



black hat[®]

USA 2018

AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS



 #BHUSA / @BLACKHATEVENTS



Lesson Learned from Virginia

A Comparative Forensic Analysis of WinVote Voting Machines

Carsten Schürmann

IT University of Copenhagen
DemTech Group

August 7, 2018

DEMTECHGROUP

DEMOCRACY, TECHNOLOGY & TRUST

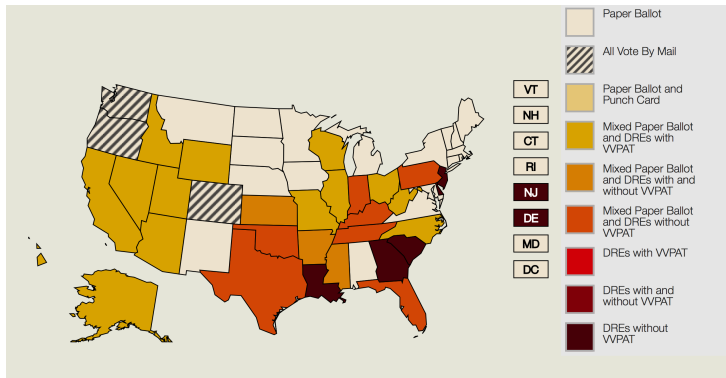
Article 21.3, Declaration of Human Rights

The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.



UNITED NATIONS

Electronic Voting Technologies, 2018 Midterm Election

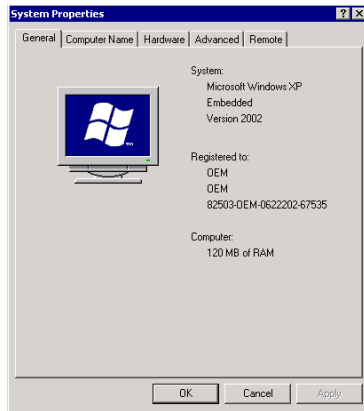


The WinVote Voting Machine



A Few Facts

- ▶ Used pervasively in Virginia (2004-2014)
- ▶ Ca. 4000 units deployed
- ▶ For this study, we secured 8 units, two SSD disks per unit, one small (32MB) and one large (384MB or 512MB)
- ▶ Open ports: 135, 139, 445, 3389, etc.
- ▶ Vulnerable to CVE-2003-0352, MS03-026
- ▶ Security Analysis [VITA Report '15]
- ▶ Status: Decommissioned



Has Someone Interfered with the Operation of this Machine?



Setup

We have no access

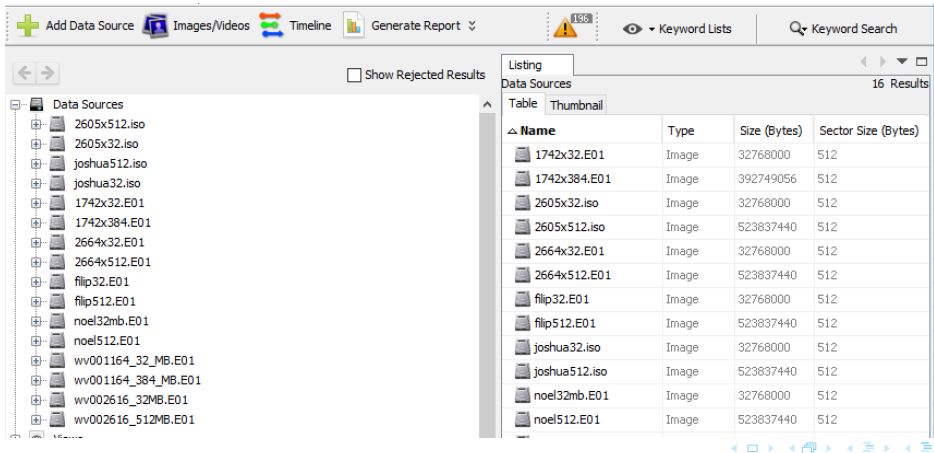
- ▶ to memory/memory dumps
- ▶ to who connected wirelessly to the WinVote
- ▶ to security event logs (which are empty)

But we have access

- ▶ to other event logs
- ▶ to forensic images of the SSD drives



Comparative Forensic Analysis of Eight Machines



The screenshot shows the Black Hat Forensic software interface. The top toolbar includes buttons for 'Add Data Source', 'Images/Videos', 'Timeline', 'Generate Report', and a 'Keyword Search' section with a search icon and a 'Keyword Lists' dropdown. A warning icon with the number '196' is also present.

