

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA

Case No. 07-22674-Civ-JORDAN/Torres

DELL INC.; AND ALIENWARE CORPORATION,

Plaintiffs,

vs.

BELGIUMDOMAINS, LLC; CAPITOLDOMAINS,  
LLC; DOMAINDOORMAN, LLC; NETRIAN  
VENTURES LTD.; IHOLDINGS.COM, INC.;  
JUAN PABLO VAZQUEZ a/k/a JP VAZQUEZ, an  
individual; and DOES 1 – 10;

Defendants.

---

**DECLARATION OF JAMES STANFORD WILSON IN SUPPORT OF PLAINTIFFS'  
MOTION FOR SANCTIONS, INCLUDING THE ENTRY OF A DEFAULT JUDGMENT**

I, James Stanford Wilson, make the following statements upon my personal knowledge and belief:

1. My name is James Stanford Wilson. I am of legal age and sound mind, and I am competent to make this declaration.

**Background**

2. I am a principal in NetEvidence, Inc., a computer forensic investigation and consulting business in operation since December 2004 in Nashville, TN. NetEvidence is a computer forensic investigation and consulting firm. I am certified as a computer forensic examiner by the recognized certifying organization, Guidance Software, makers of the EnCase software and hardware products.

Case No. 07-22674-Civ-JORDAN/Torres

3. I received my Bachelor of Science in Computer Information Systems from David Lipscomb University. In addition, I am a Certified Information Systems Security Professional, a member of the association of Certified Fraud Examiners, a licensed private investigator, and a Certified Computer Forensic Examiner. For the past six years, prior to co-founding NetEvidence, Inc., I held senior management positions in the high-tech industry including the Practice Leader of the High Tech Investigative Group and the title of Chief Information Security Officer for large New York based firms. My area of expertise includes computer forensic investigations, expert testimony, data recovery, and reconstruction of electronic data.

4. I have provided computer forensic investigation and testimony in at least the following cases:

**Little Mendelson Walnut Creek, CA**

Declaration in Pasetes v. Washington Hospital - Attorney Timothy O'Donnell - 2004

Supplemental Declaration and Mediation in Pasetes v. Washington Hospital - Attorney - Jeffrey Adams - 2005

**Stearns Weaver Miller Weissler Alhadeff & Sitterson, Miami, FL**

Affidavit in M & M Aerospace Hardware, Inc. v. Mark R. Heathcock, Peter M. Oleck, and Ascent Aerospace Fasteners, LLC. - Attorney - Joan Canny - 2005

United States District Court, Southern District of Florida

Expert Court Room Testimony in M & M Aerospace Hardware, Inc. v. Mark R. Heathcock, Peter M. Oleck, and Ascent Aerospace Fasteners, LLC. - Attorney - Joan Canny - 2006

Case No. 05-21449-CIV-Altonaga/Turnoff

United States District Court, Southern District of Florida

Case No. 07-22674-Civ-JORDAN/Torres

**Stearns Weaver Miller Weissler Alhadeff & Sitterson, Ft. Lauderdale, FL**

Expert Court Room Testimony in AutoNation v. Garrick Hatfield – Attorney - Jon Stage – 2007

In the circuit court of the 17<sup>th</sup> judicial circuit in and for Broward county, Florida  
Case No. 05-02037 (13)

**Bone McAllester Norton PLLC, Nashville, TN**

Affidavit in Jacksonville Auto Auction, Inc. vs Chuck Thompson – Attorney - Stephen Zralek – 2007

In the circuit court of the fourth judicial circuit, in and for Duval county, Florida  
Case No. 2007-CA-000337 Division CV-G

**Ball-Weed, San Antonio, TX**

Expert Court Room Testimony in USAA vs WOAI – Attorney - Bill Ford - 2004  
San Antonio City Court

**The Securities and Exchange Commission, Miami, FL**

Affidavit for the SEC Regional Director of Enforcement – Teresa J. Verges – 2001

Onsite Expert Testimony for the SEC Regional Director of Enforcement – Teresa J. Verges – 2002

