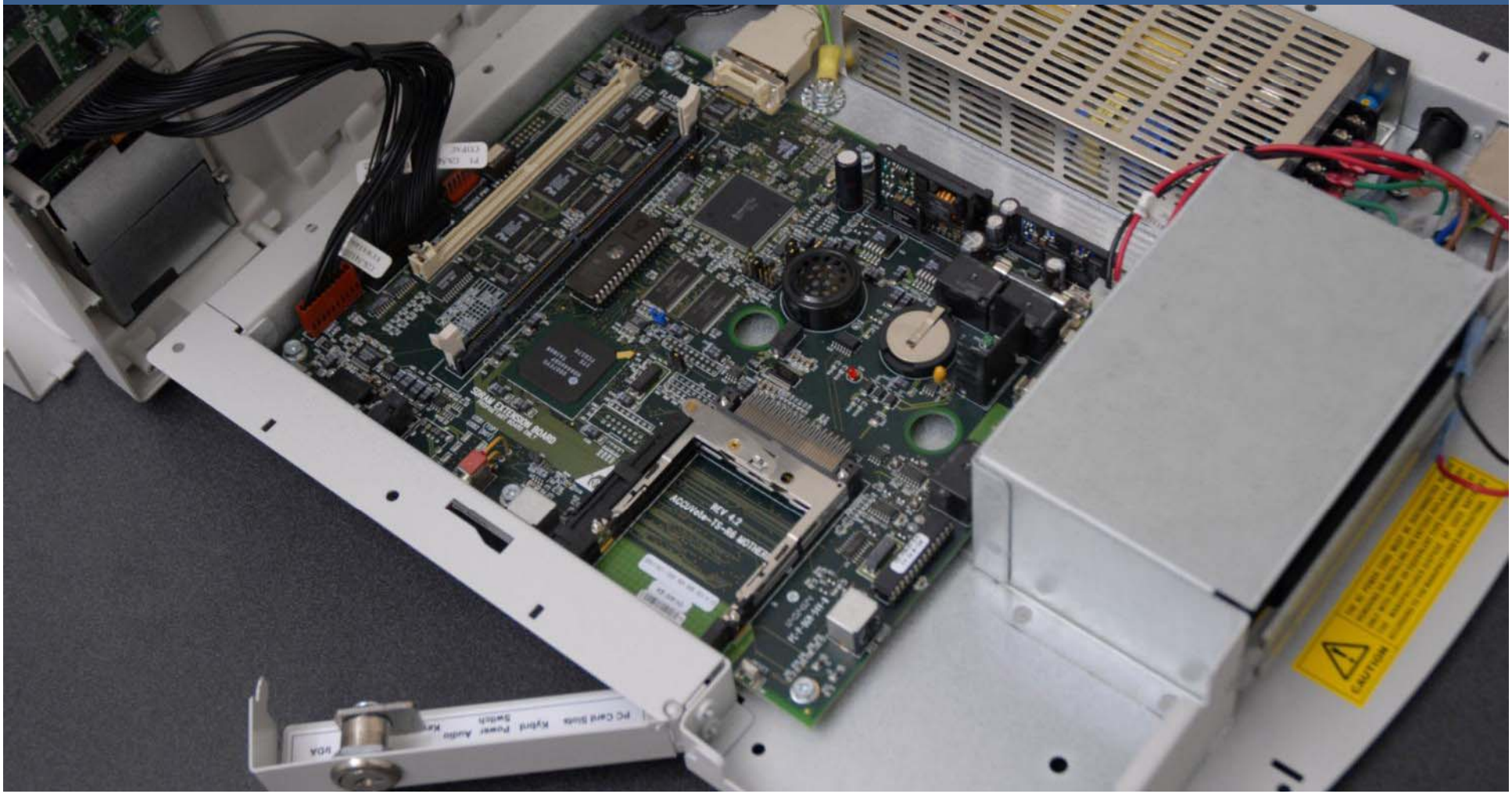
Securing Digital Democracy

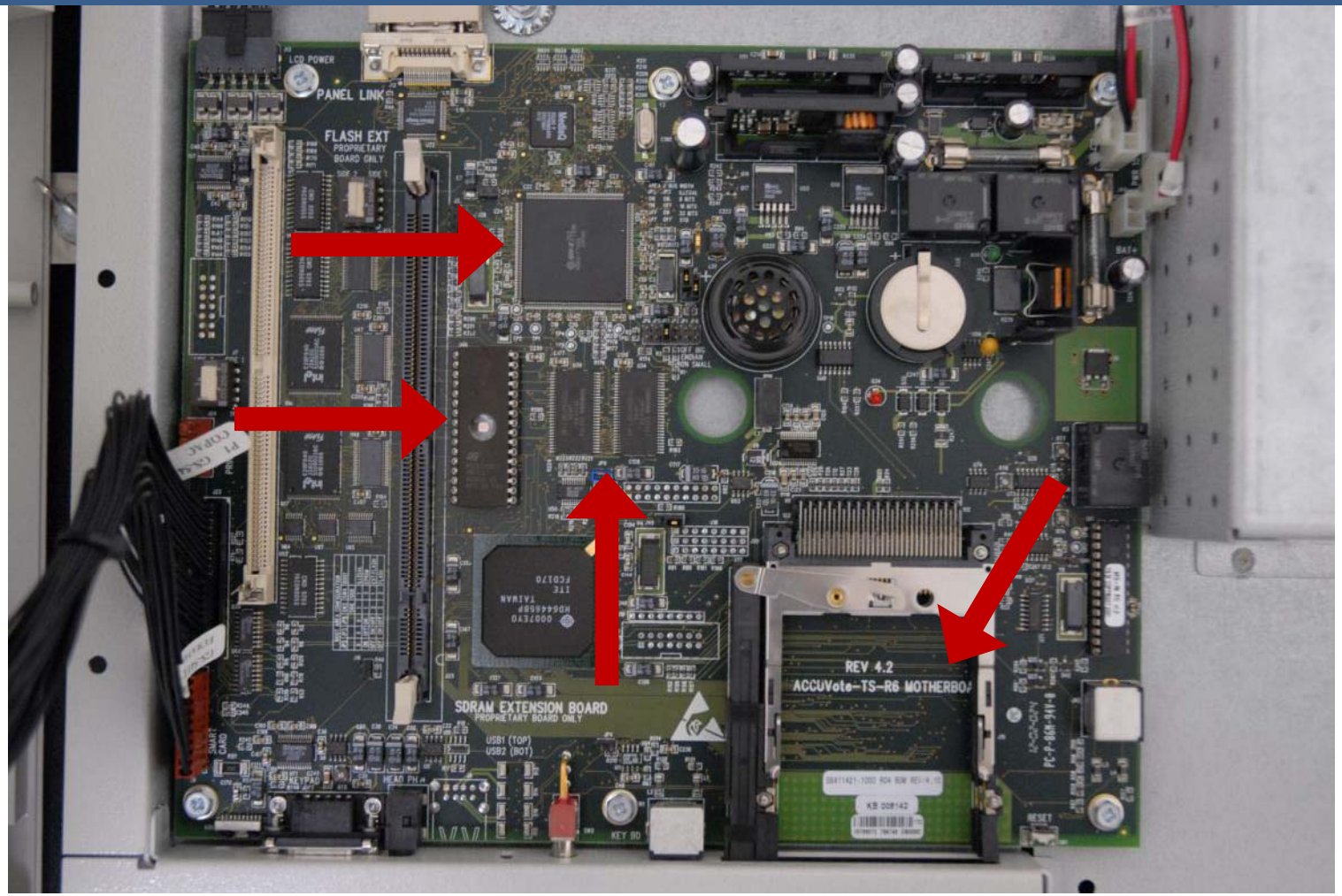
Lecture 4 | *Problems with DREs*

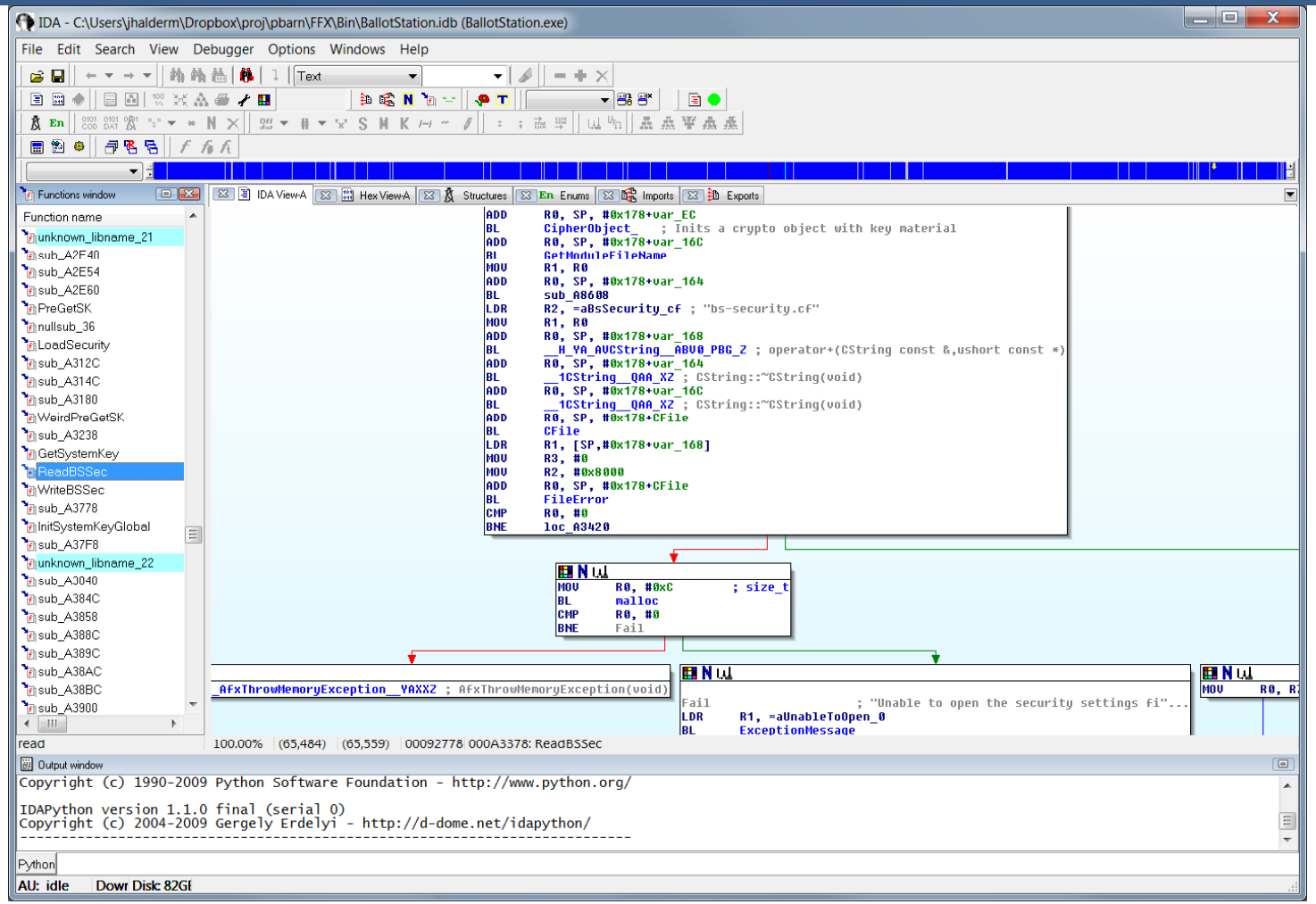
J. Alex Halderman
University of Michigan

