WHAT: Senate Hearing on the Election Audit in Maricopa County (AZ)
WHEN: 15July2021
BACKGROUND: Senators Karen Fann & Warren Peterson receive briefing from Doug Logan (Cyber Ninjas CEO, & expert in application security), Ken Bennett (former Senator & SecState), & Ben Cotton (expert in digital forensics).
Video link: https://www.youtube.com/watch?v=PG_uvVthV68

What was received? (53:00 mark)
- 385 Tabulators (Dominion ICP2)
- County EMS Server (election management system)
- Physical devices correlating to EMS work station function, to the adjudication function
- 11 hard drives (contain cloned images of various other systems within in the eco system/network).

Note: on these 11 drives, no forensically secure process was used to image these original systems, during the election process. So the dates/times on those systems were altered by their cloning process.
- Forensic copy made on all devices (physical and digital form).
- Performed key word searches
- Searched for anomalous/unauthorized internet connections to system.
- Searched for malware on systems.
- Created virtual systems of those forensic images to conduct live memory analysis of those virtual systems.

What was not received from the county (but was supposed to, to perform forensic analysis)? (55:30 mark)
Ranked in order of criticality:
- Router configuration files
- Router data

Note: County officials originally agreed to provide access to this data, in addition with the Splunk netflow data (encompassing data 90days prior to election, & 60days after election). In May, the county declined to provide this data, stating it would compromise law enforcement operations, & PII info of Maricopa residents.

Why is it important to have this data? (57:00 mark)
- The routers are critically important to verify issues the audit is discovering.

Item 1: We know via public record & public statements that there's an element of a unauthorized breach in the election system, during the Nov2020 election. The Registration server that was public facing, had unauthorized access. We know that the county knew/accepted it as an unauthorized breach, because the county issued a letter (in Jan2021) to residents who were impacted.
Item 2: The audit has shown that there are severe security problems with the way the Election Management System & network were maintained.
Ex: An average home computer will have updated/current antivirus software & patched updated within the week. This was not the case with any of the Maricopa Election Management Systems. The last time the antivirus was updated on these systems was Aug2019 (when Dominion software was uploaded onto these systems).
There have been no operating system updates/patches or antivirus updates since Aug2019.
This creates a tremendous vulnerability to these systems & could be hacked in <10min.
Sen Warren Peterson: Are the county's security concerns valid for withholding these routers?
No.
Rationale: A router is simply a 'mail courier'. When sending a letter, you write to & from addresses. The mail courier (or router) looks at the letter & knows where to route/send the letter (or data). The courier (or router) does not have the actual content of the letter. So, no PII would be seen.

IP & Mac Addresses *(1:04 mark)*
MAC Address is a unique identifier for the communicating device that sent the packet.
Sheriff Penzone said they would not get the router, due to security issues.
Q: If security is an issue, then why have these routers in the 1st place?
What the Maricopa officials tell the public is drastically different than reality in response to a legal subpoena.
From a public standpoint, Maricopa CO repeatedly stated that the election system was a closed system (it didn't touch the internet), thus, couldn't co-mingle with the data from the Sheriff's dept or other Maricopa office space. The fact that they respond to an official subpoena with justification that producing that data would compromise other Maricopa networks (that do connect to the network), is an admission that things are not like what the told the American public.

Splunk Logs, & Passwords (1:07 mark)

Issue: The Windows security log (on the EMS server) only goes back to 5Feb2021. Thus, we need to 'fill in the blanks' between 1Nov2020 - Feb2021.

Additionally, the security log was set to only retain 20MB of data. If the system goes over 20MB, it deletes the oldest entry.

That being said, on 11Mar2021, we found 37,646 queries for a blank password, on a system that only contained 8 accounts. Clearly, a script was executed by the user (EMS admin), which ultimately 'deleted' the older entries.

So, we can't see the critical info between 1Nov20-11Mar21, & we don't have the logs to know where did this script came from. If I had the router/Spluck info, I could tell who was accessing the system & where the query came from.

Tokens (1:11 mark)

Sen Warren Peterson: Why do you need the Tokens?

