your ear and apply power. Listen carefully to determine if there is no noise or if you hear a sound which sounds like an electronic motor trying to turn a spindle, but it is stuck. This sound can be one of three things which we will talk about in the Physical failure section.

What can one try when there is no sound emitting from the hard drive? Place the PCB on a functional hard drive (same Make and Model) and determine if the drive spins up. If the donor drive does not start, then there is an electronic failure. It is time to look for a donor PCB.

#### What can Fail on a PCB

Hard drives have some of their own fault protection built in. The fault protection is used to prevent the data from being damaged on the hard drive. Two items on the PCB which protect the drive are the Transient Voltage Suppression (TVS)

## Hakin9 EXTRA



Figure 1. Samsung PCB TVS Diodes and Fuse

diodes which protect the drive from voltage spikes and a fuse.

For this example, in Figure 1 we have a Samsung PCB which has three components highlighted. In the left side block are the 2 TVS Diodes and directly on the right side of the TVS diodes is the fuse. The two types of failures that I have seen are the components look fine, but with a multi-meter it is determined that they failed or there is a black scorched area where these components once were.

Test the TVS diodes and fuse using a multi-meter which is set on Ohms (200 range). For the TVS diodes when the diodes are tested, one should see the meter register low impedance ~14 Ohms, which will quickly drop indicating an open circuit. This reading indicates the diode is functional. If the impedance is close to 0.0 then the diode is most likely bad. One need only to remove the bad TVS diode from the PCB and functionality should be restored. The other component which protects the hard drive is the fuse. Using the multi-meter if the



Figure 4. Western Digital 2.5" Label

fuse measures an open circuit, then the fuse is non-functional. Soldering a small piece of wire bridging the connection should restore functionality to the drive. When one bypasses the safety measures, there is the risk of causing more damage to the drive. If the drive starts, move your data off immediately and do not use this drive after your data is recovered (Figure 1).

If these three components are not the cause of the failure, then there is another component on the PCB which is nonfunctional. At this point one can try to move the ROM chip from the patient PCB to the donor PCB. This will require that the patient ROM is removed using a Hot Air Rework station or a soldering iron. The ROM chip is usually an 8 leg chip with a model number embossed on top beginning with the number 25. As seen in Figure 2 the ROM is located in the bottom right of the picture. When removing and reinstalling the chip, ensure that the orientation of the chip remains the same. This is accomplished, in this case, by ensuring the small indentation on the bottom right of the chip is in the same orientation on the donor PCB. For other manufacturers of hard drives, one will have to research where the ROM chip is located (Figure 2).



Figure 2. Samsung PCB ROM location



Figure 4. Western Digital 2.5" PCB



Figure 5. Western Digital 2.5" PCB Number

#### **Items needed**

#### How to select a Donor PCB

There are many firms one can use to purchase just the PCB for a hard drive. To order the correct one, there are a couple of key items to look for. Hard drive manufacturers may change the functionality of a PCB for one model of hard drive several times throughout its life-cycle so one needs to look for matching numbers.

One can begin the search for a donor PCB by just placing the PCB number into a search engine. The results will more than likely return a variety of vendors who are selling only the PCB. If no results are returned, then use the drive model num-



Figure 6. Maxtor DiamondMax10 Labelt



Figure 7. Maxtor DiamondMax10 Label

ber with the PCB number. Depending on the availability of the drive and PCB one can get many 1<sup>st</sup> hit responses which is nice, but at times, I have searched months to find an obscure donor drive.

The following must be taken into consideration when selecting a donor hard drive for its PCB:

#### Western Digital 2.5" hard drive

In this example, we are looking for a PCB to use as a donor. Looking at Figure 3 we need to match the Model number, Firmware number and the Country. Model Number: WD6400BEVT Firmware Number: 22A0RT0 Country: Malaysia

(Figure 3)

On the PCB of the drive, the board number must be matched. On the 2.5" hard drive the number is located by the underline in Figure 4. The close-up view of the PCB in Figure 5 shows the PCB Number: 2060-771672-004 REV A (Figure 4-5).

#### Maxtor 3.5" Hard Drive

In this example we have a Maxtor DiamondMax10 hard drive. To find a donor PCB for this drive we need to look at the Model number as well as the GTLA number on the front label of the hard drive. The drive model number as well as the GTLA number is underlined in Figure 6. Looking closer at the drive label in Figure 7 we see the alpha numeric characters 6B300S006591A. To find a PCB which should work on this we need to match the following : **6B**300S006**59**1A (1st and 2nd characters followed by the 10th and 11th characters) (Figure 6).

#### Seagate 3.5" Hard Drive

In this example we have a Seagate Barracuda 7200.12. To find a donor PCB for this drive, one would search on the PCB number; in this case 100574451 REV B see Figure 8. Results



Figure 8. Seagate PCB Num: 100574451 REV B



Figure 10. Seagate 7200.12 Label

Figure 11. Samsung HD103SJ Label

received will show various Seagate drive models. To narrow the search look for the drives model number ST31000528AS as highlighted (Figure 9-10).

#### Samsung 3.5" Hard Drive

In this example we have a Samsung HD103SJ. To find a donor for this drive, one would search for the model number of the hard drive. From the results received find a hard drive which was built around the same timeframe as the patient figure 10. To further narrow down the search one can use the PCB number which is highlighted in figure 11.

Looking for a donor can be difficult and time consuming. One could scour through the various online sales sites to find the correct PCB. There are a variety of companies that specialize in the resale of used PCBs. They are a good source of information and can find the correct donor PCB. Of course, at times the price of a PCB is more than the entire drive. If in doubt of which one is required, the highlighted areas in the various figures will help identify the PCB which is needed.

#### **Physical Failures**

Physical failures are the worst of the three categories a hard drive can experience. These failures can range from seized bearings, damage to the read/write heads to the magnetic coating off of the platters. An incorrect analysis of the failure may cause irreversible damage to the drive. Figures 12 and 13 show what occurs when the read/write heads contact the platters.

The damage caused to the outside edge of the platters in figure 12 was caused when the heads got caught under the park ramp. The damage on the platters in figure 13 was caused by the head touching the platters.

#### **Sticktion**

Sticktion is caused when a hard drive is briefly powered up and powered down. The platters do not reach their nominal rotational speed; but, the heads unpark and float over the platter. As the platters spin down, the air bearing cannot support floating the heads over the platters and the heads land on the platters. The surface of the platters as well as the heads are very smooth, so when the heads stop on the platter the cohe-



*Figure 12. Heads getting caught under park ramp* 



*Figure 13. Head contact on platter* 

sion force is stronger than the torque produced by the motor. The drive will then emit the sound of a motor trying to start.

#### **Seized Spindle Bearings**

Seized spindle bearings will emit a sound similar to that of sticktion. If this occurs specialized equipment will be required. On some models of hard drives the platters must be removed and reinstalled on a donor Hard Drive Assembly. If one platter of a multiplatter assembly moves a micron, the data will be irrecoverable. On other drives, the spindle where the platters are attached to will have to be pressed out of the HDA, the bearing replaced by a donor bearing and the assembly pressed back into the original HDA.

When physical failures are suspected, it is best to seek the services of a Data Recovery Company.

#### How to find a Data Recovery Company

If one places the words data recovery into a search engine the amount of results are enormous, with everyone claiming to be the best. So how do you lessen your chances of sending your drive to the wrong place?

The following recommendations should be followed:

- When the company talks about their data recovery, do they discuss the three types of failures? Some companies only reveal data recovery in general terms, which may lead one to believe they can only do logical recoveries.
- Does their price list begin with "Data Recovery beginning at \$" something very tempting? This can get expensive quickly.
- When looking at the price list, are there three different price ranges one for each type of failure? If so, this is a good indication.
- Do they list any qualifications or certifications that show their skill has been tested?

In this article we have covered how a hard drive functions, the three types of failures one can be presented with and how to repair certain failures. If professional services are required how to review the different company's websites to see if they infact state they can handle all three failures as well as how they list their services and prices. Most of all, be curious on what causes drives to fail and how one can get the data back.

#### FRANK MEINCKE

is the founder and data recovery specialist at Gefund-IT (Data Rescue) who brings affordable data recovery to the clients served by his company. He is a Certified Data Recovery Professional from IA-CRB and has trained with Ace Laboratory and DeepSpar on the use of the PC-3000 for hard drive restoration and data recovery. Frank is a Certified Computer Examiner who had the privilege of training at the Defense Cyber Investigations Training Academy (DCITA) and being awarded Department of Defense Certified Digital Forensic Examiner. He maintains the credentials of EnCase Certified Examiner, AccessData Certified Examiner as well as CISSP and MCSE. During the course of his career he has attended over 1200 hours of computer specific training. When not at work, Frank enjoys being with his family and when time permits you may catch him snowboarding on the Alps during the winter.

## Do You Want to Become a Cyber Security Expert? OR ADVANCE YOUR IT SECURITY CAREER?

- Over Security has one of the largest market shares in IT
- Ø Government & Compliance Regulations are more and more enforced
- Gartner Group predicts unprecedented growth and need in Cyber Security
- Skilled Cyber Security Experts are in ever more demand

#### THE CYBER 51 EXPERT COACHING FORUM

- Individual 1-on-1 Mentoring on Ethical Hacking, Penetration Testing and IT Security
- Networking with other community members and moderators
- Access to a wealth of tools and information not found on public domain
- Permanent Job & Contract offers, Webinars and much more!

#### YOUR BENEFITS

- Become an Ethical Hacker / Penetration Tester with 1-on-1 mentoring
- Learn at your own pace at a fraction of the cost of regular courses

#### **CYBER 51 COACHING FORUM**

#### CYBER SECURITY FORUM



#### CONTENT:

- 1. General Topics
- 2. Service Assessment
- 3. Ethical Hacking
- 4. Cyber Threats
- 5. Mitigating Cyber Threats
- 6. Penetration Testing

#### CYBER 51 INSTRUCTORS

#### **OUR CERTIFICATION LEVELS:**

- Certified Ethical Hacker (C|EH)
- Forensic Investigator (C|HFI)
- Certified Security Analyst (ECSA)
- Licensed Penetration Tester (C|LPT)
- Network Security Admin (ENSA)
- ISC Consortium (CISSP)

#### FEATURES



#### ADDITIONAL FEATURES:

- 1-on-1 Coaching
- Trainers with Years of Experience
- Wealth of Tools
- Webinars
- Networking with other members
- Contract & Perm. Job Opportunities

#### WHY CYBER 51?

- Learn whenever you want to
- Dedicated 1-on-1 Coaching
- Information you will not find on public boards
- All Mentors work as Senior Security Consultants
- Frequent updates
- Great Value for money



#### CONTACT US TODAY

CYBER 51 LIMITED, 176 THE FAIRWAY, SOUTH RUISLIP, HA4 0SH, MIDDLESEX, UNITED KINGDOM EMAIL: INFO@CYBER51.CO.UK WEB: WWW.CYBER51.CO.UK

# THE MYSTERIES BEHIND DATA RECOVERY

**MIKE PAINTER** 

The purpose of this article is not only to help recover lost data, but will also help you be able to discern when it is acceptable to attempt a recovery yourself and when you should send your failed hard drive or flash drive to a data recovery specialist. You will also learn the process that is involved in retrieving lost data and some of the more common instances where data recovery services are needed.

will walk you through a few of different step by step processes involving certain failures that you might be able to recover the lost information. I will also give examples of serious failures and briefly explain the recovery processes from a data recovery specialist's perspective and finish with reiterating the dangers if a non-specialist attempts to recover lost data.

The first expectation that you should have when you are looking at a potential data recovery situation is to accept the fact that all of your data is gone for good. Why do I say this? Because I hope by starting the article off like this that it will not only encourage you to back up your valuable data, but encourage your friends, family and colleagues to start a backup as well.

Dale Carnegie touches on a topic about accepting the worst possible outcome in one of his books, *How to Stop Worrying and Start Living*, which I want to quickly summarize for you real quick. By accepting the worst possible outcome of a situation, things can only look up from there and you can begin the process of finding a remedy to your situation, if it has one. If not, you will at least be prepared for the worst and help you remain a little more at ease throughout the process.

The reason for this is because there is never a guarantee that your information will be recovered. I have experienced firsthand multiple recoveries that seem like a breeze at first or seem to be going smooth but end up turning sour out of nowhere and we were only able to recover a fraction of useful data, or none at all. If a data recovery company promises you they can get your data back this should be a red flag to look elsewhere. This gives a false sense of hope and can lead to a potentially more devastating outcome.Many miracles are performed on a regular basis in the data recovery field. I think of it as the brain surgery of hard drives. It is a very delicate process that requires extreme attention to detail and on occasion a specialized environment.

Many more times than not, data recovery specialists are able to recover data that many people would consider gone for good but there are instances where data cannot be recovered; the most common instance is a head crash. A head crash occurs when the heads either stick to the surface of the drive or physically start digging and grinding into the surface of the platters. Once the heads crash into the surface of the drive it is literally scrapped away, as information is stored magnetically on the surface of the platters.

Depending on the severity of the head crash, this can also prevent a data recovery technician from being able to recover any amount of data off the rest of the drive, even if they swap out the heads. There are some tools out there that can potentially resurface the platters to a point where it's safe for the heads to pass over. In an instance like this, one might be able to recover the data before and after the damage to the surface which potentially could lead to a full recovery; this would just depend on where the data was stored on the platters in relation to the scratch. Not every company out there will have capabilities like this and, keeping that in mind, not every data recovery company will have a class 100 clean room to open up your hard drive.

A class 100 clean room is not even necessary for most recoveries, including recoveries done at home, just the instances where a hard drive needs to be opened up for service on the inner workings of the drive. The reasoning behind this is because the heads are so close to the platters that a speck of dust or hair follicle can cause a head crash and data loss. Moisture is also an enemy as well as it can cause corrosion. If a company does not have a class 100 environment, you need to make sure they won't bother opening the drive, no matter how curious they may get. If you try to open up a hard drive yourself, you just need to make sure it is out of pure curiosity and that there is no important data that is not already backed up. Whether you open it just to see how things work or because you want to try to swap heads, opening a hard drive in a non-sterile environment can completely hinder any possibility of recovering data.

Some of the other tools used in data recovery can allow you to modify the firmware or ROM on a hard drive or even image a drive that your computer BIOS may not be able to see. Out of all the tools I have used so far, the best tool in the arsenal is going to be a hardware imaging tool. My experience is with the DeepSpar Disk Imager, also known as DDI. Like all other data recovery tools, the DDI may seem fairly pricey but this little black box will not only make its money back, but more importantly allows one to recover well over half of the recoveries you might encounter without having to perform any other work to the drive. Even after replacing heads or working with the firmware, a hardware imaging tool may still be required to image the data.

What a good imaging tool will allow you to do is build a head map of the hard drive so you can choose which heads to image first and which ones to image later. This comes in handy when a head has issues reading the information on the drive. Another handy feature to have would be like the *Select Imaging Area* function on the DeepSpar Disk Imager. This feature lets you access the Master File Table, which can be thought of as the directory on an NTFS (standard Windows partition), and search for specific file types, files or folders for you to image first. This can eliminate the need to image the entire drive which can help ensure that you're getting the data that you need before it might stop responding altogether. Unfortunately, this is not a feature for every partition type out there. There also is a big difference between a hardware imaging device and imaging software.

Software, such as the common Norton Ghost or dd in Linux, can work for imaging a failed drive but in order to use this software or similar software, a hard drive has to be in good enough condition to show up in an operating system and gain access to the surface. Usually these are only good for imaging drives with a limited number of bad sectors. Ghost has the capability of a quicker clone than dd with its ability to detect a file system and clone just the files themselves, ignoring the blank space. This is an option you can toggle in the menu of course. Dd allows for you to make a byte by byte image of a drive, which can take some time, but can be more thorough and sometimes your only option if you're limited to software. Some other very useful programs out there have the ability to recover lost or delete files and partitions.