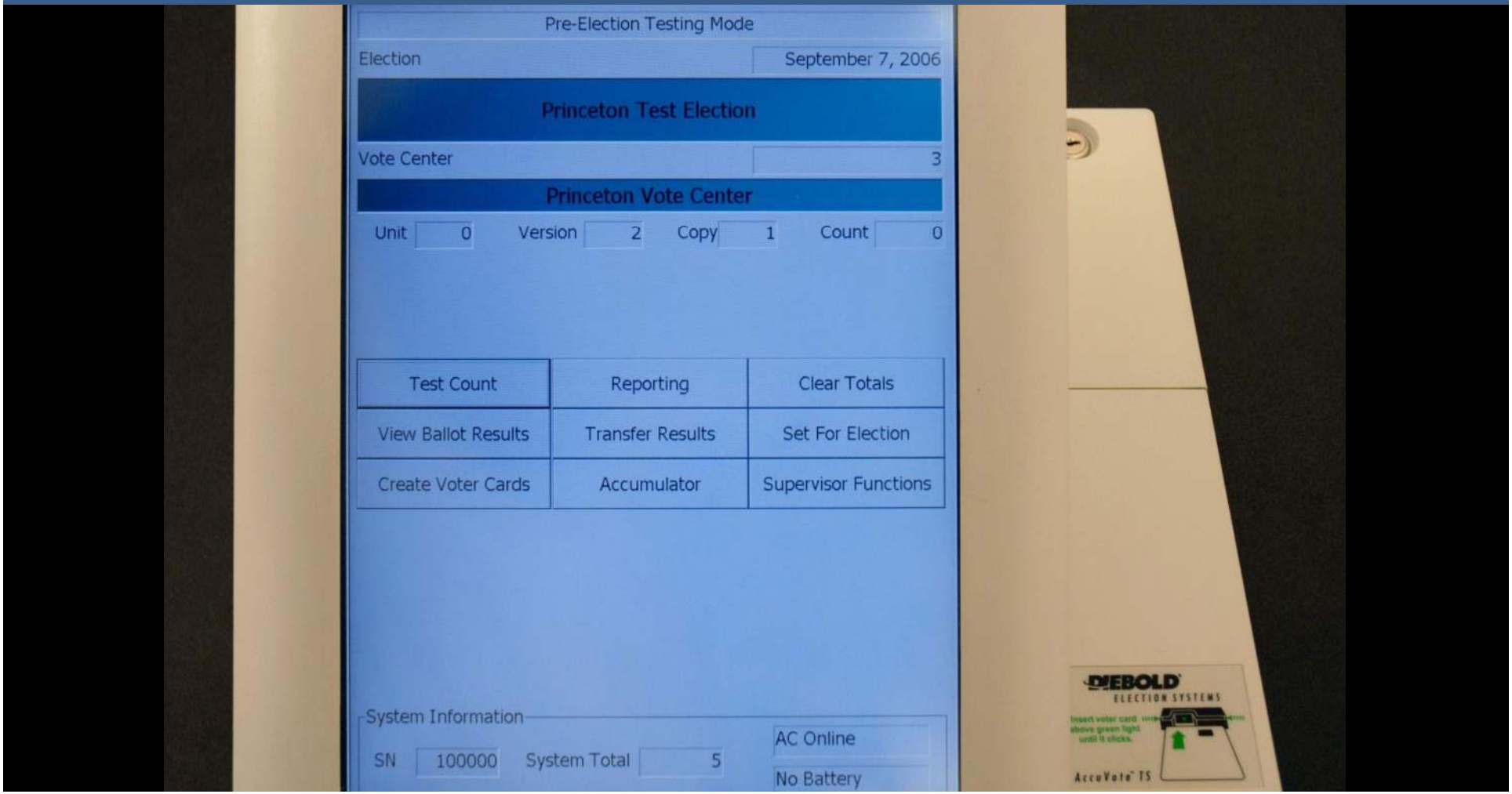
Diebold

Diebold AccuVote-TS

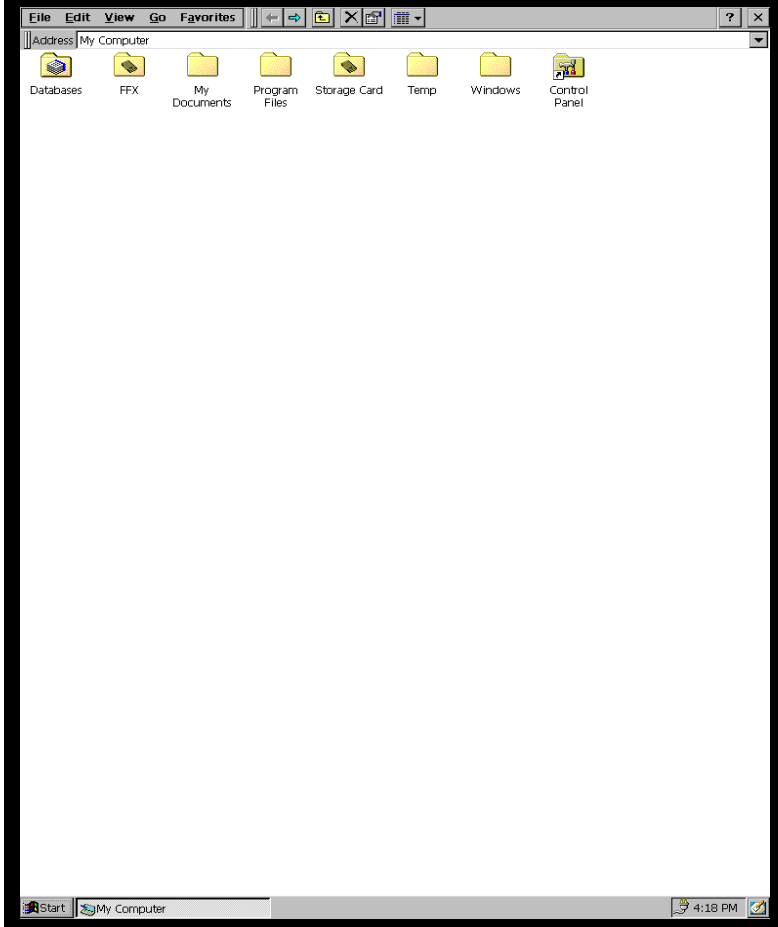

CAUTION

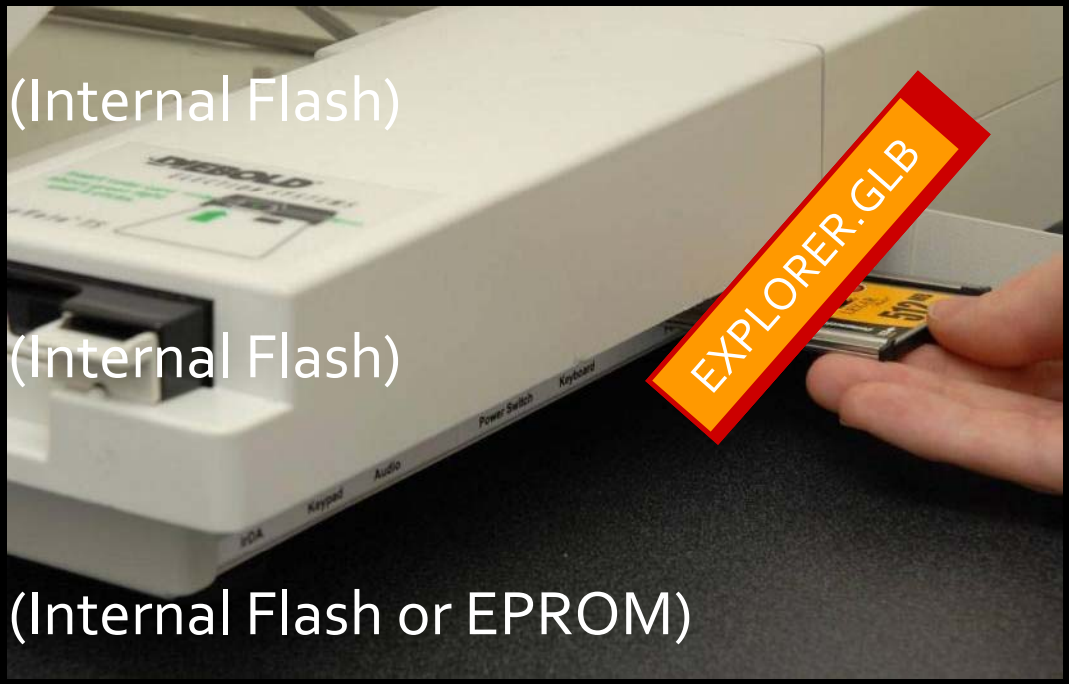

PANEL LINK
FLASH EXT
PROPRIETARY
BOARD ONLY
SDRAM EXTENSION BOARD
PROPRIETARY BOARD ONLY
REV 4.2

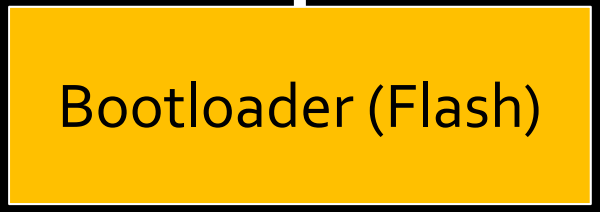

IDA - C:\Users\jhalderm\Dropbox\proj\pbarn\FFX\Bin\BallotStation.idb (BallotStation.exe)
File Edit Search View Debugger Options Windows Help
Functions window
Function name
unknown_libname_21
sub_A2F40
sub_A2E54
sub_A2E60
PreGetSK
nullsub_36
LoadSecurity
sub_A312C
sub_A314C
sub_A3180
WeirdPreGetSK
sub_A3238
GetSystemKey
ReadBSSec
WriteBSSec
sub_A3778
InitSystemKeyGlobal
sub_A37F8
unknown_libname_22
sub_A3040
sub_A384C
sub_A3858
sub_A388C
sub_A389C
sub_A38AC
sub_A38BC
sub_A3900
IDA View-A
Hex View-A
Structures
Enums
Imports
Exports
ADD R0, SP, #0x178+var_EC
BL CipherObject_ ; Inits a crypto object with key material
ADD R0, SP, #0x178+var_16C
BL GetModuleFileName
MOV R1, R0
ADD R0, SP, #0x178+var_164
BL sub_A8608
LDR R2, =aBsSecurity_cf ; "bs-security.cf"
MOV R1, R0
ADD R0, SP, #0x178+var_168
BL __H_YA_AVCString__ABV0_PBG_Z ; operator+(CString const &,ushort const *)
ADD R0, SP, #0x178+var_164
BL __1CString__QAA_XZ ; CString::~CString(void)
ADD R0, SP, #0x178+var_16C
BL __1CString__QAA_XZ ; CString::~CString(void)
ADD R0, SP, #0x178+CFile
BL CFile
LDR R1, [SP,#0x178+var_168]
MOV R3, #0
MOV R2, #0x8000
ADD R0, SP, #0x178+CFile
BL FileError
CMP R0, #0
BNE loc_A3420
MOV R0, #0xC ; size_t
BL malloc
CMP R0, #0
BNE Fail
_AfxThrowMemoryException__YAXXZ ; AfxThrowMemoryException(void)
Fail ; "Unable to open the security settings fi"...
LDR R1, =aUnableToOpen_0
BL ExceptionMessage
MOV R0, R
read
100.00% (65,484) (65,559) 00092778 000A3378: ReadBSSec
Output window
Copyright (c) 1990-2009 Python Software Foundation - http://www.python.org/
IDAPython version 1.1.0 final (serial 0)
Copyright (c) 2004-2009 Gergely Erdelyi - http://d-dome.net/idapython/
Python
AU: idle Down Disk: 82GB

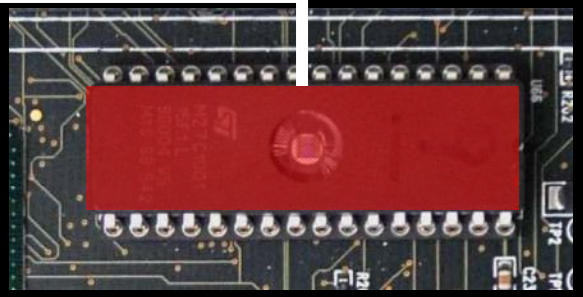

Pre-Election Testing Mode
Election
September 7, 2006
Princeton Test Election
Vote Center
3
Princeton Vote Center
Unit 0
Version 2
Copy 1
Count 0
Test Count
Reporting
Clear Totals
View Ballot Results
Transfer Results
Set For Election
Create Voter Cards
Accumulator
Supervisor Functions
System Information
SN 100000
System Total 5
AC Online
No Battery
DIEBOLD
ELECTION SYSTEMS
AccuVote TS

4.1 Diebold


File Edit View Go Favorites
Address My Computer
Databases
FFX
My Documents
Program Files
Storage Card
Temp
Windows
Control Panel
Start
My Computer
4:18 PM


(Internal Flash)
(Internal Flash)
(Internal Flash or EPROM)
EXPLORER.GLB





Failure in Dep

- Boot into Exp
- Insecure firmwa
- ROM replacement

WHAT COULD GO WRONG?

Primary Vote Record

Backup Vote Record

Audit Log

BallotStation

Stuffer

WinCE Kernel

PRINCETON BALLOT STUFFER DEMO

Select the race and candidate to fix:

President of the United States

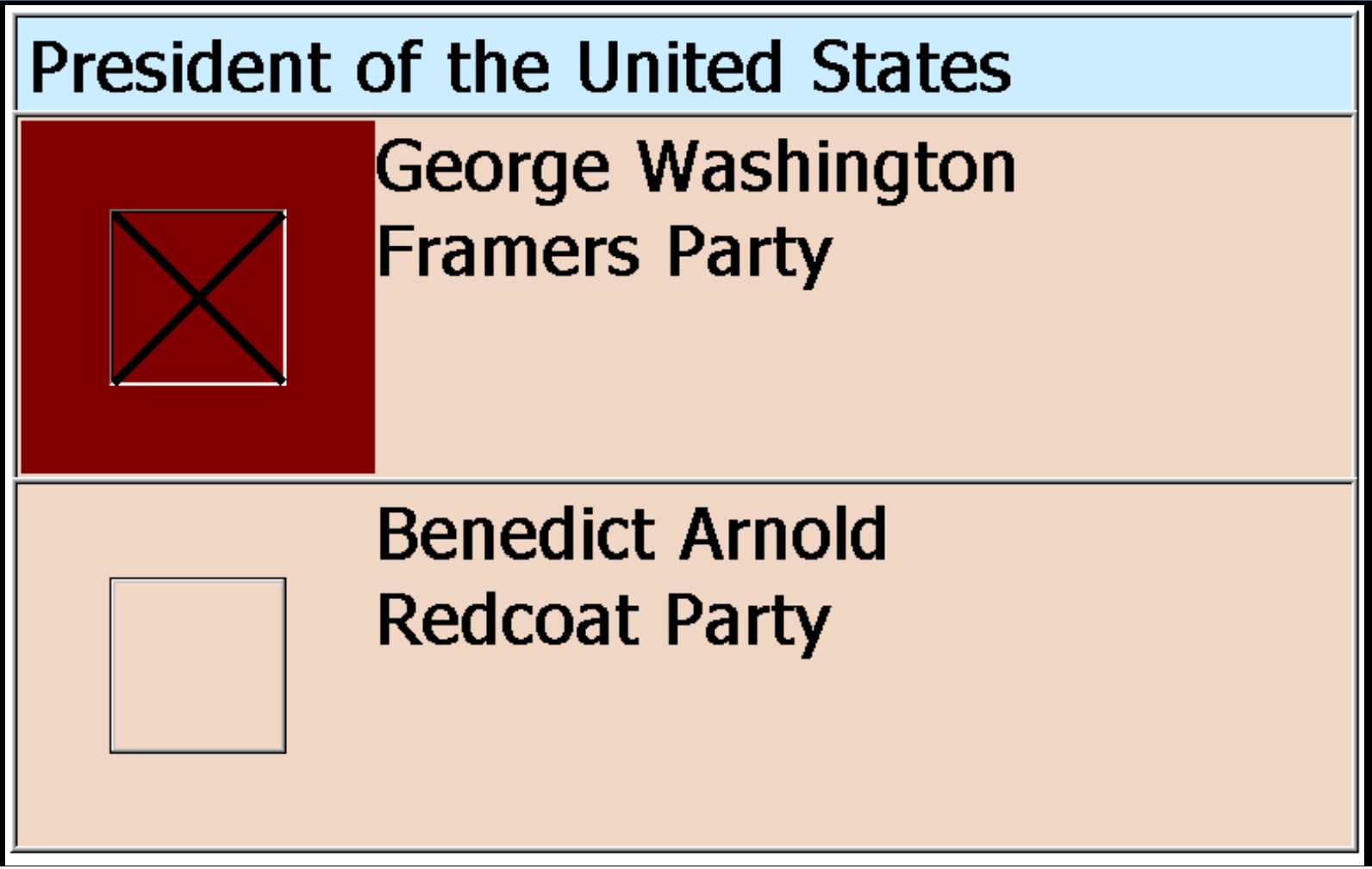
Candidate Name	Votes So Far
George Washington	0 (0%)
Benedict Arnold	0 (0%)

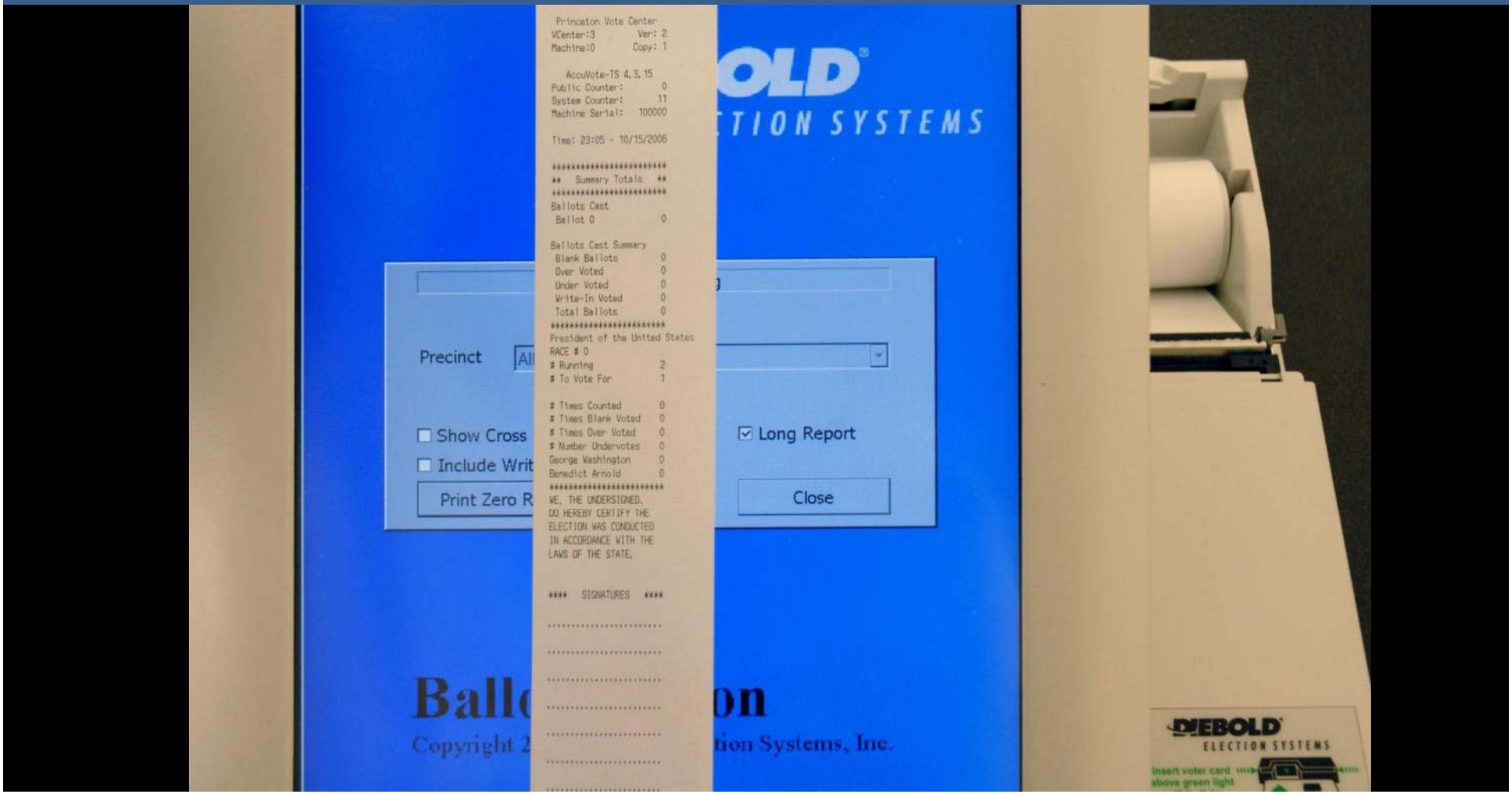
Set the final outcome: Percent for "Benedict Arnold"