Ben Cotton: Within the admin functions of Dominion ICPs, there are a couple different levels/roles in the EMS software. I have recreated a complete virtual EMS. I can burn a FOB (ibutton) key that gives me security access for whatever role I am permitted to burn in EMS. In the current EMS construct, there's only one role (a poll worker). Within the Dominion ICPs, a poll worker's role (even if given admin access), do not get access to the configuration of that device. So, on each of these ICP2, we know there are 2 NIC (network interface card?) cards, they can be configured with wireless and cellular modems. So the purpose of requiring this info is to get a configuration for each of those systems that shows how they were configured, what was (or was not) enabled, and more importantly, retrieve the MAC addresses for each device, & simply find out if any of the MAC addresses connected to the internet.

Sen Peterson: It sounds like Maricopa doesn't have access to this, & only Dominion has access. Why is it important for Maricopa to have this?

Ben Cotton: Your assumption appears to be true. When we asked them for admin level FOBs, we received a response saying they have provided everything that they have access to. The inference: only the contract Dominion employees have access to configure the ICPs, & to get access to the configuration or technician aspect of those ICPs.

ISSUE: If a county can't validate the configuration independently from the vendor, then how do you validate an election system that it is safe to vote? You can't. A county is responsible to validate/certify those systems prior to a vote.

Based on the evidence, Maricopa officials don't have the ability to independently verify the configuration of their systems without the Dominion employees.

Sen Peterson: We need a response that the county has this, & they can audit, & can look at tabulators. Need to ensure that the state is at a higher admin then the vendor.

Sen Karen Fann: Board of supervisors were going to perform the audit with us, but decided to do their own audit (with Pro VV & SLI). Their 2 audits did not come up with same results that Cyber Ninjas are showing. Why?

Ben Cotton: I would suspect that Pro VV & SLI audits didn't address the cyber security aspects that we did. Nor did they look into the commonality of passwords. We found that for all the administrative accounts, they shared the same password. That password appears to have been established at the same time that the Dominion software was installed (Aug2019). And appears to not have been changed during the entire time frame.

Sen Peterson: What would be the recommendation or industry standards with passwords?

Ben Cotton: A shared password eliminates one of the critical items of cyber security; we can't attribute the actions of a given user name, back to an individual. Because these were all shared passwords, anyone who had access, with admin account, could have been able to use any other admin account. So accountability is out the window.

We're talking about the EMS admin password, adjudication admin password...

There's a correlation between Dominion Window accounts & Dominion functions. You can't separate the 2.

EX: When you log into the EMS server, you will enter EMS admin user name, then password. This provides single sign-on access to all the functions of the EMS software. So, these 2 are tied together.

Sen Peterson: You do have the admin password for the server, but not the admin passwords for the tokens for Dominion machines?

Ben Cotton: I have the admin passwords (for the server), but not the authentication FOB, because it requires both of those items (for tabulator authentication). We were able to recover the admin passwords for the tabulator, but because we don't have the ability to burn the ibutton FOBs... it's a multifactor authentication for the tabulator.