If at some point you accidently delete a file or format your USB drive by mistake, there is still a chance you may be able to pull your information off. Once again though, there is never a guarantee. Most of this software is fairly easy to use and I will go into more detail about how to use them in a little bit. There are still a few things to keep in mind when you try to recover deleted files or partitions. Never install data recovery software on a computer that already has lost information that you need back. If you do, the files related to the program could overwrite the data that has been deleted.

When a file is deleted from a computer, it does not actually get fully erased. The space allocated to the file gets marked as free and the file remains until something else gets written over it. This saves on read and write times, as a secure deletion would immensely hinder the performance of your computer. This is also something to keep in mind the next time you decide to throw out a computer or donate one to charity. If your hard drive falls into the wrong hands and without the proper precautions, someone might be able to get a hold of all your files, or worse, your identity.

There is a great program called Data Recovery Wizard by EASEUS for recovering deleted files or partitions. There is a free demo on their website which will allow you to download 1GB of data. If you only need to recover a few word documents, spreadsheets or pdf's, this should be more than plenty.

First thing first you will need to do is to install this software on a good working computer that you are able to hook the patient drive up to. You will want to make sure the computer is off when you plug in the patient drive, especially if you're working with an IDE hard drive. After you power on the computer and get to the desktop, open up the Data Recovery Wizard Suite by clicking on the desktop icon or going to the start menu and navigating to the software in the list. Go ahead and click on deleted file recovery.



Figure 1. Data Recovery Wizard Main Menu; Here you select the type of recovery you'd like to do

At this next menu you can start customizing what you're looking for to try and speed up the process. Select whichever option would apply to you then click next.

		Deleted File Recovery
Search all lost files automatic	ally	
C Search lost files by types	Common     Common	

Figure 2. First menu after selecting "Delete File Recovery;" Customize what file types you want to look for

Now we have to select which partition we want to search for the lost files. Select the proper drive and click next and it will begin scanning the drive for deleted files.

Option C Refresh Lis	t Disk Image	
Select a partition and click NEXT to re Partition	Cover deleted files: Capacity	Deleted File Recove
C: (NTFS)	148.95 GB	WDC WD16 00AAJS-00B4A ATABus
D : Blackbeard (NTFS)	465.76 GB	WDC WD50 00AAKS-00YGA ATA Bus
E : New Volume (NTFS)	465.76 GB	WDC WD50 00AAKS-65YGA ATA Bus
F: (FAT32)	1.86 GB	SanDisk Cruzer USB Device

**Figure 3.** Partition Selection Menu; Choose the partition you wish to search for deleted files

IF you get the following prompt, let's hit ok. What it means is if we don't find your files when scanning for deleted files, we must do a complete recovery and scan the entire drive which will pull up nearly every file that has been deleted.



Figure 4. Prompt usually showing up for new users only

We are now presented with a screen that shows us the file structure of the file system. Anything with a red d represents a file or folder that has been deleted.

		WinPl	Backup Tool	
Find file by name	Search files			
Select files and click NEXT to r	ecover:	De	eleted File Rec	over
	🛄 - View 🔀 Select 💕	Deselect 🥳 State		
	File Name	File Size	File Type	M
	🔲 🔐 All Time Low - Hit The Lig	hts.mp3 3.31 MB	mp3	20

Figure 5. File selection screen; select your lost files to recover

If you don't see your files listed on the right but see a folder that says *LostFiles1*, navigate through here to try and find what you're looking for. If you would like, there is also a search option so we can search by nearly any attribute imaginable. We can search by file type, file name, date and size to name some of these options. Once you have found the files you need to recover go ahead and check the box(s) that correspond to the file(s). We now go ahead and click next, select our destination folder to recover the files to and we are done. Be sure NOT to recover the files to the drive in which you are recovering files from. Also be sure not to install this software to a drive that has missing files as it can overwrite them and hinder the chances of recovery. This is going to be the easiest and most basic recovery one can perform. From here, we are usually looking at some form of hardware issue. Depending on the type of failure it might be something that can be resolved at home with some basic tools; otherwise you are looking at some expensive specialized recovery hardware that usually isn't necessary for just one recovery.

#### **Recovering Failed Hardware**

Here are a couple more examples of ways you might be able to recover your data, this time from hardware failure. With how often I find myself using specialized hardware to recover data, I will try to keep this as basic and simple for anybody to be able to perform with standard at home tools. If anything you may just have to take a quick trip to the local RadioShack and pick up a soldering iron. I'll begin with recovering data from an external hard drive that has failed and finish with a physically broken USB drive.

Have you ever plugged in an external hard drive only to have it not show up, or even worse, it starts clicking right away? Yes, this can be a major issue but the good news is that this is an external hard drive, not an internal hard drive. Power has to pass through a little transformer box, which are much more prone to failure than a standard desktop power supply, then through a PCB that also contains the USB controller before it makes it to the hard drive. More times than not, if an external hard drive has not experienced physical damage but the hard drive refuses to show up or making abnormal noises, this can be solved simply by transplanting the hard drive to a new enclosure. Replacing the power cord might do the trick, but those are harder to get ahold of and not the likely culprit. Majority of the time the failure is on the PCB itself. So what we'll do is remove the drive and plug it directly into a desktop computer or another USB enclosure, which you can find online for around \$20.

First things first, you need to open up the enclosure. These can be very tricky as there might be some hidden screws underneath the rubber feet or labels. It may also be sealed completely with plastic clips.

The majority of the time it's a combination of the two. By opening your external enclosure you will be voiding any warranty on the drive. But if you find yourself in this scenario, I imagine this is the least of your worries.

Start by removing the rubber feet to check for screws. Once you have removed the rubber feet, you may want to grab a razor blade to remove the labels. If you are not comfortable with that, you can always poke around with a tiny Phillips or standard screw driver to see if it catches on any screws. If you find them, remove them. Now you will want to look around the outer edge and find a crease you might be able to start prying open. Sometimes applying pressure in one way or another can help open up a little bit of the drive in order for you to stick a small standard screw driver in, otherwise you will want to slowly start poking and twisting to get that first pop. I find that using two flat head screw drivers helps keep the process going, using one to hold it open while the other slides around unlocking the other clips. Be careful not to stab yourself and go slow as you are not likely on a time crunch.

Once you have a side removed you should get an idea of where to go from here. Each enclosure is different, so at this point the drive may just slide out or you might have to look around and remove some more screws. Once again, be patient. The metal they use to secure hard drives in place can have sharp corners so watch out for those. After you have removed the hard drive from the enclosure, go ahead and plug it into your computer, which should be powered off at this point. After you have plugged in the power adapter and IDE or SATA connector, go ahead and power on the computer. If the drive does not make any abnormal clicking sounds, the problem is with the enclosure and you can either purchase a new external enclosure or install this drive as a secondary drive in your desktop. If the drive does not show up or it is still clicking, then you should immediately power off the computer and seek a specialist to recover your data.

The last example I have is going to show you how to recover data from a broken USB drive. USB drives are a wonderful piece of technology that you would think is more delicate than they really are. They get plugged in and out of computers potentially dozens of times a day, tossed into the bottoms of our bags, shoved in our pockets, dropped, washed, the list goes on. With all the abuse they take it's kind of mind boggling more things don't go wrong. Over time though, all of this abuse can weaken the solder joints that hold the USB tip to the PCB. Once the solder becomes too weak it might break off or bend to the point the drive is rendered useless. This is the point we will need to have some slightly more specialized tools, at least outside of the ordinary household tool set. You will need a flat head screw driver, a soldering iron and some solder. A solder sucker or de-solder braid would be wise, my preference is desolder braid. A razor blade or hobby knife, pliers, and either a vice or a clamp may come in handy as well. You may even want to have a small chunk of foam or a folded up newspaper to protect the drive from the clamps as it's clamped down in a secure spot.

What we'll do first is open the outer shell to get to the main part of the drive.

The purpose of this is to get your data back; the state of the enclosure should be irrelevant at this point and more than likely be destroyed in the process. If it is a rubber based enclosure, you just need to carefully slide the USB drive out. If it is plastic, they're not usually meant to be opened so you will have to use some force and pry it open. Be careful not stab yourself or use too much as you don't want to damage the inner PCB any more than it already is. This inner PCB will contain the micro-controller and data chip, which needs to remain intact.

Once you have the PCB stick out of the enclosure, we will want to clamp it down on the edge of a table or in your vice. Then we will want to completely remove the tip of the USB stick. I usually add new solder to each point when de-soldering to help heat up the old solder, and make an easier target as well. Another trick would be to carefully slide the soldering iron tip under the USB pin and gently wiggle it free. Once the tip is removed, you will want to use your solder sucker or de-solder braid to clean up the board. You will want to remove all the solder from the 4 connection pins as well as the 2 pins on the side that help secure the end in place. One thing to keep in mind here is a broken USB tip can remove the solder pad, preventing you from applying new solder to the PCB. This also prevents that point from making contact with the board, thus hindering a chance for recovery.

I'd say at this point it's best to consult a data recovery specialist to get your information recovered as you are not able make this connection. A specialist might attempt to recreate this point, or they might actually swap the data chip to an identical donor. They may also have specialized hardware they can plug the data chip into which would allow them to virtually recreate the micro controller to be able to access the information. No matter the method, they have a much higher chance of recovery than a home user. If you are just curious about the process and do not have pertinent information, let's move on. If all the solder pads are intact, you can either skip ahead a paragraph or you can read on out of curiosity.

There is a chance we might be able to create a new solder point ourselves. To do this you will need your razor or hobby knife. You will need to delicately begin scrapping away at the PCB, using the lightly colored rectangle as your guide. Once you see copper, move on to the rest of the rectangle, be gentle and delicate. You do not want to leave any spots of the PCB on the copper as it will prevent the solder from sticking and making the proper connection. After you have the new copper pad, go ahead and apply some new solder to this point.

Go ahead and apply new solder to the 4 points on the PCB. You do not need to apply any solder to the holes on either side of the 4 pads as we will do this after we attach the USB tip. These merely just secure the tip in. Now we need to grab the tip and hold it with one hand, or maybe even some pliers and begin to solder the 4 pins back to the PCB.

This might work a little easier by putting a small ball of solder on the tip of your iron to help make a connection that will surround the pin. Once you have done this to each of the 4 points, go ahead and secure the 2 side points with some solder as well, don't worry if the tip is slightly crooked. As long as the data and ground pins are soldered in place and not touching each other, this should be fine. We will not be placing this back in the enclosure. At this point we are finished. If you would like, feel free to wrap the drive in electrical tape, just to be safe. Plug your drive into your computer carefully. If all goes well it should show up just fine for you to access your data, it might load a little slow, but congrats!

If it does not show up, touching up your solder job may work, but it would be best to take it to a data recovery specialist. There is a chance the micro-controller could have shorted out or you may have some bad resistors.

In conclusion, if there is any important information on the line you should seek a data recovery specialist. Unfortunately, with how specialized data recovery tools are and without proper training, it can be very difficult to perform mid-range to highlevel recoveries on your own without spending lots of money on tools you might only use once. Having said that there are still a few instances in which you can attempt a recovery yourself. The key is knowing when to attempt a recovery on your own and when you should send it out. If in doubt, seek a specialist to retrieve your precious data.

#### **MIKE PAINTER**

has been performing data recovery for over 4 years now at a local computer repair shop, helping to bridge the gap with communication between computer technicians and data recovery technicians. He started off with basic software recoveries and since moved into the more complex recoveries such as head swaps and repairing bad firmware. He's always looking for new methods to recover data, whether it's through colleagues or developing them himself. His motivation stems from the ability to retrieve valuable information for his clients that was once thought to be forever lost.

# IS DATA RETENTION STILL NECESSARY IN THE AGE OF SMARTPHONES?

MICHAEL SPREITZENBARTH AND SVEN SCHMITT

It is well known that smartphone operating systems persistently store location information in their local storage for various reasons. However, less well known is probably the fact that also various applications do this, too. In this article we will give you some hints where you can find this data on Android smartphones as well as we will present a system with which all this information can be extracted and visualized at the same time. We will also provide you with a comparison of the quality and quantity of location data gathered through data retention in contrast to the data gathered by forensic acquisition.

#### Location data in mobile phones:

In recent years, new types of mobile phones, so-called smartphones, have permeated the market. Being small personal computers, they offer much more than the possibility to make phone calls and surf the Internet. Within the last two years the mobile phone market has been restructured and the operating system Android has become the market leader with more than 50% of market share and more than 75 million sold units in the fourth quarter of 2011 [Gartner Inc. - Gartner Says Worldwide Smartphone Sales Soared in Fourth Quarter of 2011 With 47 Percent Growth - http://www.gartner.com/it/page. jsp?id=1924314]. Having such a smartphone in place, more and more users take advantage of the offered variety of applications of third party developers that are directly installed on the phone. So they are able to communicate with friends and relatives via social networks like twitter, Google+ or Facebook. To increase performance of the build-in navigation software and for several other reasons, mobile devices persistently store location data within their own local memory. In April 2011 it was reported that Android and iOS store sensitive geographical data [J. Angwin and J. Valentino-Devries. - Apple, Google Collect User Data. - http://online.wsj.com/article/SB1000142405274 8703983704576277101723453610.html] [J.R. Raphael. - Apple vs. Android location tracking: Time for some truth. – http:// blogs.computerworld.com/18190/apple android location tracking, August 2011.]. This data is stored in cache files on the system. But not only the operating system generates geographical data. Many apps that provide location–based services create and store such data, too. A short overview of the files, we will analyze in the upcoming sections can be seen in Table 1, all the corresponding apps had the development state of November 2011. Smartphones with Android Gingerbread in version 2.3.4 were used for our experiments and the analysis that can be found in this article (Table 1).

#### Starting with something easy – the cache files:

Android is maintaining two cache files with location information. One is cache.wifi (a wifi router database with MAC and GPS data of the router) the other is cache.cell (a database with the id of mobile communication cells and their GPS data). These cache files are located at /data/data/com.google.android.location/files/. Due to the fact that these files are in binary format, the Python code—snippet displayed in Listing 1 should help you to encode the actual data.

Under ideal circumstances you can find up to 200 wifi routers and up to 50 mobile communication cells with the corre-

App Name	Stirage Location	Content
System	cache.cell	Last 50 mobile telecommunication cells
	cache.wifi	Last 200 wifi routers
Camera	/sdcard/DCIM/Camera/ /sdcard/external_sd/DCIM/Camera/	Latitude and longitude of picture location
Browser	CachedGeopositions.db	Latitude, longitude, accuracy and timestamp
Twitter	AUTHOR_ID.db	Latitude and longitude of status message
	Table: statuses	
	AUTHOR_ID.db	Latitude, longitude and radius of location search queries
	Table: search_queries	
Facebook	fb.de	Latitude and longitude of status message
	Table: user_statuses	
	fb.de	Latitude, longitude and timestamp of last checkin
	Table: user_values	
Google Maps	da_destination_history	Source and destination of navigation

#### Table 1. Android applications and stored location information

#### Table 2. Important GPS data inside the Exif area [4]

Tag Name	Field Name	Tag ID
North or South Latitude	GPSLatitudeRef	1
Latitude	GPSLatitude	2
East or West Longitude	GPSLongitudeRef	3
Longitude	GPSLongitude	4
Altitude	GPSAltitude	6
GPS time (atomic clock)	GPSTimeStamp	7
GPS satellites used for measurement	GPSSatellites	8

sponding GPS data and approximate distance in these files. An example of the decoded data can be seen in Listing 2.

