



3. In connection with my current and former employment, I have supervised or participated in dozens of search warrant executions for digitally stored (computerized) records and evidence and personally analyzed over 1,500 hard drives. I am certified by the United States Department of Homeland Security as a "Seized Computer Evidence Recovery Specialist," as well as certified in computer forensics by the National White Collar Crime Center. I have conducted seminars and training for the Minnesota State Bar Association, the International Association of Chiefs of Police, the Federal Bureau of Investigation, the United States Secret Service, the New York State Bar, the Minnesota Criminal Justice Institute and the Minnesota Institute for Legal Education. Attached hereto as Exhibit A is a true and correct copy of my current curriculum vitae.

**COLLECTION OF ELECTRONICALLY-STORED INFORMATION (ESI)**

4. A complete response to discovery requests may require production of ESI in its native form, since computer-generated information (metadata) relating to a relevant document will not be produced by producing a "hard copy" of that document.

5. A complete response to discovery requests may also require a thorough forensic examination of digital media, because not all relevant ESI is active (non-deleted) data.

6. A thorough forensic examination of digital media often requires multiple analysts and may take dozens of human hours. Because of this, computer forensic examinations are most practical if conducted at the expert's home office.

7. The first step generally taken by a trained computer forensic examiner is to create a duplicate copy of an entire drive (the "Forensic Image"). This creates an accurate representation of the device, regardless of file or operating system.

8. The creation of the Forensic Image is recognized by the computer forensic community as the proper way to preserve original electronic evidence. Creation of the Forensic Image does not cause any damage to the computer.

9. The creation of the Forensic Image allows a computer forensic analyst to recreate an entire storage disk and allows him or her to analyze and recover data as if the analyst were working from the original device.

10. Merely turning on a computer will change the state of the evidence by altering critical date stamps and will potentially write over and erase existing files. For this reason, a Forensic Image should be created as soon as any electronic evidence, including relevant computer hard drive(s) and other digital media, has been identified. If relevant digital media are identified and not imaged, and the systems remain in use, data pertinent to an investigation may be overwritten or otherwise destroyed.

11. It is also important to understand that when a user "deletes" files, the files are not necessarily unrecoverable. Until the file is "overwritten" by another file, the "deleted" file is still subject to being recovered. As such, it is essential to preserve all relevant computer hard drives as soon as possible; otherwise, deleted, but relevant, data may be overwritten and destroyed.

12. It is necessary to image and analyze hard drives from any computer which may have accessed relevant data as well as any server hard drives on which the relevant data might be stored to get a complete picture of the data.

13. Should any hard drive imaging be completed by someone not trained in digital evidence preservation, or not be completed in a timely manner, there is the risk of spoliation.

### CURRENT DISPUTE

14. I have spoken with Attorneys Lisa Stratton and Jill Gaulding, counsel for Plaintiff Leticia Zuniga, regarding their concerns about defendants' production of electronically-stored information in this case.

15. I have reviewed a number of documents and communications from defense counsel, including the following:

- a. a "Chain of Custody" document entitled "Hard Drive Capture Report," dated April 23, 2010 and provided by defense counsel to Plaintiff's counsel on July 6, 2010 (attached hereto as Exhibit B);
- b. a "Report of Collection," dated July 7, 2010 and provided by defense counsel to Plaintiff's counsel on July 8, 2010, reporting how data was collected from the "F" partition on the corporate defendants' server on July 5, 2010 (attached hereto as Exhibit C);
- c. a description of the software, "Neverfail," used by the corporate defendants to replicate data from the primary server to the backup server, provided by defense counsel to Plaintiff's counsel on July 23, 2010 (attached hereto as Exhibit D); and
- d. a "Report of Collection," dated July 23, 2010 and provided by defense counsel to Plaintiff's counsel on July 23, 2010, reporting how data was collected from an external hard drive on April 23, 2010 (attached hereto as Exhibit E).

16. I understand that the corporate defendants in this case represent that they have created Forensic Images for two sources of ESI: (1) their server and (2) a computer used by their former employee, defendant Marco Gonzalez. I understand that to date, no Forensic Image has been created of Mr. Gonzalez's home computer or other electronic devices.

17. Based on the foregoing, I believe that defendants' production of ESI to date may have been inadequate and may have led to spoliation. However, I cannot draw firm conclusions without being able to conduct my own forensic examination.

18. One concern relates to defendants' limitation of the Forensic Image of their server to just one partition (the "F" partition). This is not typical, and such a limitation before the facts are known defeats the purpose of an impartial collection.

19. Another concern relates to the timing of the creation of Forensic Images. The Forensic Image of the computer used by Mr. Gonzalez was created on April 23, 2010; the Forensic Image of the corporate defendants' server was created on July 5, 2010; and no Forensic Image has yet been created of Mr. Gonzalez's home computer or other electronic devices. Had Forensic Images been created earlier, the risk of relevant data being overwritten (that is, the risk of spoliation) would have been reduced.

20. Based on the information supplied to Plaintiff's counsel, I cannot be certain that the specific methods used by Document Services, Inc. (Dsi, Inc.) to create the Forensic Images followed practices accepted by the computer forensic community. Again, being able to conduct my own forensic examination will allow me to draw firm conclusions.

21. I understand that defendants' expert searched the Forensic Images using search terms provided by defense counsel (and not shared with Plaintiff's counsel). The more reasonable practice permits each party to engage its own expert to search the Forensic Image, using search terms provided by that party and search methods that may be proprietary to the expert.

22. It may be that certain data was permanently lost, due to the potential inadequacies described above. However, it may still be possible to find relevant data, not yet produced. I have recommended to Plaintiff's counsel that the parties adopt the following protocol in order to resolve these questions about the adequacy of defendants' production and to preserve any remaining relevant data.

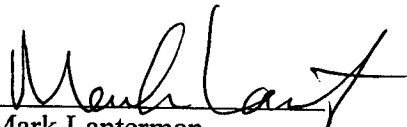
#### **PROPOSED PROTOCOL**

23. I understand that the electronic storage devices subject to analysis in this, or any, case may contain highly personal and confidential information, possibly including proprietary information, attorney-client privileged material, and non-responsive e-mail communications.

