

SAMUEL J. SERATA
20 Franklin Street
Bridgeton, New Jersey 08302
(856)451-6444
Attorney for Petitioners, Ernest Zirkle and Cynthia Zirkle,

IN THE MATTER OF THE PETITION OF
ERNEST ZIRKLE AND CYNTHIA ZIRKLE
CONTESTING PURSUANT TO *N.J.S.A*
19:29-1 THE ELECTION OF VIVIAN
HENRY AND MARK HENRY AS
DEMOCRATIC EXECUTIVE COMMITTEE
PERSONS FROM DISTRICT 3 OF
FAIRFIELD TOWNSHIP (CUMBERLAND
COUNTY),

ERNEST ZIRKLE AND CYNTHIA ZIRKLE

Petitioners,

vs.

VIVIAN HENRY, MARK HENRY, The
CUMBERLAND COUNTY BOARD OF
ELECTIONS, and GLORIA NOTO,
CUMBERLAND COUNTY CLERK,

Respondents.

SUPERIOR COURT OF NEW JERSEY
CUMBERLAND COUNTY
LAW DIVISION

Docket No. CUM-L-000567-11

Civil Action

**CERTIFICATION OF
ANDREW W. APPEL
IN SUPPORT OF
ORDER TO SHOW CAUSE**

I, Andrew W. Appel, of full age, do hereby certify:

1. I am employed as Professor of Computer Science and Chair of the Department of Computer Science at Princeton University.

2. I am serving in this case as an expert on computer science, computer security, voting machines, and election technology. On August 17th, 2011, I examined a voting machine, a laptop computer, and paper documents pursuant to an Order by this Court. In this affidavit I do not present a full expert report, but only (a) facts and expert opinions regarding conditions that I

observed relevant to the (lack of) security of impounded evidence, and (b) facts relating to my expert opinion that evidence was erased from a laptop computer on August 16th, 2011.

3. As discussed below, I believe that information was purged from the computer at 3pm on August 16th, just hours before I examined the voting machine and computer. This information could have allowed me to learn many relevant facts about the use of this computer during the month when the ballot for the primary election was being prepared—for example, whether or not unauthorized users connected to the machine and altered ballot definitions. I am not alleging that such alteration of ballot definitions did occur, but only that information appears to have been erased on August 16th that would have allowed me to determine whether or not it did occur.

Lack of security for impounded evidence

4. I arrived at the Cumberland County Board of Elections building in the company of Samuel Serata, Esq., at 10 a.m. on August 17, 2011. We met with State and County officials and employees in the room at the very front of the building, immediately inside the front door; it is a combination lobby and conference room. It was in this room that I began my examination by requesting to see the pollbooks and voting authority “tickets” from the District 3 election. I observed Ms. Lizbeth Hernandez walk into an office adjacent to this lobby; the door to this office was open when I arrived in the building and remained open the entire time. She returned from this office with pollbooks, voting authority stub books, and voting authority tickets. The documents were not in any sort of envelope or enclosure, and were not sealed in any way. She placed these documents on the conference table, and I examined them. When I was finished with the documents she returned them to the adjacent office, without (in my presence) putting them inside any kind of container or envelope.

5. I then asked to examine the AVC Advantage voting machine that had been used for the election in question. Ms. Hernandez led us down a hallway toward the back of the building to a large room that constitutes the “voting machine warehouse.” By “us” I mean all the people that were present to supervise my examination: Ms. Hernandez, myself, Mr. Serata, Deputy A.G. George Cohen, Mr. Jason Cossabon who is (I believe) an employee of the Board of Elections who does IT (information technology) support, Mr. Robert Giles (Director of Elections of the State of New Jersey), and Ms. Kimberly Procopio (attorney for the County Clerk). Upon entry to the room, I observed that there was no logging of who entered and left the room, that is, none of us had to sign in or out, and no apparent records were kept as we entered and exited.

6. The “warehouse” room contained what appeared to be 100 or more AVC Advantage voting machines, neatly arrayed in rows. Off in one corner (at a distance of about 10 feet from the rows of voting machines) was a single voting machine, serial number 23550, on which a piece of paper had been placed reading “Do not touch this machine.” Other than its separation at a distance of 10 feet and the paper sign, I saw no physical security measures to implement any sort of “impoundment” of this voting machine.

7. I proceeded with my examination of this machine. In this affidavit I am not presenting my opinions about all the technical aspects of this election, but only facts I saw that relate to the security of evidence. I will present a full expert report at another time.

8. When I had completed my examination of the AVC Advantage voting machine #23550, the six people I named earlier were led from the room (again with no logging) back to the front lobby/conference room.

