Teaching Case: Election Security and Technology Education

Garry L. White, CCP, CISSP, PhD
Dept. of CIS & QM
Texas State University
San Marcos, TX USA
Gw06@txstate.edu
0000-0003-4087-3079

***Abstract*—Democracy is based on education according to Socrates (470-390 B.C.) A lack of education leads to election problems. The 2020 presidential election has raised questions of election fraud and rigged software and the integrity of the results. Such questions can be resolved through election technology & security education. Education can put you in a position of knowledge if you find yourself in a discussion on voter fraud. The purpose of this paper is to propose a curriculum for different courses on election security and election technology to educate people. Individuals' trust of an election can be impacted by education which may overriding propaganda, and fake news. Proposed curriculum also covers misleading election numbers from statistics and Benford's Law.**

Keywords—software, database errors, voting systems, security, hash values, digital signatures, statistics, Benford's Law

I. INTRODUCTION

The 2020 presidential election has raised questions of election fraud and rigged software and the integrity of the results. Public perceptions of fraud an issue [40, 41]. "Rhetoric about 'rigged' elections has raised concerns about the solidity of public trust in the integrity of the voting system" [23]. "Doubts about electoral integrity, whether justified or groundless, can undermine faith in the legitimacy of the democratic process" [19]. Trust in electoral institutions is a rational response to knowledge, awareness and experience about how elections work [19].

The 2020 election provides an opportunity and incentive to teach election technology & security. Such questions can be resolved through education. Education can put you in a position of knowledge if you find yourself in a discussion on voter fraud. This provides an opportunity and incentive to teach security such as voting implementation of digital signatures and hash values to increase trust in the election system. The more educated, aware and efficacious the citizens, the more likely they are to trust electoral outcomes [19].

Through election technology & security education, such questions can be addressed. The purpose of this paper is to provide content (knowledge) for a curriculum that will allow people to make informed decisions concerning issues of elections and possibility increase trust in the election system. The content to be presented covers hashing and digital signatures as security measures to prove in court 1) Data protection & swap USB's/microchips, 2) rigged software, and 3) dead voters fraud. Another area to be covered is misleading numbers through 4) statistics, and 5) Benford's Law.

II. MOTIVATION

A. Socrates

Socrates was a committed democrat [43]. He insisted that only those who had thought about issues rationally should be the ones to vote, intellectual democracy. Voting needs to be connected to wisdom. And Socrates knew exactly where that would lead to a system the Greeks feared above all, demagoguery. We have forgotten Socrates's warnings against democracy. Democracy is only as effective as the education system that surrounds it [24]. Socrates said voting in an election is a skill. And like any other skill, only those who have been systematically taught should have the right to vote. Allowing citizens to vote without properly educating them is like putting ignorance in charge of a ship in a storm [33]. Socrates worried, ironically, about the corruptive influence that the democratic culture of rule by the uneducated multitude [20].

B. Need

Trust in the voting system supports the legitimacy of democracy [35]. Of the 2020 general election, around 65% of the voters trusted the results [21. 30] with 92% of Democrats and 32 percent of Republicans [22]. Trust of the U.S. election is slipping [7] especially with the Republicans. "This level of distrust is not surprising, given political rhetoric, but it certainly is concerning. Elections are the foundation of our democracy and loss of faith in the process could undermine the new administration's legitimacy and ability to get things done," said James Druckman, the Payson S. Wild Professor of political science in the Weinberg College of Arts and Sciences at Northwestern and associate director of the University's Institute for Policy Research. [21].

A question is to what extent does allegations of and beliefs in massive electoral corruption reflect a polarized society [23]. A more important question is whether education is a countermeasure to allegations and beliefs in corruption. In the 2016 Federal elections in Australia, one third of

Australians believed (falsely) that the outcome was the result of voter fraud [19]. Many Australians misunderstood their electoral system. To restore public confidence, civic education should be strengthened [19].

A responsibility of the computing professional is to understand why trust in voting is critical [15]. Democracy relies on voting to reveal the will of the voters. Another responsibility of the computing professional is to explain vulnerabilities, errors, quirks, and unknowns, and to suggest solutions/countermeasures [8]. The priority of the computing professional is to educate voters because the less educated are most likely to believe that electoral outcomes are fraudulent [19].

C. Purpose

Provide election security knowledge to the general public to increase trust in the election system.

D. Audience

Security literacy goes beyond the students in a college course. The intended audience is the public. This includes carpenters, plumbers, salesclerks, truck drivers, etc. They are the targets for hackers, identify theft, propaganda, phishing, misinformation, & ransomware.

E. Informal Security Education

Examples of informal education are news media articles & documentaries, civic organization presentations, TED Talk –public speaking broadcast, technical museums, and YouTube video clips. These are ways to provide security literacy to those who do not attend college security courses. Measuring outcomes is subjective. Expressing a degree of trust in response to a poll or survey deals with perceptions and opinions.