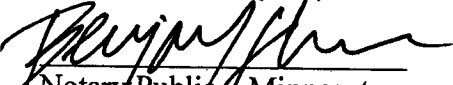
24. I am familiar with the practice in litigation of requiring and using protective orders to restrict the disclosure and use of information. I have agreed to be bound by the terms of the Protective Order in force in this case. Attached hereto as Exhibit F is a true and correct copy of the signed "Written Assurance" forms. I further agree to be bound by any other instructions of the Court.

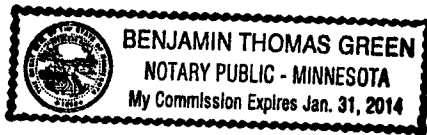
25. I have designed the following protocol to be used in the production of ESI:
- a. A Forensic Image would be made of each relevant computer or server hard drive, or other identified device, either “on site” at the computer’s location, or in my offices if the computers were to be sent to me. If conducted on site, I would make every reasonable effort to insure that the Forensic Image would be made at a time that would not be unduly disruptive to any of the participants in this matter.
  - b. I would prepare, from the Forensic Images and a list of search terms provided by Plaintiffs’ counsel, two detailed logs to be provided to counsel for the Defendants and Plaintiffs. The first log would list each relevant document on each hard drive or other device that accessed potentially relevant information with the document's file name; file extension (e.g., whether the document is a word document or e-mail); whether the file has been deleted; the date and time when the file was created, last accessed, and last altered; the size of the file; and the location of the file on the hard drive. This log would capture all potentially relevant documents anywhere on the hard drive. The second log would provide identification of each potentially relevant email and would list who send and receive the email, the date and time, the subject line and the names of any attached files.
  - c. I would provide the Defendants’ counsel with a copy of all relevant documents from the Forensic Images, from which counsel would conduct a privilege screen and determine responsive documents. I would be permitted to discuss with Plaintiff’s counsel any technical findings (e.g., evidence of file deletions, altering of documents, etc.) without disclosing to Plaintiff’s counsel the body of any communications or documents.

26. This is the same protocol that I developed for use in the 2007 Pioneer Press v. Star Tribune litigation (*Northwest Publications LLC d/b/a St. Paul Pioneer Press v. The Star Tribune Company*, File No. 62-C6-07-003489).

  
Mark Lanterman

Subscribed and sworn to before me  
this 20<sup>th</sup> day of August, 2010.

  
Notary Public - Minnesota  
My Commission Expires: 2014





**EXHIBIT A**



## Mark Lanterman

### OFFICE

601 Carlson Parkway  
Suite 630  
Minnetonka, MN 55305

### PHONE

(952) 924-9920

### FAX

(952) 924-9921

### EMAIL

mlanterman@compforensics.com

### WEB

www.compforensics.com

### Title

Chief Technology Officer

### Professional Biography

Mr. Lanterman is an eleven-year veteran police investigator. He was a member of the US Secret Service Electronic Crimes Taskforce, and has routinely assisted the Secret Service, FBI and the United States Attorney's Office as well as Fortune 500 entities across the country with computer related investigations.

Lanterman has successfully led thousands of forensic investigations, interfacing and supporting large legal organizations, corporations and government entities.

Lanterman is a sought-after speaker in the United States and abroad, and as such has presented for the Minnesota Criminal Justice Institute, the Minnesota Employment Law Institute, the Minnesota Intellectual Property Institute, the Minnesota Family Law Institute, the Minnesota State Bar Association, the California State Bar Association, the Wisconsin State Bar Association, the New York State Bar Association, the Tennessee State Bar Association, the Association of Certified Fraud Examiners, the International Association of Financial Crime Investigators, the American Society for Industrial Security, Hamline Law School, the University of Minnesota Law School, represented the US Secret Service at the International Association of Chiefs of Police National Conference.

He conducts over forty CLE classes annually and is an adjunct professor of computer forensics.

Lanterman has been a court appointed computer forensic expert to the Honorable Michael J. Davis, Chief Judge, United States District Court, District of Minnesota, to the Honorable Patricia Kerr-Karasov and the Honorable Janet N. Poston, Hennepin County District Court (Minnesota). Lanterman has given expert witness testimony in over 2,000 matters.

The Director of the United States Secret Service has recognized Lanterman for his contributions to law enforcement.

### Education

Upsala College- B.S. Computer Science (1988); M.S. Computer Science (1990)

US Department of Homeland Security- Seized Computer Evidence Recovery Specialist Certification

Minnesota Bureau of Criminal Apprehension- Management Series Certification

National White Collar Crime Center- Advanced Computer Forensics

Pennsylvania Municipal Police Officer Training

John Reid Advanced Interrogation Training

SEARCH Internet Investigation Training

**EXHIBIT B**

**Lisa Stratton**

---

**From:** Sarah Maxwell [smaxwell@millermartin.com]  
**Sent:** Tuesday, July 06, 2010 10:55 AM  
**To:** Lisa Stratton; jill.gaulding@genderjustice.us  
**Cc:** Eric Stevens  
**Subject:** Zuniga v. SMS: Electronic Discovery  
**Attachments:** ChainOfCustody.pdf

Counsel:

Please see the attached Chain of Custody beginning with DSI's collection of the hard drive, as referenced in my July 1 letter. Please let me know if you have any questions.

Thank you,

Sarah

---

**Sarah Maxwell**  
**Miller & Martin PLLC**

1200 One Nashville Place  
150 Fourth Avenue, North  
Nashville, TN 37219  
Phone (615) 744-8453  
Fax (615) 744-8633



ATLANTA · CHATTANOOGA · NASHVILLE



---

**CONFIDENTIALITY NOTICE**

The information contained in this e-mail message is legally privileged and confidential, and is intended only for the use of the addressee. If you are not the intended recipient, please be aware that any dissemination, distribution or copy of this e-mail is prohibited. If you have received this e-mail in error, please immediately notify us by reply e-mail and delete this message and any attachments. Thank you.

Please also advise us immediately if you or your employer does not consent to receipt of Internet e-mail for confidential messages of this kind.

**DISCLAIMER**

Pursuant to Circular 230 issued by the United States Treasury Department and relating to practice before the Internal Revenue Service, any comment or opinion in this communication relating to a federal tax issue is not intended to be used, and cannot be used, by a taxpayer for the purpose of avoiding tax-related penalties that may be imposed on the taxpayer.