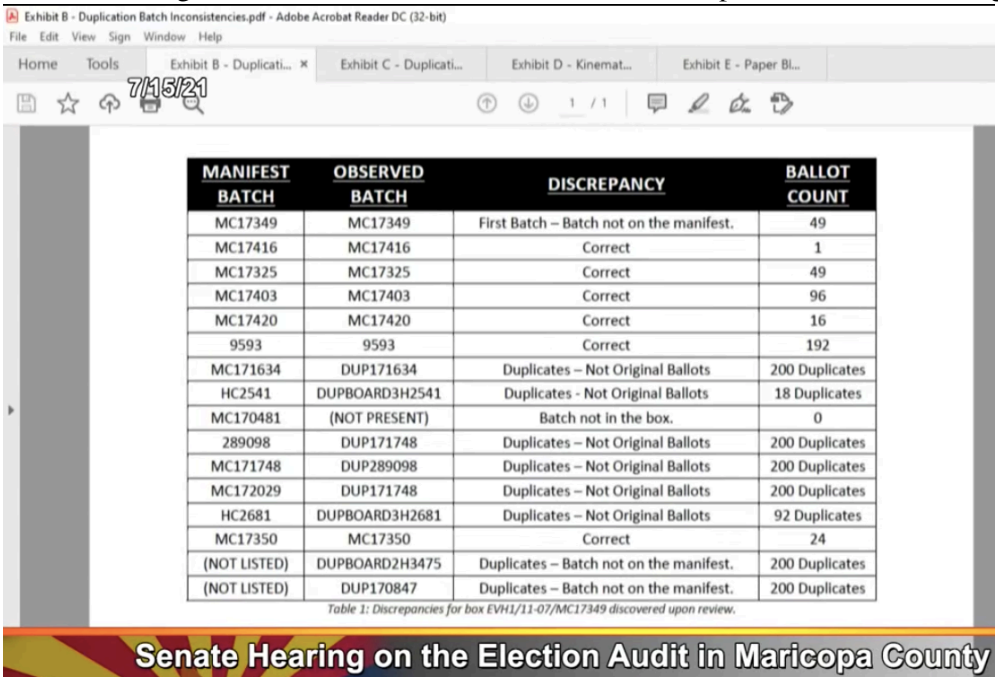
Sen Peterson: It appears that only Dominion has that?

Ben Cotton: Correct. Another critical aspect as to why I need these Splunk logs: Anonymous log-ins are normal part of windows activity. If you access a shared file in Windows (called S&V share). Part of that request, there's anonymous log-on action to the server that has the shared file. That is followed by authentication of the user (who is seeking access). As part of that normal anonymous action, the Windows logs will record the user name that is requesting the action. It will

record the IP address & the host name of the originating client. What requires additional correlation with netflow data, we're seeing anonymous log-ins at the system level that doesn't follow that pattern of windows normal behavior. Thus we need to have the additional data to validate what that activity is.

Issues With Hand Counting Ballots (1:23:30 mark)

Doug Logan: Every audit that I have been a part of, I've been able to ask questions with the organization. One of the most difficult things with this audit is to not be able to ask questions & have feedback (from Maricopa Co).
Regarding duplicated ballots, we had difficulty on how they were recorded & received.
Exhibit B: Original manifest on one of the boxes that had duplicates in it. The state gave us this.