F. Knowledge

Two supportive topics of knowledge for elections are A) hash values and B) digital signatures. They can prevent and detect rigged software and voter fraud. Findings can be used in a court of law. The following three topics will educate people with 1) data protection, 2) rigged software; how it works, how it cannot be hidden, and how it can prove in court rigged software exist or not , and 3) dead voters; why they exist and how to prove dead voters exist or not in court.

Another area of technical knowledge is misleading numbers. When people lack understanding of 4) Statistics or 5) Benford's Law, they can be easily misleading as to election outcome and voter fraud. These last two added topics will be addressed in Section V (c) of this paper.

III. CURRICULUM

Seven topics are presented as modules that can be inserted into different courses, such as security, auditing, information systems, programming, database, data mining, inferential statistics, accounting, and data analytics. The modules are viewed as stand-alone that can be fit into related courses. By teaching election technology and security across the curriculum will provide a better context and reinforcement for the topics.

IV. CASY SYNOPSIS

The seven topics (A through G) are related to courses as shown in Table I.

TABLE I. MODULES & COURSES

Module Topic	**Related courses**
1. Supportive Topics	
A. Hash Values	• Security, Auditing
B. Digital Signatures	• Security, Auditing
2. Voter Fraud	
C. Data Protection & swap USB's / microchips	• Information System
D. Rigged software	• Programming
E. Dead Voters	• Database & Data Mining
3. Misleading numbers	
F. Statistics	• Inferential Statistics
G. Benford's Law	• Accounting & Data Analytics

V. CASE MODULES

Disclaimer: The scenarios and data in these modules are examples only for demonstration and teaching purposes. The purpose is to show concepts.

A. Supportive Topics

a) Hash values module: "Hashing is the process of taking computer data as a string of information, processing this string through a specially designed mathematical function that transposes each character of the string into another character or symbol, and converts it to another (usually smaller) string known as the hash value" [16]. Sometimes, the hash value is called a message digest. An example is a check sum. The account number 4545 digits sum up to a check value of 18. The hash value is unique providing a unique file identification, has a fixed length independent of the file size, and cannot be used to recover the original data -- a one way encryption provides privacy and security when the data is shared. It shows integrity, no changes. Hash collisions are possible but are primarily theoretically probable. However, intentional collisions have occurred with weak hash functions [16].

Example: Two pdf files hash values were compared. File sizes were the same. One pdf file stated John McCain won the election. The second stated Oprah Winfrey. By using PE Lock Hash Calculator Online, hash values of the two pdf files were compared as shown in Table II.

(website: https://www.pelock.com/products/hash-calculator)

TABLE II. COMPARING HASH VALUES

File: John_McCain.pdf size: 104,331 Bytes		
Hash Name	Length (Bytes)	Hash (hex)
MD5	16	**3D515DEAD7AA16560ABA3E9DF05CBC80**
SHA1	20	2E32A0B5D30A59306F02B7B3ED63BBEB787EBDD0
SHA224	28	1DF60250F431B55B9AB0AC7BB863FDA8449DE5855…

File: Oprah_Winfrey.pdf size: 104,331 Bytes		
Hash Name	Length (Bytes)	Hash (hex)
MD5	16	**3D515DEAD7AA16560ABA3E9DF05CBC80**
SHA1	20	40842B75B907F98D90ACAB07EE8B781EAFD6CA2F
SHA224	28	CACD4B7D284A608CB42E5DE554B986A186B4B1…

Notice the collision between the two different pdf files with MD5. Unfortunately, MD5 has been cryptographically broken and considered insecure. For this reason, it should not be used for anything [26, 37]. However, this weakness can be resolved by adding a salt value to MD5 hash calculation [34].

Usage: Digital forensics professionals use hashing algorithms to generate hash values of the original files they use in investigation. This ensures that the information isn't altered during investigation since various tools and techniques are involved in data analysis and evidence collection that can affect the data's integrity. Another reason hash values are important is that electronic documents are shared with legal professionals and other parties during investigation, and it's important to ensure that everyone has identical copies of the files. The use of hashing and public key encryption to secure voting in elections began around the 1990's [36] and hashing has been used to catch online criminals [16]. These algorithms allow investigators to preserve digital evidence from the moment they acquire it to the point it's produced in court.

b) Digital Signatures module: Digital Signatures use hashing algorithms for integrity and public key certificates for non-repudiation (it came from you, and you cannot deny it). It is a subset of electronic signatures [39]. To create the Signature, involves to steps, 1) calculate a hash value, known as a Message Digest, from the message, data, or file. The Message Digest is then encrypted with the source Private Key from a PKI or Certificates of Authority. The result is the Digital Signature. The Signature itself is in hex format. To confirm, the Signature is decrypted by the source Public Key providing the Message Digest. Since the Public Key worked, non-repudiation is proven. The receiver hashes the message, data, or file. The hash value by the receiver is then compared with the Message Digest decrypted. If equal, integrity is proven.

Digital Signatures are an open system for e-business transactions. An electronic digital signature (EDS) is the "sheet anchor" for most electronic businesses (eGoverment, eCommerce, eProcrument, eHealth, eInvoicing, etc.) [28]. The IRS uses digital signatures [18].