---



# HARD DRIVE CAPTURE REPORT

v1.0

<b>CAPTURE INFO.</b>		<b>DSI INTERNAL INFO.</b>	
LOCATON: SMS Holdings ADDRESS: 7135 Charlotte Pike  CITY: Nashville STATE: TN DATE: 04/23/10 TIME: 1:00 /PM TIMEZONE: CST		CASE NO: 09-00114-V-SMS and Gonzalez CASE # <b>09-00114</b> EVIDENCE # <b>001</b> NOTES: COMPUTER NAME SMS1503	
<b>CUSTODIAN/USER INFO</b>		<b>COMPUTER SPECS:</b>	
NAME: <b>KYU YON WILKINSON</b> TITLE: LOGIN NAME: E-MAIL ADDRESS:		COMPUTER BRAND: COMPTER MODEL: SERVICE TAG: SERIAL NUMBER:	
<b>BIOS INFO.</b>		<b>HARD DRIVE INFO.</b>	
DATE: WINDOWS TIME CORRECT TIME: -8 GMT		MODEL: SERIAL #: SIZE: 38 GB	
<b>CAPTURE PROCEDURE</b>			
CAPTURE PERFORMED BY: Robert Golden			
HOW THE COMPUTER WAS SHUTDOWN: N/A – Live Capture			
HARD-DRIVE REMOVED: N/A – Live Capture			
SOFTWARE USED TO CAPTURE HARD-DRIVE: FTK Imager Lite			
SOFTWARE USED TO ANALYZE THE CAPTURE:			
<b>NOTES</b>			
00			
<b>CHAIN OF CUSTODY REPORT</b>			
<b>RECEIVED BY</b>		<b>RETURNED BY</b>	
NAME: Robert Golden DATE: 04/23/2010 TIME: <b>1:00</b> AM/PM TIMEZONE: <b>(ST)</b>		NAME: DATE: TIME: AM/PM TIMEZONE:	
SIGNITURE: <u><b>[Signature]</b></u>		SIGNITURE: _____	

**EXHIBIT C**

**Lisa Stratton**

---

**From:** Sarah Maxwell [smaxwell@millermartin.com]  
**Sent:** Thursday, July 08, 2010 5:23 PM  
**To:** jill.gaulding@genderjustice.us; Lisa Stratton  
**Cc:** Eric Stevens  
**Subject:** DSi Collection Report  
**Attachments:** Content\_7334310\_1.PDF

Counsel:

Please see the attached report from DSi, Inc. explaining the forensic collection of the hard drive from Mr. Gonzalez's former work computer. As we discussed in our telephone conference this afternoon, the report also addresses why my July 1 letter mistakenly characterized the collection as retrieving "all live data."

Please let me know if you have any questions.

Thanks,

Sarah

---

**Sarah Maxwell**  
**Miller & Martin PLLC**

1200 One Nashville Place  
150 Fourth Avenue, North  
Nashville, TN 37219  
Phone (615) 744-8453  
Fax (615) 744-8633



ATLANTA • CHATTANOOGA • NASHVILLE



---

**CONFIDENTIALITY NOTICE**

The information contained in this e-mail message is legally privileged and confidential, and is intended only for the use of the addressee. If you are not the intended recipient, please be aware that any dissemination, distribution or copy of this e-mail is prohibited. If you have received this e-mail in error, please immediately notify us by reply e-mail and delete this message and any attachments. Thank you.

Please also advise us immediately if you or your employer does not consent to receipt of Internet e-mail for confidential messages of this kind.

**DISCLAIMER**

Pursuant to Circular 230 issued by the United States Treasury Department and relating to practice before the Internal Revenue Service, any comment or opinion in this communication relating to a federal tax issue is not intended to be used, and cannot be used, by a taxpayer for the purpose of avoiding tax-related penalties that may be imposed on the taxpayer.



**REPORT OF COLLECTION**

**Document Solutions, Inc.**

**July 7th, 2010**

**Addendum**

***It appears that in a previous communication we mistakenly told Miller Martin that we collected "Live" data when we meant to say we conducted a "Live Collection". When we (DSi) speak of a "Live Collection" it is an internal description that is used when a source machine is collected while powered on and running. This in no way describes the actual data collected. The entire volume of data was collected. This includes all sectors of the volume regardless if those sectors are allocated to a file.***



## **Table of Contents**

### **Main Content**

**Section I: Case Information**

**Page 3**

**Section II: Collection Information**

**Page 3**

**Section III: Collection Details**

**Page 4**

### **Appendices**

**Appendix A: Supporting Documentation**

**Page 5 - 6**

**Appendix B: Standard Procedures**

**Page 7**

**Glossary**

**Page 8**

## **I: Case Information**

**Case#:** F\_MM015

**Case Name:** Escamilla v. SMS and Gonzalez

**Collector Name:** Robert Golden

**Source Drive Info:** Not Available – Live Collection

**EvidenceID(s)/Barcode#:** S001 / F\_MM015\_001 - 101260

**Evidence Details:** Black External Hard Drive

**Evidence Hard Drive Model:** ET-CS2PSU2-BK

**Evidence Hard Drive SN:** EH00014780

**Photographs:** Not Available (Remote Collection)

## **II. Collection Information**

**Computer Name:** SMS1503

**Acquisition started:** Fri Apr 23 11:05:41 2010

**Acquisition finished:** Fri Apr 23 11:38:07 2010

**Acquisition MD5 Hash Code:** d2b1e7a6d62c2fbdbe8db394e3bdc5

**Acquisition SHA1 Hash Code:** 14a341ea77f690008c445c373bad1224f7447dd2

**Verification started:** Fri Apr 23 11:38:07 2010

**Verification finished:** Fri Apr 23 12:12:27 2010

**Verified MD5 Hash Code:** d2b1e7a6d62c2fbdbe8db394e3bdc5

**Verified SHA1 Hash Code:** 14a341ea77f690008c445c373bad1224f7447dd2

**Collection Software:** AccessData® FTK® Imager 2.9.0.5 100406

### **III.) Collection Details**

Document Solutions, Inc. shipped SMS Holdings an external hard drive on 4/22/2010. The tracking information is as follows:

**Tracking# 7985 9674 2791**  
**To: Lee Wilkinson**  
**Service Management Systems**  
**2020 S Expressway 83**  
**C/O Valle Vista Mall**  
**Harlingen, TX 785525902**

SMS Holding's was instructed to attach this external hard drive, via USB connection, to the source computer that was to be forensically collected. The hard drive was shipped with FTK Imager which was used to conduct the collection.