**The Securities and Exchange Commission Department of Computer Forensics**

Declarations in the Enron investigation in Houston, TX - 2003

**Godwin Gruber, Dallas, TX**

Deposition and Onsite Expert Testimony – Attorney - Craig Albert – 2003

**Stikeman and Elliott, Toronto Canada, 2001**

Expert testimony in the RBC Dominion Securities vs. Andrew Rankin case  
The largest insider trading case in Canadian history

**Frost Brown Todd, Cincinnati, OH**

Radian Case Mediation – Attorney – Frederick J. McGavran - 2003

Case No. 07-22674-Civ-JORDAN/Torres

**Kutak Rock, LLP, Omaha, NE**  
Agriserv Case – Attorney – Patrick B. Griffin - 2002

**Borden Ladner Gervais, Toronto, Canada**  
407 ETR Case – 2002

**Stockwood Spies, Toronto Canada**  
Expert testimony given in “chambers” where retired judges continue to settle cases  
2001, 2002

**The computer search and data extraction**

5. Net Evidence was retained in November 2007, to conduct the forensic preservation of electronic evidence for investigative analysis in the above captioned litigation.

6. As a result, our company, NetEvidence, Inc., was asked to conduct the preservation of electronic evidence located at 11605 South West 99<sup>th</sup> Court, Miami, Florida on November 9, 2007. This location appeared to be the residence of one of the Defendants, Mr. JP Vazquez.

7. NetEvidence, Inc., was also asked to conduct the preservation of electronic evidence located in 50 NE 9<sup>th</sup> Street, Miami, Florida beginning on November 15, 2007, and continuing, as necessary. This location is a large Internet co-location facility operated by Internap Network Services Corporation.

8. Upon arrival at the 50 NE 9<sup>th</sup> Street address, the NetEvidence team was met by Mr. Vazquez, whom I previously met on November 9, 2007. Mr. Vazquez directed the team to two secured data closets, which he identified as containing the servers operated by one or more

Case No. 07-22674-Civ-JORDAN/Torres

of the Defendants in the above captioned case. Mr. Vazquez unlocked the two secured data closets allowing the NetEvidence team access.

9. Access to the two secured data closets was further controlled by a security guard at the Internet co-location facility. Prior to being allowed to enter the facility each member of the NetEvidence team was required to provide a driver's license, which was checked by the security guard against an approved entry list. Each time access to the two secured data closets was needed, Mr. Vazquez personally had to obtain the keys to the two secured data closets from the security guard.

10. Upon inspection of the two data closets I discovered that they contained 22 servers of various types (the "Servers").

11. Access to each of the Servers was password protected. Mr. Vazquez provided passwords for each of the Servers. Each password was over 15 characters long and contained both numbers, letters of mixed case, and special characters.

12. We began conducting the preservation of electronic evidence on the hard drive contained in or connected to the Servers on November 15, 2007, and concluded the preservation on November 18, 2007.

13. The process used follows the accepted methodology for conducting forensic computer investigations. These methods and principles are considered reliable within the computer forensic industry, and have been accepted as reliable in numerous federal and state courts, including the courts identified above in this Declaration.

14. We maintained the chain of custody of all the hard drives imaged during our

Case No. 07-22674-Civ-JORDAN/Torres

investigation.

**Results and Conclusions**

15. I have conducted Forensic investigation and analysis on the forensically acquired electronic data located on the Servers.

16. I discovered that activity logging was being deleted on many of the Servers. Typically this information is kept to log key activity and for security purposes. Servers of these types most often keep log files to allow reconstruction of activity by system administrators.

17. Mr. Vazquez advised me that administration of the Servers was performed remotely via the Internet.

18. I also discovered that many of the Servers were rebooted on or about November 14, 2007. Servers of these types are seldom rebooted, and in fact, aside from the recent rebooting, many of these machines were last rebooted over 100 days ago. Rebooting a server is often performed in connection with major changes to the server or to make permanent new configurations.