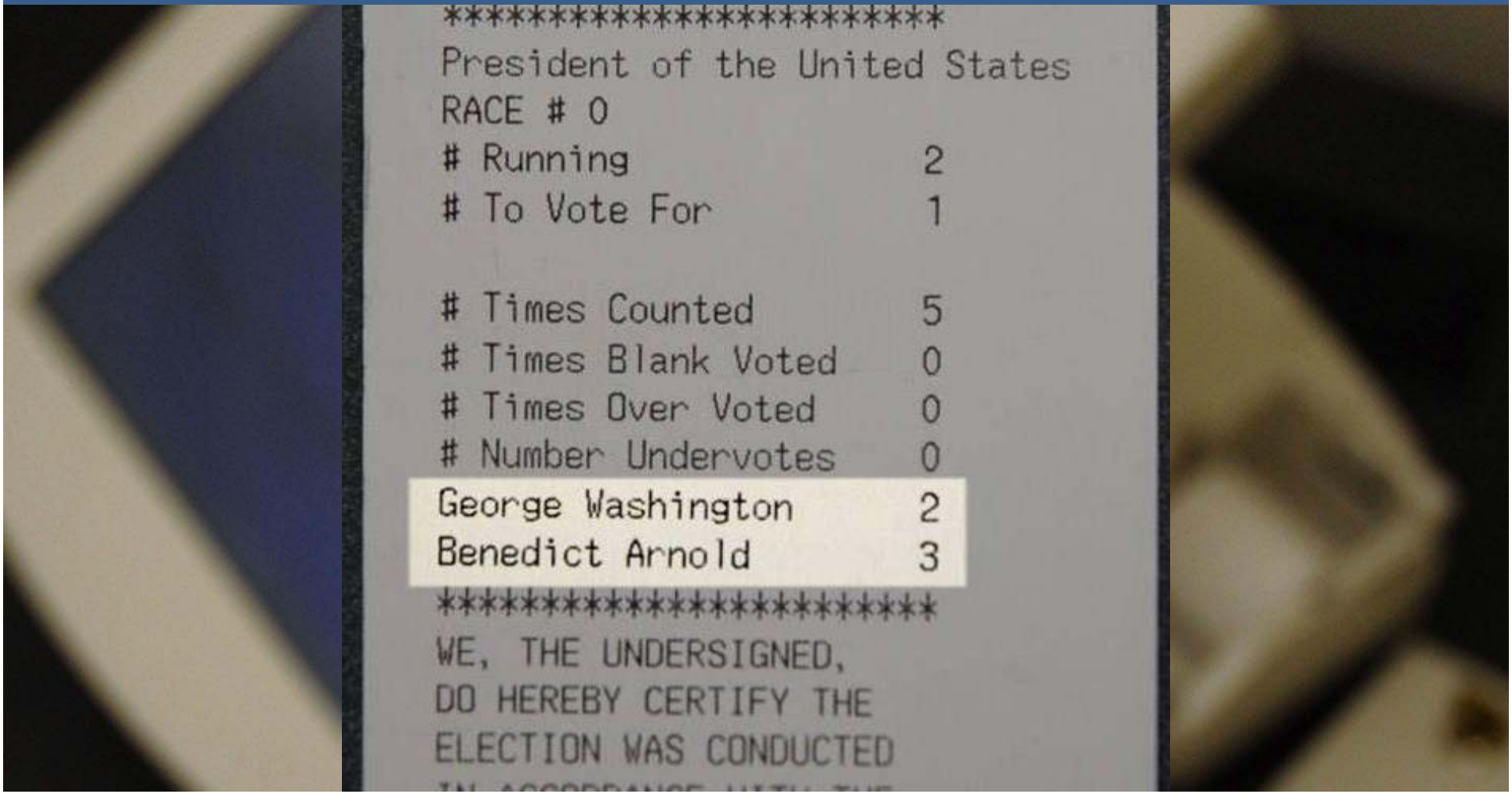
75%

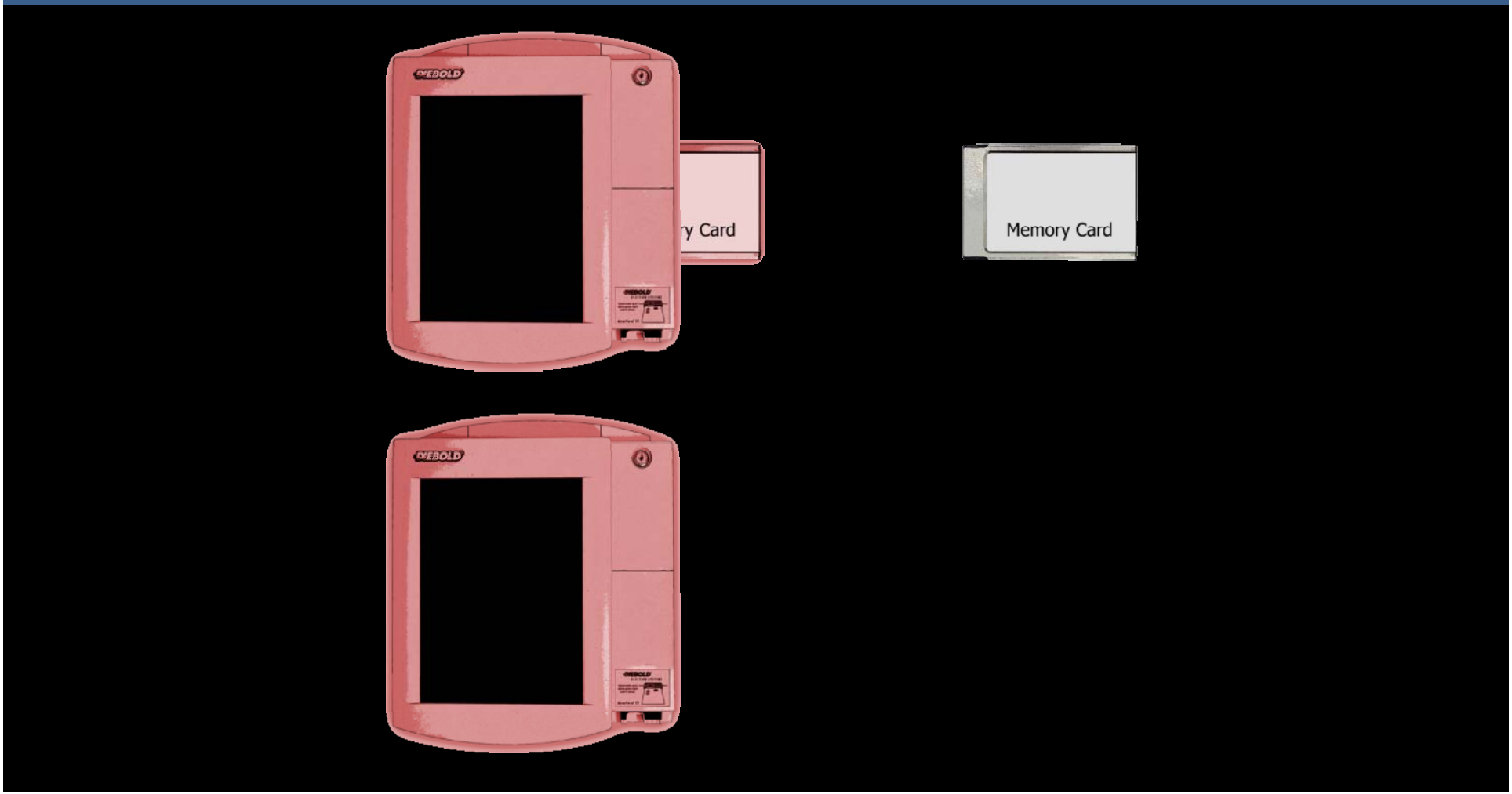
OK

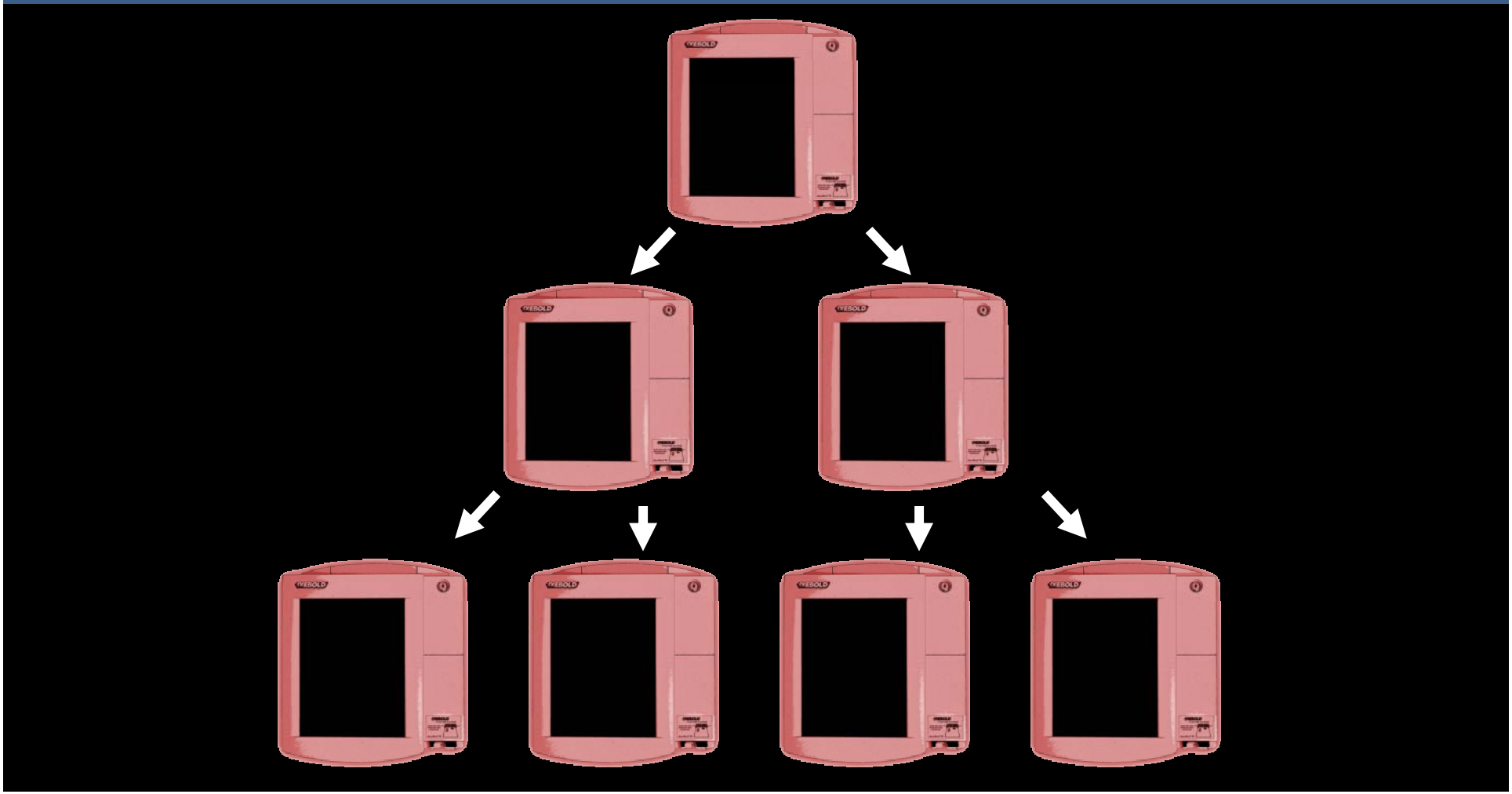
Cancel


President of the United States
George Washington
Framers Party
Benedict Arnold
Redcoat Party

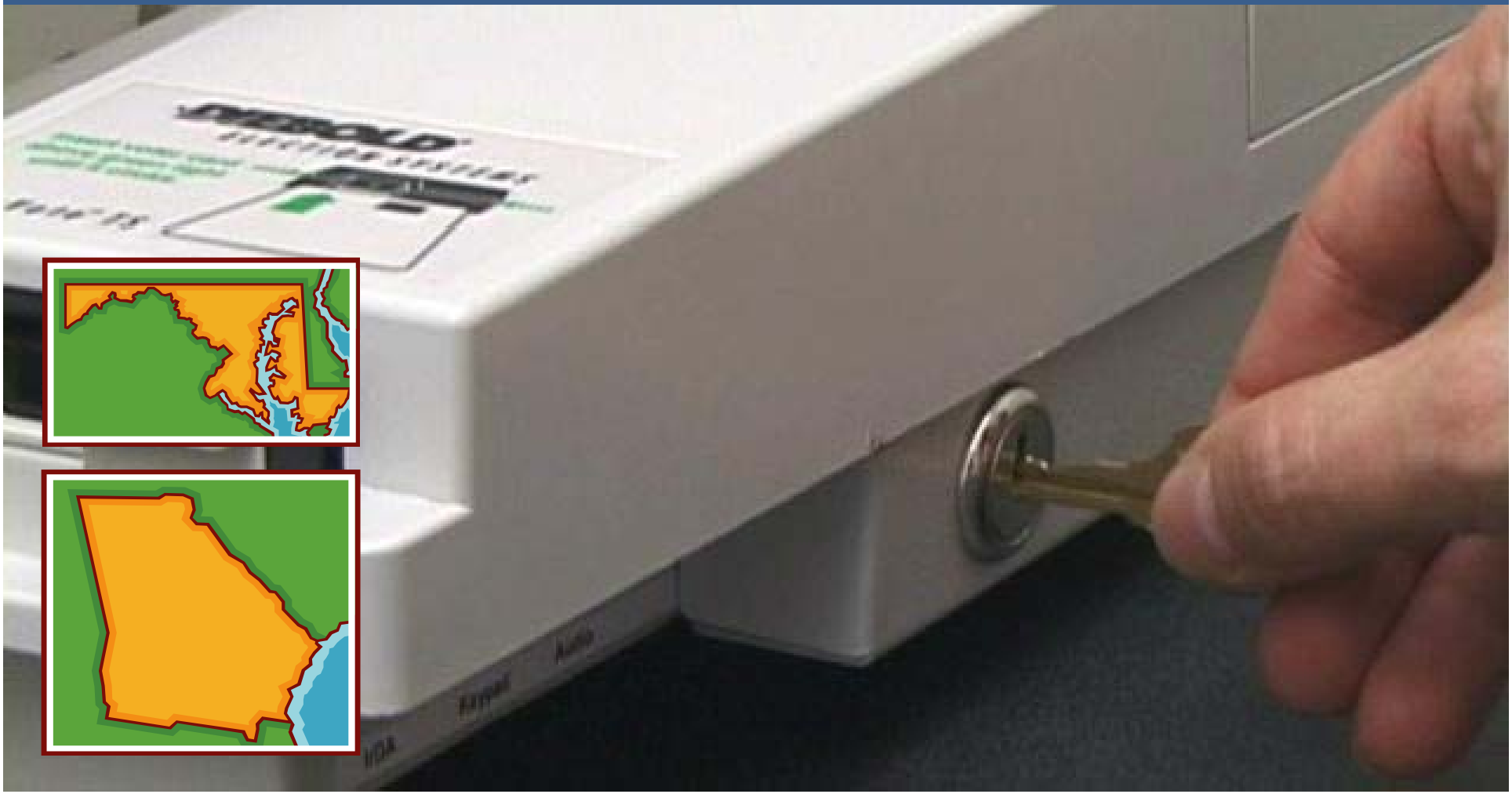

Princeton Vote Center
VCenter:3 Ver: 2
Machine:0 Copy: 1
AccuVote-TS 4.3.15
Public Counter: 0
System Counter: 11
Machine Serial: 100000
Time: 23:05 - 10/15/2006
** Summary Totals **
Ballots Cast
Ballot 0 0
Ballots Cast Summary
Blank Ballots 0
Over Voted 0
Under Voted 0
Write-In Voted 0
Total Ballots 0
President of the United States
RACE # 0
Running 2
To Vote For 1
Times Counted 0
Times Blank Voted 0
Times Over Voted 0
Number Undervotes 0
George Washington 0
Benedict Arnold 0
WE, THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED
IN ACCORDANCE WITH THE
LAWS OF THE STATE.
**** SIGNATURES ****
TION SYSTEMS
Precinct
Show Cross
Include Writ
Print Zero R
Long Report
Close
Copyright
tion Systems, Inc.
DIEBOLD
ELECTION SYSTEMS
Insert voter card
above green light


****
President of the United States
RACE # 0
Running 2
To Vote For 1
Times Counted 5
Times Blank Voted 0
Times Over Voted 0
Number Undervotes 0
George Washington 2
Benedict Arnold 3
****
WE, THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED


DIEBOLD
ry Card
Memory Card
DIEBOLD




WHAT
COULD GO
WRONG?




DIEBOLD
IrDA
Keypad
Audio


Automatic Refreshment Centre
by BARTECH
WICHTIG
IMPORTANT
IMPORTANTE
COORS
LIGHT
Seagram's
Ginger
Coca-Cola
Coke

Transfer & Transport Cases
DIMS-NeT/Voter Registration
Voting Booths & Ballot Boxes

Replacement Access Keys

- 2 keys that allow easy service access to the Tally Printer and replacement battery compartment

GS-567311-1000 **$5.90** USD per set
$6.90 CAD per set

Enter a quantity

add to your order ▸

ORDER BY PHONE 800.769.3246

More Goes Wrong

Source Code Review of the Diebold Voting System

Joseph A. Calandrino
Princeton University[1]

Ariel J. Feldman
Princeton University

J. Alex Halderman
Princeton University

David Wagner[2]
U.C., Berkeley

Harlan Yu
Princeton University

William P. Zeller
Princeton University

July 20, 2007

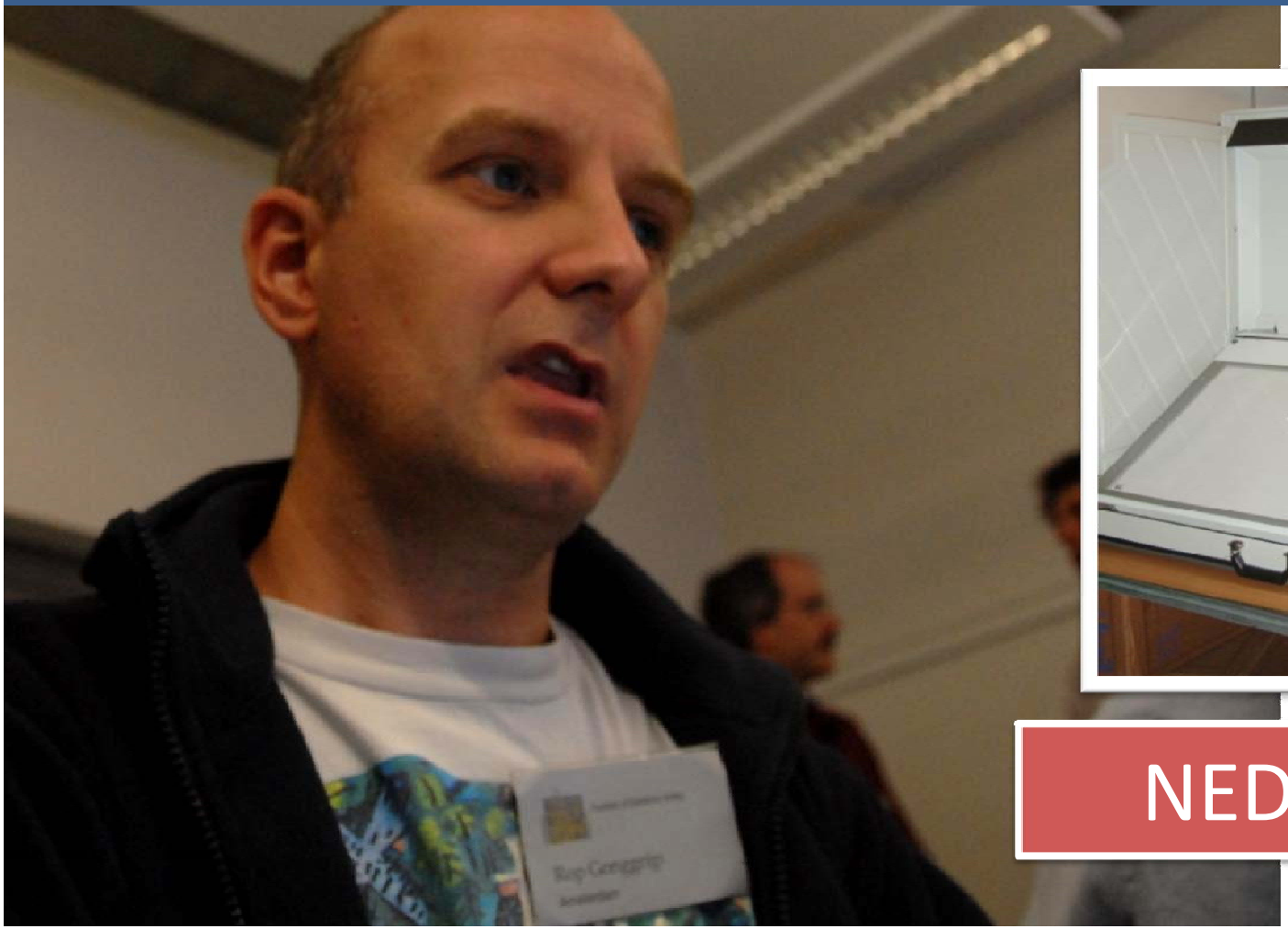
This report was prepared by the University of California, Berkeley under contract to the California Secretary of State as part of a "Top-to-Bottom" review of electronic voting systems certified for use in the State of California.