The main window is divided into two panes. The left pane, titled 'Data Sources', shows a tree view of the loaded data sources:

- 2605x512.iso
- 2605x32.iso
- joshua512.iso
- joshua32.iso
- 1742x32.E01
- 1742x384.E01
- 2664x32.E01
- 2664x512.E01
- flip32.E01
- flip512.E01
- noel32mb.E01
- noel512.E01
- wv001164_32_MB.E01
- wv001164_384_MB.E01
- wv002616_32MB.E01
- wv002616_512MB.E01

The right pane, titled 'Listing', shows a table of 16 results. The table has columns for 'Name', 'Type', 'Size (Bytes)', and 'Sector Size (Bytes)'. The data is as follows:

| Name | Type | Size (Bytes) | Sector Size (Bytes) |
|---------------|-------|--------------|---------------------|
| 1742x32.E01 | Image | 32768000 | 512 |
| 1742x384.E01 | Image | 392749056 | 512 |
| 2605x32.iso | Image | 32768000 | 512 |
| 2605x512.iso | Image | 523837440 | 512 |
| 2664x32.E01 | Image | 32768000 | 512 |
| 2664x512.E01 | Image | 523837440 | 512 |
| flip32.E01 | Image | 32768000 | 512 |
| flip512.E01 | Image | 523837440 | 512 |
| joshua32.iso | Image | 32768000 | 512 |
| joshua512.iso | Image | 523837440 | 512 |
| noel32mb.E01 | Image | 32768000 | 512 |
| noel512.E01 | Image | 523837440 | 512 |

Forensic Objectives

- ▶ Did anyone access the machine exploiting known vulnerabilities?
- ▶ Did anyone install rootkits/malware?
- ▶ Did anyone use the voting machines for other purposes?
- ▶ Did anyone mock with the binaries?

The First Impression

| | | | | |
|-------------------------|----------------|-------------------------|--------------------|--|
| Removable Disk (D:).lnk | D:\ | 2004-07-25 22:53:09 PDT | 2664x512.E01 | |
| Removable Disk (D:).lnk | D:\ | 2004-07-25 22:53:09 PDT | wv002616_512MB.E01 | |
| Removable Disk (D:).lnk | D:\ | 2004-07-25 22:53:09 PDT | 2605x512.iso | |
| 白雪-千古绝唱.mp3.lnk | D:\白雪-千古绝唱.mp3 | 2004-07-26 18:41:30 PDT | 2664x512.E01 | |
| 白雪-千古绝唱.mp3.lnk | D:\白雪-千古绝唱.mp3 | 2004-07-26 18:41:30 PDT | wv002616_512MB.E01 | |
| 白雪-千古绝唱.mp3.lnk | D:\白雪-千古绝唱.mp3 | 2004-07-26 18:41:30 PDT | 2605x512.iso | |

HexStringsFile MetadataResultsMessageIndexed TextMediaOther Occurrences

Result: 1 of 1Result

←→

Recent Documents

| Type | Value | Source(s) |
|-------------|--|----------------|
| Path | D:\白雪-千古绝唱.mp3 | RecentActivity |
| Path ID | -1 | RecentActivity |
| Date/Time | 2004-07-26 18:41:30 | RecentActivity |
| Source File | /img_2664x512.E01/vol2/Documents and Settings/Administrator/Recent/白雪-千古绝唱.mp3.lnk | |
| Artifact ID | -9223372036854775281 | |

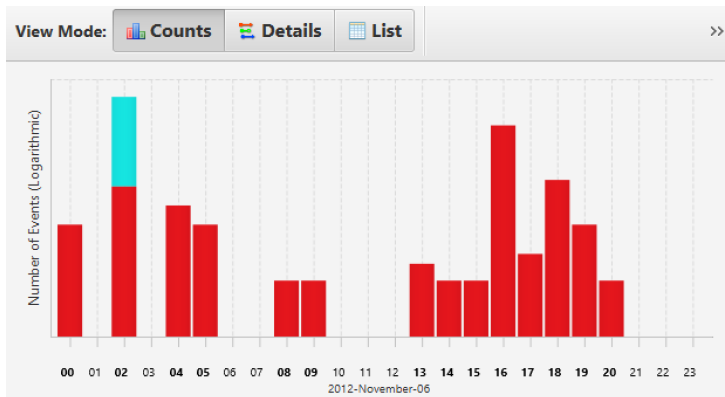
https://www.youtube.com/watch?v=z6rLSF7m__w

We also found ...