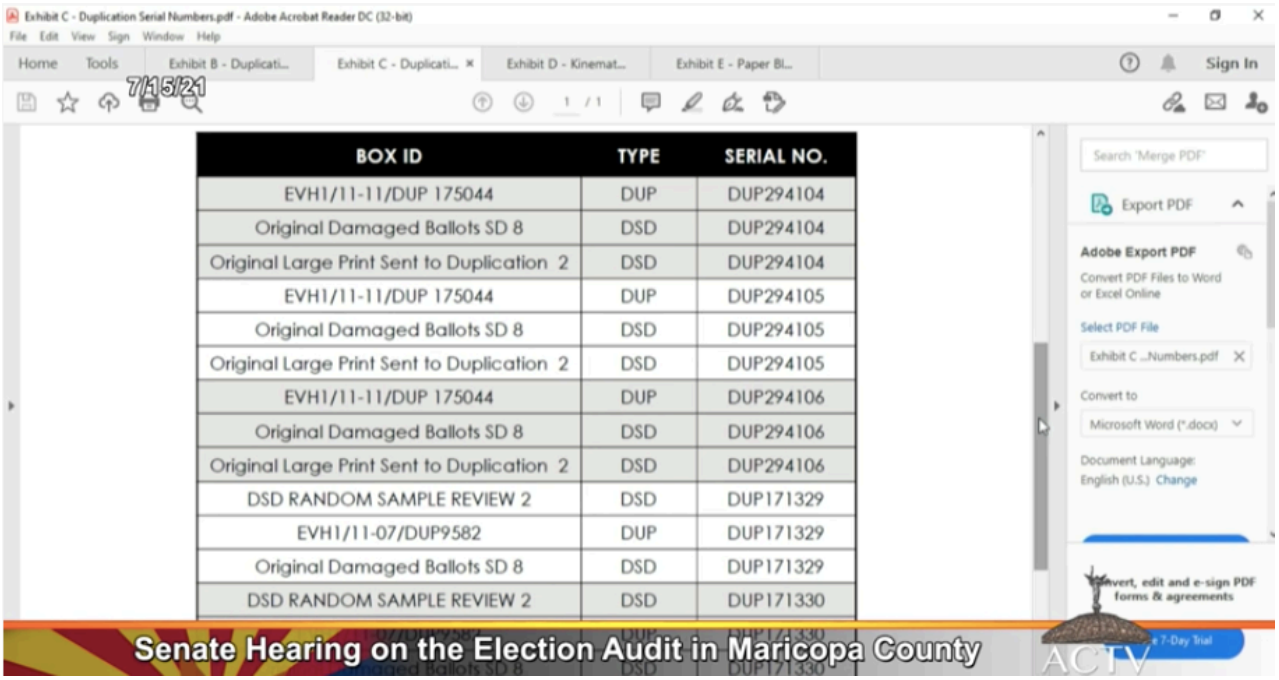


MANIFEST BATCH	OBSERVED BATCH	DISCREPANCY	BALLOT COUNT
MC17349	MC17349	First Batch – Batch not on the manifest.	49
MC17416	MC17416	Correct	1
MC17325	MC17325	Correct	49
MC17403	MC17403	Correct	96
MC17420	MC17420	Correct	16
9593	9593	Correct	192
MC171634	DUP171634	Duplicates – Not Original Ballots	200 Duplicates
HC2541	DUPBOARD3H2541	Duplicates - Not Original Ballots	18 Duplicates
MC170481	(NOT PRESENT)	Batch not in the box.	0
289098	DUP171748	Duplicates – Not Original Ballots	200 Duplicates
MC171748	DUP289098	Duplicates – Not Original Ballots	200 Duplicates
MC172029	DUP171748	Duplicates – Not Original Ballots	200 Duplicates
HC2681	DUPBOARD3H2681	Duplicates – Not Original Ballots	92 Duplicates
MC17350	MC17350	Correct	24
(NOT LISTED)	DUPBOARD2H3475	Duplicates – Batch not on the manifest.	200 Duplicates
(NOT LISTED)	DUP170847	Duplicates – Batch not on the manifest.	200 Duplicates

Table 1: Discrepancies for box EVH1/11-07/MC17349 discovered upon review.

Reference Observed Batch. The first couple are correct, but DUP171634... note name convention looks to be an original (MC171634), but it actually is a duplicate.
Note: If a ballot that can't be run through the tabulator (ie damaged, braille ballot, or Uniform Oversees Citizen Absentee Voter Act (UOCAVA), etc), they have to create a duplicate & then run through tabulator.
So there's original ballots & then the duplicates.
Approx 50,000 total = 25,000 (originals) + 25,000 (duplicates).
To ensure ballots are not double counted, it's very important to be able to match up 1 to 1. In fact, there's a Statute that mandates there's to be a serial # on the original that matches up to the serial # on the duplicate, to make sure they are match 1 to 1. Make sure the original is exact same as the duplicate. When we received a manifest of the state's originals & realized they were duplicates, it creates things that are a lot more complicated/difficult for us.
Ex:
-Several items that were not listed on the manifest that were actually in the box
- There's items on the box that wasn't observed on the manifest
- With the braille ballot box, it was labeled braille but there were other ballots that we weren't expecting to be there.