Available at http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm

Hart

Sequoia

Diebold



NEDAP ES3B

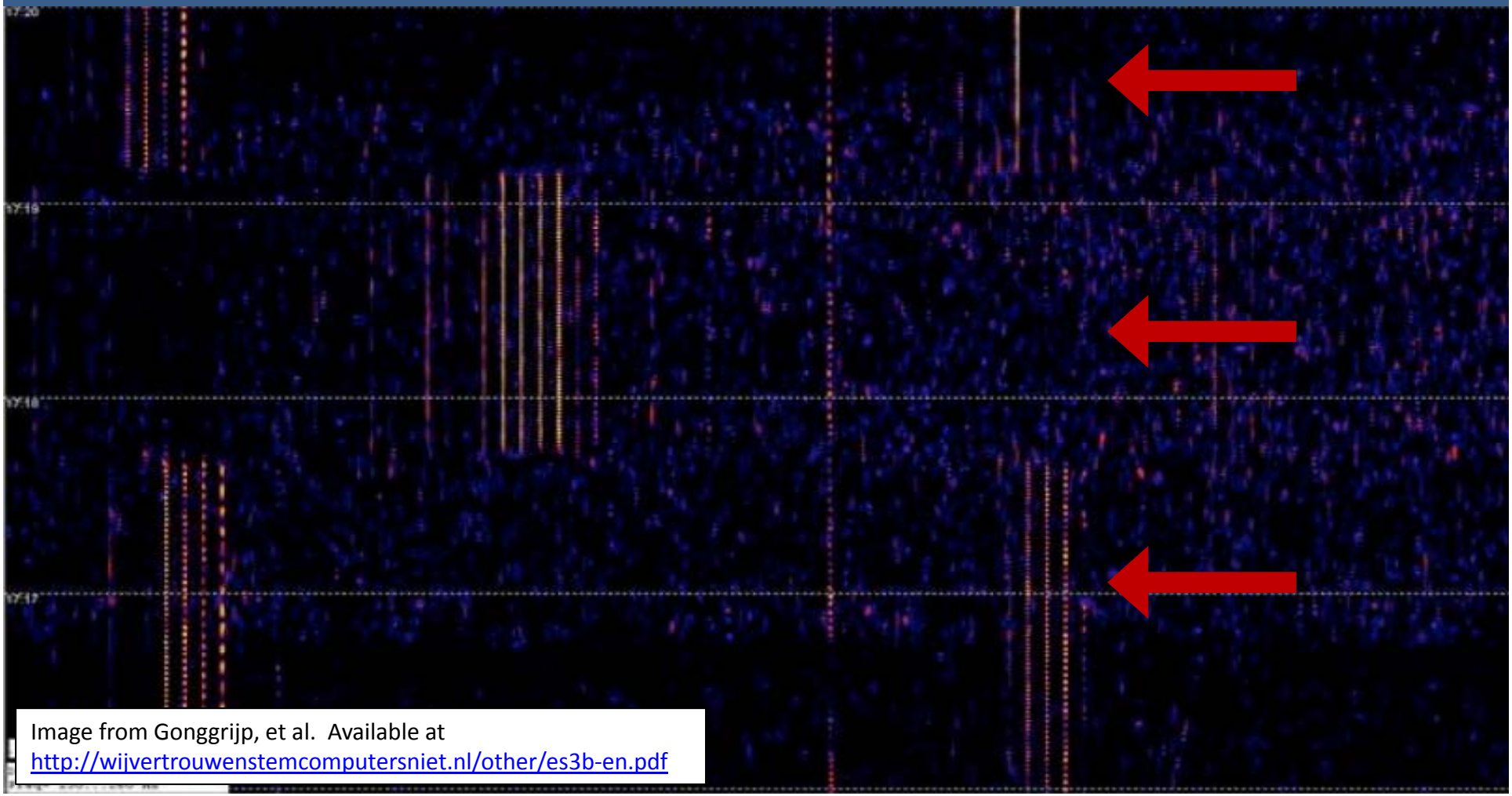
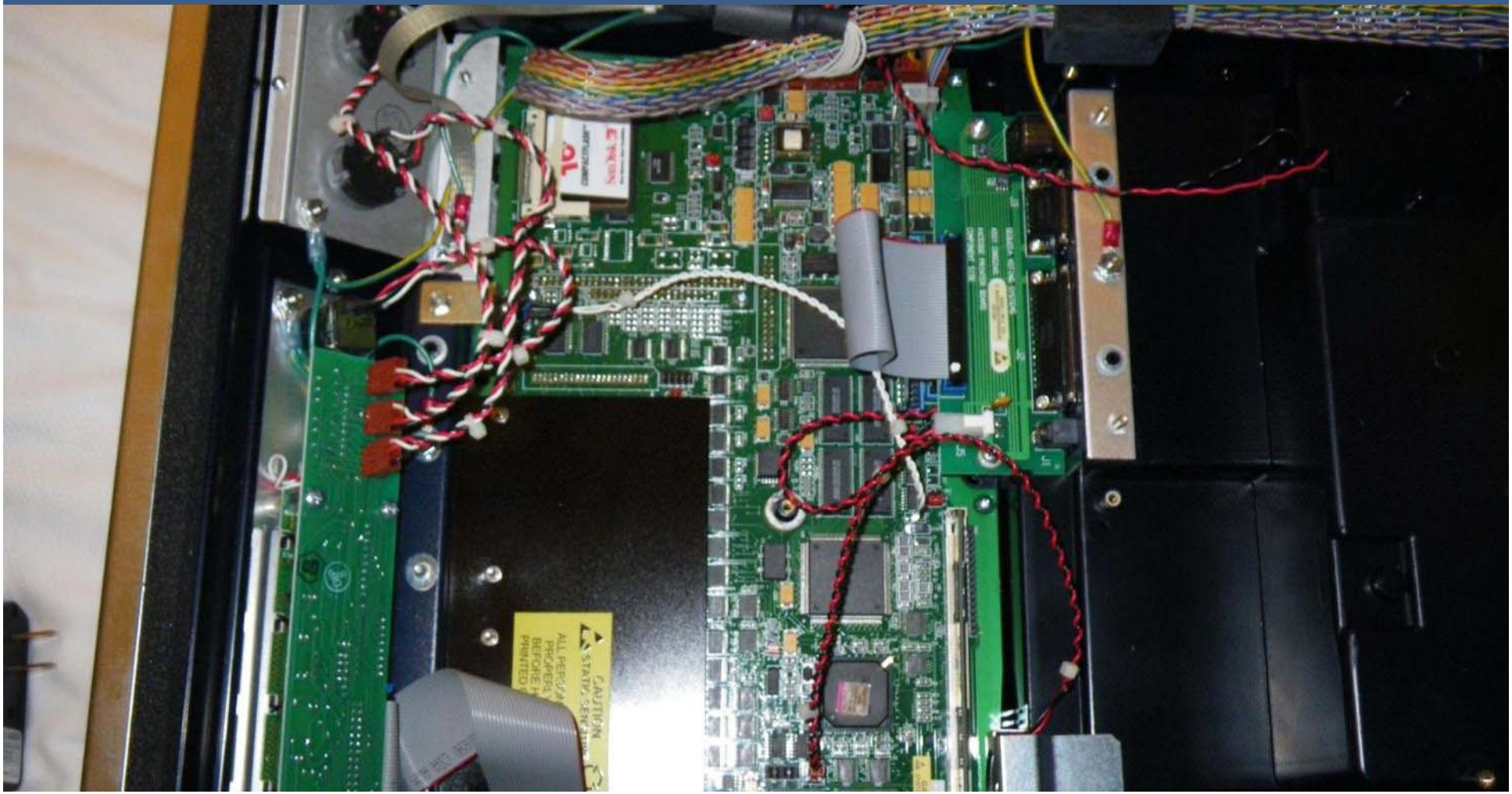


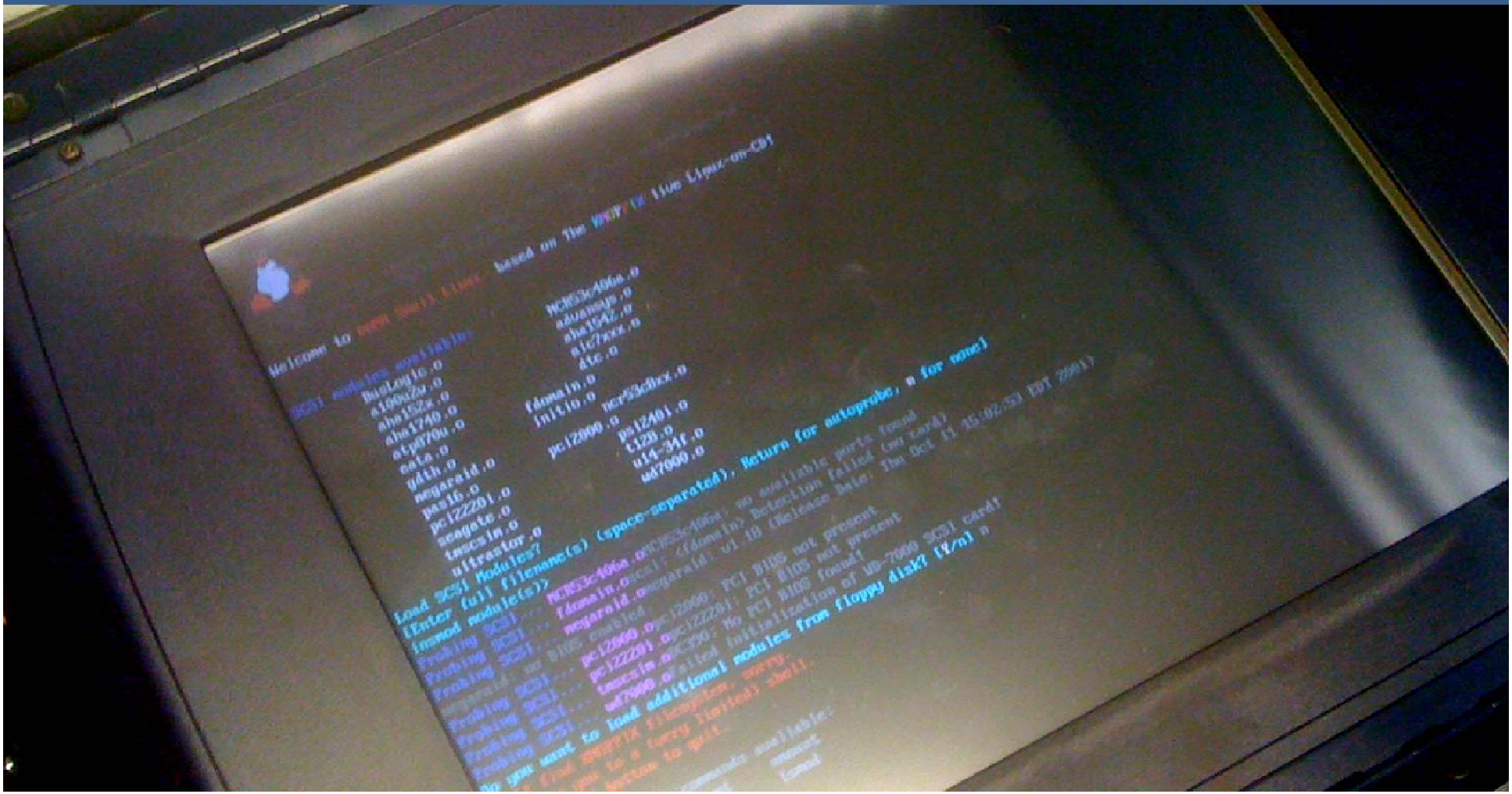
Image from Gonggrijp, et al. Available at http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf

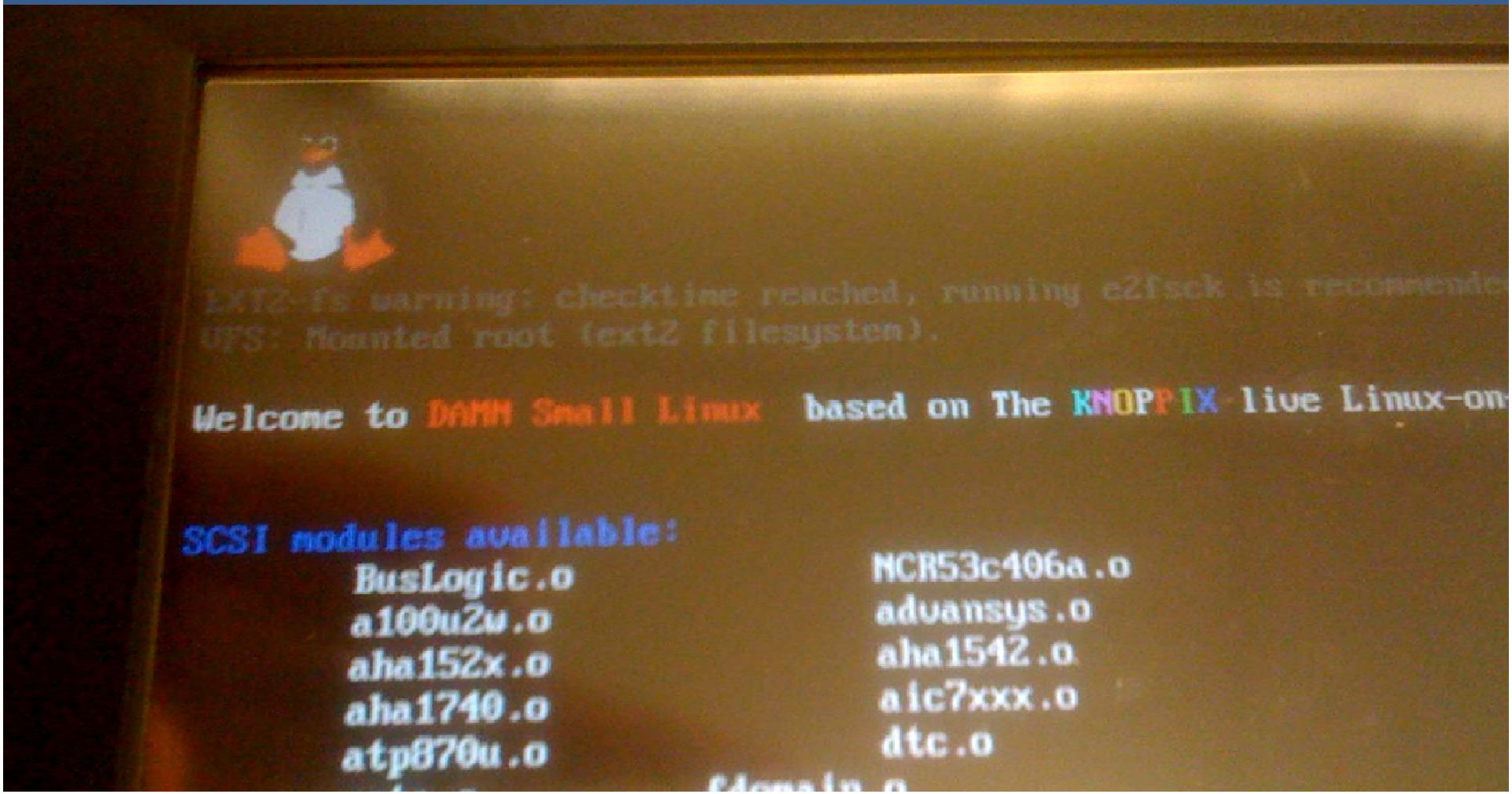
Image from Gonggrijp, et al. Available at http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf

Sequoia AVC Edge




COMPACTFLASH
SanDisk

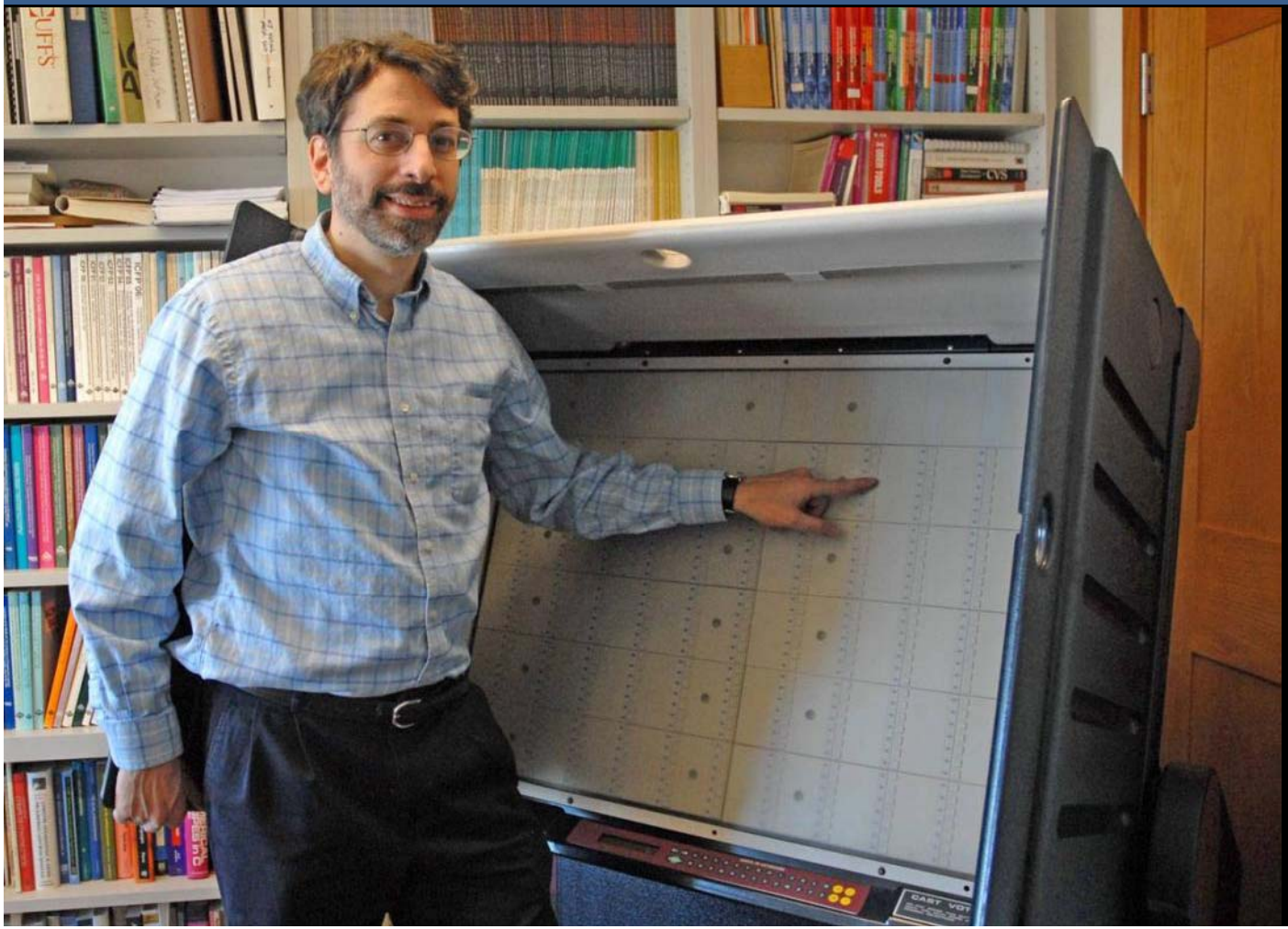

Welcome to
SCSI modules available:
BusLogic.o
a100u2w.o
aha152x.o
aha1740.o
atp870u.o
eata.o
g_t1h.o
megaraid.o
pas16.o
pci22201.o
seagate.o
tmscsim.o
ultrastor.o
NCR53c406a.o
advansys.o
aha1542.o
aic7xxx.o
dtc.o
fdomain.o
initio.o
ncr53c8xx.o
pci2000.o
ps12401.o
t128.o
u14-34f.o
u67000.o
Load SCSI Modules?
[Enter full filename(s) (space-separated), Return for autoprobe, n for none]
insmod module(s)
Probing SCSI...
Probing SCSI... no BIOS enabled
Probing SCSI...
Probing SCSI...
Probing SCSI...
Probing SCSI...
Probing SCSI...
Do you want to load additional modules from floppy disk? [y/n] n


EXT2-fs warning: checktime reached, running e2fsck is recommende
VFS: Mounted root (ext2 filesystem).
Welcome to DAMN Small Linux based on The KNOPPIX live Linux-on
SCSI modules available:
BusLogic.o
a100u2w.o
aha152x.o
aha1740.o
atp870u.o
NCR53c406a.o
advansys.o
aha1542.o
aic7xxx.o
dtc.o