Computer laws from many countries have provided greater cyber-security by the acceptance of digital signatures as legal evidence in courts [1, 6, 12, 25, 44]. "These laws share one overriding principle: Signatures bear equal legal standing whether they are ink or electronic" [12]. "All 50 US states as well as Washington DC, Puerto Rico, and the US Virgin Islands also have laws regarding the use of electronic signatures" [12].

B. Voter Fraud

a) Data Protection module:

System:

Can fraud votes can be added, deleted, and shifted to the vote data file at will in real time on Election Night? Here are mechanisms that protect the vote data file.

Log Files. Changes coming from outside the system or from unknown/unauthorized sources, are recorded in firewall and system logs [7, 11].

File Permissions. Every user or system, including Administrators, by default are denied all file permissions. The only exceptions are the file owner with full control allowed and the processing software with only modify, write permissions. All other permissions for the software are denied [10].

File Attributes. The file owner, who has full control, can set the vote data file attribute to *Read-only* after votes are processed. Also, the file owner can set the file attribute *Hidden* to prevent the file name to be displayed anywhere in

the system. This will require authorized users to know the specific file name and specific location in the system to access the file [42].

Network Controls. In a network system the file can be set to non-share, where only the owner can access it. The network systems can also hide the file through Access-Based Enumeration (ABE) or having a "$" on the file name or folder.

Honey Pot. A decoy file, which looks real, can be created. This is known as a Honey Pot [17]. Here is an example.

Decoy file:

C:\precient01\datafiles\confidential\Vote_Count_File.xls.

The file is shared, has allow R/W permissions with the rest of permissions denied, and is behind a firewall.

Real file:

C:\clerk01\drawC\workfiles\AB01.xls

File is not shared, hidden with deny permissions as default for everyone except for the owner. It is also password protected and is encrypted.

Other Controls. Firewall can block traffic based on the destination file. Intrusion detection systems can detect and respond when there is an unauthorized access. Finally, the best control is a stand-alone system, the computer with the file is not connected to the outside world.

Hardware:

USB's or micro memory chips. It is not easy to swap USB's or micro memory cards. They have serial numbers embedded internally and externally. Physical access to the hardware can be restricted to only an authorized user. There is separation of duties of authorized users and multi-person control with impartial observers. Finally, there is "chain of custody" documentation of the hardware. Who is always in possession of the hardware and the serial numbers are recorded.

b) Rigged software module:

Excessive rhetoric about "rigged" elections could lessen the trust of elections by voters [23]. Here are two possible ways the vote counting program can be rigged, 1) initial counter, 2) shift vote count based on random selection, 3) execute rigged code only on election day, and 4) delete rigged code after election day.

Initiate counters. Candidates counters are to be initialized at 0. However, in the program the favored candidate's counter is initialized at +100 and the unfavored candidate's counter is initialized at -100. This shifts 100 votes from the unfavored candidate to the favored candidate. Total votes cast will not change. Table III shows as example.

TABLE III. CORRECT VS RIGGED

```
Correct Prog Pseudo-code
Initialize counters:
Mary count = 0000
Bob count = 0000
Read vote
If vote = Bob
Then add 1 to Bob count
If vote = Mary
Then add 1 to Mary count

File size* = 450 Bytes
Hash Value* = 45A3C29EA
Digital Signature* = 736A8B76C

Rigged Prog Pseudo-code
Initialize counters:
Mary count = +100
Bob count = -100
Read vote
If vote = Bob
Then add 1 to Bob count
If vote = Mary
Then add 1 to Mary count
File size* = 450 Bytes
Hash Value* = 68DE124A8
Digital Signature* = 88CC34A3

* values are examples to show concepts.
```

Even though the number of characters and file size are the same, the Hash Values and Digital Signatures are different. If the Correct Program is provided for testing and certification, the Hash Values and Digital Signature of the programs used at polling sites must be the same as the tested and certified program.

Shift votes based on random selection. If the unfavored candidate gets a vote, a random number is generated, say between 1 and 20. If that random number is a specific number, say 17, then the vote is counted for the favored candidate. This will shift 5% of the votes from the unfavored candidate to the favored candidate. Total votes cast will not change.

If the Rigged Program contained the following added code to shift 5% of votes based on a random number, the number of characters and file size will be different. The Hash Values and Digital Signatures also will be different. Again, if the Correct Program is provided for testing and certification, the Hash Values and Digital Signature of the program used at polling sites must be the same. See Table IV.

TABLE IV. RANDOM SELECT TO SHIFT VOTE

```
If vote = Bob
Then If RND(20) = 17
Then add 1 to Mary count
Else add 1 to Bob count
```

Execute rigged code only on election day. The code to alter the counters can be written so as not to take effect until actual vote counting begins on Election Day. See Table V.

TABLE V. RIGGED EXECUTES ON A DATE

```
If vote = Bob AND date = election date
Then If RND(20) = 17
Then add 1 to Mary count
Else add 1 to Bob count
If vote = Mary
Then add 1 to Mary count
```

Pre and post test data will not detect this rigged code. Hence, the rigged program could be used at polling stations. However, a recount of votes the next day will have different results. If code desk checking uses a correct program, lacks election date code, the correct program will have a different Hash Value and Digital Signature and file size from the rigged program used at the polling stations on election day.