Another good point to search for location data – the pictures: Nearly all smartphones have a build–in camera. This camera is able to add special meta data to the pictures the user is taking. This meta data contains the type of the camera, ISO, resolution of the picture, the timestamp when the picture has been taken and location data. If the picture was taken outside a building, the location data is quite accurate and so, this data is qualified for an exact movement profile. To find this data inside a JPEG picture you have to search for the Exif [Standard of Japan Electronics and Information Technology Industries Association – Exchangeable image file format for digital still cameras: Exif Version 2.2 – http://www.exif.org/Exif2–2.PDF]

Listing 1. Python code-snippet to encode the location cache files of an android system

#### Listing 2. Decoded cache.wifi and cache.cell

key	accuracy	confidence	latitude	longitude		timestamp		
		00.1			0.0	40.200010	0 507504	00/05/11 04-06-10 10000
		00:1e:3	08:82:79:31	55	92	49.308010	8.38/324	09/05/11 04:26:12 +0200
		00:23:0	08:ae:29:90	104	87	49.368626	8.588344	09/05/11 04:26:12 +0200
		228:1:6	506:430744	1623	75	47.257888	7.695389	08/13/11 12:04:21 +0200
		228:1:6	506:430742	1433	75	47.266354	7.711417	08/13/11 12:06:33 +0200

# Hakin9 EXTRA



Figure 1. Movement profile generated from data stored on one of our smartphones

area in the byte code of the picture file. The interesting parts of the Exif area are listed in Table 2. On most of the smartphones you can find the pictures either in /sdcard/DCIM/Camera/" or in /sdcard/external\_sd/DCIM/Camera/ (Table 2).

#### Looking for the needle in a haystack – the applications:

As mentioned before, there are thousands of applications in the Android–Market, which request the permission to access location data while installing the app. If you try to generate a movement profile of a smartphone user, the databases of these apps are a good point to search for further location data. In this article we will focus on some of the most commonly installed apps: Twitter, Google Maps, the Android Browser and Facebook.

Each Android application has its own directory, either on the internal memory or on the external sd–card. The structure of the application directories is /data/data/PACKAGE\_NAME/. Inside this directory you normally find a subdirectory with the SQLite databases of the application that we will explain in the upcoming sections.

To get the interesting information from Twitter, you have to analyze the database that can be found in /data/data/com.twitter.android/databases/USERID.db. In this database the table statuses is located. This table holds all status updates that have been twittered by the user. Each status is stored with the corresponding status content, a timestamp, the user id, latitude and longitude. Another interesting table within this database is search\_queries. This table holds meta data to every search the user did through the Twitter app with the actual position of the user (latitude and longitude), time and the query.

Google Maps has one database of interest for gathering location information: /data/data/com.google.android.apps. maps/databases/da\_destination\_histor Here, the application stores all navigations the user has requested. For a forensic acquisition only the start point of a navigation is of interest, because there is no evidence that the user really travelled to

the destination.

Another application where you can find traces of location data is the build–in Android Browser. In the database directory of this app you can find a file called *CachedGeopositions.db*, which contains latitude, longitude and a timestamp of the last position the smartphone was active and has used the browser. This data is used for location–based results of Google search queries.

The last application we will analyze in this article is the Facebook app. Within the main database file *fb.db* are two tables of interest for our investigation: *user\_statuses* and *user\_values*. In the first table (*user\_statuses*) you are able to find latitude and longitude of each status message the user posted on his wall (assuming that the user didn't switch off the positioning service of Facebook). In the second file you can find the last position the user did a so-called check–in with corresponding latitude, longitude and timestamp.

#### **Building the big picture:**

After we got all the data from cache files, pictures and application databases, we now want to merge these data to generate a movement profile of the smartphone user. In our approach we use the Google Maps JavaScript API [Google Inc. – Google Maps JavaScript API v3 – http://code.google.com/intl/de–DE/ apis/maps/documentation/javascript/] and create an interactive map, with every data point and the corresponding accuracy displayed as a circle with an icon representing the kind of data. When moving the mouse to one of the icons, some more information like name of the picture and time the picture was taken will be displayed. An example of such an interactive map can be seen in Figure 1.

Generating movement profiles fully automated – ADEL: ADEL (Android Data Extractor Lite) [M. Spreitzenbarth, S. Schmitt and F. Freiling – Forensic Analysis of Smartphones: The Android Data Extractor Lite (ADEL) – The 2011 ADFSL Conference on Digital Forensics, Security and Law, Richmond, Virginia, 2011)] is a forensic data extraction and analysis tool for the Android platform. The tool consists of multiple scripts (modules) written in Python and can be extended rather easily. It is able to automatically dump predefined SQLite database files from Android devices as well as it can extract the content stored within the dumped databases. A flow chart showing the structure of ADEL is depicted in Figure 2. In the first step, ADEL establishes a connection to an Android device via the Android Debugging Bridge (adb), dumps predefined SQLite databases off the phone and stores them on the investigator's machine (dump module). All of the following steps are performed on the created database copies in read–only mode, thus ensuring the integrity of underlying data (Figure 2).

In the second step contents within the dumped database copies are analyzed and extracted (analysis module). Therefore we developed a specialized parser module for the SQLite database file format [SQLite. – The SQLite Database File Format. – *http://www.sqlite.org/leformat2.html*]. It extracts the contents by directly parsing the database file and does not issue SQL statements to a running SQLite instance. After having extracted the contents, an XML–based report is generated in order to ease further use and depiction of data (report module). The report can, e.g., be viewed in an ordinary web browser and be refurbished with the help of an XSL file.

In the current development state, the following information can be dumped and analyzed with ADEL:

- telephone and SIM–card information,
- address book and call lists,

- · calendar entries,
- browser history and bookmarks,
- SMS messages and
- location data of the most popular apps and the system.

One disadvantage of ADEL is the fact that it can only be used with mobile phones that provide root access and an insecure kernel flag.

#### Some background information on data retention:

In 2006 the European Union issued a directive [European Parliament and the Council of the European Union. - Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. - Official Journal of the European Union, L 105:0054-0063, 2006.] to harmonize the regulations within the EU member states regarding the retention of data generated by publicly available electronic communications services. One main goal of this directive was to allow law enforcement to access traffic data of suspects, e.g., to find out with whom the suspect had communicated or which digital services he had used. In addition to data about individual communications, the directive also demanded that certain location data are retained. More specifically, the directive requires retaining the following data for at least six months:

• Identity and exact GPS position of the radio cell from which the user started a phone call.



Figure 2. System workflow of the Android data Extractor Lite

# Hakin9 EXTRA

Table 3. Comparison of th	e data points gathered	through ADEL and a	lata retention
---------------------------	------------------------	--------------------	----------------

· · ·	-	
Data Source	Smartphone	Data Retention
Cell ID	50	3223
Wifi	200	
Twitter	9	
Facebook	15	
Pictures	20	
Android Browser	2	
Google Maps	4	

 Identity and coordinates of the radio cell that has been active at the beginning of a GPRS data transmission.

• The time stamp belonging to this data.

Comparison between data retention and forensic acquisition: We used the data set provided by Spitz [ZEIT online. – Tell–all telephone. – *http://www.zeit.de/datenschutz/malte-spitz-dataretention*] as a comparison to our measurements with ADEL. This data set was collected within six months by a large German network operator according to the regulations of the EU data retention directive [European Parliament and the Council of the European Union. – Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. – Official Journal of the European Union, L 105:0054–0063, 2006.] Spitz' data set contains only GPS co-



Figure 3. Number of data values from data retention compared to forensic investigation

ordinates of the base station locations and a rough direction of the radio beam. So we had to make an assumption regarding accuracy of these measurements. Since cell site locations are smaller in densely populated areas than in the countryside and Spitz mainly had visited larger cities we assumed that the accuracy was in the range between 501 and 1000 meters most of the time. The rest of the time we assumed accuracy of at least 1000 meters (Table 3).

In Table 3 we provide an overview of the average data that has been restored from the smartphones we had used in two field experiments (one field experiment in late 2011 [M. Spreitzenbarth, S. Schmitt and F. Freiling - Forensic Analysis of Smartphones: The Android Data Extractor Lite (ADEL) - Advances in Digital Forensics VIII, G. Peterson and S. Shenoi, Ed., New York, NY: Springer Science+Business Media, 2012.] and another one in early 2012). We also add to the table some entries that refer to Spitz' data. We scaled down the number of data points in the data set to cover approximately the same time frame that was covered by the field experiments. As one may see clearly, the number of found data points from data retention is by far greater than the numbers found during the forensic analysis of smartphones. However, in this case we are dealing with mobile telephony cells only, while the data records of the smartphones show various other sources. The difference of the number of data records found is probably caused by the fact that the smartphones only save the last 50 mobile telephony cells (Figure 3).

Figure 3 compares the accuracy and number of location information of the smartphones with the accuracy of retained data. On the top of the figure the average smartphone data are shown. On the bottom you see the data of the data retention dataset. Here it is clearly noticeable that the number of data points of data retention are usually much greater as compared to a forensic analysis. If one considers the accuracy of data on the other hand, one can see that data retrieved from forensic



Figure 4. Percentage of time where the smartphones were traceable

#### Is data retention still necessary in the age of smartphones?

analysis has its majority in the interval of 50 to 100 meters. The data of the data-retention, in contrast, has its focus in the realm of above 500 meters. From this it can be concluded that the analysis of stored data with the help of ADEL allows for a far more exact positioning of the user.

To draw further conclusions we set the number of data points, including the stored timestamps, in relation to the maximum possible time period (see Figure 4). Since the data basis of our experiment bears on a time frame of two weeks, the maximum time in which the user is traceable sums up to 20.160 minutes. Taking the dashed part of the figure into consideration, it is evident that in our case, when dealing with data-retention, the user is traceable in about 83% of the time. On the contrary, the smartphones of our forensic analysis are on average traceable for about 18% of the time only (see the bold line in Figure 4).

#### Limitations:

We could also add some privacy enhancing techniques, e.g., to store less information on the smartphone from the beginning. For examples, the option *Use wireless networks* in the device's *Location and Security* settings menu could be disabled. After this step the cache.wifi and cache.cell will be deleted. Further possibilities to reduce storage of location information are to turn off the options *Geotagging* in the camera settings and *Use my location* in the privacy settings of the device. In any case, when dealing with location information one has to consider the possibility that retrieved data may not be reliable to a certain extent. This holds true for location data regarding wifi routers in particular since this data is sent to Google as soon as a wifi router is found for the first time. Furthermore, when dealing with apps like Facebook and Google+ it is possible to link to a certain location although the user is currently not there.

#### Conclusion

On the headline of this article we raise the question if data retention is still necessary. Unfortunately, the answer is not obvious. Comparing the two analyses it is evident that the data of the forensic analysis are far more precise with respect to the positioning. However, data also exhibits clearly more time-related gaps. In case of crime-related analysis a positioning of 18% is quite low as compared to the data-retention with about 83%. However, if the eligible time lies within the range of available data, a forensic analysis will deliver considerably better results since the exactness of retrieved data is significantly greater, allowing for a more precise assignment of user and location.



#### **MICHAEL SPREITZENBARTH**

is a PhD student at the Friedrich–Alexander–University, Erlangen–Nuremberg. He is doing his main research in mobile phone forensics and the analysis of mobile security threats like malicious applications and information leakage. If you are interested in further news and insights in

the field of Android forensics as well as mobile security threats feel free to visit http://forensics.spreitzenbarth.de



#### **SVEN SCHMITT**

is an external PhD Student at the Friedrich–Alexander– University, Erlangen–Nuremberg. His research interests in the area of digital forensics include database forensics and live forensics.





# Fix Windows Registry & Repair PC Errors!



Free scan your Computer now! Improve PC Stability and performances Clean you registry from Windows error

Instant Scan

# CONTENT-AWARE RECOVERY OF EMAIL MESSAGES AND DATABASES

**DMITRY SOLOP** 

Today's data recovery techniques rely heavily on content-aware algorithms instead of using the possibly corrupted file system as the only source of information about disk location of files being recovered. Often referred to as signature-search algorithms, these technologies read the entire disk surface sector after sector in order to discover the missing files.

his article reveals the internals of one of such algorithms in application to recovering email databases and individual email messages in RFC -822 format, discussing quirks and issues the developers faced when implementing content-aware recovery of users' emails. The article comes from the developers of numerous data recovery tools employing signature-search algorithms in their products. Expertise shared by the developers will help computer users better understand strengths and weaknesses of much-touted content-aware algorithms. The article will also benefit software developers, giving them valuable hints and steering them in the right direction when implementing signature search techniques for various purposes.

#### What Can Be Recovered

Our content-aware algorithms can discover email messages in databases in many popular formats including MS Outlook (PST), Mozilla Thunderbird, and RFC-822 EML format. PST files are de-facto standard in most offices using MS Outlook, while EML format is heavily utilized in many free email clients such as those used in Unix and Linux systems, Microsoft Vista Mail and Live Mail. Interestingly, Mozilla Thunderbird makes use of the EML format regardless of storing mail in a solid database file. Its database is, in fact, a linear storage of individual EML files separated with program-specific tags.

#### **Many Email Applications but Only Two Formats**

Fortunately, recognizing just two email storage formats is well enough for successful recovery of emails and databases produced by most popular email clients. In fact, we're using two branches of the signature-search algorithm. One branch handles PST databases in binary format, while the second one takes care of text-only EML and Thunderbird files.

To illustrate how the algorithm works, we'll be using Delphi code using WinAPI. No cross-platform compatibility was planned or intended at the time of initial development, but cross-platform developers will certainly get the main idea.

# Text Files and RFC-822 EML: Simple Format, Complex Recovery

Text is an incredibly simple format. At the same time, missing text files are tough ones to recover. The thing is, unlike many binary formats such as PDF, DOC or ZIP, text files do not contain information about their length or location on the hard drive. We can't just read sectors on the disk looking for ASCII text. If we do, we'll inevitably end up with tons of garbage.

We faced this exact problem when developing SoftAmbulance software family. The tools are designed to recover missing and deleted files of various types from badly damaged, corrupted, formatted and repartitioned disks. That's to say, the type of disks that may no longer hold their file systems intact, so we can't reliably rely on FAT or NTFS records to discover the location of the file on the hard disk.

The main idea behind our approach is that EML files are not exactly text files. In addition to message body, which might be HTML or text in whatever encoding, emails contain structured headers in a strictly defined RFC-822 format.

#### Listing 1.

```
type
 TBoolAnsi = array[AnsiChar]of Boolean;
 TBooleArr = packed array[WideChar]of boolean;
 // Create a list of valid ANSI characters in user's
 // currently selected locale
function AnsiInitialize_LOCALE_USER_DEFAULT(var boolAnsi: TBoolAnsi): Integer;
var
 c: AnsiChar;
 CharType: word;
begin
  for c := Low(AnsiChar) to High(AnsiChar) do
   boolAnsi[c]:= GetStringTypeExA(LOCALE USER DEFAULT, CT CTYPE1, @c, 1, CharType)
                 and (CharType<>0)
                 and (CharType and C1 CNTRL = 0)
                 and (CharType and C1_PRINTABLE <> 0);
end;
```

Strictly speaking, RFC-822 is a text format. However, it has enough of a structure for our algorithm to detect the beginning of an EML file. The assumption we made is everything that goes after the RFC-822 header that's **not** text is **not** part of an EML file.