9. Pursuant to this Court’s Order, which permitted me to examine “any laptop or other computers used to program the ballot on the Voting Machine and to tabulate election

results,” I asked to examine such computer(s). Ms. Hernandez led me (and the others named above) into a small conference room immediately adjacent to the front lobby. At the time we approached this room, the door to the room was open and no one was inside. In the room was a laptop computer set up on a table, as shown in Figure 1.

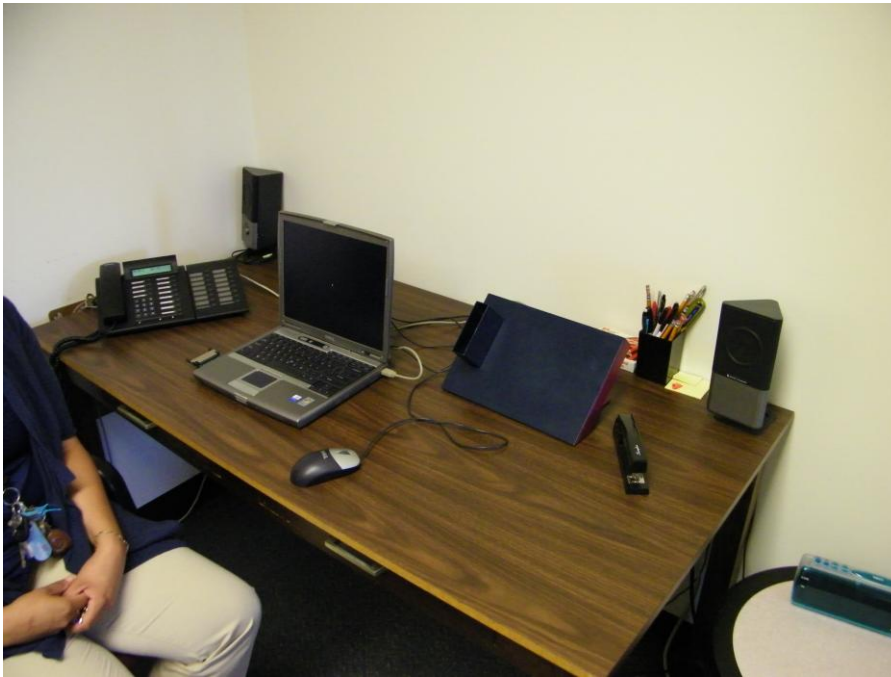


Figure 1.

10. I will refer to this as the “WinEDS laptop”: it is an ordinary laptop computer, running the Microsoft Windows XP operating system, and on which is installed the WinEDS application. WinEDS is software sold by Sequoia Voting Systems for the purpose of programming ballot definitions (which are electronic files), for writing these ballot definitions into voting-machine cartridges, and for tabulating election results.

Erasure of evidence from the hard drive of the WinEDS computer

11. During my examination of this computer I took many photographs, as permitted by the Order. Upon returning to my office later on August 17th and reviewing my photographs, I noticed that the laptop computer had been tampered with, in a way that I will describe.

12. Part of my examination of this laptop computer was to determine whether it contained security vulnerabilities that might have permitted unauthorized persons (perhaps “hackers” on the Internet) to tamper with ballot definitions. The Opinion of Judge Linda Feinberg of the Superior Court (Law Division) dated February 1, 2010 [henceforth, Feinberg Opinion] requires “**HARDENING GUIDELINES ANTI-VIRUS SOFTWARE**” to be implemented. The purpose of these “hardening guidelines” is to reduce the number of security vulnerabilities in WinEDS laptops. For example, “hardening” might include changing the software settings of the Microsoft Windows operating system on a computer so that no one can log into the computer from an external network.

13. Page 187 of the Feinberg Opinion requires,

Chapter Eight of the Sequoia Voting Systems, Election Management System Manual, entitled “Additional Security Guidelines,” dated March 5, 2008, identifies steps to take to ensure an election tabulation environment as free from outside contamination as possible. It specifically recommends that certain steps be taken.

This document is under seal. Therefore, the court will not disclose the specific recommendations. Based on the testimony adduced at trial, Sequoia recommends customers to install both hardening and anti-virus applications. Additionally, customers are advised that laptops not be connected to the Internet or be used for any other purpose. The record reflects that New Jersey has not adopted any of the hardening guidelines and that anti-virus software, if installed, is done so sporadically.

According to Sequoia, hardening techniques and anti-virus software are available at little or no cost to the State. This shall be completed on or before the 120 days set forth in the prior section.