Delete rigged code after election day. A rigged program can be written to self-delete the rigged code after votes are counted so that literally no post-election trace remains. But this changes the before and after election Hash Values and Digital Signatures. The change in the programs Hash Value will show the program changed for unknown reasons after the election.

To prove in court election software was rigged. The evidence needed to prove in court the program was rigged are 1) Hash Values of program, 2) Digital Signature of program, 3) Test data documentation, and 4) Separation of duties documentation, the testers were independent of the program's developers. The Hash Values will show integrity, nothing was changed in the program and properly identifies the program used. The Digital Signature will show non-repudiation, you wrote a rigged program.

c). Dead Voters Module

To prove in court that dead people voted requires the comparison of two databases, death certificates from the country's Department of Vital Statistics database and voter registration records from the country's Election Commission database Both databases have common data fields: first name, last name, date of birth, gender, current address, and in some cases Social Security Number.

Mismatches and data entry errors. The more complex are the rules regulating voter registration and voting, the more likely voter mistakes, clerical errors, and the like will be wrongly identified as "fraud" [32]. A report found that "most voter fraud are clerical errors or bad data matching practices" [2]. Comparing the two databases can have problems of mismatches and data entry errors. This can lead to errors in listing voters as dead [4, 8, 14]. Table VI is a list of some mismatches and data entry errors.

TABLE VI. MISMATCHES & DATA ENTRY ERRORS

- Same names but missing parts of birthdates.
- Is the name Terry or Terrie?
- Middle initial missing.
- Registered in two places due to moving.
- Out of 180 people, 2 can have the same DOB (month, day).
- Father and son have the same names, but the son has Jr. after name. They have the same address.
- Voter matches the death record but died after voting.
- Gender not entered.
- Have two very similar names, for example John H. Mandel and John H. Mandell.

Examples of mismatches and data entry errors. In the Georgia 2000 Election, there were 5,412 votes alleged to be cast by dead voters over a 20-year period. The allegations were based on mismatches and errors between voter rolls and death lists [4, 8]. In the Colorado 2020 Election, more than 3,000 voter records claimed to be fraudulent. It was found that people claimed dead and voted were alive [14]. Mismatch comparisons and data entry errors explain this. If 1,000,000 records were compared, with 1% mismatches & errors rate, you will have 10,000 dead voters.

To prove in court there were Dead Voters. The compared records from the Dept. of Vital Statistics and Election Commission must be scrubbed and cleaned (fix mismatches & errors). This is standard procedure for Big Data. Hash values of the database files need to be checked to ensure integrity, nothing was changed, and presented to the court. Digital Signatures also need to be presented to the court to show that the sources of the records were from the Dept. of Vital Statistics and Election Commission.

C. The Technology of Misleading Numbers

a) Statistics module:

"Misleading statistics refers to the misuse of numerical data either intentionally or by error. The results provide deceiving information that creates false narratives around a topic. Misuse of statistics often happens in advertisements, politics, news, media, and others" [5]. For example, "I have statistics that prove it is impossible." This statement contains errors in Statistical definitions. Statistics prove nothing. It only show/support/suggest/probability. Statistics expresses a level of confidence – 95% probably correct, but 5% possibility of being wrong. For example, 8 numbers on a lottery ticket to win has a probability of 1 in 13,983,816. So, is it impossible to win the lottery? But someone wins the lottery.

Conditions change over time. "Purposeful bias is the deliberate attempt to influence data findings without even feigning professional accountability. Bias is most likely to take the form of data omissions or adjustments to prove a specific point" [5]. This can lead to poor decision-making due to misinformation [5]. Here is an example of misleading statistics. Although the calculations can be correct, change in conditions are ignored. For example:

2014 election	Jane 59% of precinct #05
2018 election	Jane 45% of precinct #05
Probability: 1 in 14,000,000,000 (P< .0001). Therefore: 99.99% confident fraud occurred.	

An analysis compared the numbers and percentages of votes for a candidate in 2020 with those of another candidate in 2016. The concluded the statistical improbability of the winner winning the popular vote was 1 in 1,000,000,000,000,000 [31]. For the comparison between two candidates, the State noted that a calculation assumed that voters in a state would vote the same way in two consecutive elections four years apart. Because the elections were separate events by four years, any analysis based on this assumption is worthless [31].

This would be correct IF CONDITIONS WERE EXACTLY THE SAME AS THE PREVIOUS ELECTION. However, over the years, things change; different opponent candidate, demographics of precinct changes, more registered voters, economy changes, people move in and out of the precinct. Hence, the conclusion cannot be supported.

Criteria sampling vs random sampling. Again, calculations can be correct, but the design logic can be wrong. Hence, giving misleading conclusions. Statistics are based on random sampling; every member of the population has an equal chance to being selected. For example, two random samples are taken from the voter population. The first sample had 55% of the votes for Jane and the second sample had 58% votes for Jane. There is no significant difference between the two samples. However, if the first sample had 55% of votes for Jane and the second sample had 31% for Jane, there would be a significant difference, suggesting fraud with the second sample. See Fig. 1 Random sampling below.