In order to detect what's text and what is not, we're creating an array of characters that are considered valid text symbols corresponding to ANSI character set of user's currently selected locale. Listing 1 shows how this works in Ansilnitialize\_LOCALE\_USER\_DEFAULT and WideInitialize\_LO-CALE\_USER\_DEFAULT functions. In Windows world, we're utilizing the LOCALE\_USER\_DEFAULT constant. The functions return an array of characters that are considered valid

Table	e 1.																														
0	1 2	2	3	4	5	6	7	8	9	1 0	1	2	3	4	5	6	7	8	9	2 0	1	2	3	4	5	6	7	8	9	3 0	1
dwMa	agic																														
CRCH	Partia	al																													
wMag	gicCli	ien	t													wVe	er														
wVei	Clien	nt														bPl	atfc	rmCr	reate	e				bPl	atfo	rmAc	ccess	3			
dwRe	eserve	ed1																													
dwRe	eserve	ed2																													
bid	Jnused	ł																													
bidì	VextP																														
bidl	lextB																														
dwUı	nique																														
rgn	id[] (	(128	byt	tes)																											
qwU	nused																														
root	: (72	рĀ.	tes)																												
dwA	lign																														
rgbl	FM (12	28 3	oyte	s)																											
rgbl	FP (12	28 ł	pyte	s)																											
bSer	ntinel	1						bCı	rypt	Meth	od					rgt	Rese	erve	d												
bidl	VextB													_										_							
dwCl	RCFull	1												_											_						
ullH	Reserv	ved																													
dwRe	eserve	ed																													
rgbI	Reserv	ved	2																					bRe	eser	ved					
rgbI	Reserv	ved	3 (3	2 b	yte	s)																									

```
Listing 2. looking for PST headers and detecting PST file size
type
 TPWS Data = record
  pBuff: Pointer;
   buffSize: Integer;
   Stream: TStream;
   Output Ext : TPWS Extension;
   Output_size: int64;
 end;
function CheckHeader(var Data: TPWS_Data): boolean;
const
  Pst_File_Header = $4E444221; // !BDN
 ver1 = $0E;
 ver2 = $17;
 REST = 253952;
type
 PPST_Header = ^TPST_Header;
 TPST_Header = packed record
  MagicHeader: Cardinal;
   unk1: Cardinal;
   unk2: word;
   Version: byte;
   res1: packed array[0..156] of byte;
   File Size1 : integer;
   lastSegment1: integer;
   res2: packed array[0..7] of byte;
   File Size2 : Int64;
   lastSegment2: int64;
 end;
var
 Header: ^TPST Header;
 fileSize: int64;
 bFSize32, bFSize64: Boolean;
begin
// Algorithm:
\ensuremath{//} If the two bytes representing version number are valid, then
    If "size" value is obviously invalid (is less than
     or equal to zero or equals MaxInt), calculate size based
     on contextual data;
     Else use value from the FileSizeX field;
// Else assume calculated and stored sizes are the same
\ensuremath{{\prime}}\xspace // in order to be valid for one version or another
 Result:=False;
 if PPST Header(Data.pBuff).MagicHeader <> Pst File Header then
   Exit:
   Header:=Pointer(Data.pBuff);
   Result:=True;
   Data.Output Ext:=FilePst.Extension;
    Data.Output_size:=-1;
    // Далее пробуем определить длину файла
    if (Header.Version=ver1)or(Header.Version=13) then begin
     fileSize:= 0;
     if (Header.File_Size1 > 0) and (Header.File_Size1 < MaxInt) then
       fileSize:= Header.File Size1;
      if (Header.lastSegment1 > 0) and (fileSize = 0)
       and (Header.lastSegment1 < MaxInt - REST )
      then
       fileSize:= Header.lastSegment1 + REST;
```

```
// Setting length value
     if fileSize > 0 then
       Data.Output size:= fileSize;
   end else
     if Header.Version=ver2 then begin
       fileSize:= 0:
       if (Header.File Size2 > 0) and (Header.File Size2 < FilePst.MaxFileSize) then
         fileSize:= Header.File Size2;
        if (Header.lastSegment2 > 0) and (fileSize = 0)
          and (Header.lastSegment2 < FilePst.MaxFileSize-REST)
        then
         fileSize:= Header.lastSegment2 + REST;
      // Setting length value
       if fileSize > 0 then
         Data.Output size:=fileSize;
     end else begin
       // Если Header.Version не верен
       bFSize32:= (Header.File_Size1 > 0) and (Header.lastSegment1 > 0)
             and (Header.lastSegment1 < MaxInt - REST )
             and (Header.File_Size1 - Header.lastSegment1 <= REST );</pre>
       bFSize64:= (Header.File Size2 > 0) and (Header.lastSegment2 > 0)
             and (Header.File Size2 < FilePst.MaxFileSize)
             and (Header.lastSegment2 < FilePst.MaxFileSize - REST )
             and (Header.File Size2 - Header.lastSegment2 <= REST );
        if (bFSize32 <> bFSize64) then begin
          // Setting length value
          if bFSize32 then
           Data.Output size:=Header.File Size1;
          if bFSize64 then
            Data.Output size:=Header.File Size2;
       end:
     end;
end;
```

text symbols for the user's currently selected locale. The rest is quite simple. The algorithm is reading consecutive sectors on the disk looking for signs of a typical RFC-822 header. We're using a weighed score method that triggers when a few typical strings such as «x-mailer:», «mime-version:», «from:» «date:», «content-type:», «subject:» etc. are discovered in close proximity. When the algorithm believes a valid RFC-822 header is discovered, it starts verifying consecutive sectors for text data by checking sectors it reads against the boolWide array containing what we consider to be valid text characters.

Of course, our text detection algorithm is also weighed score based. We'll consider data a text if less than 2 per cent of characters fall outside of the defined list of text symbols. When the 2 per cent threshold is reached, the data is considered binary; the algorithm stops there and returns the location of yet another EML file.

Knowing the beginning (RFC-822 header) and end of an email message, the data can be saved as a regular EML file.

When looking for Mozilla Thunderbird files, the list of RFC-822 headers is extended with two extra fields specific to that email client: «x-mozilla-status:» and «x-mozilla-status2:».

#### **Recovering Outlook PST Files**

The simplest and most widely utilized way to locate Outlook Personal Folder (.pst) files on the disk is looking for PST binary header structures starting with "!BDN" string.

Located at the very beginning of the file, the header structure contains essential information about the PST file. For data recovery purposes, PST file size is the most important piece of information available in the header. Although the layout of the header structure differs slightly between Unicode and ANSI versions, the differences are minor enough to consider it being a single format instead of employing two different branches of the data recovery algorithm.

Tables 1 and 2 demonstrate the differences between Unicode and ANSI headers. In order to determine the size of the PST file, we'll need to discover which format it's in. The value Table 2.

0 1 2 3 4 5 6 7		6 7 8 9 <mark>2</mark> 1 <u>2 3</u>	4 5 6 7 8 9 <mark>3</mark> 1
dwMagic			
CRCPartial			
wMagicClient		wVer	
wVerClient		bPlatformCreate	bPlatformAccess
dwReserved1			
dwReserved2			
bidNextB			
bidNextP			
dwUnique			
rgnid[] (128 bytes)			
root (40 bytes)			
rgbFM (128 bytes)			
rgbFP (128 bytes)			
bSentinel B	bCryptMethod	rgbReserved	
ullReserved			
dwReserved			
rgbReserved2			bReserved
rgbReserved3 (32 bytes)			

of the wVer parameter defines PST format as ANSI (values 13 and 14) or Unicode (23).

The following listing illustrates how our algorithm searches for PST file headers and determines the size of the PST file.

By using the code shown in Listing 2, one can reliably detect the type and size of a PST file. Knowing the exact position of a PST file on the disk, one can easily extract and save the file.

It's important to note that all information being recovered must be written onto a different disk. Otherwise, one faces the risk of overwriting information instead of recovering it. Of course, this rule equally applies to all other types of data being recovered.

#### What about PST Encryption?

PST data blocks are encoded. However, they are not technically encrypted in a truly forensic sense. According to Microsoft, "These algorithms only provide data obfuscation and can be conveniently decoded once the exact encoding algorithm is understood. Moreover, only end-user data blocks are encoded in the PST. All the other infrastructure information, including the header, allocation metadata pages and BTree pages are stored without obfuscation. In summary, the strength of the encoded PST data blocks provides no additional security beyond data obfuscation."

As such, PST encryption does not present a particular challenge. We don't even need to decode information as only user data (actual email messages, appointments, organizer information etc.) is being encrypted, while all headers and technical information are left in their plain form.

To quote Microsoft again, "The PST Password, which is stored as a property value in the Message store, is a superficial mechanism that requires the client implementation to enforce the stored password. Because the password itself is not used as a key to the encoding and decoding cipher algorithms, it does not provide any security benefit to preventing the PST data to be read by unauthorized parties. Moreover, the password is stored as a CRC-32 hash of the original password string, which is prone to collisions and is relatively weak against a brute-force approach".

From what you see, using a password to protect Microsoft Outlook (PST) files is not a good idea. Not only does it fail to provide any sort of protection against unauthorized access to user's personal information, but the cryptographically insecure CRC-32 hash makes it a perfect target for an accelerated brute-force attack.

For these reasons, our data recovery algorithms will not use passwords when recovering PST files (or, rather, when creating a new PST file on another disk).

#### Conclusion

With multiple email clients available on the market, the majority of formats can be actually recovered with just two algorithms. After reading this article, you have learned how to detect the beginning and end of an EML file, distinguish between text and binary data, and discover the location of PST files. The issue of PST encoding was covered to demonstrate the encryption is not of an issue from consumer data recovery standpoint (and is of negative value from forensic standpoint, presenting a security issue regarding the insecure password hashing prone to fast brute-force attacks).

#### DMITRY SOLOP

is a leading developer managing the entire range of email recovery products offered by SoftAmbulance. With more than five years of experience, Dmitry knows everything about email, disk and data recovery techniques. He developed key algorithms currently employed in SoftAmbulance products. Dmitry has a B.Sc. in Applied Mathematics and Social Informatics. He is currently busy developing a database recovery product to fix MS SQL, MySQL, MS Exchange, Active directory, MS Sharepoint, and MS Project Server files. He is also involved in the maintenance of existing email recovery products.

# CODENAME: SAMURAI SKILLS COURSE

# Penetration Test Training Samurai Skills

- You will learn Real World Hacking Techniques for Targeting, Attacking, Penetrating your target
- · Real Live Targets ( Websites , Networks , Servers ) and some vmware images
- · Course Instructors are Real Ethical Hackers With more than 7
- years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- \* Every Month New Videos ( Course Updated Regularly )
- Suitable Course Price for ONE Year Support
- \* Take Our course at your own pace ( any time , any where )
- \* Our Course is Totally Different from Other Courses ( new Techniques )

## Hakin9 EXTRA

# HEAD IN THE CLOUD – FEET ON THE GROUND

#### **ARIEL BERKMAN AND DANIEL KARIO**

In the last couple of years we have been witnessing a tendency of clients moving their in-house IT systems to the cloud. We argue that the ability to internally restore data by employees of the organizations via their IT department, and further by the IT departments at datarecovery labs is becoming a non-trivial task.

M oreover, individuals relying on SaaS providers (e.g. GMail, Facebook, Twitter, Salesforce) are unaware of the risks of losing their cloud-data and find themselves contacting data-recovery labs for assistance, despite the latter's inability to assist in such matters. We discuss several key factors that should be matched by the customer of such cloud services and elaborate on some real life examples.

#### Introduction

In the last couple of years we have been witnessing a trend of moving internal IT systems to the "cloud". The delivery of computing as a service rather than a product, whereby shared resources, software, information and systems are provided as a utility over the internet.

The main motivations for this process are to increase the efficiency of the IT department with cost savings and improved management. The typical and reasonable assumption is that the availability of the data in the cloud will be as good as the availability of the systems of the company before the move to the cloud. Indeed, cloud service providers are carefully defining the SLA for the availability of *the cloud based service* in their offering, but what about the availability **of the data** and the its backup (and restore) policy?

#### Theory

The typical CIO and IT manager are well aware of the complexities relating to backups of complex IT systems. This is mounted to the difficulties with restoring onto a live system, performing the restore in minimum time, and periodically testing the validity of the backups. Actually, this complex nature of the backup and restore processes are one of the motivations to move to the "cloud" in the first place. The complexity is driven from various elements:

- The size of the data to backup and restore is growing very fast.
- The frequency of the backup required by the users is growing – as the data is changing and accumulating more quickly.

- The duration of the backup is growing, and the backup process is becoming more complex.
- The backup process of a live system ("Hot backup") is adding further complexity to the underlying system and the backup process.
- The growing costs of backup software licenses and equipment.

The act of migrating the data from the organization to the cloud service provider (together with the responsibility to backup the data and restore it when necessary) might give a false sense of safety. It is somehow assumed that all the difficulties related to backing up and restoring the data is suddenly gone. And that it's safe to assume that the service provider will overcome these issues perfectly.

Unfortunately, this is not the case.

We had encountered numerous cases whereby cloud service providers suffer from data loss, without the ability to properly recover. Either by taking very long hours to bring the system and its data back online, or fail to restore some of the user data altogether. Multiple such cases had been recently on the news (see below).

In some occasions, the restoration procedure fails and datarecovery companies are asked to assist in recovering the client's data. However, in such occasions even further complexity is exhibited. Since shared resources are used to service multiple-clients, utilizing the services of data-recovery labs might affect other users' resources (e.g. when some storage components needs to be taken apart and examined) and as such might be more harmful than useful.

The inherent difficulty in designing, implementing and testing the backup and restore of a typical SaaS (cloud) provider is increased further by the variance of the requirements by their different customers. For example – in the case of a data-loss incident (like human error, virus, physical malfunction, sabotage etc.) the cloud service provider is required to recover the latest working backup (assuming such a backup really exists) – for example, a backup that

was made twelve hours prior to the incident. But is a twelvehour old backup good enough for the client? The answer highly depends on the set of expectations of the customer. While a small domestic company might be okay with losing twelve-hours worth of emails (or not even notice the missing emails), a large multinational company will surely notice the missing emails – some of which might be critical to its workings.

Is the backup and restore policy of the cloud service you are using adequate to your company's needs? Here are some categories you might want to look into:

- Data Retention Period what is the total duration of the time the backed-up data is kept by the service provider? A Day, a week, a month, a year? The answer is highly dependent, of course, on the nature of the data, the rate of changes in the data, the importance of the data, regulation and many other factors. The parameter is highly dependent on the exact requirements of your organization. But what is the cloud provider actually doing?
- Backup Frequency how frequent is the backup taking place? Is it an ongoing backup? Every hour? Every 12 hours? Once a week? The growing rate and complexity of the data combined with the desire to save all the information together with the meta-data makes a high frequency backup rather challenging. Advanced data storage devices contain sophisticated mechanisms to ease this tasks for example snapshots and storage virtualization but they are not complete solution, complex to manage by themselves, costly and might not scale well.
- Backup policy and disaster recovery plan (DRP) cloud service providers that hold valuable or sensitive data and are aware of the risk of losing information prepare for possible data loss by integrating a set of backup procedures and disaster recovery plan from common set of disaster scenarios. These plans are prepared by a domain expert and should be in line with the customer requirements, especially regulation requirements (if exists), to be able to allow the customer to recover all their data and even more importantly to minimize the restore time. Typically, in a case of a disaster the panic and confusion are great, and the duration between the disaster and the successful restore is critical. Since these restore processes are complex, the cloud service provider should practice the recovery process to find and mitigate possible errors in it.

Other factors should also be taken into consideration – is there a backup of the data off-site? (How far is this place?), which backup and storage technology is the cloud service provider using, and how reliable is it? These factors can help evaluate the maturity of the cloud service provider, and it is highly recommended that these factors will be verified with the service provider to see that the company demands for data availability are matched with the service provider capabilities.