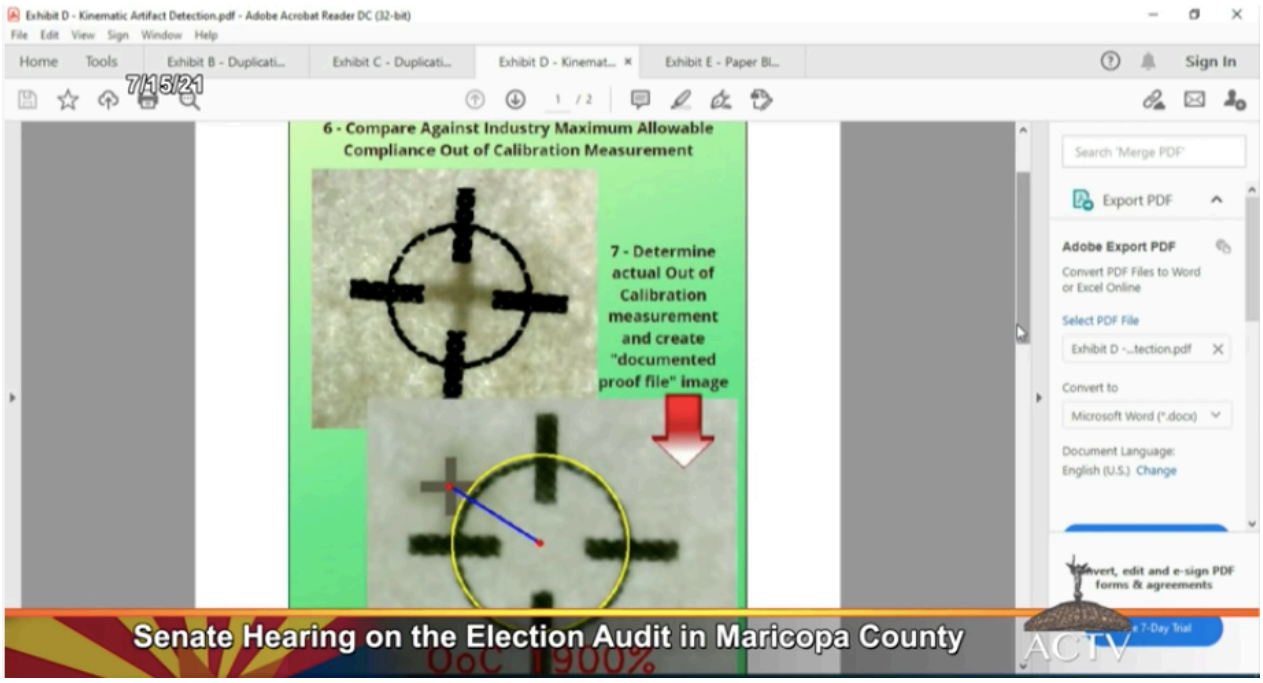
Exhibit C (1:28 Mark)



BOX ID	TYPE	SERIAL NO.
EVH1/11-11/DUP 175044	DUP	DUP294104
Original Damaged Ballots SD 8	DSD	DUP294104
Original Large Print Sent to Duplication 2	DSD	DUP294104
EVH1/11-11/DUP 175044	DUP	DUP294105
Original Damaged Ballots SD 8	DSD	DUP294105
Original Large Print Sent to Duplication 2	DSD	DUP294105
EVH1/11-11/DUP 175044	DUP	DUP294106
Original Damaged Ballots SD 8	DSD	DUP294106
Original Large Print Sent to Duplication 2	DSD	DUP294106
DSD RANDOM SAMPLE REVIEW 2	DSD	DUP171329
EVH1/11-07/DUP9582	DUP	DUP171329
Original Damaged Ballots SD 8	DSD	DUP171329
DSD RANDOM SAMPLE REVIEW 2	DSD	DUP171330

Ex: Serial numbers should be unique. So an original ballot should have a unique serial #, & its duplicate should have the same serial #.
Column1 (**Box ID**): Box that ballot came from
Column 2 (**Type**): DUP (duplicate) or DSD (original ballot)
Column 3 (**Serial #**)
Note: in column 3, there are serial #s in groups of 3, which shouldn't happen. So we have 2 original ballots that had the same exact serial #. and only one that were duplicated from it.
There's also some ballots that don't have any serial #.
So the statue was not followed, which adds a lot of confusion. It makes it very difficult (if not impossible) to do an audit.