... on four WinVote machines

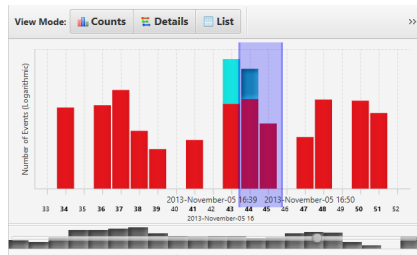
- ▶ Traces of software to rip CDs (No1 CD Ripper)
- ▶ Software to broadcast MP3s (Wingsofts Ancer.exe)

Presidential Election, USA, November 6, 2012



Gubernatorial Election, Virginia, November 05, 2013

- ▶ 60+ files in Windows/System32 flagged as modified (including cmd.exe)
- ▶ WinVote/winvote.exe flagged as modified
- ▶ Time: 16:44-16:45 (Autopsy time)
- ▶ Observed on one machine only








| Virginia Election | Date | # | Irregularities |
|-------------------|-------------|---|---|
| Presidential | Nov 2, 2004 | 5 | NONE |
| Gubernatorial | Nov 8, 2005 | 5 | 3 WinVotes dial out (19:22 no success, 19:26, 19:48 success) |
| Senate | Nov 7, 2006 | 5 | NONE |
| State | Nov 6, 2007 | 5 | NONE |
| Presidential | Nov 4, 2008 | 4 | NONE |
| Gubernatorial | Nov 3, 2009 | 4 | NONE |
| House | Nov 2, 2010 | 3 | NONE |
| State | Nov 8, 2011 | 4 | NONE |
| Presidential | Nov 6, 2012 | 7 | NONE |
| Gubernatorial | Nov 5, 2013 | 7 | 1 Winvote machine 60+ system files flagged as modified |

Evidence-Based Elections

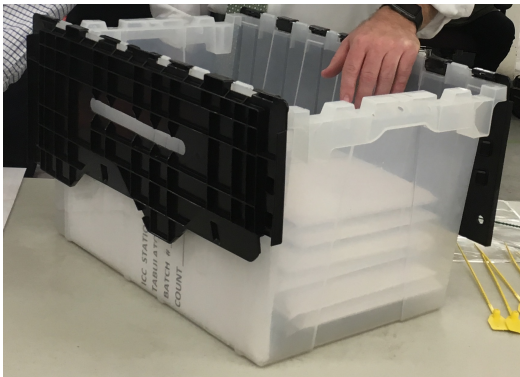
Colorado Presidential Race Results: Hillary Clinton Wins

BY THE NEW YORK TIMES AUG. 1, 2017, 11:23 AM ET

| CANDIDATE | PARTY | VOTES | PCT. | E.V. |
|---|-------------|-----------|--------------|----------|
|  ✓ Hillary Clinton | Democrat | 1,338,870 | 48.2% | 9 |
|  Donald J. Trump | Republican | 1,202,484 | 43.3 | — |
|  Gary Johnson | Libertarian | 144,121 | 5.2 | — |
|  Jill Stein | Green | 38,437 | 1.4 | — |
|  Evan McMullin | Independent | 28,917 | 1.0 | — |
| ▼ Others | | 27,418 | 1.0 | — |

100% reporting (3,040 of 3,040 precincts)

What is better form of evidence?



Building Confidence in an Election Outcome

“Risk-limiting audits provide statistical assurance that election outcomes are correct by manually examining portions of the audit trail —paper ballots or voter-verifiable paper records.” [Stark '12]

Risk Limiting Audit

- ▶ Secured paper trail
- ▶ Ballot manifest
- ▶ Look for statistical evidence that tempering occurred
- ▶ Draws a *truly* random sample and check!
- ▶ Method auto-corrects or in the worst case triggers a full recount

Initial sample size

Contest information

Ballots cast in all contests: Smallest margin (votes): 136,386. Diluted margin: 4.77%.

Contest 1. Contest name:

Winners:

Reported votes:

| Candidate Name | Votes |
|-----------------------------------|----------------|
| Candidate 1 Name: Hillary Clinton | Votes: 1338870 |
| Candidate 2 Name: Donald J. Trump | Votes: 1202484 |
| Candidate 3 Name: Gary Johnson | Votes: 144121 |
| Candidate 4 Name: Jill Stein | Votes: 38437 |
| Candidate 5 Name: Evan McMullin | Votes: 28917 |

Audit parameters

Risk limit:

Expected rates of differences (as decimal numbers):

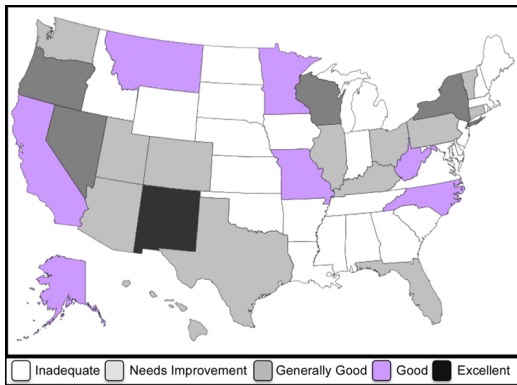
| Overstatements. | 1-vote: | 2-vote: |
|------------------|--|---|
| Understatements. | 1-vote: <input type="text" value="0.001"/> | 2-vote: <input type="text" value="0.0001"/> |

Starting size

☒ Round up 1-vote differences. ☐ Round up 2-vote differences. 142.



Post Election Audits, 2018 Midterm Election



Conclusion

Use Paper and Do Your Audits!