#### Practice

In this section, we will try to analyze common data-loss cases and compare the possible solutions when the service is given as a cloud based service with the *traditional* approach of company based IT systems and services. All of the cases shown are real life cases of real people from the last year (2011-2012). We are witnessing more and more such cases, as the shift to cloud based services is on the rise. "... I'm using cloud based service for my company's web site (they have templates for flash and nice content). I accidentally overwrote parts of my site content with some old dummy content. I didn't save the site content on my computer. How do I restore the site content back? "

#### Fig 1. Web site collision

In the traditional IT world, the answer for such case is relatively straight forward: contact your content/web admin, and ask her to restore the disk's content/site content to the latest backup. The backup software usually provides a simple interface which allows for quick detection of the modified files and allows restoring them to their original location.

In the cloud based service world however, things might be trickier. Not all web services save backups as snapshots "per user", not all of them provide the user with the functionality of selecting which files to restore (selective restore), and finally not all of them give the ability to restore pages derived from templates owned by the site. In this case the restore operation has to be executed manually, on a per-page basis, during a long downtime of the site.

"... Someone took over my email account and deleted everything !"

#### Fig 2. Account hijack

In the traditional IT world, the email content is backed up and can usually be restored to the last backup relatively quickly. The password of the account will be reset and the user can quickly get back to normal operation (several hours of email might be lost, but that's usually acceptable). If several hours' loss is unacceptable, or the backup is not working altogether, a data-recovery company might be contacted and asked to assist in recovering the last backup, or recovering from the media that contained the email data before it was deleted.

In the cloud this might be much more complicated. Most email providers by default will not allow you to restore deleted emails (that is if they were *permanently* deleted by deleting them from the trash). Organization and individuals can purchase archiving services (for example from vendor likes *http://www.google.com/ postini/* for Gmail or from other third party vendors) to overcome this issue, but in many cases do not as they are unaware of the risks. If the organization is subject to regulations (e.g. SoX, PCI etc) or in the midst of a legally bounding process (E-Discovery process during a trial), having no email archive will result in no access to deleted emails.

Finally, a hijacked email account, if not part of a domain (or an admin account in a domain) might be difficult if not impossible to re-gain. Some methods exist to recover a hijacked account, but if the proper measures had not been taken beforehand, chances are your email account – with its data – is gone forever as there might not be a way to distinguish the real owner from the *new* one.

... If you've deleted a message permanently, by clicking Delete Forever in your Spam or Trash, you won't be able to recover

# Hakin9 EXTRA

the message using the Gmail interface. In the past, users have reported that they are missing all of their messages as a result of unauthorized access. If your account was compromised and you would like us to investigate whether recovery is possible, please first complete this process to secure your account and then file a report. (taken from formal Google web site). "

"... I lost my password to my cloud based ERP account, cannot recover it, I need to approve some invoices fast. What can I do?"

#### Fig 3. Lost password

Traditional IT world: use the restore password procedure. A quick call to the help desk, reset your password (Authenticate via phone if nothing else works). If in urgent need of support – escalate via phone.

Cloud based world: Indeed, no data is lost at the cloud based service. The only thing that needs recovering is the password for the user. However, instead of talking to internal IT, now the user needs to deal with service provider in an out-of-band procedure (most of which only have email support). This is not simple if there is difference in service hours, serious language barrier, or strict procedures of the provider that are not part of the corporate culture of the customer. In the event when time is scarce, like the one mentioned above, the restore process can be quite painful.

"... I'm using a cloud based CRM. We have data with cross relationship. I accidently added some garbage data, and noticed only after few weeks. How can I clean it? ..."

#### Fig 4. CRM case

First, let's explain this scenario. The main issue here is data corruption by the user – in most cases, accidentally. From the service provider's stand point, the system was working just as it should have. However, from the user's standpoint a restore is required. The situation is trickier still since cross relationship is involved. We will use some naïve example to illustrate this. Think of a *customer* table, where each customer has a car with some model, and the model is taken from the *car models* table. This is the simplest form of *primary key* <-> *foreign key* relationship. Now assume that the user added some corrupted (garbage) car models, and then added some customers with cars of these models.

After some time (usually days to weeks) the corrupted data is revealed. Now the user is faced with a problem – how and what data to roll back? They cannot simply restore the car models table, since some records are linking to it. A lot of data has already been changed in the system (added/removed/changed), so a full roll back is not an option either. The only approach left is a manual, tedious analysis and repair of the relevant data using current and older snapshots of the entire data.

This is an over simplified example of course. Think of a typical CRM system, where the tables lying *underneath* the system are complex, rich with fields, and contains a mesh of cross relations. The restore task in a real life case of data corruption is non-trivial at best. In both the *traditional* IT and the cloud based world this is not an easy task. But whereas in the *traditional IT* world, the IT department will provide you with complete backups from different time periods (depending on the retention policy defined by the organization to be the right one for it), the cloud provider will not grant you this data. It might show you some history of changes for certain fields or tables, but these would be limited and difficult to work with and will not allow you to repair a large set of errors.

Similar recovery scenarios will also be required when intentional data deletion (be it due to a malicious user or a cleanup process gone awry) or data corruption occur in your CRM data (e.g. an integrated system with a bug causing some unexpected data to be introduced or otherwise corrupted).

For complete snapshots of your CRM data you would have to use third party tools such as OwnBackup - *http://www.ownbackup.com* that provides nightly snapshots of i.e. Salesforce CRM data elements.

Google's Gmail had a glitch introduced that caused 30,000 users or so to lose email, chat and contacts from their Gmail accounts. The cause appears to be a bug in a software update.

Fig 5. Gmail is down

Due to various reasons – some of which mentioned above –cloud based services are subject to malfunction and downtime and in some cases data-loss. Examples of cloud-services malfunction resulting in data-loss are not as rare as people might think. Here are some recent examples:

Gmail losing some 30,000 email data due to an upgrade error: http://www.informationweek.com/blog/229300876

Amazon EC2 malfunction resulting in multiple website being down: http://www.nytimes.com/2011/04/23/technology/23cloud.html

Megaupload taken down by feds, what about all the legitimate data? http://www.bbc.co.uk/news/technology-16642369

#### Summary

The growing dependency of modern company on digital information, combined with the trend of moving IT systems to the cloud requires some deep inspection of the backup and restore policy of the cloud based service and vendor. It is highly recommended a customer of such cloud based service will verify with the vendor that their data availability requirements are matched with the abilities of the provider. Another alternative is to use third-party backup solutions that match the needs of the customer and ensure a backup of their own is available if need comes.

#### ABOUT US

Recover IT, LTD (http://www.recover.co.il) specializes in data recovery from complex IT systems, servers, raids, VM images, backup tapes, hard disks, flash based devices (including SSD) and more. Recover IT develops and manages a unique backup service for cloud based services – see https://ownbackup.com. Recover IT holds an ISO 9001:2008 certificate for data recovery and information re-construction and provides service to global fortune 2000 companies.

#### DANIEL KARIO AND ARIEL BERKMAN

(danny.kario@ownbackup.com) (ariel.berkman@recover.co.il) have over 10 years experience in the IT world. Specifically in the information security and storage related systems.





#### Main Features of StaffCop:

Screenshot recording Application monitoring E-mail monitoring Web site monitoring Chats/IM activity recording USB device monitoring **Clipboard monitoring** Social Networks Monitoring Search Term Tracking File and Folder tracking Keystroke recording System Event Monitoring Whitelists and Blacklists PC activities reporting Stealth installation/monitoring Strong security Alert notifications Remote Install / Uninstall

StaffCop Standard allows you to monitor all activities on company computers and prevent the unauthorized distribution of sensitive corporate information.

## StaffCop will help you:

To locate possible data loss channels and prevent loss To gain insight into how your employees spend their work time To increase company and departmentals efficiency

## You need StaffCop to:

Gather work time efficiency statistics Easily control your employees in real-time mode Improve discipline and motivation of your employees

## Who needs StaffCop:

CEO/CTO Corporate Security Manager HR Manager System Administrator

More Information, Demo Versions, Videos and Technical Guides -

# www.STAFFCOP.com

# Phone: +1-707 -7098405 Skype: staffcop.com Email: sales@staffcop.com, paul@atompark.com



# WHAT'S WRONG WITH MY DRIVE?!?

#### KEN KRAUSS

Although the computer world is moving towards solid state technology in hard drives, a majority of the hard drives in use today have moving parts, and where there are moving parts, there are increased chances for failure. The parts inside your hard drive are moving at amazing speeds within microscopic tolerances of one another and your data is saved in a few grams or at most a few ounces of metal and ceramics.

M ost of us really take for granted the miracle of technology.... Until your computer won't boot up, or until the cat or dog knocks your laptop off your desk, or until you accidentally kick your external drive, or until that cup of coffee just seems to jump out of your hand, or until you just hear a flurry of whirring and clicking from your computer but no action... And then you suddenly realize... You have no backups of your wedding photos, baby photos, customer lists, emails, accounting files, client files, hundreds or thousands of dollars of movie and music purchases..... Everything you've ever done business-related..... ARHHHH!

These are all stories I've heard in my ten years experience running a tech service that does data recovery. Actually, stories I've heard too often, and in a panic. But most of us have been living and using technology for decades, and because of that, we have a false sense of trust that the technology won't fail us. I've been using computers for years, and I've never lost any data, you might think. I know people say to keep backups religiously, but with this new computer technology, I just don't think it's as important as it used to be, you might try to rationalize to yourself. But let me assure you, it will fail you! If it hasn't already, it will at some point, and the law of averages is that if you use technology everyday all day like many of us do, it will fail you sooner than the average person.

Let me take this opportunity to tell you to put down the magazine or step away from the computer and go burn a DVD backup of your data. Any data. Just pick something. I'm serious – I know you need to! Even if you're the baddest backer-upper on the block, you probably STILL need to make a backup DVD right now. I don't care even if you've been a loyal subscriber to one of the cloud backup providers – keep local copies of all important data too! If you don't have any offsite backups right now, burn two copies of that backup DVD and take the second copy to a family member's house, or a friend's house, or get a safety deposit box at the bank and keep it there. I'm not a big fan of using either thumb drives or external drives as backups because they crash frequently, but they're better than nothing. But, I can't stress enough how important it is to keep a local copy and an offsite copy of all your important data. That's COPIES of your important data. Like beer and money, you can only have too few backups, not too many.

Luckily, in most cases, your data can be saved if you still have the crashed hard drive, thumb drive, memory card, or computer. Now, this doesn't mean you can skate by a little longer without keeping adequate backups – go burn another backup DVD just for thinking that! What this means is that you should calm down and take a deep breath if you're reading this trying to figure out how to get all your important data off your crashed drive, or if you're a network administrator or computer tech who has reluctantly found yourself in front of a frantic co-worker, client, friend, or family member who has just had a data loss. There is hope if you're facing a data disaster, and hopefully you'll find what you need to recover your important data in this article.

#### Mentally Reconstruct What Was Happening at the Time of Failure

First off, try to mentally reconstruct what went wrong. Don't do anything with the drive itself yet, but spend a moment trying to identify what sort of data disaster you're facing. Had the hard drive been making strange noises? Was there some sort of electrical surge or outage? Did the computer have a bad virus? Was the drive damaged somehow, such as being dropped, kicked, jolted (even as little as keys or a cell phone being dropped on a laptop), damaged by liquids, overheated (either by sun /heat exposure, or in an overheating computer), or somehow damaged by another failed part in the computer such as a bad motherboard or power supply? Was the external drive or thumb drive pulled out of the computer without properly ejecting the drive from the operating system? Did you just accidentally delete files that you needed, or reformat your external hard drive rather than the new thumb drive that you wanted to format?

Rarely in my experience do drives just fail completely with no singular damaging event or repeated abuse, unless they're many years old. Even then, it doesn't happen often. Most of the time there is some sort of event that pushes your system over the edge and ends up in a data recovery situation, or your drive starts misbehaving but doesn't immediately fail completely. There is a point where all hard drives are going to stop working, and your care of the hard drive and the computer it's in or attached to can extend it's life. Also, your recognition of computer or hard drive issues as they are just beginning to happen can greatly reduce the frustration and heartache you're bound to experience at some point if you continue using a computer or hard drive that is failing.

Computers and hard drives today are remarkably quiet, so if yours is making noise, it's a sign of trouble. If the sound is from your case fan, replace it, because a case fan that's not working can cause many other issues, including ruining other parts and possibly damaging your hard drive if your computer overheats. The only other thing in your computer that could be making noise (besides your CD/DVD drive) is your hard drive, and if your hard drive starts making strange noises, you need to act quickly. Don't put it off. A web search will turn up lots of audio and video of failing hard drives, and I would urge you to become familiar with them so that you can recognize signs of trouble in your drives.

#### What Can Go Wrong, and Why

Data recovery situations will fall into five broad categories: either the problem will be with hardware your computer is connected to, the problem will be with the operating system files that normally run your computer, you have some sort of hardware failure with your hard drive, you have a *software* issue with the file or partition structure, or you're looking for accidentally deleted files. There is nothing else it could be, although sometimes you could be seeing more than one issue, such as when a hardware failure causes software corruption. Your quest in data recovery situations is going to be to categorize your problem in one of these areas because your priorities and methods of recovery will differ.

In most potential *data recovery* situations, the problem will actually be with something that isn't the hard drive, or is just a corruption of the operating system files, and that is usually the best outcome you could hope for. Your data (ESPECIALLY if there's no backup copy) if usually worth far more than whatever piece of failed hardware or corrupted operating system it's plugged into. If your external hard drive (or phone) has failed, try opening the case to reach the actual hard drive inside. Unless you're looking for accidentally deleted files, you're not going to know what you're facing until you power up the drive, and when you power up the drive, the clock could be ticking on your chances to easily recover the data you seek. Be ready to do a complete data recovery on the drive when you plug it in the first time, even if you only suspect a failed power supply or a fouled-up operating system.

If you're after accidentally deleted files, stop using the computer until you're ready to do a full data recovery because continuing to use the computer will greatly reduce your chances of



Figure 1. Anatomy of a Hard Drive

recovering your files. However, if you stop using your computer immediately, your chances of recovering all your accidentally deleted files are excellent. If you have used the computer for a while after deleting the needed files, you might not find EVE-RYTHING you're looking for, but it is still worth an attempt. I have found files deleted years earlier by clients during a data recovery, and since this data recovery scenario does not often involve a hard drive with any software or hardware issues, recovery should go quickly. The only way to recover accidentally deleted files is low-level data recovery, so feel free to skip ahead in the article to the section covering that technique if you're looking for accidentally deleted files. Much of this article is devoted to diagnosing corrupted, failing or failed hard drives, and that probably won't apply to you if you're just looking for accidentally deleted files (or an accidentally deleted partition).

Data recovery and computer forensics share many techniques, and you will probably be shocked at how much data you will actually find on a hard drive if you have never done data recovery before. In fact, I try to always tell my clients who are married and share a computer that if they are keeping secrets from one another on the computer (be it a secret lover, porn, gambling, etc.), the process of data recovery might bring that to light. Anyway, data recovery often involves a drive that has serious issues. In computer forensics, someone might be trying to hide files and data from you, but at least the drive works! If your drive has hardware issues, it will add to the time it will take to do any sort of data recovery, and that will add to your frustration. If you're in a data recovery situation and your hard drive is not displaying signs of hardware failure, consider yourself lucky because things will go much more quickly. Doing data recovery on a large drive with many bad sectors might take more than a week to perform ONE data recovery pass of the drive.

Let's be completely honest: hardware issues with your hard drive are evil. Do whatever you can to avoid them. Don't subject your hard drives to any sort of shock, especially while they're turned on, and if you suspect any hardware issues may be occurring with your hard drive, replace it immediately. Hardware issues can also masquerade as something else, such as a virus or spyware infection that you just can't seem to remove because the computer will take a while to boot, be slow during use, and even stop working all together. For this reason, I always consider a reported virus or spyware infection a potential data recovery situation where the hard drive hardware is failing.