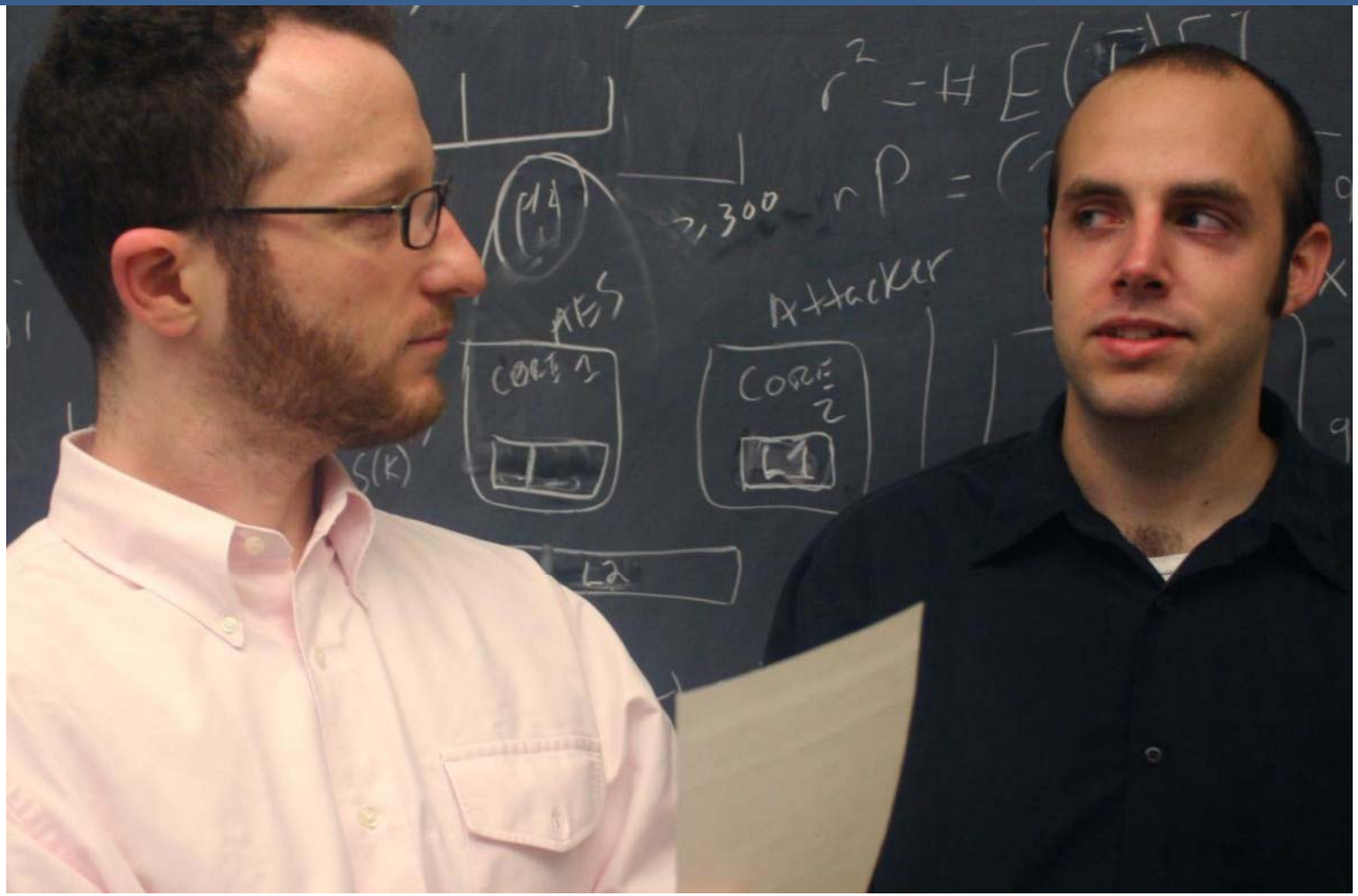

TOUCH
YOU MAY CHANGE
WRITE-IN
CONTINUE
REVIEW
COMPLETE
PAC-MAN

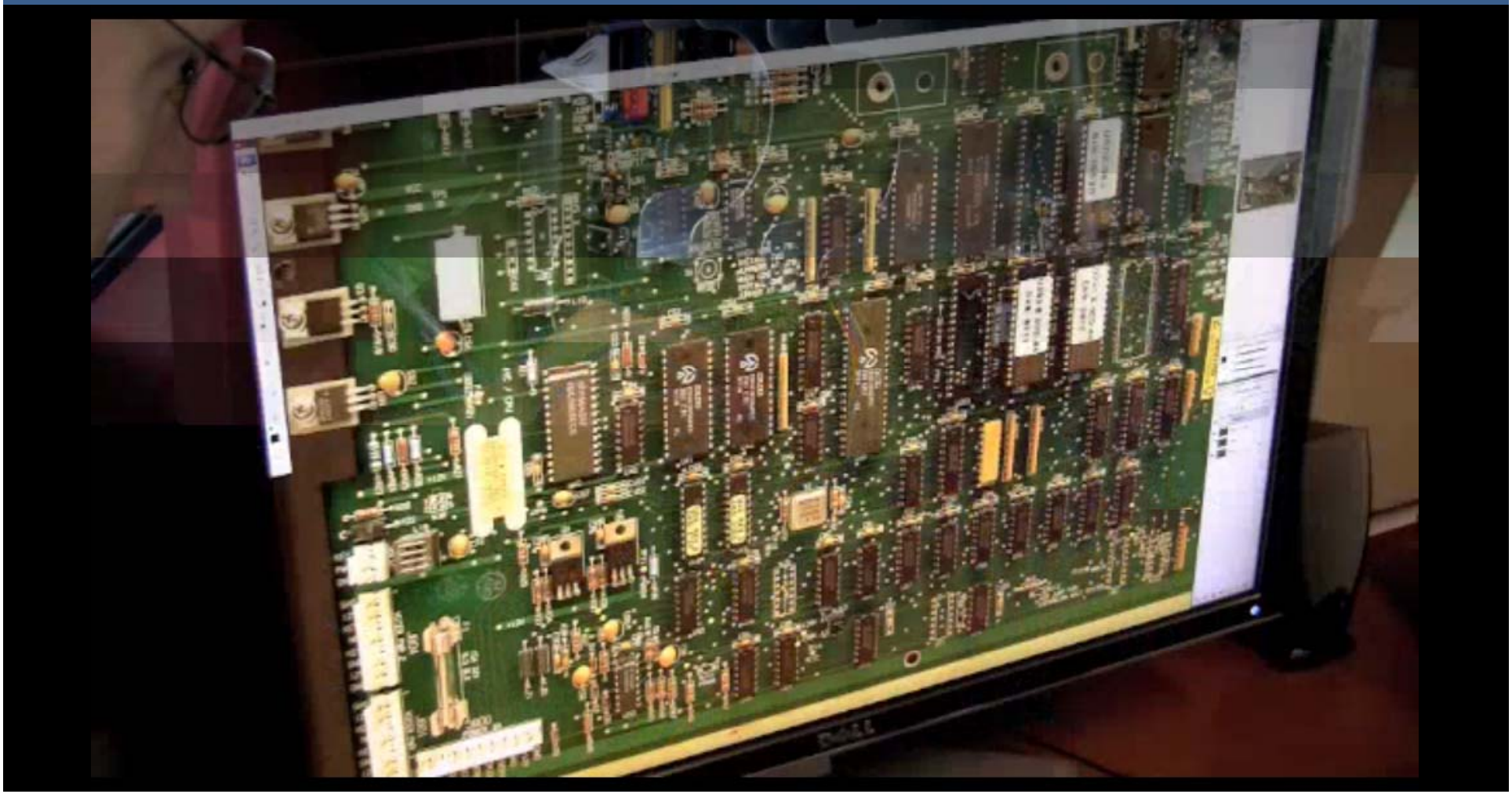

PAC-MAN

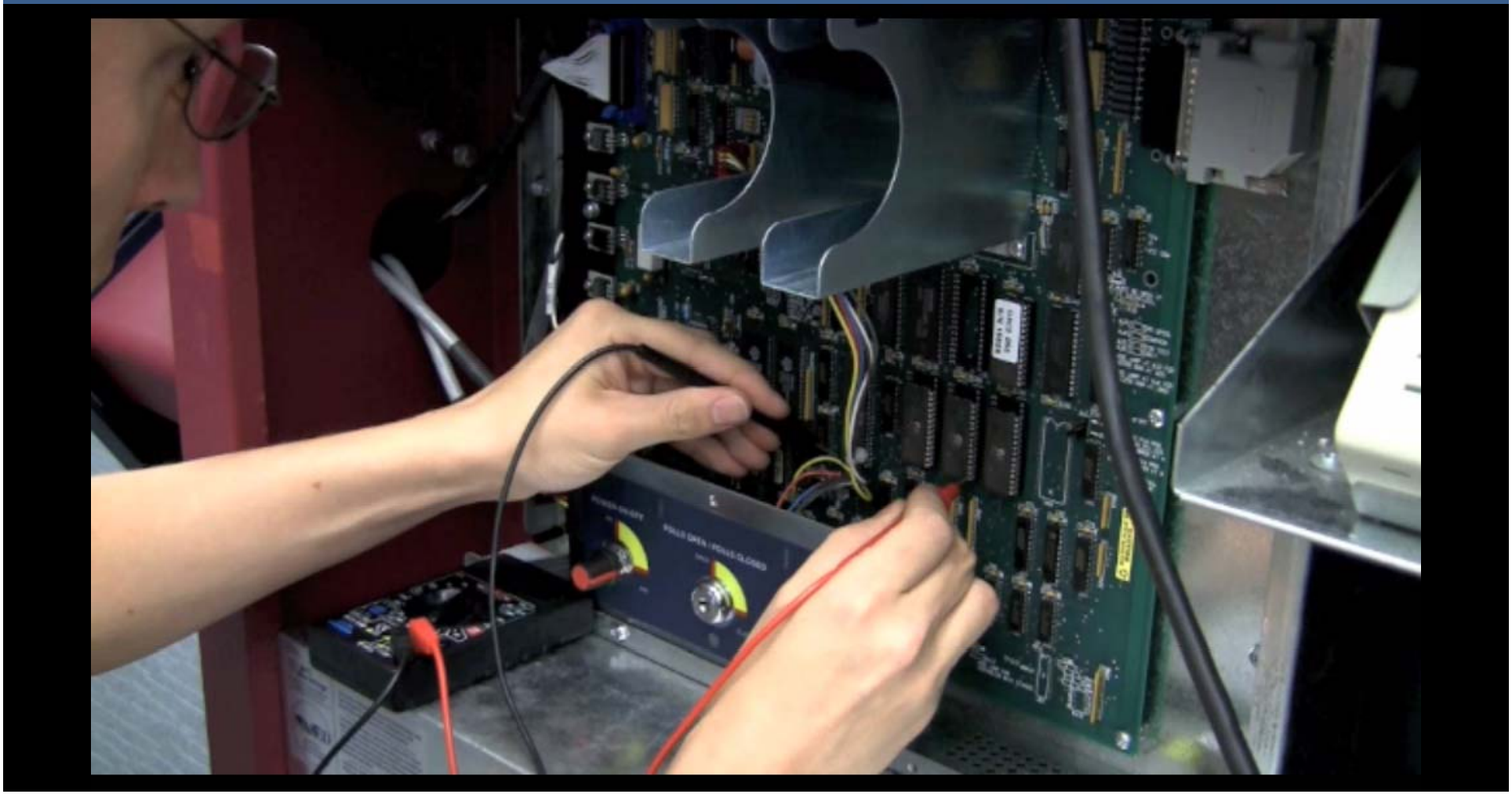
The Test of Time

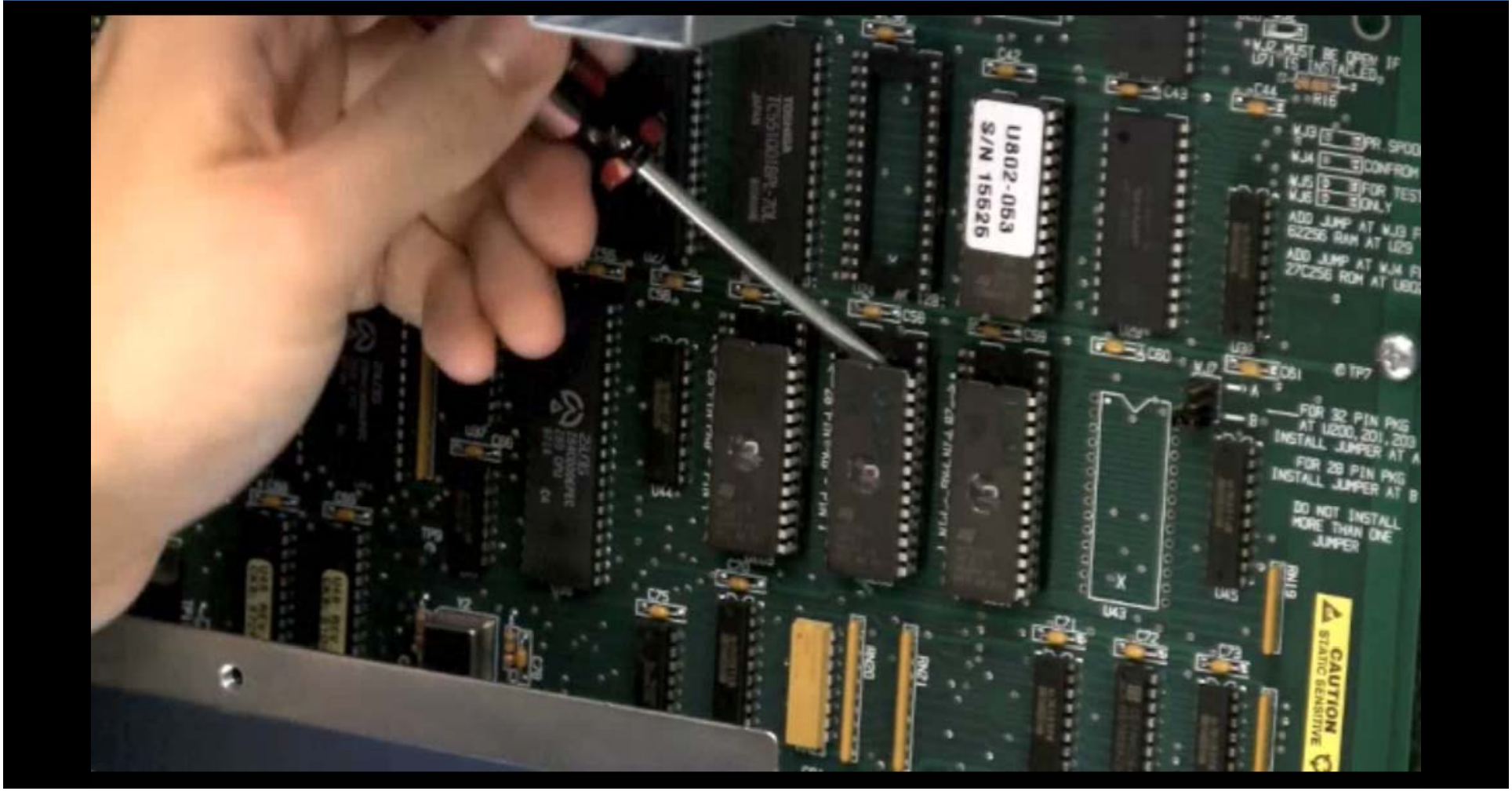


Sequoia
AVC Advantage

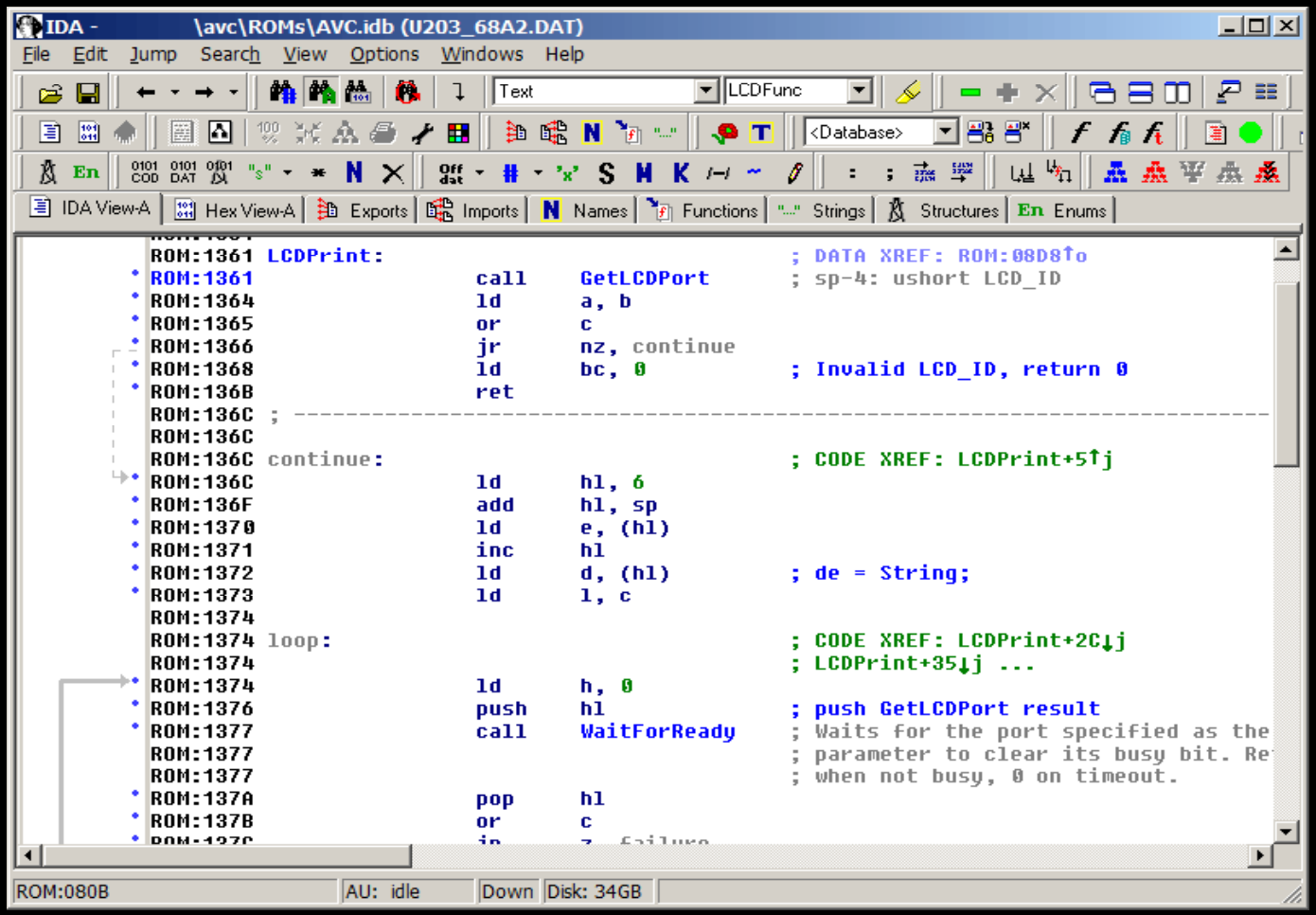

AES
Attacker
Core 1
Core 2
L1
L2



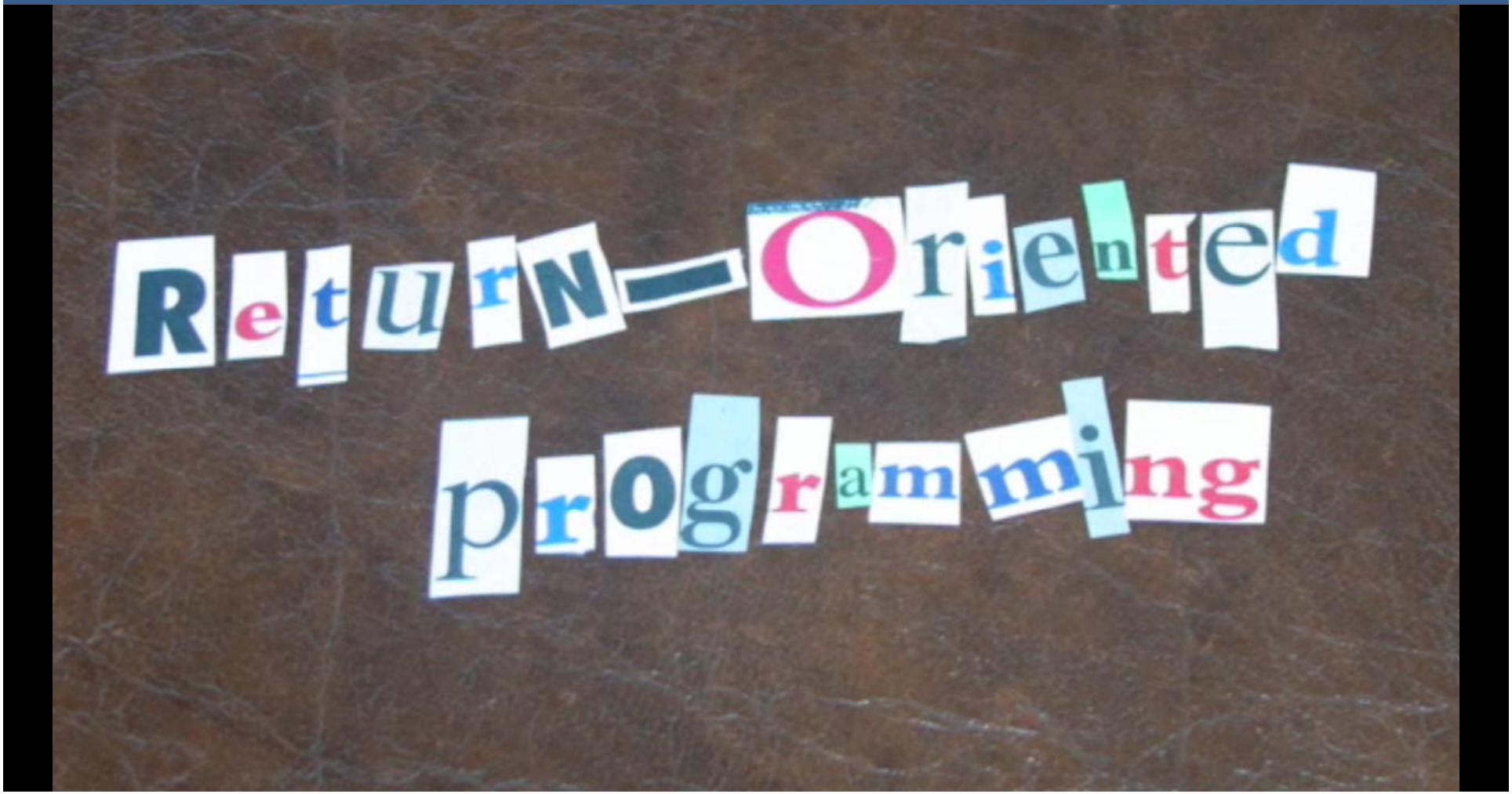


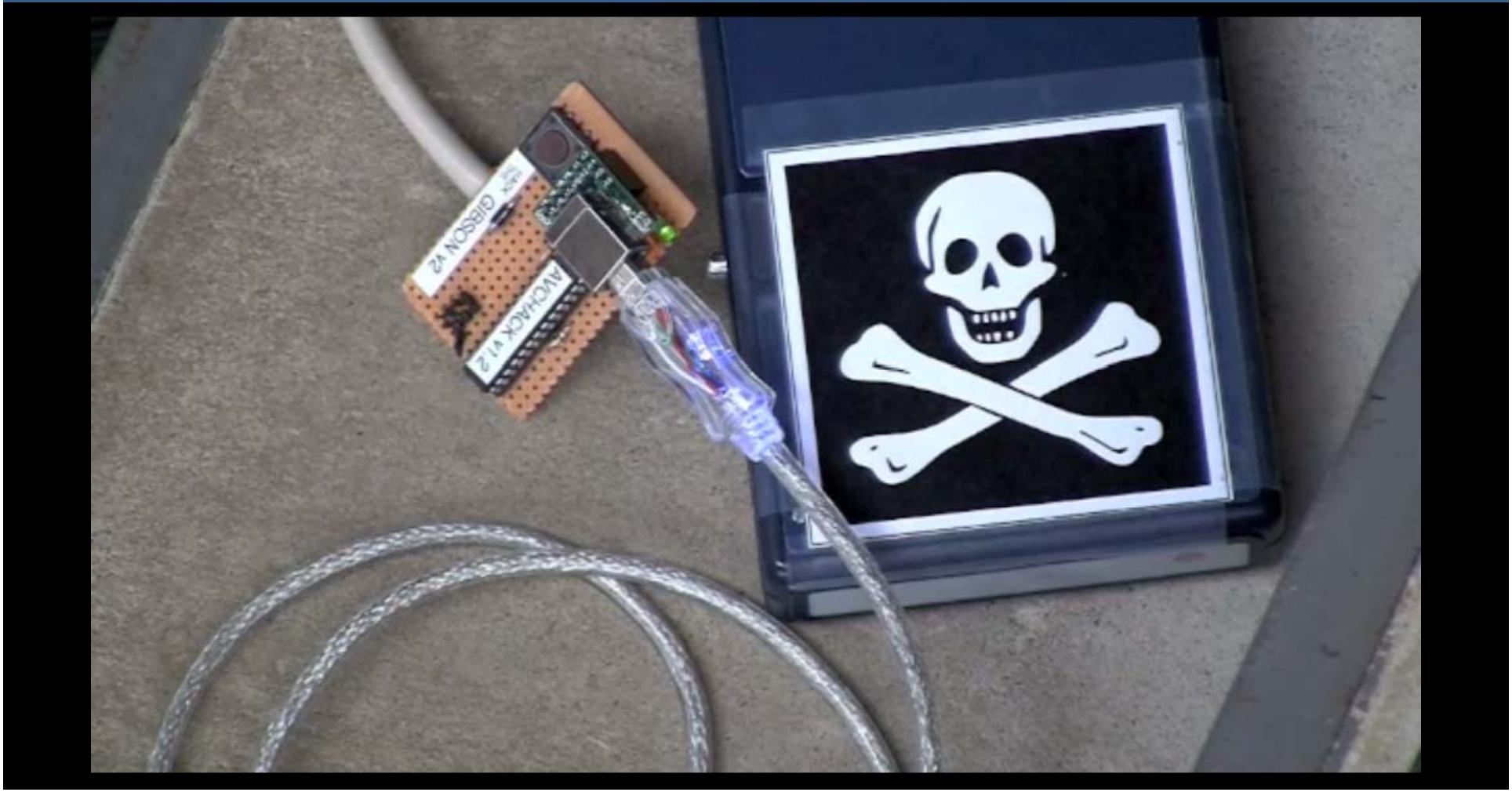

U802-053
S/N 15525
FOR 32 PIN PKG
AT U200,201,203
INSTALL JUMPER AT A
FOR 28 PIN PKG
INSTALL JUMPER AT B
DO NOT INSTALL
MORE THAN ONE
JUMPER
CAUTION
STATIC SENSITIVE

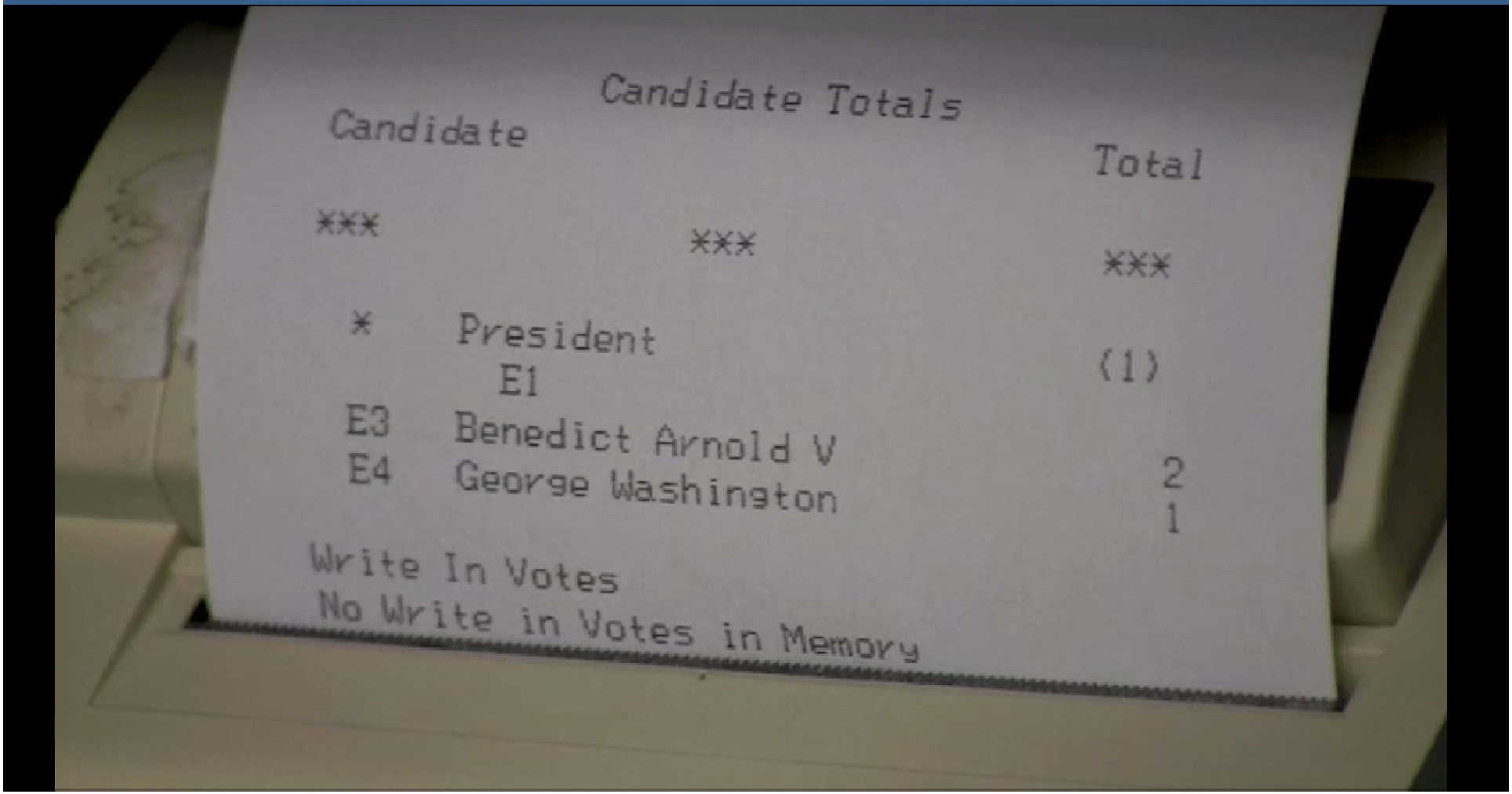

MacBook


IDA - \avc\ROMs\AVC.idb (U203_68A2.DAT)
File Edit Jump Search View Options Windows Help
Text
LCDFunc
<Database>
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
ROM:1361 LCDPrint: ; DATA XREF: ROM:08D8↑o
ROM:1361 call GetLCDPort ; sp-4: ushort LCD_ID
ROM:1364 ld a, b
ROM:1365 or c
ROM:1366 jr nz, continue
ROM:1368 ld bc, 0 ; Invalid LCD_ID, return 0
ROM:136B ret
ROM:136C ; ---
ROM:136C
ROM:136C continue: ; CODE XREF: LCDPrint+5↑j
ROM:136C ld hl, 6
ROM:136F add hl, sp
ROM:1370 ld e, (hl)
ROM:1371 inc hl
ROM:1372 ld d, (hl) ; de = String;
ROM:1373 ld l, c
ROM:1374
ROM:1374 loop: ; CODE XREF: LCDPrint+2C↓j
ROM:1374 ; LCDPrint+35↓j ...
ROM:1374 ld h, 0
ROM:1376 push hl ; push GetLCDPort result
ROM:1377 call WaitForReady ; Waits for the port specified as the
ROM:1377 ; parameter to clear its busy bit. Re
ROM:1377 ; when not busy, 0 on timeout.
ROM:137A pop hl
ROM:137B or c
ROM:080B
AU: idle
Down
Disk: 34GB