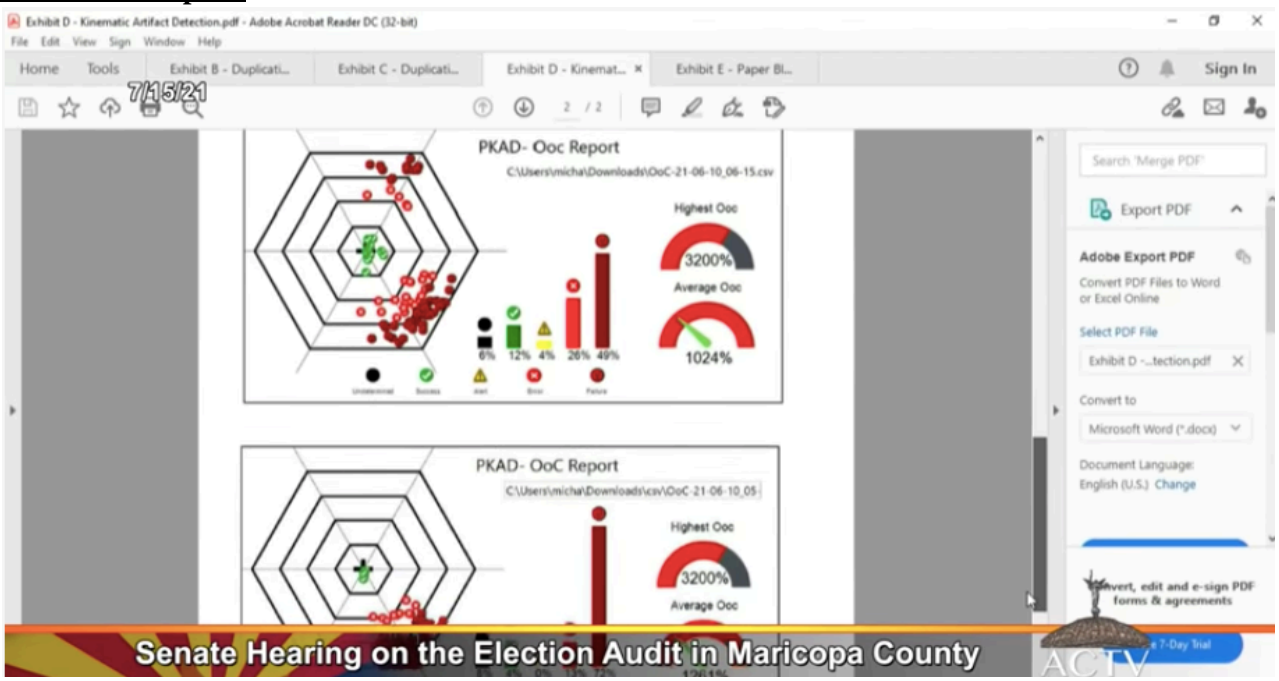
Paper Examination Issues (1:31 mark)
Exhibit D:



We used Kinematic Artifact Detection to look at ballots processed (to figure out how they worked/function).
Ballots are designed/aligned such that if the ink bleeds through, it won't impact the other side.