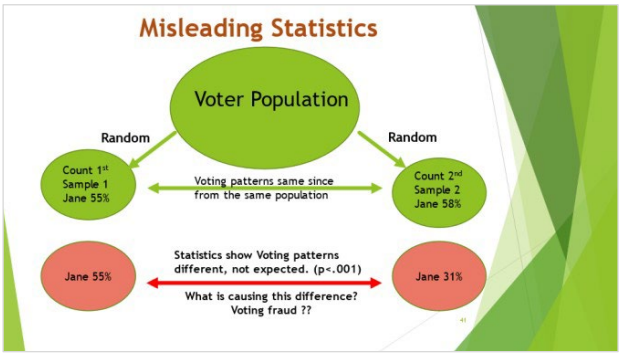

Fig. 1. Random Sampling.

If the first sample counted precincts that favored Jane, a criterion, and the second sample counted precincts that favored John, there would be a significant difference between Jane's counts in the two samples. Because of the criteria, you have two different populations. The statistics support the Precinct that favored John, voted mostly for John. See Fig. 2. Criteria sampling.

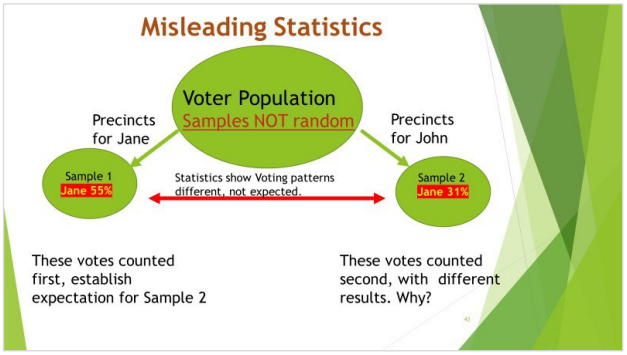

Fig. 2. Criteria Sampling.

For the early versus late comparison, the assumption is that early and late votes were randomly selected from the same population when they were not [31]. If you count the votes cast on election day first, then later count the votes that were absentee/early voting, you are dealing with two different populations; samples are not random from the same population. "You will end up with a statistical error called '**selective bias**.' To avoid this issue, you should always pick a **random sample** of people from the same population"[5]. Otherwise, any differences in voting counts will be due to different population characteristics. See Fig. 3. Two Populations.

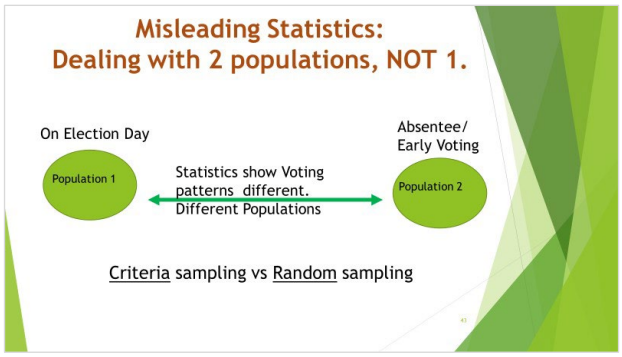

Fig. 3. Two Populations.

b) Benford's Law module

Benford's Law has been used inappropriately to try to show voter fraud [3, 9, 29].

"Social media users have been sharing posts that say a mathematical rule called Benford's Law provides clear proof of fraud in the U.S. presidential election. However, research papers and academics consulted by Reuters

consistently say that deviation from Benford's Law does not prove election fraud took place" [38].

Benford's Law looks at the 1st Digit frequency in a set of numbers, i.e., the digit "8" is 5% of first digits in a set of numbers in Fig 4. Benford's Law graph [13]. It is used to detect accounting fraud. Can it detect voter fraud? The following is an explanation as to what Benford's Law is, how it works, and why it is inappropriate to show voter fraud.

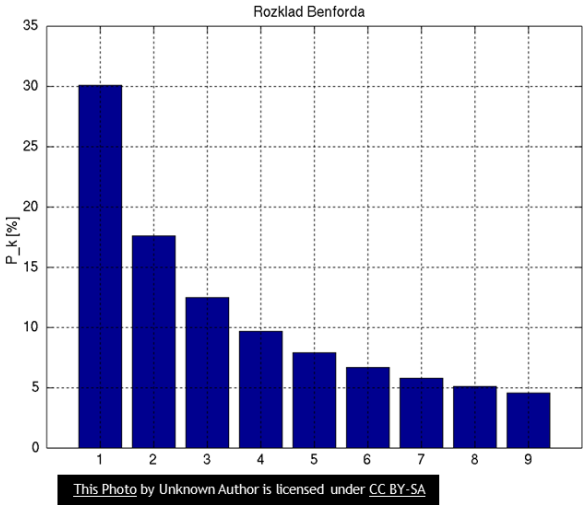

Fig. 4. Benford's Law graph.