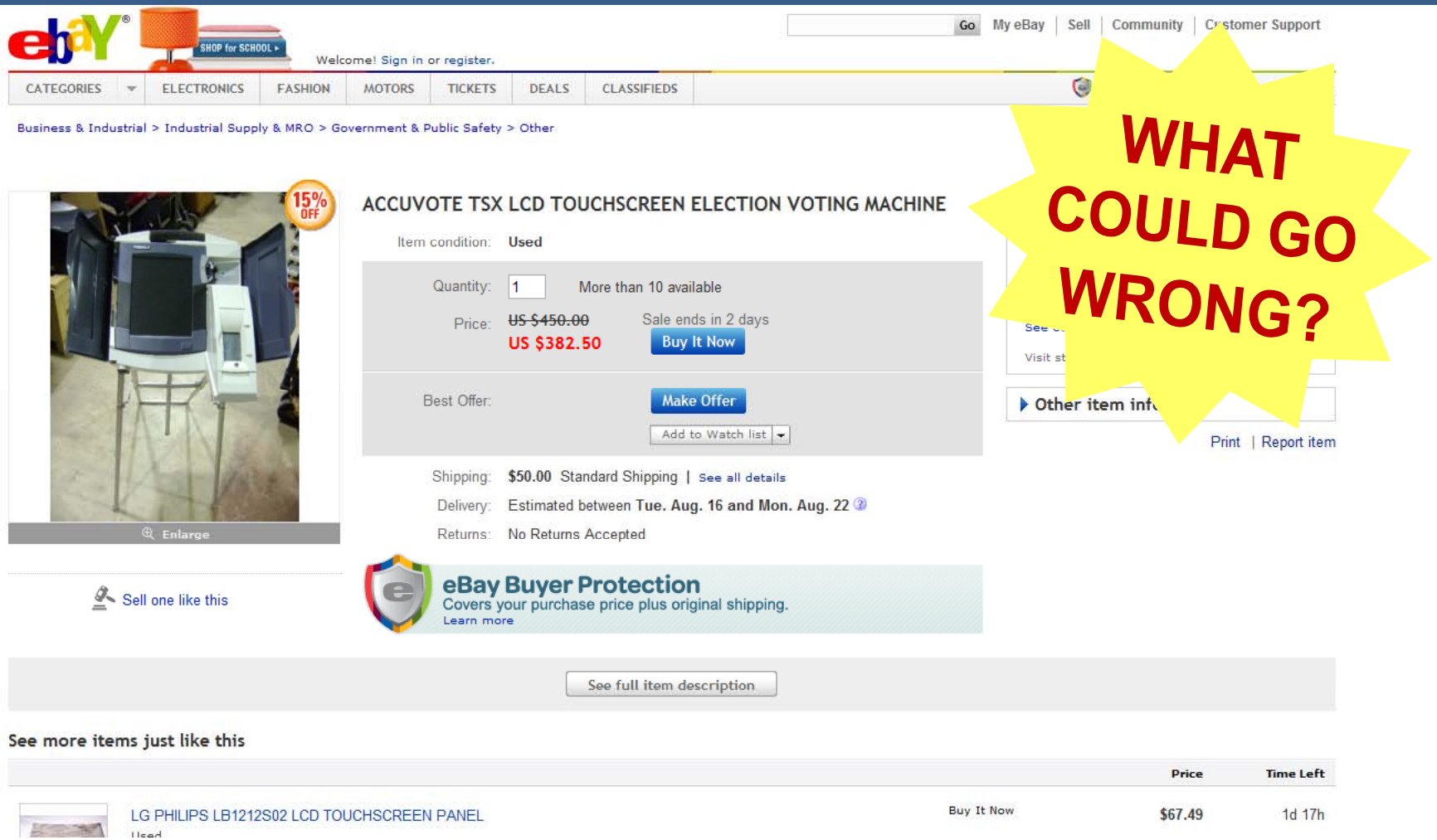

The Other Michael
by Hilton Als
BRIAN URQUHART: MIDEAST FOLLIES
A hundred years at the wheel
David Arnold
Ronald Fraser
Frances Wilson
Fiona Gruber
'The Beauty & Terror of Science'
An epic in prose
Joan Acocella: Golden Thrill
Seeking Growth, Cisco Reroutes Decisions
Michael Massing:
The Good News about the Internet
Health Care: The Fateful Moment
by Theodore Marmor & Jonathan Oberlander
ROGER COHEN:
THE IRAN TRAGEDY
'The Wind in the Willows'
by Michael Dirda


Return-Oriented
programming


GIBSON V2
AVCHACK V1.2


Candidate Totals
Candidate
Total
***
***
***
* President
E1
(1)
E3 Benedict Arnold V
E4 George Washington
2
1
Write In Votes
No Write in Votes in Memory

Diebold AccuVote-TSx


ebay
SHOP for SCHOOL
Welcome! Sign in or register.
Go
My eBay
Sell
Community
Customer Support
CATEGORIES
ELECTRONICS
FASHION
MOTORS
TICKETS
DEALS
CLASSIFIEDS
Business & Industrial > Industrial Supply & MRO > Government & Public Safety > Other
15% OFF
Enlarge
ACCUVOTE TSX LCD TOUCHSCREEN ELECTION VOTING MACHINE
Item condition: Used
Quantity: 1 More than 10 available
Price: US $450.00
US $382.50
Sale ends in 2 days
Buy It Now
Best Offer:
Make Offer
Add to Watch list
Shipping: $50.00 Standard Shipping | See all details
Delivery: Estimated between Tue. Aug. 16 and Mon. Aug. 22
Returns: No Returns Accepted
Sell one like this
eBay Buyer Protection
Covers your purchase price plus original shipping.
Learn more
WHAT COULD GO WRONG?
Other item info
Print | Report item
See full item description
See more items just like this
Price
Time Left
LG PHILIPS LB1212S02 LCD TOUCHSCREEN PANEL
Used
Buy It Now
$67.49
1d 17h

Source Code Review of the Diebold Voting System

Joseph A. Calandrino
Princeton University[1]

Ariel J. Feldman
Princeton University

J. Alex Halderman
Princeton University

David Wagner[2]
U.C., Berkeley

Harlan Yu
Princeton University

William P. Zeller
Princeton University

July 20, 2007

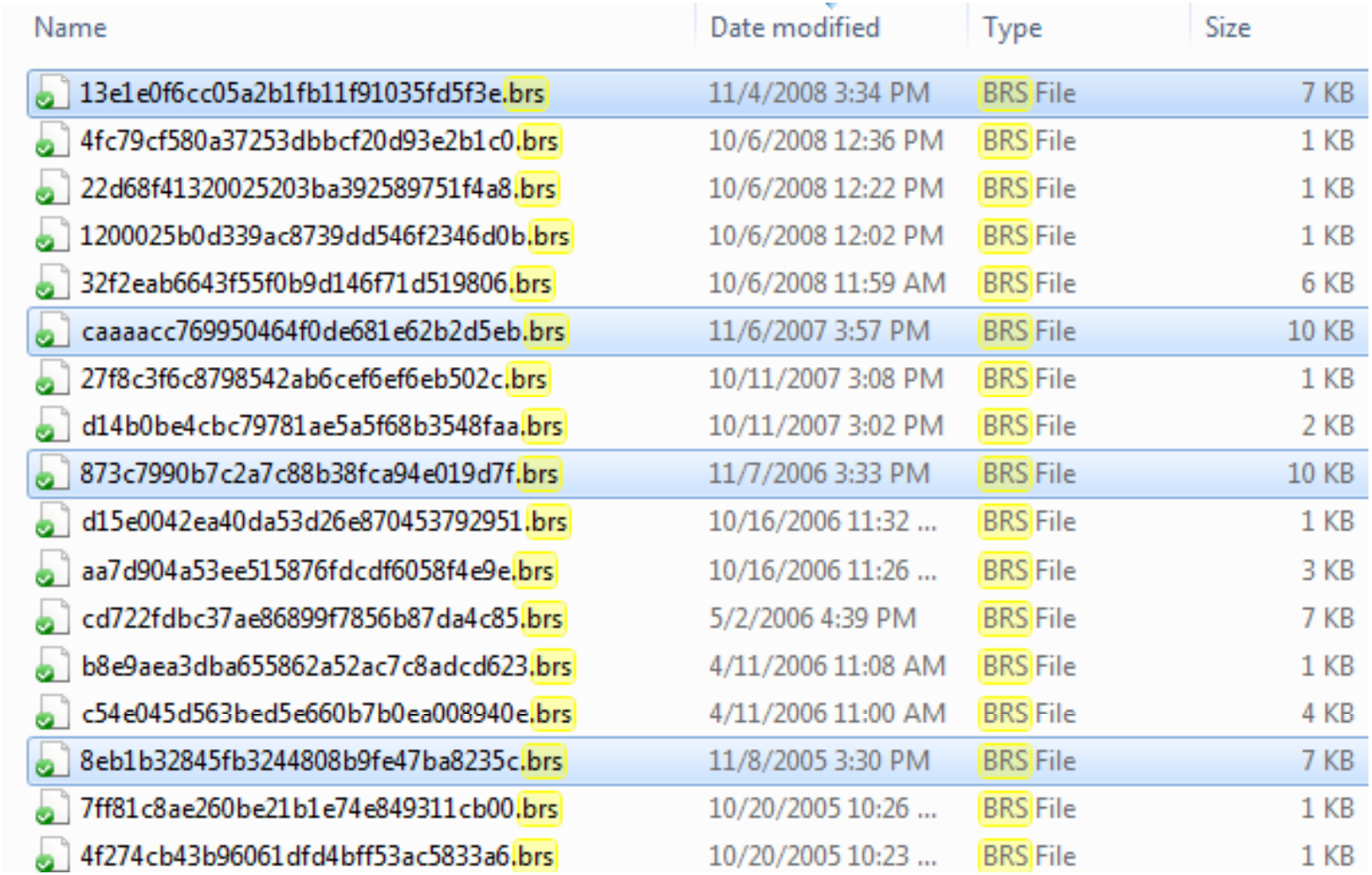
This report was prepared by the University of California, Berkeley under contract to the California Secretary of State as part of a "Top-to-Bottom" review of electronic voting systems certified for use in the State of California.

Source Code Review of the Diebold Voting System

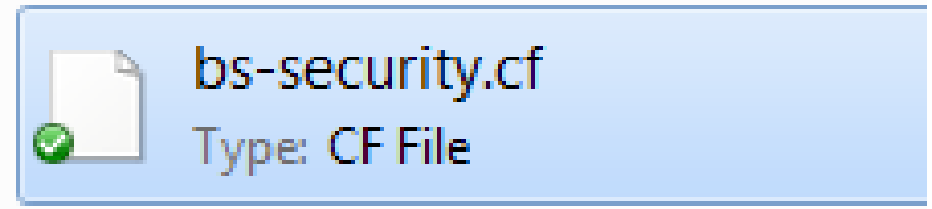
Issue 5.2.22: *Files on the voting machine are not securely erased when they are deleted.*

BallotStation deletes files from the memory card or the machine's internal flash memory at various times during the election process. For instance, it allows election officials to delete the backup copies of old ballot results and audit logs that are stored on the machine. Deleting old these files is important for safeguarding the secrecy of the ballot, since, as described above, the contents of the files may reveal how voters voted.

However, when BallotStation delete files, it does so using the standard Windows `DeleteFile()` API. This function removes the file from directory listings, but it does not securely erase the contents from the memory card. Even after being deleted, the data will remain in the memory card until it are overwritten with other data, which may take multiple election cycles. An attacker with access to the memory card, unsupervised physical access to the machine, or the ability to run malicious software on the voting machine might be able to recover the contents of these files even after BallotStation deletes them.



Name	Date modified	Type	Size
13e1e0f6cc05a2b1fb11f91035fd5f3e.brs	11/4/2008 3:34 PM	BRS File	7 KB
4fc79cf580a37253dbbcf20d93e2b1c0.brs	10/6/2008 12:36 PM	BRS File	1 KB
22d68f41320025203ba392589751f4a8.brs	10/6/2008 12:22 PM	BRS File	1 KB
1200025b0d339ac8739dd546f2346d0b.brs	10/6/2008 12:02 PM	BRS File	1 KB
32f2eab6643f55f0b9d146f71d519806.brs	10/6/2008 11:59 AM	BRS File	6 KB
caaaacc769950464f0de681e62b2d5eb.brs	11/6/2007 3:57 PM	BRS File	10 KB
27f8c3f6c8798542ab6cef6ef6eb502c.brs	10/11/2007 3:08 PM	BRS File	1 KB
d14b0be4cbc79781ae5a5f68b3548faa.brs	10/11/2007 3:02 PM	BRS File	2 KB
873c7990b7c2a7c88b38fca94e019d7f.brs	11/7/2006 3:33 PM	BRS File	10 KB
d15e0042ea40da53d26e870453792951.brs	10/16/2006 11:32 ...	BRS File	1 KB
aa7d904a53ee515876fdcdf6058f4e9e.brs	10/16/2006 11:26 ...	BRS File	3 KB
cd722fdbc37ae86899f7856b87da4c85.brs	5/2/2006 4:39 PM	BRS File	7 KB
b8e9aea3dba655862a52ac7c8adcd623.brs	4/11/2006 11:08 AM	BRS File	1 KB
c54e045d563bed5e660b7b0ea008940e.brs	4/11/2006 11:00 AM	BRS File	4 KB
8eb1b32845fb3244808b9fe47ba8235c.brs	11/8/2005 3:30 PM	BRS File	7 KB
7ff81c8ae260be21b1e74e849311cb00.brs	10/20/2005 10:26 ...	BRS File	1 KB
4f274cb43b96061dfd4bff53ac5833a6.brs	10/20/2005 10:23 ...	BRS File	1 KB