14. During the trial of Gusciora v. Corzine I examined, under seal, the “Additional Security Guidelines” that Judge Feinberg refers to. I will not disclose the specific recommendations. However, I am generally familiar with the kinds of “hardening guidelines” that the Microsoft Corporation, or the National Institute of Standards and Technology,

recommend for those users who wish to tighten the security settings of their Windows computers, and I can say that the Sequoia recommendations are similar in many ways to those guidelines.

15. Judge Feinberg's Opinion describes the process by which the Sequoia "hardening guidelines" would be installed on a WinEDS laptop computer. In describing the testimony of Edwin Smith (Vice President of Sequoia Voting Systems Inc.), pages 76-77 of the Feinberg Opinion contain,

QUESTION: How much time is involved for, say, a medium-sized county to wipe out their WinEDS computers and then reinstall a clean copy of the WinEDS program?

ANSWER: Time, medium size county. To reinstall.

COURT: Well, if he has any personal knowledge. How long does it take to reinstall WinEDS on a machine?

WITNESS: I have seen it done in four hours for a medium-size county, several hundred thousand registered voters.

16. That is, the process of installing the "hardening guidelines" is to "wipe out" the WinEDS computer, that is, (1) erase everything from the hard drive; (2) install a clean copy of the Windows operating system; (3) change several of the "security settings" of Windows, (4) install the WinEDS application program. Steps (1) and (4) are described explicitly in the Question/Answer dialog from Judge Feinberg's opinion. I have personal technical knowledge, both in general (regarding standard industry practice) and from my review in 2009 of Sequoia's hardening guidelines, that all four steps would be included in the process of installing "hardening guidelines."

17. During my examination on August 17th, 2011: to determine whether any sort of hardening guidelines had been installed, I reviewed the "Local Security Policy" accessible through the "Control Panel" of the Windows operating system. Upon a review of the photographs that I took of these "Local Security Policy" settings, it is clear that some sort of "hardening guidelines" have been applied, and everything I observe there is consistent with my understanding of the Sequoia-recommended hardening guidelines.

18. Some of the security settings that I observed in the "Local Security Policy" direct the Windows operating system to log certain events that are not normally logged in the default settings as Windows comes "from the factory." Therefore I also examined the log files for these events. I did this by selecting "Event Viewer" from the Control Panel.

19. Figure 2 shows the "System" event log. The most recent event in this log took place on 8/17/2011 at 11:10 a.m., and the oldest event took place on 8/16/2011 at 3:04 p.m.