Here is an example of Benford's Law on the election between Jane and John. See Fig. 5 and Fig. 6, Bob vs Sue, below. In this scenario, Jane wins the election over John. But Jane's voting results violate Benford's Law, while John's voting results agrees with Benford's Law. Does this show voter fraud favoring Jane?

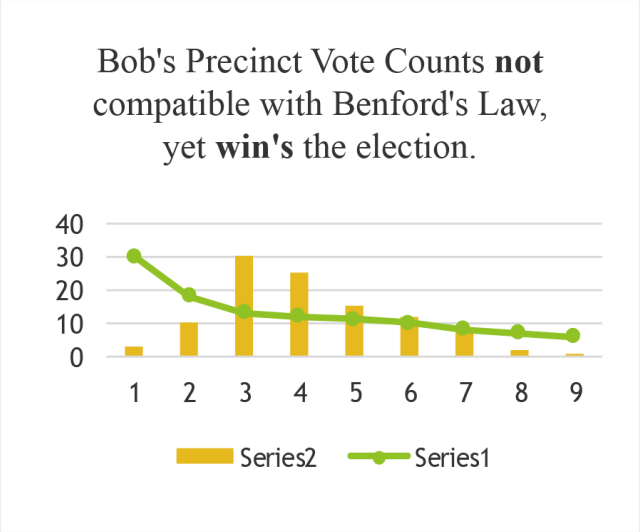

Fig. 5. Benford's Law violated yet win with higher votes.

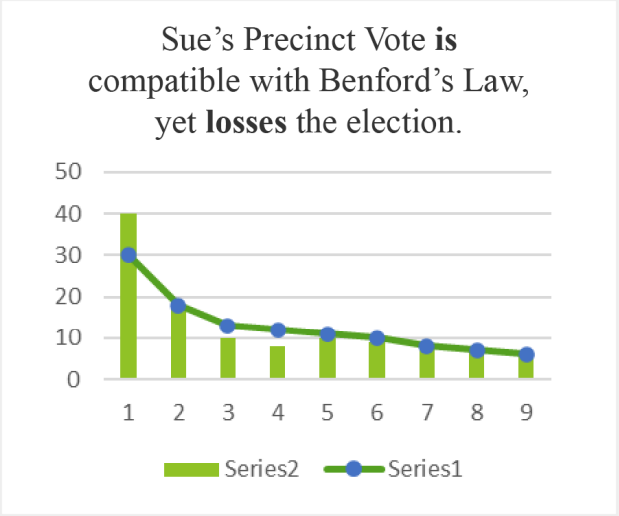

Fig. 6. Benford's Law agreed yet lose with lower higher votes.

Here is an example of precinct voting results.

	Jane	**John**	**Total**
Precinct 1	900	600	1500
Precinct 2	800	400	1200
Precinct 3	900	100	1000
Precinct 4	600	200	800
Precinct 5	800	100	900
Precinct 6	825	175	1000
Totals	**4825 WIN**	**1575**	**6400**

Note that Jane's 1st digits are high (9,8,9,6,8,8) because she got more votes and won. This violates Benford's Law. John's 1st digits are low (6,4,1,2,1,1) because he got less votes and lost. His data agrees with Benford's Law. In an election, numbers are DEPENDENT with each other. They have to add up to a total. Benford's Law requires numbers to be INDEPENDENT of each other, like accounting data.

Another reason against using Benford's Law is that it requires numbers with a big spread of magnitude order, i.e. 1,000's, 10,000, 100,000, 1,000,000 …. [13]. Precincts have small ranges; 1 to 3,000 due to counting of votes by hand when precincts were first established. Hence, Benford's Law is inappropriate to detect voter fraud.

VI. CONCLUSION

Can trust of elections be restored through education of election security and technology? Can education override the tools of propaganda, misleading information, emotions, and fake news? These are the tools to swaddling public opinion as feared by Socrates. Education creates a position of knowledge when discussing voter fraud. This paper provides content to educate people to think rationally and participate in intellectual democracy. This builds confidence in election voting and people can make informed decisions.

REFERENCES

[1] Blythe, S. E. (2008). Croatia's computer laws: promotion of growth in E-commerce via greater cyber-security. *European Journal of Law and Economics*, 26(1), 75-103. https://dx.doi.org/10.1007/s10657-008-9053-y

[2] Brennan Center for Justice (January 31, 2017). *Debunking the Voter Fraud Myth*. New York University School of Law. https://www.brennancenter.org/sites/default/files/analysis/Briefing_Memo_Debunking_Voter_Fraud_Myth.pdf

[3] Brown, M. (2012). DOES THE APPLICATION OF BENFORD'S LAW RELIABLY IDENTIFY FRAUD ON ELECTION DAY? A Thesis submitted to the Faculty of the Graduate School of Arts and Sciences of Georgetown University. https://repository.library.georgetown.edu/bitstream/handle/10822/557850/Brown_georgetown_0076M_11716.pdf?sequence=1&isAllowed=y

[4] Buettner, R. (2004). Exposed: Scandal of Double Voters. *Daily News* (N.Y.), Aug. 22, 2004