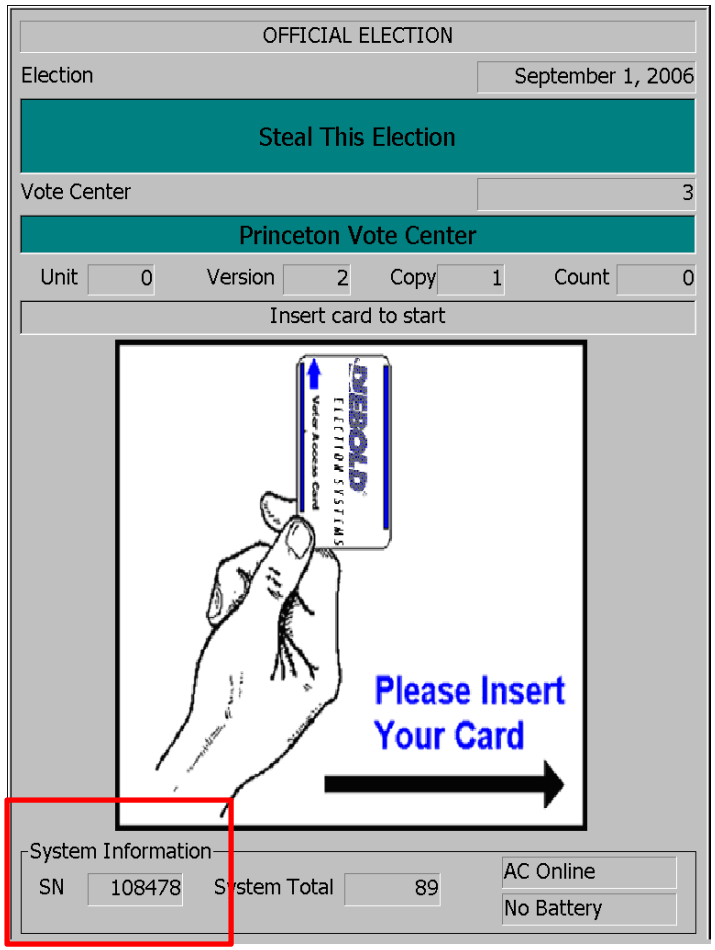

bs-security.cf
Type: CF File

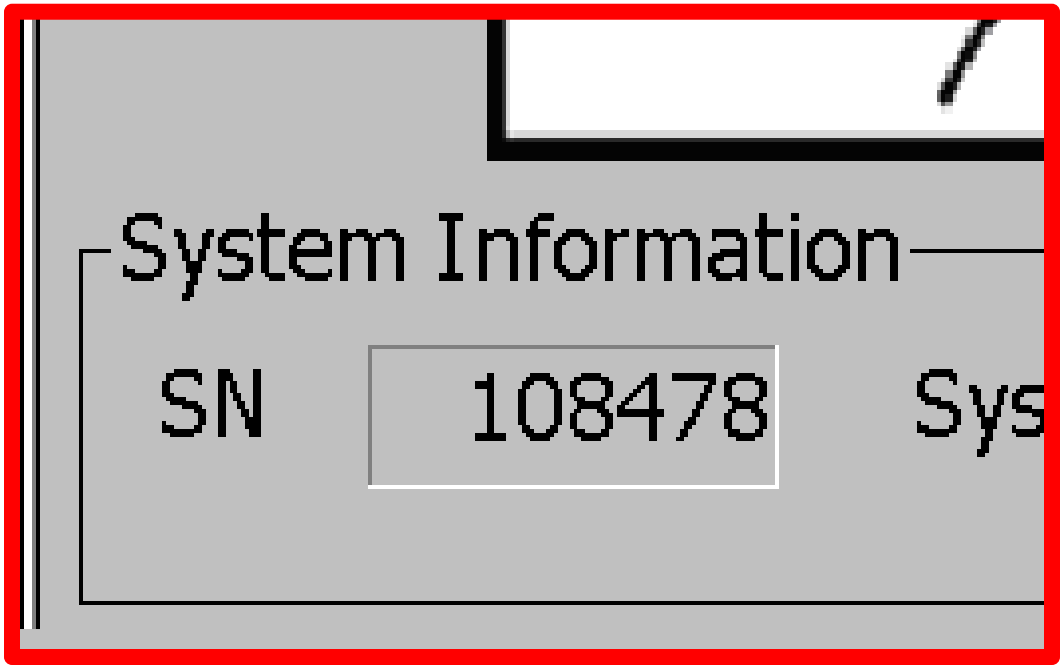
Source Code Review of the Diebold Voting System

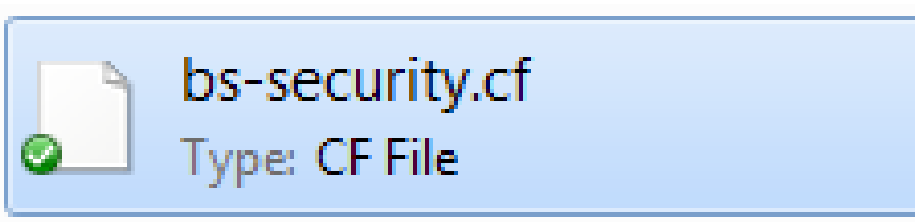
Issue 5.2.5: *Keys used to secure smart cards and election data are not adequately protected.*

The AV-TSX uses security keys for various security purposes, including authenticating election definition files, encrypting and authenticating ballot result files, validating voter smart cards, and generating ballot serial numbers. Older Diebold machines used hardcoded keys set when the software was compiled. The version of the AV-TSX that we studied retains those hardcoded keys but also allows county election officials to change the keys that the machine uses. Officials can set three keys, the 64-bit *Smart Card Key*, the 16-bit *Smart Card Magic Number*, and the 128-bit *Data Key*. (Internally, these are labeled `SCKey`, `SCMagic`, and and `DESKey`, respectively, though the system no longer uses the DES cipher.)

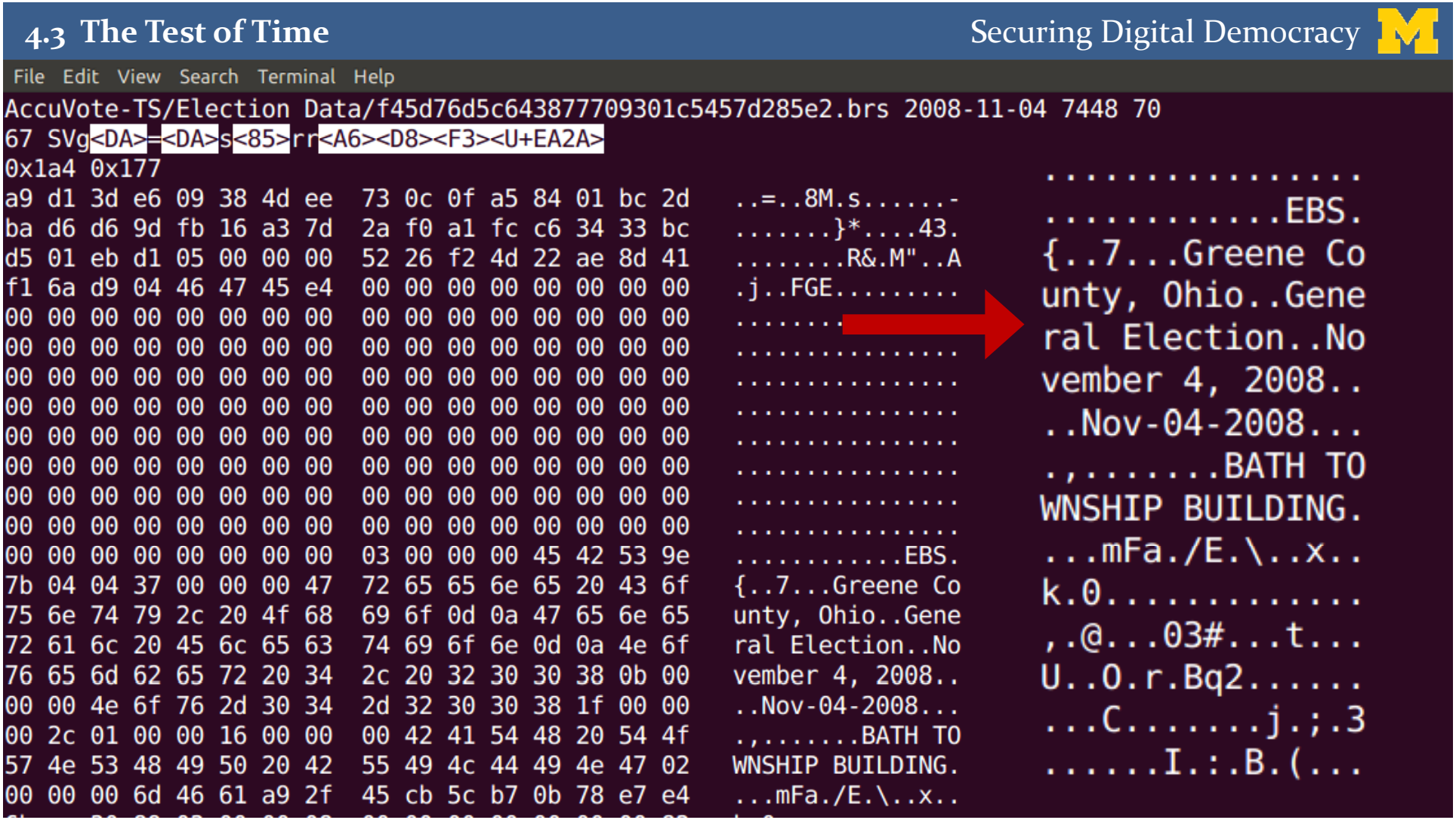
The machine stores the Smart Card Key, Smart Card Magic Number, and Data Key in a file in its internal flash memory. This file, `bs-security.cf`, resides in the same directory as `BallotStation.exe`. BallotStation encrypts the contents of the file (using AES128-CBC) with a third key called the *System Key*. However, the value of the System Key is not a secret—rather, it is the hash of the machine's serial number. The

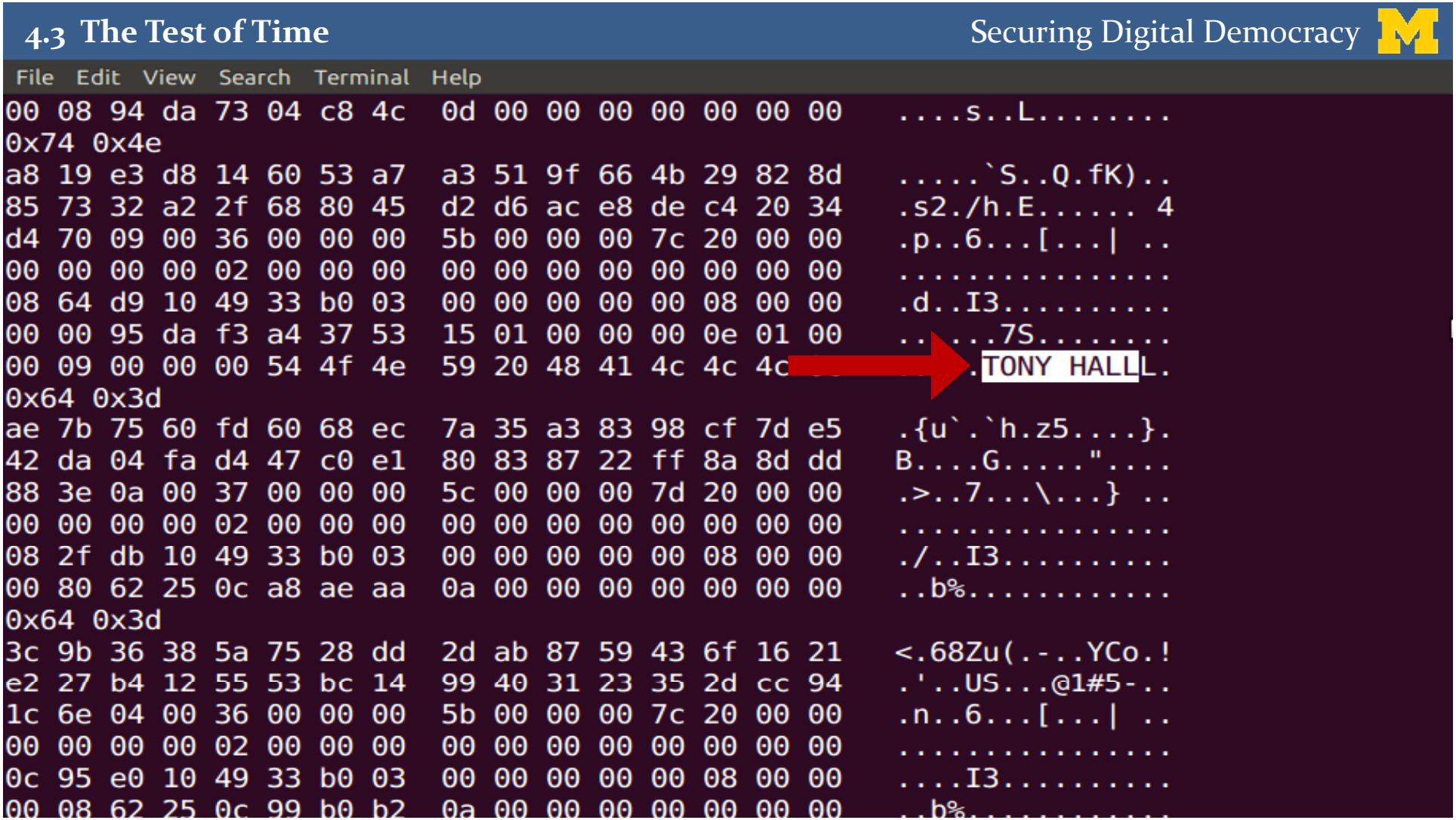

OFFICIAL ELECTION
Election
September 1, 2006
Steal This Election
Vote Center
3
Princeton Vote Center
Unit 0
Version 2
Copy 1
Count 0
Insert card to start
Please Insert
Your Card
System Information
SN 108478
System Total 89
AC Online
No Battery


System Information
SN
108478
Sys



```
./datakey.py bs-security.cf
53 45 43 44 41 54 41 00  7d fe 00 00 08 00 10 00   SECDATA.}.......
4e 1f 55 bf 5a 3b 22 33  00 00 00 00 00 00 00 00   N.U.Z;"3........
53 56 67 da 3d da 73 85  72 72 a6 d8 f3 ee a8 aa   SVg.=.s.rr......
```


File Edit View Search Terminal Help
AccuVote-TS/Election Data/f45d76d5c643877709301c5457d285e2.brs 2008-11-04 7448 70
67 SVg<DA>=<DA>s<85>rr<A6><D8><F3><U+EA2A>
0x1a4 0x177
a9 d1 3d e6 09 38 4d ee 73 0c 0f a5 84 01 bc 2d ..=..8M.s......-
ba d6 d6 9d fb 16 a3 7d 2a f0 a1 fc c6 34 33 bc ....}*....43.
d5 01 eb d1 05 00 00 00 52 26 f2 4d 22 ae 8d 41 ....R&.M"..A
f1 6a d9 04 46 47 45 e4 00 00 00 00 00 00 00 00 .j..FGE.........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 03 00 00 00 45 42 53 9e ....EBS.
7b 04 04 37 00 00 00 47 72 65 65 6e 65 20 43 6f {..7...Greene Co
75 6e 74 79 2c 20 4f 68 69 6f 0d 0a 47 65 6e 65 unty, Ohio..Gene
72 61 6c 20 45 6c 65 63 74 69 6f 6e 0d 0a 4e 6f ral Election..No
76 65 6d 62 65 72 20 34 2c 20 32 30 30 38 0b 00 vember 4, 2008..
00 00 4e 6f 76 2d 30 34 2d 32 30 30 38 1f 00 00 ..Nov-04-2008...
00 2c 01 00 00 16 00 00 00 42 41 54 48 20 54 4f .,.......BATH TO
57 4e 53 48 49 50 20 42 55 49 4c 44 49 4e 47 02 WNSHIP BUILDING.
00 00 00 6d 46 61 a9 2f 45 cb 5c b7 0b 78 e7 e4 ...mFa./E.\..x..
....
............EBS.
{..7...Greene Co
unty, Ohio..Gene
ral Election..No
vember 4, 2008..
..Nov-04-2008...
.,.......BATH TO
WNSHIP BUILDING.
...mFa./E.\..x..
k.0.............
,.@...03#...t...
U..O.r.Bq2......
...C.......j.;.3
......I.:.B.(...


File Edit View Search Terminal Help
00 08 94 da 73 04 c8 4c 0d 00 00 00 00 00 00 00 ....s..L........
0x74 0x4e
a8 19 e3 d8 14 60 53 a7 a3 51 9f 66 4b 29 82 8d .....`S..Q.fK)..
85 73 32 a2 2f 68 80 45 d2 d6 ac e8 de c4 20 34 .s2./h.E...... 4
d4 70 09 00 36 00 00 00 5b 00 00 00 7c 20 00 00 .p..6...[...| ..
00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 ....
08 64 d9 10 49 33 b0 03 00 00 00 00 00 08 00 00 .d..I3..........
00 00 95 da f3 a4 37 53 15 01 00 00 00 0e 01 00 ......7S........
00 09 00 00 00 54 4f 4e 59 20 48 41 4c 4c 4c .TONY HALLL.
0x64 0x3d
ae 7b 75 60 fd 60 68 ec 7a 35 a3 83 98 cf 7d e5 .{u`.`h.z5....}.
42 da 04 fa d4 47 c0 e1 80 83 87 22 ff 8a 8d dd B....G.....".....
88 3e 0a 00 37 00 00 00 5c 00 00 00 7d 20 00 00 .>..7...\...} ..
00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 ....
08 2f db 10 49 33 b0 03 00 00 00 00 00 08 00 00 ./..I3..........
00 80 62 25 0c a8 ae aa 0a 00 00 00 00 00 00 00 ..b%............
0x64 0x3d
3c 9b 36 38 5a 75 28 dd 2d ab 87 59 43 6f 16 21 <.68Zu(.-..YCo.!
e2 27 b4 12 55 53 bc 14 99 40 31 23 35 2d cc 94 .'..US...@1#5-..
1c 6e 04 00 36 00 00 00 5b 00 00 00 7c 20 00 00 .n..6...[...| ..
00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 ....
0c 95 e0 10 49 33 b0 03 00 00 00 00 00 08 00 00 ....I3..........
00 08 62 25 0c 99 b0 b2 0a 00 00 00 00 00 00 00 ..b%............

Issue 5.2.19: *Ballot results files store votes in the order in which they are cast.*

The AV-TSX records votes in an encrypted ballot results file (`.brs`) stored on the removable memory card with an identical backup held in internal flash memory. The ballot results file consists of a series of records, one for each ballot cast. Each record includes a 32-bit ballot serial number, a 32-bit timestamp (in UNIX format), and a representation of the voter's selections. After each vote is cast, the machine simply appends another record to the end of the ballot results file.


DIEBOLD
Diebold Election Systems
General Election

Securing Digital Democracy

Lecture 4 | *Problems with DREs*

J. Alex Halderman
University of Michigan