On 4/23/2010 Robert Golden went to the local SMS Office located at:

**7135 Charlotte Pike**  
**Nashville, TN 37209.**

Robert remotely connected to the machine SMS1503 in the remote office. The software used to create the remote collection is a product called Kaseya (for additional details on Kaseya and or the version you will need to contact SMS directly). Kaseya uses VNC or Virtual Network Computing to initiate the connection to the remote system. Using FTK Imager Lite 2.9.0, a live forensic image of the data was created. The data was captured into a raw image format on the external hard drive provided. The information on the drive was verified by MD5 and SHA1 hash code verification.

# APPENDIX A: Supporting Documentation

## Evidence Capture Report

		<h3>HARD DRIVE CAPTURE REPORT</h3>		<small>v1.0</small>
<b>CAPTURE INFO.</b> LOCATON: SMS Holdings ADDRESS: 7135 Charlotte Pike  CITY: Nashville STATE: TN DATE: 04/23/10 TIME: 1:00 /PM TIMEZONE: CST		[REDACTED]		
<b>CUSTODIAN/USER INFO.</b> NAME: <i>KYU YON WILKINSON</i> TITLE: LOGIN NAME: E-MAIL ADDRESS:		<b>COMPUTER SPECS:</b> COMPUTER BRAND: COMPUTER MODEL: SERVICE TAG: SERIAL NUMBER:		
<b>BIOS INFO.</b> DATE: WINDOWS TIME CORRECT TIME: -8 GMT		<b>HARD DRIVE INFO.</b> MODEL: SERIAL #: SIZE: 38 GB		
<b>CAPTURE PROCEDURE</b>				
CAPTURE PERFORMED BY: Robert Golden				
HOW THE COMPUTER WAS SHUTDOWN: N/A - Live Capture				
HARD-DRIVE REMOVED: N/A - Live Capture				
SOFTWARE USED TO CAPTURE HARD-DRIVE: FTK Imager Lite				
SOFTWARE USED TO ANALYZE THE CAPTURE:				
[Empty]				
<b>NOTES</b>				
<p><i>00</i></p>				
<b>CHAIN OF CUSTODY REPORT</b>				
<b>RECEIVED BY</b> NAME: Robert Golden DATE: 04/23/2010 TIME: <i>1:00</i> AM/PM TIMEZONE: <i>(ST)</i> SIGNATURE: <i>[Signature]</i>		<b>RETURNED BY</b> NAME: DATE: TIME: AM/PM TIMEZONE: SIGNATURE: _____		

**Chain of Custody Documentation**

MEDIA DETAILS: 001280		CUSTODY ENTRIES			
Media ID	1118	Time In	Time Out	Logged By	Comment
Barcode	001280	5/14/2010 9:01:58 AM		Golden, Robert	Initial Check-in
Media ID (copy #)	C:\M04010_041				
Media Type	Hard Drive				
Media Category	Forensic				
Delivery Method	Hard To Hand				
Access	Access				
CUSTODIANS:					
Unknown: Unknown					



COC\_InternalSystem  
.jpg

## **APPENDIX B: Procedures**

### **a.) Evidence / Case Numbering**

Each piece of media is assigned a unique barcode and label called a POM. The POM and barcode information is generated automatically by our Chain of Custody software and is determined by the following:

**POM (Piece of Media) ID=CLIENT PREFIX + PROJECT NUM\_MEDIA NUM**

- CLIENT PREFIX—acronym for client's name
- PROJECT NUM—consecutive number based on project count
- MEDIA NUM—sequential identifying number specific to project.

### **b.) Data Verification and Validation**

It is policy of Document Solution, Inc. to create two forensic copies of any media/data received for analysis. In the case of a live collection only a single image is created and the second copy is made back at the Document Solutions forensic lab. This creates a working copy and a pristine copy of the original media. The copies are verified against the original by using an MD5 and/or SHA1 hash code. The hash codes of the original data are generated during the acquisition process and the acquired data hash codes are verified against this original hash code. Once the acquisition and evidence hash verification is complete the original data can be hash coded again to ensure the integrity of the source data.

### **d.) Write Blocking**

Document Solutions uses multiple write blocking methods depending on the device we are write blocking. We ensure proper procedures by using a multitier approach when available. This ensures us that if one of the write block methods was to fail our backup method would still protect the integrity of the media. All write blocking methods are tested for accuracy.

### **f.) Evidence Handling and Chain of Custody**

Document Solutions currently uses a multi level chain of custody and evidence handling process. This process begins with the entering of into our COC application. The application uses a two tier identification and authorization process (biometric finger print and user name and password). This ensures that all those who access our database have proper authority to do so. Evidence are only accessible from a single point: the evidence room. The evidence room is a single entry point room that is secured with biometric fingerprint access and monitored via multiple motion activated security cameras. Evidence is then put in an evidence container for storage.

## **Glossary**

**Hash:** A mathematical algorithm that represents a unique value for a given set of data, similar to a digital fingerprint. Common hash algorithms include MD5 and SHA.

**Hash Coding:** To create a digital fingerprint that represents the binary content of a file unique to every electronically-generated document; assists in subsequently ensuring that data has not been modified.

**Virtual Network Computing (VNC):** is a graphical desktop sharing system that uses the RFB protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network.

**EXHIBIT D**



**Lisa Stratton**

---

**From:** Sarah Maxwell [smaxwell@millermartin.com]  
**Sent:** Friday, July 23, 2010 4:19 PM  
**To:** Lisa Stratton; 'Jill Gaulding'  
**Cc:** Eric Stevens  
**Subject:** SMS Backup Servers  
**Attachments:** DS-FS-8-09-lo.pdf

Counsel:

Please see attached description of the software used to replicate data from SMS's primary server to the backup server in real time.