Let's quickly take a look at the anatomy of a traditional hard drive (see Figure 1). There are only a few major parts, and despite the difference in size, a desktop-sized drive and a laptop-sized drive are almost identical inside. The power and data cables of the computer plug into the printed circuit board of the drive, which is connected to the spindle motor and actuator arm inside the drive body. The spindle motor turns a set of ceramic or glass platters (yes, they are fragile!) that can store electrical charges, which are attached to the axle of the spindle motor. Read-write heads on the actuator arm move back-and-forth across the surface of the platters, close enough to read and set the electrical charges on the platters, but not touching them. This is so close that specks of dust cannot pass between the platters and read-write heads. The concept of a cylinder comes from the area the multiple read-write heads can access at one time, since the read-write heads are also stacked so that they can access both sides of each platter in the drive (Figure 1).



Figure 2. Using a Forensics Write Blocker for Safety

Everything has a limited working life, and hard drives are no different, especially with their moving parts and microscopic tolerances. Remember, *hardware issues with your hard drive are evil.* If you do suspect hardware failure in your drive (drive noises, drive disappearing from operating system, drive freezes during use, lots of bad sectors appearing), you need to get your data off of it as quickly as possible without taxing the drive excessively unless you're prepared to spend two thousand dollars (\$US) or more to recover your drive's data.... maybe. The hardware issues could be ruining your drive further every second you use it, as the read-write heads could be gouging the platters, for example.

If sending your drive to be repaired in a cleanroom environment is within your price range, stop using the drive entirely and ship it off, although there is still no guarantee your data will be recovered. There are not many companies that provide this difficult and technical service, but DriveSavers (800-440-1904 / DriveSaversDataRecovery.com) and Silicon Forensics (714-680-3188 / SiliconForensics.com) are two companies in the US that have excellent reputations. The drive platter itself where the actual data is stored could be damaged (broken or scratched), rather than one of the mechanisms that simply accesses the data within the drive. However, if your spindle bearings are burned out, physical repair is your only option since the seized bearings won't allow the platters to turn in order to read the data off them.

If you even *suspect* you have a hardware failure occurring with your drive, but aren't going to have it rebuilt in a cleanroom environment, don't power up the computer or hard drive unless you have at least enough storage space on another attached drive to hold a full copy of the data you care about. You power up the drive, and the clock could be counting the final seconds of that drive's useful life. Have a plan about what data is the most valuable, and try to recover that data from the drive first when you do finally power it up.

#### **Assemble Your Tools**

Ideally, have another working computer to perform the data recovery with that has a RAID hard drive array with enough free space to hold two or three complete copies of the EN-TIRE hard drive that holds the data you're seeking, at least one more working hard drive at least as big as your damaged one, a forensic write blocker (see Figure 2), at least one data recovery program, at least one program of hard drive utilities, at least one drive cloning utility, and then use a battery backup to add an extra layer of protection from power outages and surges while you're performing your hard drive analysis and/ or data recovery (Figure 2).

Why RAID? It allows you to effectively make two copies of the data off your crashed hard drive at the same time. Why so much free space? If you have to do low-level data recovery, you're going to have lots and lots of files to save, and you're probably going to want to do several low-level passes to make sure you find the files you're after. Why the forensics write blocker? Your computer can write to the drive in the



Figure 3. Prosoft Engineering Data Rescue for Mac's Quick Scan Interface

background, which could overwrite the files you're seeking, so the forensics write blocker ensures your computer only writes to the drive when you're meaning to. What software will you need? The one that fixes your problem or finds your files, of course! Like virus removal, if the first tool you try doesn't work, just keep trying other tools until you find one that works.

Realistically, you're probably not going to have the superdeluxe data recovery setup, but having the right tools for the iob will give you the best chance of recovering what you seek. There are two things you absolutely need: a working hard drive with as much storage space as possible - ideally at least TWICE the total size of the drive you're recovering data off of, and three or even four times the size of the failed drive would be better (yes, this means you want a 3TB drive to recover a 1TB failed drive) -- and a way to run an operating system without using the files on the drive you're doing the data recovery from. If you don't have another computer to plug the drive into, that means you're going to need a live CD to boot an operating system into memory while you perform the data recovery because it's simply impractical to do data recovery on the drive that is running your operating system, and you would be reducing your chances of recovering your data to do so anyway.

Many Linux distros, data recovery and file utility programs are design to be used as live CDs, but most of the time, I pull the hard drive out of the host computer and install it as a slave drive in another computer for data recovery and analysis. As I mentioned before, most *data recovery* situations are actually failures of something else in the computer, and using a live CD, you are not going to be able to effectively diagnose these types of problems, but they are handy at times, and sometimes they are all you have available. Using a live CD will also likely take longer than data recovery and analysis running from another computer, but it will work if you have patience.

#### Make a Plan

In short, know what you're looking for. *Everything* isn't a good answer here. Surely, you're going to care about some of your data more than others – are your family pictures more important than your media library? Probably! But is your email more important that your client files, and is your contacts list more important than your accounting files? That is for you to decide. Write out all the things you're trying to find, where those files and folders are in the file structure (often this is your *My Documents* folder), what types of files they are (.DOC, .JPG, .MP3, etc.), and prioritize those files so that you save the most important things first if you have the chance.

Let's take a second to review things before we power up the crashed hard drive for the first time in a data recovery situation. Hardware failures in your hard drive are going to be very difficult to overcome and you may only have minutes before your hard drive fails completely, so you want to be prepared for the worst when you plug it in the first time after you realize you might be in a data recovery situation. Luckily, hard drives often show signs of failing for a time before they fail altogether unless they've suffered a serious hardware failure, such as seized spindle bearings or broken platters. You have enough storage space available to hold all the files you seek, and you have prioritized those files so you can immediately retrieve your most important files first and then move onto files of lesser importance if your drive continues operating.

Recover My	/ Files Wizard	
æ	What would you like to do?	
E	Fast File Search	Search for: • Becently deleted files
	Complete File Search	Recently deleted files     Recently deleted folders     Temporary files     Full cluster level search     of hard drive (Lost files)
OVG	Fast Format Recover	This search will take longer than a "Fast Search" however, it will potentially recover more files.
Reg	Complete Format Recover	Manually Set Options
	For support visit us at: <u>http://support.getdata.com</u>	
Show Wi	izard on Startup	Back Next > Cancel

Figure 4. GetData Recover My Files for Windows' Complete Scan Interface

🐨 Recover My Files - (Registered to Ken Krauss)					
Eile <u>R</u> ecover <u>H</u> elp					
Start Search 🎒 Save Files 🗸 🌱 Filter 🕅 Op	tions. 🕜 Help 🍖 Update				
File Type View Folder View	Name	Size	Туре	Recovery	Folder
	MFT 51427     MFT 51427     MFT 51429     MFT 51429     MFT 51429     MOT2331.ini     CLSIDs.sbs     A0072331.ini     CLSIDs.sbs     A0073806.ini     A0074046.dll     CLSP.sbs     MN17AG10CZ01137wav     MN17AG10CZ01171wav     NM17AG10CZ01173wav     MN17AG10CZ01173wav     MN17AG10CZ01173wav	1 KB 1 KB 6 KB 11 KB 546 KB 11 KB 468 KB 2010 KB 5 KB 31 KB 31 KB 27 KB 49 KB 34 KB	wav res ini sbs ini chm dll sbs wav wav wav wav wav wav wav	Very Good Very Good Overwritten Very Good Overwritten Medium Very Good Very Good Very Good Very Good Overwritten Overwritten	E:\Lost Files\ E:\Lost Files\ E:\[00051172]\hel01\ E:\[00050386]\ E:\[00009899]\ E:\Program Files\Spybot - Se E:\System Volume Informatio E:\Program Files\Spybot - Se E:\[System Volume Informatio E:\Program Files\Spybot - Se E:\[00043897]\m17ag\10cz( E:\[00043897]\m17ag\10cz( E:\[00043897]\m17ag\10cz( E:\[00043897]\m17ag\10cz(
	MM17AGGRIFU3012wav	44 KB 43 KB	wav wav	Overwritten	E:\{00043897}\m17ag\gnr03 E:\{00043897}\m17ag\10cz(
					2
Preview Event Log					
Property Value					
Filter OFF Found: 37222 Selected iter	ns: 326 (45.2 MB)				ii:

Figure 5. GetData Recover My Files for Windows' Found Files Interface

di l	What file types would you like to recover? (tick a box)	
	Encapositional Concomprime ( . ope)	~
5	FormZ Document (.fmz.fzb)	_
	— 🔲 🔬 Freehand 10 (fh10fh11)	
	- 🖂 🧕 Freehand 7 to 9 ( .fh7 .fh8 .fh9)	
	📄 🔄 🧕 Fuji Camera Raw (.raf)	
	🛛 🖳 📃 🧃 GIF graphics file ( .gif)	
	🚽 🔲 🍲 GIS ShapeFiles ( .shp)	
	GUE Map file (.gue.gmp)	
0	IPEG 2000 ( .pz)	
3	- V 🖬 JPEG Standard Graphics file (JEE format) ( ing ing	
UT:	- I is Lightwave object ( .lwo)	
2	🗌 🧱 Lightwave scene ( .lws)	3
allow P.		×

Figure 6. GetData Recover My Files for Windows' File-Types-to-Recover Interface

#### Power Up Your Crashed Drive – Work Your Plan

Time to begin the process of analyzing your crashed hard drive! Turn on your computer that has the crashed drive installed as a slave drive, or boot your computer up with a live CD. When the operating system has finished loading, look to see if you can browse your *crashed* hard drive (or the hard drive out of your non-working computer) normally using the File Explorer (Windows) or Finder (Mac). If you see your hard drive files and you don't suspect hard drive hardware failure, your data recovery is complete! Go ahead and make backup copies of your important data to be safe, but often as a system admin or computer tech diagnosing computer issues, trying to access hard drive data will be your initial step in diagnosing a non-working computer. If you find a hard drive working perfectly, you can check things like the memory, motherboard, and processor for failure.

If you are able to see your files on the crashed drive, but you do suspect hardware failure in the drive, start copying your important files to the recovery drive you're using to save the recovered files. Copy what's most important to you first, and allow the copy process to complete before starting to copy other files. Starting multiple simultaneous file copy processes will tax the drive more than a single file copy process at a time, and if you suspect hardware issues with your drive, you don't want to tax it anymore than necessary. Multiple simultaneous file copy processes will also take longer than a series of individual file copy processes, so just be patient and copy one chunk of files and/or folders at a time.

If your drive drops out while copying, you're going to have to figure out what files it had and hadn't copied when (if?) you get it back up and recognized by the operating system. Copy your most important files first, let that process complete, then copy your next most important files, let that complete, etc. until you have copied all your files, or until your drive is dropped by the operating system. If that happens, your best bet is to try to reboot, and keep your fingers crossed that your drive comes up again, or replace the printed circuit board on the bottom of the drive where the power and data cables connect to the drive. Again, using a drive with failing hardware could do even more damage to the drive, but I have recovered lots of data this way, and it is much easier and cheaper than sending the drive off to be rebuilt in a cleanroom.

A good practice is to do a bit-by-bit clone of a drive before beginning a data recovery, however at this point in the process, we're still analyzing the drive to see how bad the issue is, using the process of copying your most important data to



*Figure 7.* GetData Recover My Files for Windows' Deleted Partition Interface

determine how serious your drive's issues are. If your hard drive is showing signs of hardware failure, I feel that getting your most important data is often more important than making a complete backup copy of the drive at this point. After retrieving your most important data, if your drive is still working, you can make a complete copy then while knowing you already have your most important files. Again, this is a judgment call, but I feel if you have a chance to copy your most important data, take it.

If what you consider the most important data on the drive is a large portion of the overall drive space, or if your drive is not showing any signs of hardware failure, or if your data is extremely valuable to you, you might want to make a bit-by-bit clone of the drive now and do the data recovery on the cloned drive so that you have the original drive as backup. You might also be using a forensics write blocker in between your computer and the drive you are trying to recover data off of so that no data is changed on your hard drive without your meaning to make those changes, because your important data might be overwritten if this happens.

If your drive does not have any type of hardware failure, you can make all the copies of the drive, or data recovery passes, as you like. As long as you don't actually write to the drive or change its contents in another way (such as Windows Disk Check – remember I recommend a forensics write blocker to keep this from happening), your drive issues should not get worse. If drive issues do get worse, this is a sign of hardware failure.

#### Where Did My Files Go?

If your hard drive's file system is not recognized by the operating system but it does see the drive attached in Windows' Device Manager, or in System Profiler or Drive Utility (Mac), or if you've accidentally deleted files or an entire drive partition, this is where the real data recovery begins. Take heart though, because in my decade of running a tech service, I have only seen a few drives that were damaged bad enough not to be able to recover all or a majority of the data off them using the techniques in this article, and those drives suffered serious abuse. Again, proper care of your hard drive is extremely important in keeping yourself out of data recovery situations! And you're only going to be in a data recovery situation if you haven't been backing up your important data, so please do that regularly, and you'll rarely, if ever, get caught in a data recovery situation!

You might imagine your hard drive structure as a huge wall of mailboxes, and initially, all the mailbox doors are open. As data is saved, those mailboxes are filled and the mailbox doors are closed to signify that they are storing something important (your files). When you delete a file, all that happens is the computer opens the *door* on the *mailbox* that held your file, signifying that that space can be used again to store something else, but the data remains in the mailbox until it is used again to store another file. This is why accidentally deleted files, or an accidentally deleted partition, have very high rates of successful recovery when you stop using your computer, laptop, tablet, camera, phone, or other device as soon as you realize you have accidentally deleted something. In a similar vein, secure delete programs go through all the data compartments on your hard drive and replace the data compartments with all zeros or random data. If you have used a secure delete program, you have little chance of recovering your data, unless you are able to stop it from completing.

The issues that could cause your files or file system to be unreadable by the operating system are really too numerous to mention but your issues could stem originally from power surges, power drops, or complete power loss while your computer is operating, particularly while writing data; failure of another computer component; shocks to the drive while it is writing data; a virus or other malware corrupting the drive's Master Boot Record (MBR) while trying to install a rootkit; some sort of error while using a hard drive utility such as file defragmentation or repartitioning; disconnecting your drive from the operating system without properly ejecting it first; failed operating system update; computer overheating; weak charge in certain file sectors; corrupted partition table or file chain; scratches on physical media such as CDs or DVDs; and damage to the drive heads and/or drive platters.

#### Three Types of Data Recovery vs. Fixing the Drive's Issues

No matter what type of file system is on your crashed drive, the types of data recovery you do is going to break down into a few main types. Primarily, low-level data recovery focuses on the file structure, or it focuses on the file contents. The trade-off between these two types of data recovery is that the type of data recovery that focuses on the file structure, normally termed a quick scan (see Figure 3 for Prosoft Engineering Data Rescue for Mac's Quick Scan interface), is usually going to preserve chunks of your folder structure and file names, but not as reliably the file contents, while the type of data recovery that focuses on the file contents, normally termed thorough scan or complete scan (see Figure 4 for GetData Recover My Files for Windows' Complete Scan interface), will be your best bet for finding the intact files you desire, however there is going to be no file names or folder structure to help you - you literally have the needle-in-a-haystack task of looking through the thousands, or hundreds of thousands, of un-named files the process will find on your drive in order to find your important data (Figure 3) (Figure 4).