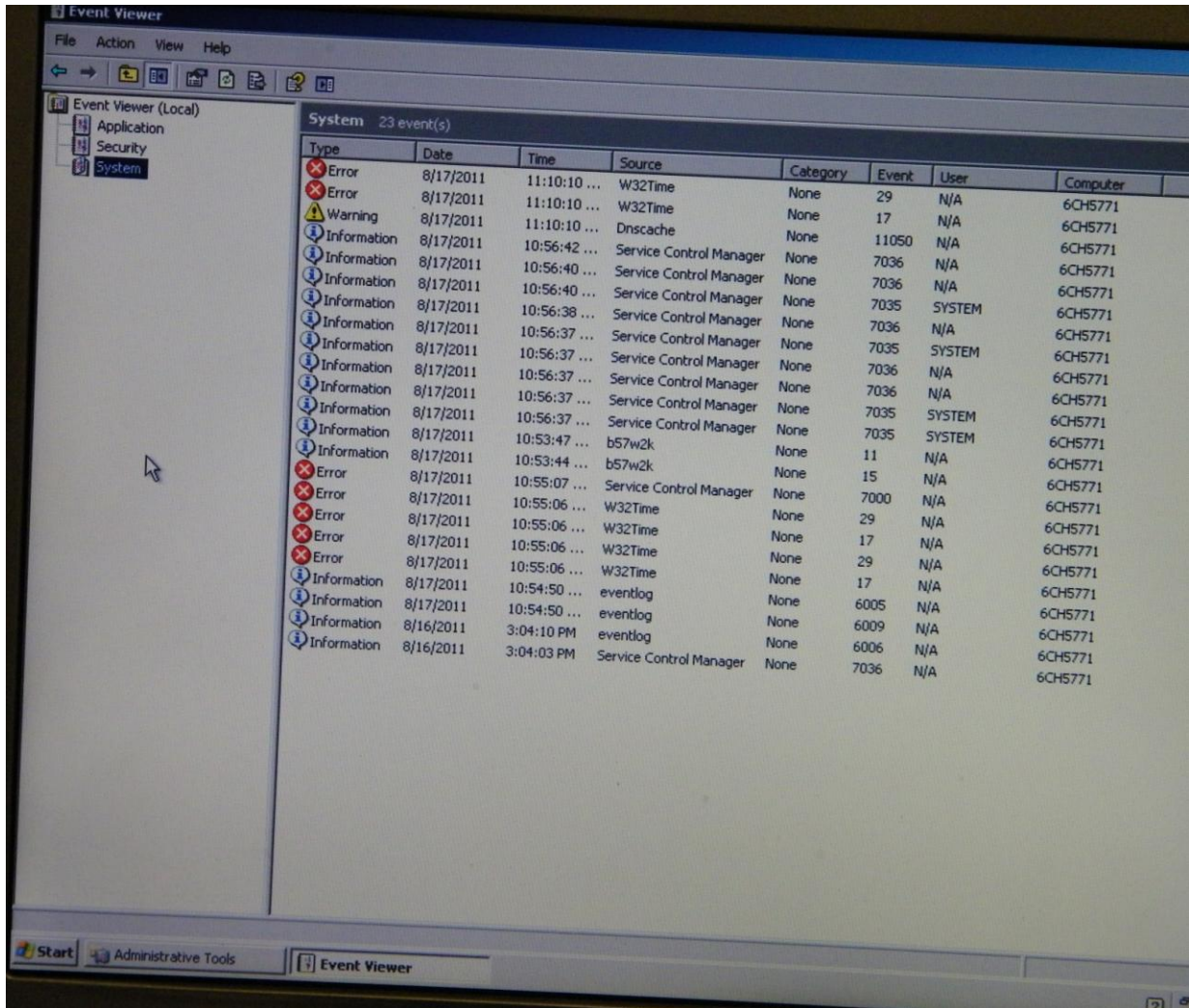


Figure 2

20. Similarly, the “Security” event log (not illustrated here) has several hundred entries, the newest at 8/17/2011 at 11:09 a.m., and the oldest on 8/16/2011 at 3:03 p.m.

21. Both logs start on Tuesday afternoon just after 3 p.m. the day before my examination. The date of my examination was arranged several days in advance.

22. I can find only 3 possible hypotheses that, from a technical point of view, can explain the state of these logs:

- a. The “hardening guidelines” (as described by Mr. Edwin Smith in his testimony) were applied to this computer on the afternoon of August 16, 2011, the day before my examination.

b. Until August 16th at approximately 3pm, logging was not enabled, but then on August 16th logging was turned on for the first time, and then events started to be recorded in the logs.

c. Logging had been turned on before August 16th, but on August 16th the logs were erased. (Erasing the logs can be done by an Administrator of the machine, sitting at the console.)

23. I regard hypothesis (a) as the most likely, and I regard hypotheses (b) and (c) as unlikely. There would be no good reason to perform action (c) in isolation, and (in standard industry practice) action (b) would most likely be performed in the context of an organized installation of hardening guidelines, that is, my hypothesis (a).

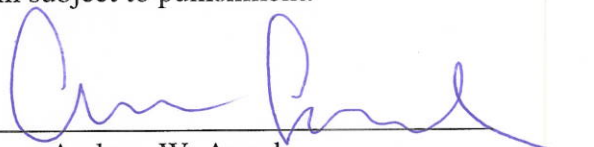
24. Further examination of the computer by an expert could distinguish between these hypotheses.

25. The standard installation of hardening guidelines, consistent with standard industry practice (according to my own knowledge) and with Mr. Smith's testimony about Sequoia's own hardening guidelines, is that the computer's hard drive is "wiped" (erased) before proceeding with the rest of the installation. If indeed the full "hardening guidelines" were installed on August 16th that means that evidence on this computer relevant to the ballot definition for an election in District 3 would also have been erased.

26. The erasure of this evidence hampers my ability to fully examine the technical issues relevant to this case. For example, I cannot fully investigate the sequence of actions performed on this computer during the month when the ballot definition for the primary election was prepared. I cannot fully investigate whether an unauthorized person connected to this machine over a computer network, or whether such person altered any data (including ballot definitions). If indeed the hardening guidelines were installed on August 16th, then such evidence would have been erased on the day before my examination.

I certify that the foregoing statements made by me are true. I am aware that if any of the foregoing statements made by me are willfully false, I am subject to punishment.

Dated: August 18, 2011


Andrew W. Appel

Pursuant to the provisions of *R. 1:4-4, I*, Samuel J. Serata, Attorney for Petitioners, hereby certify that Andrew W. Appel acknowledged the genuineness of the above signature and that a copy with the original signature will be filed if requested by the Court.

Dated: August 18, 2011

Samuel J Serata