Thank you,

---

**Sarah Maxwell**  
**Miller & Martin PLLC**

1200 One Nashville Place  
150 Fourth Avenue, North  
Nashville, TN 37219  
Phone (615) 744-8453  
Fax (615) 744-8633



ATLANTA • CHATTANOOGA • NASHVILLE



---

**CONFIDENTIALITY NOTICE**

The information contained in this e-mail message is legally privileged and confidential, and is intended only for the use of the addressee. If you are not the intended recipient, please be aware that any dissemination, distribution or copy of this e-mail is prohibited. If you have received this e-mail in error, please immediately notify us by reply e-mail and delete this message and any attachments. Thank you.

Please also advise us immediately if you or your employer does not consent to receipt of Internet e-mail for confidential messages of this kind.

**DISCLAIMER**

Pursuant to Circular 230 issued by the United States Treasury Department and relating to practice before the Internal Revenue Service, any comment or opinion in this communication relating to a federal tax issue is not intended to be used, and cannot be used, by a taxpayer for the purpose of avoiding tax-related penalties that may be imposed on the taxpayer.

---

**neverfail**<sup>®</sup>

PREDICT · PROTECT · PERFORM

## Product Overview

# Neverfail for File Server

## Keeping your Information Flowing 24x7

The drive in business to minimize IT investments and maximize productivity through shared resources was the impetus behind the evolutionary shift from mainframes to networked computers and peripherals. Today, even small businesses depend heavily upon the bottom-line advantages of file servers that enable employees to share their files. Just how much would it cost your company in lost productivity and profitability to go a day without Microsoft® file servers? With Neverfail for File Server, you'll never have to know.

The most important consideration in protecting your Microsoft file server environment is creating a real-time, duplicate copy of your file server data. Neverfail Heartbeat sits at the core of Neverfail's suite of affordable, "cluster-class" solutions, replicating data from your active to your passive server, whether they reside in the same server room, or across the globe.

### Avoiding a Single Point of Failure

Business documents are often stored in shares on file servers, which are in constant flux as files are created, edited and deleted. In addition, new shares may be created, existing shares may be deleted or renamed and security settings or attributes can be modified.

Typical file server backup strategies that mix frequent incremental backups with occasional full backups may work in theory, but they cannot prevent losing changes to data after the last backup was finished. In addition, these types of backups do not address the redundancy required for high-availability. Backup archives may be available, but restoring data from multiple tapes is a time-consuming process with an open invitation for error.

Neverfail for File Server automatically configures protection for all of your file servers as they are created, edited, or deleted, and continually reconfigures itself to ensure that any and all changes are included in its replication set. The file server's data is always up-to-date and fully protected — no manual intervention is required thus eliminating a single point of failure.

### Keeping Business Connected

Neverfail for File Server can be used in conjunction with Microsoft's Volume Shadow Copy Service (VSS) for added levels of protection. By configuring VSS with different

## Neverfail Benefits

- Keep data flowing without interruption
- Avoid planned and unplanned downtime
- Protect against hardware and configuration failures
- Leverage Neverfail Tertiary™ for Multi-tier HA and DR
- Fail over in less than two minutes
- Fail back without service interruption
- Self configuration with no scripting
- Automated monitoring for improved reliability
- Requires no SAN or Cluster technology
- Supports LAN and WAN deployments
- Eliminate bandwidth barriers using Neverfail WANSmart™
- Rapid implementation
- Monitor all components, hardware agnostic
- Part of Neverfail's end-to-end constant availability suite

snapshot intervals on your primary and secondary Neverfail servers, more frequent copies of old data are maintained. The combination of VSS and Neverfail for File Server gives you a robust failover environment that provides continual access to files, while doubling the performance of VSS in retrieving deleted documents compared to VSS alone.

Only Neverfail delivers a solution designed from the ground up to keep users working through any type of IT outage. Neverfail's state-of-the-art replication technology ensures there is always a complete, consistent and up-to-date copy of the primary server available on a secondary server. If anything goes wrong, applications and users are seamlessly connected -- without interruption -- to the secondary server, while our persistent connection layer means applications and users continue working without any delay.

Business continues.

### Built-in Reliability

Because every application can be a potential single point of failure, it is important to take steps to prevent them from failing in the first place. Neverfail provides predictive technology

**PRODUCT OVERVIEW**

that can be used to carry out periodic health checks or continuously monitor the state of the server. Neverfail SCOPE (Server Check, Optimization, and Performance Evaluation) is designed to evaluate the stability and reliability of the hardware, software, network and configuration that underpins the applications. SCOPE allows you to be confident that you have the best practice in place to avoid outages wherever possible.

When Neverfail detects an IT condition that is likely to result in an outage, the software can take a variety of preemptive measures to fix the source of the problem (such as attempting to restart a service).

**No Recovery Required**

Delivering continuous availability means there is no time to rely on traditional backup/recovery techniques or even continuous data protection. Traditional protection strategies will require a recovery; databases will need to be rebuilt, configurations checked, users notified of the outage. Today's companies cannot afford to have downtime of their business critical applications.

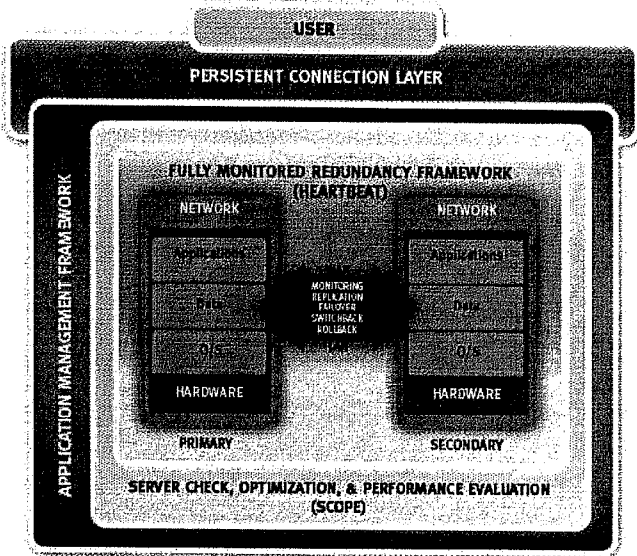
Neverfail maintains a complete, consistent and up-to-date copy of the applications and the configuration. This is more than just a copy of the data. Neverfail provides a complete, ready-to-go clone of the server, including any configuration changes that may have been applied since the application server was first installed.