19. Forensic investigation revealed that the hard drives in nine of the Servers were intentionally wiped clean using a process writing all zeros to the drives. This technique is often employed to render recovery of data stored on hard drives impossible.

20. Forensic investigation revealed evidence on 5 of the Servers that the computer program BCWipe had been used in a process to write all zeros to the drives. BCWipe is a software program sold by Jetico, Inc. to wipe data from hard drives. Jetico's website, available at <http://www.jetico.com/bcwipe.htm>, describes BCWipe as follows:

Case No. 07-22674-Civ-JORDAN/Torres

Wiping is a term used to describe the process of shredding the contents of a file or disk space. It is impossible to restore any data that has been properly wiped.

BCWipe software enables you to confidently erase files that can never be recovered by an intruder. BCWipe complies with options to invoke either the US Department of Defence (DoD) standard or the Peter Gutmann wiping scheme.

21. Forensic investigation revealed that BCWipe was used to destroy the data on November, 12, 2007.

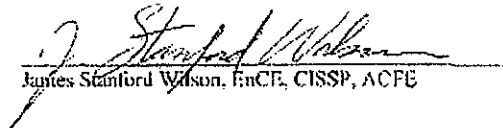
22. Forensic investigation revealed that at least 9 of the 22 Servers contained empty hard drives or hard drives intentionally wiped clean.

SIGNATURE ON NEXT PAGE OF DECLARATION

Case No. 07-22674-Civ-JORDAN/Torres

I declare under penalty of perjury that the foregoing is true and correct.

Signed on this 4<sup>th</sup> day of January, 2008.

  
James Stanford Wilson, EnCFE, CISSP, ACFE



**CERTIFICATE OF SERVICE**

I hereby certify that on January 5, 2008, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF. I also certify that the foregoing document is being served this day on all counsel of record or pro se parties identified on the attached Service List in the manner specified, either via transmission of Notices of Electronic Filing generated by CM/ECF or in some other authorized manner for those counsel or parties who are not authorized to receive electronically Notices of Electronic Filing.

*/s/ Mimi L. Sall* \_\_\_\_\_

Case No. 07-22674-Civ-JORDAN/Torres

**Dell Inc. and Alienware Corporation vs. Belgiumdomain, LLC, et al.**  
**Case No. 07-22674-Civ-JORDAN/Torres**  
**United States District Court, Southern District of Florida**

<p>Lawrence P. Rochefort, Esquire E-mail: <a href="mailto:lawrence.rochefort@akerman.com">lawrence.rochefort@akerman.com</a> Christopher S. Carver, Esquire E-mail: <a href="mailto:christopher.carver@akerman.com">christopher.carver@akerman.com</a> AKERMAN SENTERFITT SunTrust International Center Suite 2500 One S.E. Third Avenue Miami, Florida 33131 Tel.: 305-374-5600 Fax: 305-374-5095 Attorneys for BelgiumDomains, LLC, CapitolDomains, LLC, DomainDoorman, LLC, Netrian Ventures, Ltd., and iHoldings.com, Inc. Service by CM/ECF</p> <p>Joel R. Dichter, Esquire E-mail: <a href="mailto:jdichter@NewmanDichter.com">jdichter@NewmanDichter.com</a> Derek Newman, Esquire E-mail: <a href="mailto:derek@NewmanDichter.com">derek@NewmanDichter.com</a> Newman Dichter 505 Fifth Avenue South, Suite 610 Seattle, WA 98104 Tel.: 206-274-2800 Fax: 206-274-2801 (Moving for Admission Pro Hac Vice) Service by CM/ECF</p>	<p>Richard Baron, Esquire Email: <a href="mailto:rbaron@bellsouth.net">rbaron@bellsouth.net</a> Richard Baron &amp; Associates 501 NE 1st Avenue Suite 201 Miami, FL 33132 Tel. 305-577-4626 Fax: 305-577-4630 Attorneys for Defendant Juan Pablo Vazquez Service by CM/ECF</p>
--	---

AFB IRV1110839.1-\*01/4/08 5:41 PM