[5] Calzon, B. (Dec 28th, 2021). *Misleading Statistics Examples – Discover The Potential For Misuse of Statistics & Data In The Digital Age*. Data Pine, Berlin, Germany. https://www.datapine.com/blog/misleading-statistics-and-data/

[6] Corbitt, T. (2002). Encryption and digital signatures. *Management Services*, 46(10), 20. https://libproxy.txstate.edu/login?url=https://www.proquest.com/trade-journals/encryption-digital-signatures/docview/234342860/se-2?accountid=5683

[7] Crowell, W. P. & Miller, G.A. (2021). Trust in U.S. Elections Is Slipping. It's Time to Go on Offense. Barron's July 27, 2021. https://www.barrons.com/articles/trust-in-u-s-elections-is-slipping-its-time-to-go-on-offense-51627328925?form=MY01SV&OCID=MY01SV

[8] Davis, J. (2000). Even Death Can't Stop Some Voters. *Atlanta J.-Const*., Nov. 6, 2000.

[9] Deckert, J. & Myagkov, M. & Ordeshook, P.,C. (2011). Benford's Law and the Detection of Election Fraud. *Political Analysis* (2011) 19:245–268. doi:10.1093/pan/mpr014

[10] Eau Claire (2022). Network: Establishing Windows File and Folder Level Permissions. University of Wisconsin, Eau Claire, WI. https://www.uwec.edu/kb/article/drives-establishing-windows-file-and-folder-level-permissions/

[11] Crowdstrike (September 23, 2022). LOG FILES EXPLAINED. https://www.crowdstrike.com/cybersecurity-101/observability/log-file/

[12] Flaherty, D. C., & Lovato, C. (2014). DIGITAL SIGNATURES AND THE PAPERLESS OFFICE. *Journal of Internet Law*, 17(7), 3-12. https://libproxy.txstate.edu/login?url=https://www.proquest.com/trade-journals/digital-signatures-paperless-office/docview/1512406552/se-2?accountid=5683

[13] Golbeck, J. (November 12, 2020). *Op/ed: Breaking the (Benford's) Law?* Maryland Today, University of Maryland. https://today.umd.edu/oped-breaking-benfords-law-1ccdc2ba-c7b0-4515-a1ea-103f16607f5c

[14] Guajardo, A. (2020). *JeffCo Republican Party claims dead people voted in the election, Denver7 discovered some are alive*. Denver 7. Posted at 11:03 AM, Dec 19, 2020. https://www.thedenverchannel.com/news/local-news/jeffco-republican-party-claims-dead-people-voted-in-the-election-denver7-discovered-some-are-alive

[15] Hill, R. (Mar 2020). Coding for Voting. *Communication of the AMC*, 63(3), 8-9. https://dx.doi.org/10.1145/3379491

[16] Hoffman, S. (2010). An Illustration of Hashing and Its Effect on Illegal File Content in the Digital Age. *Intellectual Property & Technology Law Journal*, 22(4), 6-0_1. https://libproxy.txstate.edu/login?url=https://www.proquest.com/scholarly-journals/illustration-hashing-effect-on-illegal-file/docview/227149161/se-2?accountid=5683

[17] Imperva (2022). Honeypot. Austin, Tx. https://www.imperva.com/learn/application-security/honeypot-honeynet/#:~:text=A%20honeypot%20is%20a%20security%20mechanism

[18] IRS extends acceptance of digital signatures, emailed documents. (2021). *Practical Tax Strategies*, 106(2), 1. https://libproxy.txstate.edu/login?url=https://www.proquest.com/trade-journals/irs-extends-acceptance-digital-signatures-emailed/docview/2522189641/se-2?accountid=5683

[19] Karp, J. A. & Nai, A. & Norris, P. (2018). Dial 'F' for fraud: explaining citizens' suspicions about elections. *Electoral Studies*, 53 (2018), pp. 11-19.

[20] Klonoski, R. J. (2014). Plato's Invisible Hero of Democracy: Socrates in the Republic and Crito. Journal of Academic Emergency Medicine Case Reports / Akademik Acil Tip Olgu Sunumlari Dergisi, 5(10), 7–20.

[21] Kulke, S. (2020). 38% of Americans lack confidence in election fairness. Northwestern Now, December 23, 2020. https://news.northwestern.edu/stories/2020/12/38-of-americans-lack-confidence-in-election-fairness/ (accessed August 3, 2021).

[22] Laughlin, N, & Shelburne, P. (2021). How Voters' Trust in Elections Shifted in Response to Biden's Victory: A survey research project gauging how voters responded to unprecedented electoral conditions. *Morning Consult, Inc*. Jan. 27, 2021. https://morningconsult.com/form/tracking-voter-trust-in-elections/ (accessed August 3, 2021).