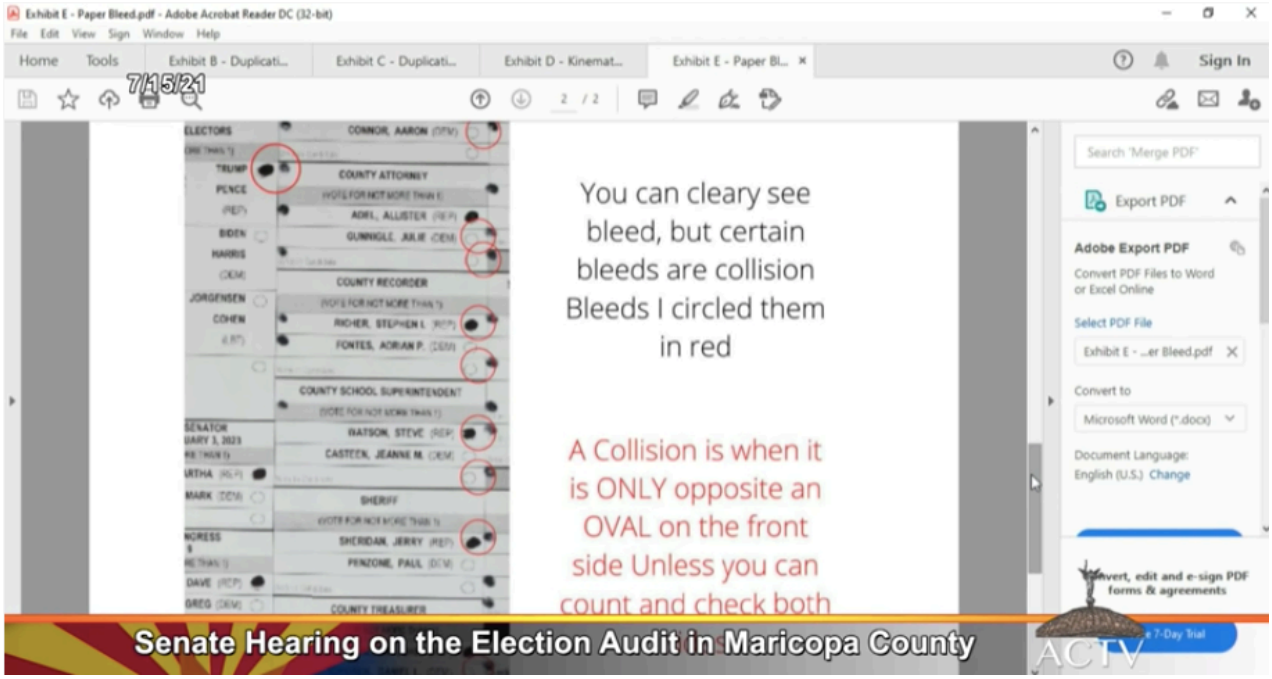
If properly aligned, the cross should be in the circle, like a cross-hair (if you held the paper up in the back-light).
Top image is slightly offset. This is the max threshold to be offset, so there are no issues.
Bottom image: cross is 1900% offset. This is from an actual ballot from Mericopa that was out of alignment.

PKAD Ooc Report:



Graphic: you want to be in the bullseye. Note the check marks.
The average offset was 1024%. The worst ballot alignment was 3200%.
Sen Peterson: What happens to these offset ballots?

Exhibit E (1:34 mark):



If it bleeds through, it could potentially cause an over vote and/or an unintended vote.
Note: If there is a bleed-though, there shouldn't be an issue since the county uses 'votesecure' paper. Votesecure paper has a special coating on it.
Next Image: Here is an actual ballot with bleed through. Our ongoing analysis will try to answer the impact of bleed-though. Again, there shouldn't be bleed-through, but we are seeing a lot of bleed-through, and ballots printed on very thin paper.

Sen Karen Fann: What causes such an offset?
The printer is not properly calibrated.
Most of the ballots printed from Ron Beck Firm were spot on, but there was a lot of ballots on demand, that were printed at the voting centers. Approx 168,000 ballots (election day) were printed on demand. We're actually seeing more than that & trying to figure out where they were printed & what that is tied to.

Back up to the paper examination issue. (1:38 mark)
Maricopa claims that they use paper, but we're seeing that they are not. How do we get documentation as to what the truth is?
We can request info on paper purchase, where did they purchase

Voter Date Analysis (1:38:30 mark)
Sen Karen Fann: Regarding canvassing, it seems that the only way to verify is to canvass. However, the Dept of justice sent a letter that they were concerned about voter intimidation. Interesting after the White House announced that they were going to knock on the door for vaccination verification.
Is canvassing necessary?
Based on the data we are seeing, I highly recommend canvassing. We need to know if it is real problems or clerical errors.
Ex: 74,243 mail in ballots, but no clear record of them being sent.
Note: **EV32** (gives record when a ballot is sent) & **EV33** (gives a record when a ballot is received).
So, **EV32 > EV33.**
Also, we can tie mailed ballots to a specific individual. So, we have 74,243 ballots that came back, but no clear indication that they were sent. 74k is a large number & merits knocking on doors.
Sen Peterson: How did you come up with that?
Looking at EV32 & EV33 forms from the county.
Sen Karen Fann: Is there another way to get that info?
Request info from the US postal service, & there's additional records of rejected/returned ballots.