If there is an availability threat, an administrator can fail over from the primary to the secondary server at the click of a button, or Neverfail can automate the whole process based on user-defined criteria. Administrators with limited knowledge of the application installation can easily fail over using best practice knowledge already embedded into Neverfail's product architecture.

**Hurricane, Flood, Fire - Business Continues**

Keeping your business running through natural and man-made disasters can literally be a matter of life or death. The ability to use all applications can be even more important in this situation. That's why the Neverfail architecture is designed to allow remote deployment of the secondary server. Neverfail's secondary server can be located in the same room, the same building or in a different part of the world. To further simplify the process, Neverfail makes sure the WAN doesn't get in the way by using compression to optimize replication, even when bandwidth is an issue and data volumes need to be reduced.

**NEVERFAIL SCHEMATIC OVERVIEW**



**Protection Out-Of-The-Box**

Embedded within Neverfail for File Server is all the knowledge to make continuous availability a reality. Data locations, registry entries and databases are all cloned automatically. Failure detection is embedded. Complex fail over processes are a thing of the past.

**Protecting the File Servers**

Neverfail for File Server is the product you need to protect your file servers and corporate data. It monitors and protects all file stores and makes sure that all changes to the data and files are always replicated and up-to-date. Without continuous availability of corporate data and file stores, the ability to interact with your customers and react to changing business climates is lost. If servers fail the impact is the same. Productivity dies, decisions are not made, business stops.

This is why the same Neverfail architecture provides continuous availability for Microsoft Exchange®, Lotus Domino®, BlackBerry® Enterprise Server, SharePoint®, SQL Server®, IIS® and File Server®.

With Neverfail, businesses can rely on all of their application implementations.



North America  
 T: +1 512-327-5777  
 Email: info@us.neverfailgroup.com  
 Europe  
 T: +44 (0) 870 777 1500  
 Email: info@neverfailgroup.com  
 Netherlands  
 T: + 31 294 237545  
 Email: info@neverfailgroup.com

Germany  
 T: +49 (0)69 7593 8433  
 Email: info@neverfailgroup.com  
 Middle East  
 T: + 971 4 360 2436  
 Email: mena@neverfailgroup.com  
 Asia Pacific  
 T: +61 2 8448 8192  
 Email: apj.info@neverfailgroup.com



**EXHIBIT E**

**Lisa Stratton**

---

**From:** Sarah Maxwell [smaxwell@millermartin.com]  
**Sent:** Friday, July 23, 2010 4:20 PM  
**To:** Lisa Stratton; 'Jill Gaulding'  
**Cc:** Eric Stevens  
**Subject:** Server Collection Report  
**Attachments:** Content\_7387883\_1.PDF

Counsel:

Please see attached report regarding the collection of the SMS server on July 5, 2010.

Thank you,

---

**Sarah Maxwell**  
**Miller & Martin PLLC**

1200 One Nashville Place  
150 Fourth Avenue, North  
Nashville, TN 37219  
Phone (615) 744-8453  
Fax (615) 744-8633



ATLANTA • CHATTANOOGA • NASHVILLE



---

**CONFIDENTIALITY NOTICE**

The information contained in this e-mail message is legally privileged and confidential, and is intended only for the use of the addressee. If you are not the intended recipient, please be aware that any dissemination, distribution or copy of this e-mail is prohibited. If you have received this e-mail in error, please immediately notify us by reply e-mail and delete this message and any attachments. Thank you.

Please also advise us immediately if you or your employer does not consent to receipt of Internet e-mail for confidential messages of this kind.

**DISCLAIMER**

Pursuant to Circular 230 issued by the United States Treasury Department and relating to practice before the Internal Revenue Service, any comment or opinion in this communication relating to a federal tax issue is not intended to be used, and cannot be used, by a taxpayer for the purpose of avoiding tax-related penalties that may be imposed on the taxpayer.

---



**Report of Collection**  
**Document Solutions, Inc.**  
**July 23, 2010**

# Table of Contents

---

## **Main Content**

**Section I: Case Information – page 3**

**Section II: Collection Information – page 3**

**Section III: Collection Details – page 4**

## **Appendices**

**Appendix A: Supporting Documentation – page 5**

**Appendix B: Standard Procedures – page 6**

**Glossary - page 7**

## I. Case Information

---

**Case Number:** F\_MM015  
**Case Name:** Escamilla v. SMS Holdings & Gonzalez  
**Collector Name:** Andy Spore  
**Source Drive Info:** RAID Configuration  
**Evidence ID(s)/Barcode:** S002 / F\_MM015\_002 - 3667119  
**Evidence Details:** Samsung 1 TB Internal Hard Drive  
**Evidence Hard Drive Model:** HD103SJ  
**Evidence Hard Drive Serial Number:** S246J90Z356789

## II. Collection Information

---

**Server Name:** SMSFP01  
**Acquisition Started:** Mon Jul 05 11:19:44 2010  
**Acquisition Finished:** Tue Jul 06 03:47:11 2010  
**Acquisition MD5 Hash Code:** 06ebf08432a4766938e87cdfa57d8b3a  
**Acquisition SHA1 Hash Code:** 9de544eeeb3e93ff237dea4b1084c28eae0e4f89  
**Verification Started:** Tue Jul 06 08:53:31 2010  
**Verification Finished:** Tue Jul 06 15:05:36 2010  
**Verified MD5 Hash Code:** 06ebf08432a4766938e87cdfa57d8b3a  
**Verified SHA1 Hash Code:** 9de544eeeb3e93ff237dea4b1084c28eae0e4f89  
**Collection Software:** AccessData® FTK® Imager 2.5.3.14 071018



## III. Collection Details

---

On July 5<sup>th</sup>, 2010 Andy Spore met Scott Emerson of SMS Holdings at Peak 10, Inc., located at the address below. Mr. Emerson escorted Mr. Spore into the facility and was present at all times when Mr. Spore was in the building.

Peak 10, Inc.