[23] Levy, M. (2021). Winning cures everything? Beliefs about voter fraud, voter confidence, and the 2016 election. *Electoral Studies* 74(2021)102156. https://doi.org/10.1016/j.electstud.2020.102156

[24] Life, T. S. (2017, July 18). Why Socrates Hated Democracy. World History Encyclopedia. Retrieved on 6/22/2021 from https://www.worldhistory.org/video/1223/why-socrates-hated-democracy/

[25] Lubben, N., Karenfort, J., & Sommer, C. (2001). Recent developments in telecommunications and Internet regulation in Germany. *International Financial Law Review*, , 99-104. https://libproxy.txstate.edu/login?url=https://www.proquest.com/scholarly-journals/recent-developments-telecommunications-internet/docview/233194444/se-2?accountid=5683

[26] Manley, G. (April 20, 2020). What Is MD5 and Why Is It Considered Insecure? Section. https://www.section.io/engineering-education/what-is-md5/ (accessed June 10, 2021).

[27] Masters, A. B. (Nov. 15, 2020). Benford's Law and Election Data: Why do first digits of votes diverge from Benford's distribution? Accessed: https://anthonybmasters.medium.com/benfords-law-and-election-data-1b69d6ab7a0

[28] Melashchenko, A. O., & Perevozchikovaa, O. L. (2011). The national system of digital signatures as an open system. *Cybernetics and Systems Analysis, 47*(5), 827-834. https://dx.doi.org/10.1007/s10559-011-9362-y

[29] Mebane, W. R. (Nov. 10, 2020). Inappropriate Applications of Benford's Law Regularities to Some Data from the 2020 Presidential Election in the United States. University of Michigan, Haven Hall, MI 48109-1045. Professor Mebane in the Department of Political Science and Department of Statistics, and a Research Professor , Center for Political Studies, University of Michigan. https://websites.umich.edu/~wmebane/inapB.pdf

[30] Mercuri, R. T. & Neumann, P. G. (June 2021). Inside Risks: the Risks of Election Believability (or Lack Thereof). *Communications of the ACM*, 64(6), 24-30. DOI:10.1145/3461464.

[31] Miao, W, & Pan, Q. & Gastwirth, J.L. (2022) A Misuse of Statistical Reasoning: The Statistical Arguments Offered by Texas to the Supreme Court in an Attempt to Overturn the Results of the 2020 Election. *Statistics and Public Policy*, 9:1, 67-73, DOI: 10.1080/2330443X.2022.2050327

[32] Minnite, L.C. (2007). The Politics of Voter Fraud. Project Vote, Washington D.C. https://www.projectvote.org/wp-content/uploads/2007/03/Politics_of_Voter_Fraud_Final.pdf

[33] Montmorency, R. (July 10, 2020). Why Socrates Hated Democracy. *Nspirement*. Retrieved on 6/22/2021 from https://www.nspirement.com/2020/07/10/why-socrates-hated-democracy.html

[34] Moore, P. (May 27, 2016). Why an unsalted MD 5 hash is bad practice. Stefan. https://svanas.medium.com/why-an-unsalted-md5-hash-is-bad-practice-6a0d7d017856 (accessed June 10, 2021).

[35] Norris, P. (2014). Why Electoral Integrity Matters. Cambridge University Press, New York

[36] Nurmi, H. & Salomaa, A. & Santean, L. (1991). Secret Ballot Elections in Computer Networks. *Computers & Security*, 10 (1991) 553-560.

[37] Rasjid,Z. E. & Soewito, B. & Witjaksono, G. & Abdurachman, E. (2017). A review of collisions in cryptographic hash function used in digital forensic tools. *Procedia Computer Science*, 116, 381-392. ISSN 1877-0509, https://doi.org/10.1016/j.procs.2017.10.072.

[38] Reuters (Nov. 10, 2020). Fact check: Deviation from Benford's Law does not prove election fraud. https://www.reuters.com/article/uk-factcheck-benford/fact-check-deviation-from-benfords-law-does-not-prove-election-fraud-idUSKBN27Q3AI

[39] Rihaczek, K. (1994). Data interchange and legal security - Signature surrogates. Computers & Security, 13(4), 287. https://libproxy.txstate.edu/login?url=https://www.proquest.com/scholarly-journals/data-interchange-legal-security-signature/docview/207373815/se-2?accountid=5683

[40] Sances, M.W. & Stewart III, C. (2015). Partisanship and confidence in the vote count: evidence from U.S. National elections since 2000. *Electoral Studies* (40) (2015), pp. 176-188.

[41] Stewart III, C. & Ansolabehere, S. & Persily, N. (2016). Revisiting public opinion on voter identification and voter fraud in an era of increasing partisan polarization. *Stanford Law Rev*., 68 (2016), pp. 1455-1489.

[42] University Information Technology Services (January 2018). In Windows, what are file attributes, and how can I change them? Indiana University. https://kb.iu.edu/d/aift#:~:text=To%20view%20or%20change%20the

[43] Vlastos, G. (1983). The Historical Socrates and Athenian Democracy. *Political Theory*, 11, 495-516.

[44] Xenakis, J. J. (1998). John Hancocks, electronically. CFO, 14(3), 30. https://libproxy.txstate.edu/login?url=https://www.proquest.com/trade-journals/john-hancocks-electronically/docview/196812320/se-2?accountid=5683