Voter Rolls (1:43 mark)
Issue: 11,326 people were not on the 7Nov-version of the voter rolls (which was after votes were cast), but they show up on 4Dec-version of the voter roles. Note that these voters show as having cast a ballot for this election.
I cannot think of an explanation for this, but would like to ask the county for some type of explanation.

Issue: AG Hobbs requested the registration date for voting be moved up to election day, but a court case ordered it be moved back to 15Oct. Based on the registration info, we found in the voter roles, 3,981 individuals voted in this election, their data showed up in the canvass, but they were registered after 15Oct.

Issue: 18,000 voted in a election, but were soon removed from the voter roles after the election.
The original voter records are kept at the county level (shared electronically on a daily basis with the SoS office),
SoS receives info from vital records & courts, then sent to county level (inform who died, incompetent, loss of voting rights, etc).

Envelopes (1:47 mark)
Issue: We have an affidavit that specifically stated that when mail-in ballots were received, there were so many, that the standards were reduced every every time. Initially there were 20pts of comparison for signature. Then after some time they were told to go to 10pts of comparison, then 5pts. Eventually they were told to let every mail-in ballot to go through.
It's important to get the mail-in ballot images to see
how many blank signatures went through, because it could have a material impact of the election.
Sen Karen Fann: Do we not have those images of the envelopes?
We do not have those images. Maricopa stated that they provided us with images of the envelopes, but specifically the folder they pulled for us on a specific drive, deals with voter registration details. It has nothing to do with the receiving of ballots. We specifically asked the county, "Are you saying that in that folder we should have the envelopes that were utilize to deliver in this past election?" Their response was: There's envelopes in that folder." So they did not clearly answer our question.
Mr Bennett: I recommend they be re-subpoenaed. On a separate device, not co-mingled with other folders. Their response is that it's on the Lacie 5TB HD, affidavits folder, that's 1.83TB big.

An extensive forensic search for the mail-in ballots, was done on the drive & the only images contained on the Lacie drive are the original voter registration affidavits. Nothing to do with the mail-in ballots.

List (1:50 mark)

Sen Peterson: Summarize what you need to complete the forensic audit (that hasn't already been mentioned).

-Regarding the changes to the voter rolls, there were things that shouldn't have changed. Request a full back up copy of voter roles. Who made the changes? When? Why? IP addresses.

- Chain of custody: challenge every aspect of chain of custody.
- Regarding duplicate ballots, there's software (Novis?) that's used & part of the duplication process. It was discovered in a court case that some of the duplication was not properly attributing results for the original candidate.
- Any reports of the breach with voter rolls (ie where Maricopa announced to voters that there was a breach in security). There's been minimal info/reports on that. Any internal reports, the level, & how far would be helpful. Were the systems impacted this election cycle?

Sen Karen Fann: Is this the same breach where the FBI raided that house?

Mr Logan: I believe that is the same.

- We request that all portable media, or external hard drives that contained election definitions, election results, backups, or similar data... we know from photos from Mtech that there were at least 3 orange drives, which we received one of them. And reviewing the wording of the subpoena "portable media" & "external drives" were not included. We believe there are backups that would help us in our analysis.
- Election Dept shares a network with the sheriff's Dept. Request a network diagram to show how it is connected.
- Request digital copies of all versions of policies/procedures associated with election.

Ex: Ballot storage is not clearly written out.

- Subpoena tabulation logs (Blue sheets)
- Subpoena records of all mailed out ballots & what was rejected.
- Copies of all files transmitted for duplicating damaged ballots. To print ballots, there had to be a request sent.
- Records of paper distributed to vote centers.
- Info dealing with adjudication of ballots.
- Total count of UOCAVA ballots. How were they sent? How were they received?