7100 Commerce Way

Brentwood, TN 37027

The server rack was opened and the specified server was accessed using log-in credentials provided specifically for the collection by SMS Holdings and Peak 10. A CD loaded with Helix 3 Incident Response software was inserted into the server and FTK Imager 2.5 was launched from the disc. A 1 TB internal hard drive was connected to the back of the server via a hard drive enclosure with a USB connection as the evidence drive.

Mr. Spore then initiated a logical capture of the "Data" (F:\) partition on the server. The data was captured to a Linux DD forensic image format. This partition was specified by SMS Holdings and Miller & Martin prior to the collection as the only partition on the server containing user data. A logical capture acquires all data on a specified partition, including unallocated space.

After the capture was launched, the server rack was closed and locked by Mr. Emerson. Tamper evident security tape was placed on the rack doors to ensure that the server was not physically accessed during the collection. None of the temper evident tape was disturbed until it was removed at the end of the collection by Mr. Spore. Barcodes for the security tape are as follows:

**Console Front: D183063**

**Server Front: D183065**


**Console Back: D183064**

**Server Back: D183062**

The collected evidence was then confirmed as a bit-for-bit duplicate of the original data by MD5 and SHA1 hash code verification.

# Appendix A: Supporting Documentation

**Evidence Capture Report:**

		<b>HARD DRIVE CAPTURE REPORT</b>		<small>v1.0</small>
<b>CAPTURE INFO</b> LOCATION: <i>PERK 10, INC.</i> ADDRESS: <i>7100 COMMERCE WAY</i> CITY: <i>BROWNSBORO</i> STATE: <i>TN</i> DATE: <i>7/5/10</i> TIME: <i>11:15</i> <i>AM</i> PM TIMEZONE: <i>CDT</i>				
<b>CUSTODIAN INFO</b> NAME: <i>MULTIPLE</i> TITLE: LOGIN NAME: E-MAIL ADDRESS:		<b>COMPUTER INFO</b> COMPUTER BRAND: <i>DELL POWEREDGE 1900</i> COMPUTER MODEL: SERVICE TAG: <i>SR6V6X</i> SERIAL NUMBER:		
<b>BIO INFO</b> DATE: TIME: <i>SERVER DATE/TIME CURRENT</i>		<b>PERIPHERAL INFO</b> MODEL: <i>RMD</i> SERIAL #: SIZE:		
<b>CAPTURE PERFORMED BY:</b> <i>ANDY SPANE</i>				
<b>HOW THE COMPUTER WAS SHUTDOWN:</b> <i>NOT SHUT DOWN</i>				
<b>HARD-DRIVE REMOVED:</b> <i>NO</i>				
<b>SOFTWARE USED TO CAPTURE HARD-DRIVE:</b> <i>FTK IMAGER VIA HELIX</i>				
<b>SOFTWARE USED TO ANALYZE THE CAPTURE:</b>				
(CONT.)				
LOGICAL CAPTURE OF F:\ DRIVE ("DATA") ON SASFP01. SECURITY BAR CODES: FRONT - <i>D1B3063, D1B3065</i> BACK - <i>D1B03062, D1B3064</i> MD5 HASH: <i>06ebf08432a4766938e87cdfa5748b3a</i> SHA1 HASH: <i>9de544eeeb3e93ff237dea4b1084c28eae0e4f89</i>				
<b>RECEIVED BY</b> NAME: <i>ANDY SPANE</i> DATE: <i>7/6/10</i> TIME: <i>7:37</i> <i>AM</i> PM TIMEZONE: <i>CDT</i> SIGNATURE: <i>R. Adams Spive</i>		<b>RETURNED BY</b> NAME: DATE: TIME: AM/PM TIMEZONE: SIGNATURE: _____		

## Appendix B: Procedures

---

### **a.) Evidence / Case Numbering**

Each piece of media is assigned a unique barcode and label called a POM. The POM and barcode information is generated automatically by our Chain of Custody software and is determined by the following:

**POM (Piece of Media) ID=CLIENT PREFIX + PROJECT NUM\_MEDIA NUM**

- CLIENT PREFIX—acronym for client's name
- PROJECT NUM—consecutive number based on project count
- MEDIA NUM—sequential identifying number specific to project

### **b.) Data Verification and Validation**

It is the policy of Document Solutions, Inc. to create two forensic copies of any media/data received for analysis. In the case of a live collection only a single image is created and the second copy is made back at the Document Solutions forensic lab. This process creates a working copy and a pristine copy of the original media. The copies are verified against the original by using an MD5 and/or SHA1 hash code. The hash codes of the original data are generated during the acquisition process and the acquired data hash codes are verified against this original hash code. Once the acquisition and evidence hash verification is complete the original data can be hash coded again to ensure the integrity of the source data.

### **c.) Write Blocking**

Document Solutions uses multiple write blocking methods depending on the device we are write blocking. We ensure proper procedures are followed by using a multitier approach when available. This ensures us that if one of the write block methods were to fail our backup method would still protect the integrity of the media. All write blocking methods are tested for accuracy.

### **d.) Evidence Handling and Chain of Custody**

Document Solutions currently uses a multi-level chain of custody and evidence handling process. This process begins with the entering of evidence into our COC application. The application uses a two tiered identification and authorization process (biometric finger print and user name and password). This ensures that all those who access our database have proper authority to do so. Evidence is only accessible from a single point: the evidence room. The evidence room is a single entry point room that is secured with biometric fingerprint access and monitored via multiple motion activated security cameras. Evidence is then put in an evidence container for storage.

# Glossary

---

**Hash:** A mathematical algorithm that represents a unique value for a given set of data, similar to a digital fingerprint. Common hash algorithms include MD5 and SHA.

**Hash Coding:** To create a digital fingerprint that represents the binary content of a file unique to every electronically-generated document; assists in subsequently ensuring that data has not been modified.

**RAID: (Redundant Array of Independent Disks)** A group of hard disks that operate together to improve performance or provide fault tolerance and error recovery through data striping, mirroring, and other techniques.

**Unallocated Space:** Space on a hard drive that potentially contains intact files, remnants of files, subdirectories or temporary files which were created and then deleted by a computer application, the operating system or the operator.

**Partition:** A partition can be thought of as a division or "part" of a real hard disk drive. Multiple partitions on a single hard drive appear as separate drives to the operating system.