Nearly all data recovery software products on the market today include both of these types of scans, and I recommend doing both types as a habit if you have space on the drive you're using to save your recovered data. It is hard to know sometimes if you have truly recovered everything you're looking for, and doing both types of data recovery initially might save you time and effort down the road if you realize some data is missing (see Figure 5 for GetData Recovery My Files for Windows' found files interface). Also, specifying fewer types of files to recover is another technique that may recover more of your data if your first pass wasn't as successful as you had hoped (see Figure 6 for GetData Recovery My Files for Windows' file chooser interface) (Figure 5) (Figure 6).

Data recovery programs often have scans that look for deleted files, and these are actually similar techniques as the *quick scan* and *complete scan* just discussed, but applied only to the empty space on your drive rather than the entire hard drive. Because an un-delete scan will cover less area and require less time than a full scan, start here if you are looking for accidentally deleted files (see Figure 7 for GetData Recovery My Files for Windows' deleted partition interface). If you're looking for an accidentally deleted partition, or if your un-delete scan didn't find your files, do a complete scan (Figure 7).

The third type of data recovery you may need focuses on amplifying the charge of the storage medium, such as old floppy disks or old memory cards that have lost their charge, or reading from scratched CDs or DVDs by averaging out the data retrieved from multiple passes over the drive. Jufsoft's BadCopy Pro is an example of this type of data recovery program. Often, this type of data recovery will work when other methods of data recovery fail, given a drive or disk with no other hardware issues. Some data recovery or forensic analysis programs will allow you to actually see the hexidecimal data on the drive, so that you can spot and correct errors, but this is a very advanced technique.

In a data recovery scenario, you might have the option of fixing the issues with the hard drive's software structure if a corrupted software structure is what is causing the issues with the drive. This is an excellent method of data recovery in my opinion, because it is relatively quick and you're recovering the entire drive including the file names and file structure (see Figure 8 for Alsoft DiskWarrior for Mac's interface). In my experience, many, even most, issues can be fixed with hard drive utilities, so be very thorough with them. You might even try putting your drive into another type of operating system as some issues will seem to disappear by doing so. Macs can read Windows FAT32 volumes natively and Windows NTFS volumes using MacFuse and NTFS-3G, while Linux can read Windows and Mac volumes natively (Figure 8).

If your hard drive hardware is failing, trying to fix software issues on the drive will not really help you and could actually hurt you because you could be using the last precious moments your drive is still operating without using them to save as much of your important data as possible. Also, performing software fixes to the drive will change the hard drive's contents, which could overwrite your important data if you haven't already saved it. Perform any low-level data recovery BE-FORE you attempt software fixes if you're working on your only copy of the hard drive (remember I suggested cloning the drive if possible before beginning the data recovery process).

#### **Replacing the Printed Circuit Board**

Replacing the printed circuit board (PCB) of your failed or crashed drive is actually pretty easy to do and will solve a sig-

000	🖋 Alsoft DiskWarrior
W	Directory Hardware
Please ch	oose a disk from the popup menu below and then click the Rebuild button to rebuild the directory.
Mac HD	•
Director	y cannot be rebuilt because this is the startup disk. y cannot be rebuilt, DiskWarrior resides on this disk. • This disk is a Pure Mac OS Extended disk. • This disk does appear on the desktop. • This disk is 931.39 GB in size.
	<ul> <li>Advanced</li> <li>Device ID: disk0s10</li> <li>Sectors: 1,953,261,184</li> <li>Sector Size: 512 Bytes</li> <li>File System Type: HFS (Extended, No wrapper)</li> <li>Model: SAMSUNG HD103UJ</li> </ul>
	Graph Rebuild

Figure 8. Alsoft DiskWarrior for Mac Main Interface

nificant amount of drive hardware failure where you don't have bad sectors appearing and your drive isn't making strange noises such as buzzing, grinding, or clicking. If your drive has a bad PCB, the operating system might not see the hard drive, or it may disappear from the operating system while in use. If your operating system can see the drive, but cannot access any data, you probably have some sort of issue with the spindle motor and/or bearings, and sending the drive off to be rebuilt in a cleanroom is the only chance you have to recover your data.

In order to replace the PCB, you will need an identical hard drive (same manufacturer, model, size, and version) to remove the new PCB from. There are a few screws holding the PCB in place on the bottom of the drive which you will need to unscrew. After removing those screws, gently separate the PCB from the hard drive body (see Figure 9). There may be a foam pad with adhesive between the PCB and hard drive body that might make this process difficult, so work slowly and gently so that you don't bend or break the PCB. Repeat this process on your damaged drive, then reverse the process to put the working PCB on the hard drive body that holds your data. If you can't find an identical hard drive to take a working PCB from, and you have exhausted all your other options, try to find a drive that's close to your failed drive. Something from the same line of hard drives from the same manufacturer might work. You may damage your drive if you try, but if you have no other options, it won't really matter if you turn your drive into a doorstop (it's already a doorstop, isn't it?), and who knows - you might get lucky. What absolutely needs to happen is for the contact points on both the data transfer unit and the spindle motor to line up properly with the appropriate contacts on the PCB (Figure 9).

#### **Summary**

Hopefully, this article has taught you something about data recovery, and maybe even helped you through your first data recovery process. Data recovery is very gratifying for me, as I am often able to help people find precious memories and important files they are desperate to retrieve. Working with technology is often a thankless job, but recovering valuable data will be rewarded with lots of appreciation.

Now, go burn another backup DVD of your data, just for more insurance against file loss! I know there is probably *something* you'd lose if your hard drive failed today... Burn that to DVD right now! My heart skips a beat every time I get a frantic phone call from clients whose hard drives failed without any backups. If you are in a data recovery situation, I know that panic, and I hope I have provided enough insight in this article to help you through it successfully!

#### **KEN KRAUSS**

is a computer security consultant, network administrator, and web developer living in Kansas City, Missouri, USA. He holds many certifications including ISC<sup>2</sup> Certified Information Systems Security Professional (CISSP); CIW Security Analyst; and CompTIA Security+, Network+, and A+. He has helped everyone from home users to large

companies with their technology challenges through his businesses Computer Help Personalized (CHPKC.net), Kansas City Web Development (KCWebDev.com), and Vertical Data Recovery (VerticalDR. com). One of his current passion projects is a news, weather and traffic hyper-local website network. Visit InTownSF.com for more info.



Figure 9. Replacing a Hard Drive's Printed Circuit Board (PCB)



Szukaj nas takze na







www.ashampoo.com

# COMPUTER HARD DRIVE RECOVERY: TIPS, TRICKS AND SCAMS

#### **GORDON BELL**

Your computer contains very important files on it. Work files, personal documents, tax receipts and other files that would be hard to recreate. You probably also have thousands of digital pictures spanning the past 10 years or so, as society has moved away from film and towards all digital content. Losing all the pictures of your children or family events from the past years can be devastating to even think of. w

his article will give you information of what to do in case you have a computer emergency as well as details on some of the scams and dirty tricks that are out there in the wild. For the sake of this article, I will concentrate on two distinct, common computer problems: Logical and Physical hard drive failures.

**Logical Hard Drive Failure** occurs when your hard drive becomes corrupted by the operating system (over time) or by a virus. The directory on the hard drive is corrupted to the point where it locks up and you get a blue screen / grey screen upon start up or in the case of an external drive, it won't mount or

show up on the desktop. Physically the drive is still fine, but the drive directory is preventing you access to the data on the drive. In this case, recovery software can get beyond the directory issues and allow you to recover any and possibly all files over to a second hard drive. It is never recommended to perform a "software repair" to the hard drive in question as that may cause additional damage to the drive data and overwrite important files during the repair attempt.

If your main hard drive is corrupted, you will need a recovery software tool that can boot up your computer (look for software that includes a bootable CD or DVD). These types of products save you from the need to remove the hard drive or hook the computer up to an-



other computer for the recovery process. Look for companies that offer free demos to try-before-you-buy to ensure that the software is able to see the hard drive, allows a full scan and shows you all the files that are recoverable.

If the corrupted hard drive is an external drive, you can simply run recovery software on your computer to scan that bad hard drive. Most well-known recovery software will allow you to demo the software to make sure it can "see" the bad hard drive. If one piece of software cannot see the drive, don't give up hope, try another product... One good way to qualify a company is to check out their "About Us" page on their

> website. A good company will give you details of who they are, including their street address and phone numbers. By giving that info out, the company is automatically connected to their customers in a closer relationship, so they have to work hard to make the product top-quality. For other companies that only give you an email address or support form to fill out, they are more insulated from the customers and may use that to avoid issues and problems should they arise for their customers. Remember, it only take a few dollars to make a website and charge your credit card. Make sure the company behind the website is indeed a legitimate company. Many new "companies" come onto the marketplace with great looking websites and tons of award logos and reviews from the top magazines. Upon further investigation, these award



logos and reviews are all fake, taken and added to a company's website to fool the public. The companies are based in countries where a lawsuit (from the magazines) would never take place, and therefore the magazines are helpless in trying to get the companies to remove the fake reviews and stolen award logos. Even if a company claims they have a Satisfaction Guarantee or Money-Back guarantee, that too might be a lie, only found out after you purchase and try to get your money back. The key is to do some research and make sure the company is legitimate. Also realize that there are many brand new "review" websites created each day online, many of which are paid-affiliates, getting a cut of the purchase after you read their "reviews". Knowing this, you may be able to picture how certain bad products have lots of glowing reviews online (the reviewers are many times part of an elaborate team of affiliates or employees, all with the same goal of promoting a product they may be making a commission on).

If your hard drive is still not seen by software, a good trick to try is putting into a different enclosure. It might cost you \$20-\$50 for a new enclosure, but by trying that first, you can save yourself from an expensive physical recovery if it's not necessary.

**Physical Hard Drive Failure** occurs when one of the mechanisms inside of your hard drive breaks or fails. Realizing that your hard drive is spinning around inside at speeds of up to 10,000 rotations per minute (even faster in some top-speed drives), you can imagine that something might go wrong at some point in time, especially when they are trying to cut costs for producing these hard drives. Once you've determined that your hard drive is suffering from a physical issue, you need to take time to find a computer recovery service that you can trust with your data. Employee background checks, secure storage of your hard drive, a certified cleanroom and technical expertise are all needed to protect you from harm and provide the best chance at recovering the data

A physical hard drive recovery service is expensive. Think of them as brain surgeons for your computer. Yes, if you scratch your arm, you mom can easily clean you up and throw on a band-aid, but if you need brain surgery, you can't trust your mom to do the job. The same is true for physical hard drive recovery. You can't go to an all-around computer store to get this done. Likewise, you can't trust your IT uncle or Geek friend to do it either. Physical computer recovery requires specific tools, costing \$15,000 and up, as well as a cleanroom and years of daily recovery experience. Your IT uncle or geek friend just doesn't have the tools, facilities or technical experience to perform this type of work. In fact, if you let them try, they will almost surely cause more damage to the drive, making the professional's job even harder (as in more expensive for you). You wouldn't trust your mom to perform brain surgery on you so don't trust non-professionals to check out your hard drive.

What to be weary of for hard drive recovery services: Low-Cost / Maximum Cost Guarantees: Any company that promises you a "Guaranteed" cost of \$399 or \$499 without ever seeing your drive. That will not get you physical recovery. When they claim that, they are hoping you send the hard drive in without trying a software solution yourself. If they get the job and the software solution works, they can charge you that amount. If the recovery does indeed require physical recovery work, they can try to re-quote you or send it back and say they weren't able to recover it. You may want to check to see what their return shipping costs are, to make sure they aren't trying to make money off of that as well. They might also contact you and say that "they" can't get the data back for you (at that guaranteed low cost), but they can pass the drive onto

switch technique to be careful of. **Cleanroom or Kindacleanroom:** Make sure the company has a cleanroom—Sure, they may say they do on their website, but we all know the web really isn't policed. If they have a cleanroom, they would be proud of it and show it off with a picture or two on their website. If someone opens your hard drive in a non-cleanroom environment, your drive will likely suffer damage that will either make the data unrecoverable (due to scoring caused by particles) or will make it more difficult and more expensive for the eventual recovery. Do not trust that they have a cleanroom just because they say they do, require some proof.

a partner who can (no guaranteed cost). It's the old bait-and-

Uncle Leo and His Bag-o-Tricks: Everyone has a friend or family member that is always looking for outlandish ways to deal with a problem. Of course you want to find a no-cost solution to the problem, and if that solution happens to be some weird, unknown remedy, it'll make you feel even more proud knowing you used some low-tech trick many others might not know about.

One of the most common tricks you'll find mentioned when it comes to hard drive problems is the old stick-it-in-the-freezer trick. This is attempting to deal with a problematic electronics board, which over time has expanded ever so slightly to the point where certain connections on the PCB are no longer





engaging correctly. The act of freezing the drive seeks to shrink that PCB board back into a state where the connections are valid again, allowing the drive to function. The problem with this trick is that is can many times lead to irreparable harm to the drive. That is, if there is any moisture in the drive, that moisture will freeze into ice, and you are now dealing with ice on the platter. Also, even if you're lucky and the drive has no moisture present inside, the drive will indeed warm back up while it is spinning (as you're working with it to get the data from it), so the PCB will expand again and the drive will fail again. The other main problem with this so-called remedy is that as dangerous to the data as it is, it is only trying to remedy one distinct physical issue with a drive, and your drive may not be suffering from that issue. It would be akin to taking a potentially lethal pharmaceutical drug to try and cure you of liver cancer, but you had not yet determined if you had cancer of the liver, or cancer at all, you just knew you were sick. Such a drastic, risky trick should never be attempted with any important data. Always assume the trick will likely not work and the data will also be destroyed. If you are ok with that possibility, then it could be a last-ditch-effort for some data that is not really that important to you.

Another trick is to try and drop the hard drive or jerk the hard drive to get it to begin functioning again. This trick is attempting to deal with Head Stiction, which occurs when the drive heads have attached to the platters outside of their landing areas. The goal is to jerk them back into place via this physical impact or jolt. This really is a carnival-game-of-chance which usually results in severe platter scoring (surface damage to the platters) or spindle failure. Both of these failure scenarios would typically lead to higher recovery costs and also lower your chance at data recovery.

Virtual Recovery Shops: Make sure the company actually exists and does the work themselves. Many people are setting up websites with great stock photos, industry keywords and a phone number or email address. They get you to send the drive to them but in reality they don't do any of the work themselves. What they will do is send your drive to a few shops, seeking out the best price. Then they contact you back and give you an inflated price. If the shop can do it for \$1000, they might contact you and say it's \$3000... You might say you can't afford that, but you then negotiate down to \$2000, thinking you're getting a great deal. In reality, you just paid double what it would've cost you if you contacted the legit place by yourself.

**Trustworthy/Background Checks:** The last thing you want to do is send your computer hard drive to someone you can't trust. Personal photos, banking information and other personal data should be entrusted only to a professional company. You don't want your personal pictures posted online or your financial information rifled through. Make sure all their employees undergo a background check and make sure the company itself has a good standing with a service like the Better Business Bureau or similar consumer protection agency. You can also ask the recovery company to provide you with a signed Non-Disclosure Agreement (NDA) to further protect your data from being exposed in any way.

#### Scams and Dirty Tricks:

One of the worst things seen in the computer recovery industry is the outright scams and dirty tricks that are prevalent.

Lock Your Drive: You send your drive off to a company and they quote you \$2000.. Yikes, that's a lot, so you send it to a few other companies, but the other companies say they can't get any data from the drive no matter what the cost. Ok, the original company, although expensive, must be good, since they're the only ones that are able to get any data for you. It's expensive but seemingly the only option. What may have happened, and it happens every day, is that original shop may have locked your drive with a password. Only they know what that password is now, so anyone else looking at it might not have access to the data... So they've in essence locked you into their service and their price—You have no other option.. Dirty....