**Linux DD Image:** An image format containing the contents and structure representing a data storage medium or device, such as a hard drive. A DD image is created by making a bit-for-bit copy of the source medium, thereby perfectly replicating the structure and contents of a storage device.

**EXHIBIT F**

EXHIBIT A  
WRITTEN ASSURANCE

MARK LANTEMAN declares that:

I reside at 601 CARLSON DR. # 630 in the City of MINNETONKA,  
County of HENNEPIN, State of MINNESOTA. My telephone number is  
952-924-9920.

I am currently employed by COMPUTER FORENSIC SERVICES, located  
at SAME, and my current job title is  
CTO.

I have read and I understand the terms of the Protective Order dated 7-23-10,  
filed in Case No. 09-CV 2120 (JMR/JSM) pending in the United States District Court of  
Minnesota. I agree to comply with and be bound by the provisions of the Protective Order.  
I understand that any violation of the Protective Order may subject me to sanctions by the  
Court.

I shall not divulge any documents or copies of documents, designated  
"Confidential" obtained pursuant to such Protective Order, or the contents of such  
documents, to any person other than those specifically authorized by the Protective Order.  
I shall not copy or use such documents except for the purposes of this action and pursuant  
to the terms of the Protective Order.

As soon as practical, but no later than 30 days after final termination of this action, I  
shall return to the attorney from whom I have received them, any documents in my

possession designated "Confidential," and all copies, excerpts, summaries, notes, digests, abstracts, and indices relating to such documents.

I submit myself to the jurisdiction of the United States District Court for the District of Minnesota for the purpose of enforcing or otherwise providing relief relating to the Protective Order.

Executed on 7-6-10  
(Date)


  
(Signature)

EXHIBIT A  
WRITTEN ASSURANCE

MARK LANTEKMAN declares that:

I reside at 62 Carlson Pkwy, #630 in the City of MINNETONKA,  
County of HENNEPIN, State of MINNESOTA. My telephone number is  
952-924-9920.

I am currently employed by COMPUTER FORENSIC SERVICES, located  
at SHAME, and my current job title is  
CTO.

I have read and I understand the terms of the Protective Order dated 3-8-10,  
filed in Case No. 09-CV-2120 (JMR/JSM), pending in the United States District Court of  
Minnesota. I agree to comply with and be bound by the provisions of the Protective Order.  
I understand that any violation of the Protective Order may subject me to sanctions by the  
Court.

I shall not divulge any documents or copies of documents, designated  
"Confidential" or "Attorneys Eyes Only" obtained pursuant to such Protective Order, or the  
contents of such documents, to any person other than those specifically authorized by the  
Protective Order. I shall not copy or use such documents except for the purposes of this  
action and pursuant to the terms of the Protective Order.

As soon as practical, but no later than 30 days after final termination of this action, I  
shall return to the attorney from whom I have received them, any documents in my



possession designated "Confidential" or "Attorneys Eyes Only" and all copies, excerpts, summaries, notes, digests, abstracts, and indices relating to such documents.

I submit myself to the jurisdiction of the United States District Court for the District of Minnesota for the purpose of enforcing or otherwise providing relief relating to the Protective Order.

Executed on 7-6-10  
(Date)


  
(Signature)

EXHIBIT A  
WRITTEN ASSURANCE

Benjamin Green declares that:

I reside at 601 Carlson Pkwy. #630 in the City of Minnetonka,  
County of Hennepin, State of Minnesota. My telephone number is  
952-924-9920.

I am currently employed by Computer Forensic Services, located  
at 1001 Carlson Pkwy, Ste. 630, Minnetonka, MN, and my current job title is  
Operations Manager.

I have read and I understand the terms of the Protective Order dated 2-23-10  
filed in Case No. 09-CV 2120 (JMR/JSM) pending in the United States District Court of  
Minnesota. I agree to comply with and be bound by the provisions of the Protective Order.  
I understand that any violation of the Protective Order may subject me to sanctions by the  
Court.

I shall not divulge any documents or copies of documents, designated  
"Confidential" obtained pursuant to such Protective Order, or the contents of such  
documents, to any person other than those specifically authorized by the Protective Order.  
I shall not copy or use such documents except for the purposes of this action and pursuant  
to the terms of the Protective Order.

As soon as practical, but no later than 30 days after final termination of this action, I  
shall return to the attorney from whom I have received them, any documents in my

possession designated "Confidential," and all copies, excerpts, summaries, notes, digests, abstracts, and indices relating to such documents.

I submit myself to the jurisdiction of the United States District Court for the District of Minnesota for the purpose of enforcing or otherwise providing relief relating to the Protective Order.

Executed on 7/6/2010  
(Date)

  
(Signature)

EXHIBIT A  
WRITTEN ASSURANCE

Benjamin Green declares that:

I reside at 601 Carlson Pkwy, Ste. 630 in the City of Minnetonka,  
County of Hennepin, State of Minnesota. My telephone number is  
952-924-9920.

I am currently employed by Computer Forensic Services, located  
at 601 Carlson Pkwy, Ste. 630, Minnetonka, MN, and my current job title is  
Operations Manager.

I have read and I understand the terms of the Protective Order dated 3-8-10,  
filed in Case No. 09-CV-2120 (JMR/JSM), pending in the United States District Court of  
Minnesota. I agree to comply with and be bound by the provisions of the Protective Order.  
I understand that any violation of the Protective Order may subject me to sanctions by the  
Court.

I shall not divulge any documents or copies of documents, designated  
"Confidential" or "Attorneys Eyes Only" obtained pursuant to such Protective Order, or the  
contents of such documents, to any person other than those specifically authorized by the  
Protective Order. I shall not copy or use such documents except for the purposes of this  
action and pursuant to the terms of the Protective Order.

As soon as practical, but no later than 30 days after final termination of this action, I  
shall return to the attorney from whom I have received them, any documents in my

possession designated "Confidential" or "Attorneys Eyes Only" and all copies, excerpts, summaries, notes, digests, abstracts, and indices relating to such documents.

I submit myself to the jurisdiction of the United States District Court for the District of Minnesota for the purpose of enforcing or otherwise providing relief relating to the Protective Order.

Executed on

7/6/2010  
(Date)

  
(Signature)