Clone Then Ruin Your Drive: A similar dirty trick is where a company may get your drive and then quote you say, \$3000. Of course you say no to that and want them to send it back to you. In the meantime, they've already cloned the drive, so they have a good copy of the data on something back in their lab. They will then physically damage your drive in what looks like a naturally occurring way, which makes the data unrecoverable. So you get your drive back and send it to other shops... The other shops will look at the damage (which looks all legit) and tell you that they can't get anything from a drive in that condition. Once again, the first company looks like a hero, being able to recover data from a drive that no one else can... So you send the drive back to them, which they receive, and they get the data from that clone they have. You walk away thinking, "Wow, that company was expensive, but they sure are great, they got it back when everyone else said it was impossible!"

**Punishment for shopping price:** Another dirty trick is where you send your drive to a company and they quote you.



150 5

CLEANROOM

ACCREDITED

BUSINESS



The pricing is high, so you want to shop it around. They return the drive to you and you send it out to a few other shops, getting quotes. I turns out that the first place was the best price,

so you go back to them. However, they now tell you that "your drive has been opened in an unclean environment, which has contaminated the platter and now it's going to cost another \$1000 on top of that original quote". Wow, now you're mad at the other companies, since one of them must've opened your drive in a dirty environment and now it's gonna cost you even more to get your data back! In reality, the original company might be scamming you. They will in essence punish you for shopping the drive around, and in the meantime, they will use this as a way to ruin the reputation of the other service companies you sent your drive to. We have seen this happen before and did an experiment to prove what was going on. We knew about this scam being used by a very large recovery house here

in the U.S. We had someone pose as a customer send a drive to that service shop. They quoted the recovery and the fake customer asked to have his drive returned, since he couldn't afford the amount. When the drive was received back from that



original service shop, the fake customer just let the drive sit in his office.. About a month later, we had him put some stickers from our company onto the outside case of his hard drive (non-tamper stickers usually affixed to a drive after servicing or inspection). Note, the customer never opened up his hard drive, and he never sent it to us to open up. He simply



took a few stickers and stuck them to the outside of the drive. He then sent the drive back to the original company. They received it and saw those stickers and assumed "oh, he sent it to someone else to get a quote."- That original company then contacted the fake customer and told him, "your drive has been opened in an unclean environment, which has con-

> taminated the platter and now it's going to cost another \$1000 on top of that original quote." ---- That's right, they assumed his drive was sent off to a competing company (heck, the evidence was there because those stickers were there, right?). They tried to make the second company look bad, but in reality it exposed that they were indeed performing this scam.

#### Conclusion

As a computer user, you are likely never really worrying about your important computer files like digital photos and videos, financial documents and digital music files. Yes, there are backup solutions readily available for a low cost, but most of us seem too busy to take time to ensure we're protected. For that reason, many computer

users find themselves panicking once a computer crash occurs. It is during this crisis that you must take time out to investigate your possible solutions and then find a truly trustworthy company to work with. Simply searching the web for positive reviews or "customer" recommendations is no longer a reliable way as this is being abused by fake review sites and paid-for customer review postings. A great way to find out more about a company is to use the old-fashioned telephone communication model. Call up the company and talk to them, hear what they have to say and ask many questions. Ask them to call you back and see if they do. Do they respond to you in a manner that satisfies your needs as a potential customer? If not, then they are likely to fail you even if you become a paying customer. Take time now to backup your computer files as that provides you with a great defense to avoid having to use a computer recovery service in the first place.

#### **GORDON BELL**

is President of The Data Rescue Center, a computer recovery service founded by Prosoft Engineering. The Data Rescue Center was founded with the express goal of providing professional-level hard drive recovery options with no-nonsense pricing and honest policies. Gordon has over 18 years experience in sales and marketing for high-tech firms in the California Bay Area. In his spare time Gordon enjoys playing basketball and golf, visiting the Napa wine country with his wife Jennifer and spending time with their two young children.

## Hakin9 EXTRA

# **INTERVIEW** WITH DMITRY KISSELEV

## Hi Dmitry, thank you for taking the time to answer a few questions.

I'm happy for the opportunity to help your readers learn more about data recovery trends.

You have a fairly vast background dealing with multiple different technologies and forms of data recovery, migration and discovery. One of your many achievements is a distributed cloud based disk diagnostic system. Can you tell me a little bit about this, how it works and what it offers?

In today's global demand for instant information, our business partners need a solution for advanced disk drive diagnostics that would not only provide them with the knowledge and expertise in the professional in-lab data recovery services field, but also have the ability to deploy the services in locations around the world. In order to address that need, we developed software which relies on the public cloud for its functionality, allowing us to deploy disk diagnostics abilities to our clients around the world. The proprietary system is currently being used by our business partners, enabling them to diagnose hard disk failure on site. in front of their endcustomers. The tool saves money, time and resources because it eliminates the need to ship every single data recovery case to be evaluated in our labs. Instead, the end-customer can remotely get a comprehensive diagnostic result of their hard disk drive on the spot.

#### What types of cloud storage environments you work with? On average how large are they? What's the most common way of distributing data in these large environments? What type of fault tolerance software do you deal with the most?

We have clients with data loss scenarios in both public and private cloud storage environments. We can't predict what environment we deal with each time. One thing for

sure is that there are several virtual storage technology vendors out there and we are ready to address them all. As a data storage manufacturer, we have access to proprietary technology and firmware that no other data recovery company out there has.

One observation is that we haven't seen a significant difference in the size of the data set stored in the cloud from an enterprise level. On the other hand, as one would suspect, consumers tend to store less data in the cloud, because most consumers just don't have the same amount of data as a business entity would. Unrelated to the size of the data set, the value attached to the data is what dictates whether a customer wants our services or not. I believe that consumer-oriented cloud recovery is just emerging. In most scenarios, a public storage infrastructure doesn't expose us to the level of physical storage access we need, so solutions are lim-



**DMITRY KISSELEV** has been at the forefront of the data recovery field since the late nineteen nineties. For the past several years, he has been leading Seagate Technology's data recovery research and development organization. He is a key contributor to the company's service portfolio growth. His dedication and knowledge of data recovery techniques built significant trust and reputation for Seagate among data recovery professionals around the world. Dmitry pioneered several innovative breakthroughs in data recovery methodology.

When not hacking into hard disk drives or storage devices, he enjoys hiking and takes part in "geocaching" activities in sunny California's Santa Cruz mountains with his daughter and dog. Dmitry holds a Master of Science degree in Computer Science from Ivanovskij Gosudarstvennyj Energeticeskij University in Russia. ited to what we can access in the virtualized storage view. As a result, we have a limited ability with performing data recovery in that instance. When dealing with private or hybrid clouds, we often have a much deeper access and work with the hardware. That ability allows us to provide a wider range of data recovery options to clients who experience data loss. Those type environments are usually based on virtualized storage solutions from VMware, Oracle, Microsoft, etc.

In regards to your line of work, how much different is cloud storage from any other large scale storage deployment? It is guite different. We are facing new challenges when working in these environments. In a public cloud storage setting, we face the issue of not having access underneath the virtual storage layers. That takes away options for recovering data related to physical storage failures. In the private cloud setting, we are dealing with additional layers of abstraction. Hypervisors and the like create storage containers which are often physically layered on top of distributed SAN and virtualized between multiple servers and applications. This set up creates a complex mesh of data. In order to successfully complete recovery in such an environment, we often need to reverse-engineer the complete path to the location between byte stored virtually by application to the physical byte location. It's a very tedious and complex job to do.

In a single hard disk drive data recovery scenario, we normally don't have those extra layers. The absence of these layers makes this type of data less complex compared to virtualized storage. In this environment, we rely on our robust years of experience and expertise dealing with data recovery from file system structures, a much easier vehicle to interpret how data was originally laid out.

Russia. In terms of data redundancy and reliability, what helpful pointers can you give someone to look for in a cloud storage provider? What security concerns should they be aware of?

Our experience shows that most of the data loss situations are preventable. Unfortunately, data redundancy and reliability play the last role in data loss prevention best practices. Quite often, users will leverage data redundancy and reliability as replacements for good backup. The majority of the data loss problems occur as a result of user error or the backup errors. Hardware failure is another cause. It's good to remember that real-time data between backup cycles can be lost due to physical failures. That is where the concept of fault tolerance and reliability plays out. Consequently, when you are choosing a cloud storage provider or solution, make sure that you think about disaster recovery and prevention and discuss this topic with your provider. Note also that a disaster recovery plan addresses not just redundancy or reliability but how the data will be retrieved when those options fail. And finally, a disaster recovery plan is only good if it is current and tested on a regular basis.

In the case of consumer applications, backing data up using services like Amazon S3 or Google storage in the cloud is good but also making sure that it is not the only place where data is stored keeps the integrity of the data seamless.Data loss also occurs due to security breaches. In the public/hybrid cloud environment, security becomes a major concern because the data is not in the user's physical possession. Be aware of the different legal implications of where data is stored as well. A physical data location is quite often an issue due to countries data privacy regulation. Pay attention to how data is secured on the cloud. Now think not just about your own system security but security of your data stored somewhere else. A good storage design integrated with information security experts and legal consultants can save many headaches in the future.

# You lead a team of data recovery engineers at Seagate, what are some of the current data recovery challenges you encounter?

Data recovery is challenging but rewarding. It's like solving a complex puzzle every time. No data recovery job is the same. People and companies have unique traits and so does their data and the way they store it. We face new challenges every single day. In the eyes of the customers, our engineers are heroes. Each customer has his or her own story and issue related to data loss, from drowning a laptop in the river to mistakenly swapping an incorrect drive in a SAN storage box. On top of that, the storage and computer industries are ever evolving with more innovation, bringing more and more complex challenges to keep us on our toes.

Today's hot topics are virtualization, solid state drives and mobile devices. We are dealing with new technologies used in the spinning magnetic disks, in RAID and by storage appliance manufactures as well as a slew of new storage applications.

#### There have been some papers published regarding data deletion concerns with SSDs. What is your opinion about this wear leveling issue with SSDs? How does your team handle recovery on SSDs? Is recovery on an SSD much different from a mechanical HDD?

SSD and data recovery from flash media are definitely hot topics today. Flash-based storage occupies segments of the storage market. We see anything from HDD, low / portable storage devices such as USB sticks, thumb drives, mobile devices to enterprise level low latency / high throughput storage. As we face new storage media, we have been able to create different solutions to recover the data of all types of customers. We are finding that flash media is not as reliable as disk drives and carry new properties that have not been seen before in disk drive designs. For example: to store data on the flash cell, designers have to take into consideration a variety of electric properties of the cell and how densely it can be packed. It requires new algorithms to be created in order to increase the reliability and lifespan of flash media. In addition, the ability to access data stored in flash in a non-sequential manner requires a new approach to storage, data retrieval and erasure. A lot of start-up companies have jumped into the flash storage market. I believe there are over 100-200 vendors in the SSD space compared to only a few HDD vendors. Each SSD company seems to bring their own design recipe. What looks like a competitive differentiator for these companies actually result in the fact that data and layouts are getting encrypted on the media for intellectual property (IP) protection. For us, as data recovery organization, even when we are able to read the data directly, if the flash crystal dies, we no longer are able to reproduce the original data due to encryption. In our research, we made some discoveries that are helping us overcome this challenge to provide solutions for our customers whose data is not encrypted by SSD or Flash storage controllers.

#### When dealing with magnetic platters, there are a handful of products that perform tasks like talking straight ATA, working with the system area, reverse reading, double check bits and such. Do you recommend any recovery products that can do whatever may be equivalent SSD for smaller shops?

The design of SSD drives brings a completely different set of properties that needs to be taken in consideration during the data recovery process. When a drive is physically functional, it is possible to use the same technology that is already available for mainstream HDD devices. It's a different story when a drive has a physical failure, something like a burned out Printed Circuit Board (PCB). A physical failure involves corruption in the system area. I'm afraid that as of today, data recovery tools available in the market don't offer solutions for modern SSD. A few options exist, taking the approach of rebuilding the translation tables and Error Correction Code (ECC) from images read from flash memory chips. Unfortunately, that approach is becoming quickly obsolete and no longer applies to modern SSD drives (e.g. based on SandForce or similar chipsets). The good news is, this technique is still applicable to the older generations of SSD and other flash storage media. We are seeing that several larger data recovery companies are investing heavily into developing data recovery techniques from SSD media to provide solutions for their customers. It will likely to take at least another year or two before data recovery solutions will become mainstream and readability available for smaller shops.

#### I would assume your group handles a lot of RAID Array work. Do you still get a fair amount of tape recovery work? Do you prefer to work with one technology over the other?

You are right, Michael. We help customers with a variety of RAID Array devices, anything from standalone DASD, SAN to NAS storage systems. RAID is a quite a popular option for customers to store data when they need performance and reliability. Unfortunately, these customers still lose their data in the same way as on any other storage devices. Thinking that redundancy is a replacement of backup is never the answer for disaster readiness. Often times, hardware failure causes data loss due to negligence, such as letting an array run in a degraded state and waiting until the next disk fails. It also happens during the reconfiguration process, such as expanding or rebuilding parity.

Furthermore, you would think that with so many disk drives around, many solutions are available to replace tapes. In reality, the industry still manufactures tapes and IT organizations have been using tape storage in the past several decades. In some cases, we've needed to go back to past data due to legal requirements. Come to find out, media and data migration customers find degraded tapes when facing the need. Even though mistakes and physical issues exist in tape storage, quite a few customers still have tapes as their only way to backup their data. It is so interesting to me that the volume of tape data recovery is large enough for to even have people and companies specialize just in that topic. Tape data recovery is similar to SSD in a sense that it requires different recovery techniques than for HDDs. Data loss causes and customer types are also different to what we normally see with disk drives situations. We deal with problems caused by torn and overwritten tapes, fire and water damaged ones, as well as simple damaged blocks on media. Since tape technology is on the decline, we help customers who are no longer supporting legacy tape environments but need to restore data from it or migrate it over to new technologies. Other customers are forced to look at their tape due to legal, electronic discovery request. We help customers in all of these situations.

#### Thank you again for taking the time to talk to us.

Thank you Nick and Michał for your interest in this subject. It was a pleasure to take part in this interview.

By Nick Baronian





From the researcher who was one of the first to identify and analyze the infamous industrial control system malware "Stuxnet," comes a book that takes a new, radical approach to making Industrial control systems safe from such cyber attacks: design the controls systems themselves to be "robust."

Ralph Langner started a software and consulting company in the industrial IT sector. Over the last decade, this same company, Langner Communications, became a leading European consultancy for control system security in the private sector. The author received worldwide recognition as the first researcher to technically, tactically, and strategically analyze the Stuxnet malware.

> www.momentumpress.net 222 E. 46th Street, #203 New York, NY 10017



# Get the best real-world Android education anywhere!

# Attend Attend The Android Developer Conference May 14-17, 2012 San Francisco Bay Area

AnDevCon is the biggest, most info-packed, most practical Android conference in the world!

"AnDevCon was an informative and comprehensive presentation of Android development concepts, tools and techniques."

-Patrick Burrell, Sr. Research Scientist, Amway

"The conference is worth the time and expense. It's a great place to meet talented people in the Android industry."

-Keith Collins, CTO, Neusoft

"AnDevCon is great for networking, learning tips and tricks, and for brainstorming innovative, new ways to create apps."

-Joshua Turner, Software Engineer, Primary Solutions

- Choose from over 65 Classes and Workshops!
- Learn from the top Android experts—including speakers straight from Google!



B Follow us: twitter.com/AnDevCon

AnDevCon<sup>™</sup> is a trademark of BZ Media LLC. Android<sup>™</sup> is a trademark of Google Inc. Google's Android Robot is used under terms of the Creative Commons 3.0 Attribution License.

A BZ Media Event

# Register NOW at www.AnDevCon.com