December 3, 2020

King et al. v. Whitmer et al., **Case No. 2:20-CV-13134**

United States District Court for Eastern District of Michigan

Expert Report of Russell J. Ramsland, Jr.

Russell J. Ramsland, Jr.

1) There are many reasons to be concerned about the Dominion Voting System and the results it produces. It is well documented and demonstrated that it's heritage and software origins are extremely unsettling, given its close relationship to Smartmatic and Scytl, facts that have only become clearer with the 4 redacted declarations I have now seen from Spider. For this reason, any analysis as to the integrity of any election conducted using Dominion should be executed with a healthy degree of skepticism, and evidence of abnormal results should be over-weighted, if anything.

Our team has extensive experience as white hat hackers and employ many methodologies and tools to trace and certify connections between servers, network nodes and other digital properties and probe for network system vulnerabilities. In addition to Robtex and Spiderfoot, we also employ such tools as Whois, GeoIpLookup, nslookup, host, ipinfo.io, etc.

From our own company's work, I can attest to the credibility and veracity of the information contained in the four redacted declarations by Spider. Along with several others, we have found many of the same connections, relationships and vulnerabilities. Further, Clarity Elections and Scytl are integral to the network as well as Dominion and Edison Research and they too have multiple vulnerabilities and their vulnerabilities represent further vulnerabilities into Dominion.

For instance, inside the SCYTL System at a point called staging.scytl.us, malware called QSnatch is visible. QSnatch represents a deep vulnerability to any election system that touches it such as Dominion and Edison Research. QSnatch characteristics include:

- **CGI password logger -** This installs a fake version of the device admin login page, logging successful authentications and passing them to the legitimate login page.
- **Credential scraper** – This grabs the credentials of any administrator whose system loads any information into Scytl or Clarity Elections which includes Dominion and Edison Research. This means the credentials of every county election official of every state where Dominion manages elections in the U.S. are vulnerable to being compromised and utilized by unauthorized persons. This includes all counties in Georgia and the counties in Michigan which use Dominion.
- **SSH backdoor –** This allows the cyber actor to execute arbitrary code on a device.
- **Exfiltration –** When run, steals a predetermined list of files which includes system configuration & log files. Encrypted with hacker's public key and sent to their infrastructure over HTTPS.
- **Webshell functionality –** Allows an attacker remote access
- **Persistence & Mitigation –** The malware itself can make it impossible to run needed firmware updates. Once infected, a full factory reset must be done on the device prior to doing a firmware update to stop vulnerability.

Here is its location:

Here it can be seen embedded:

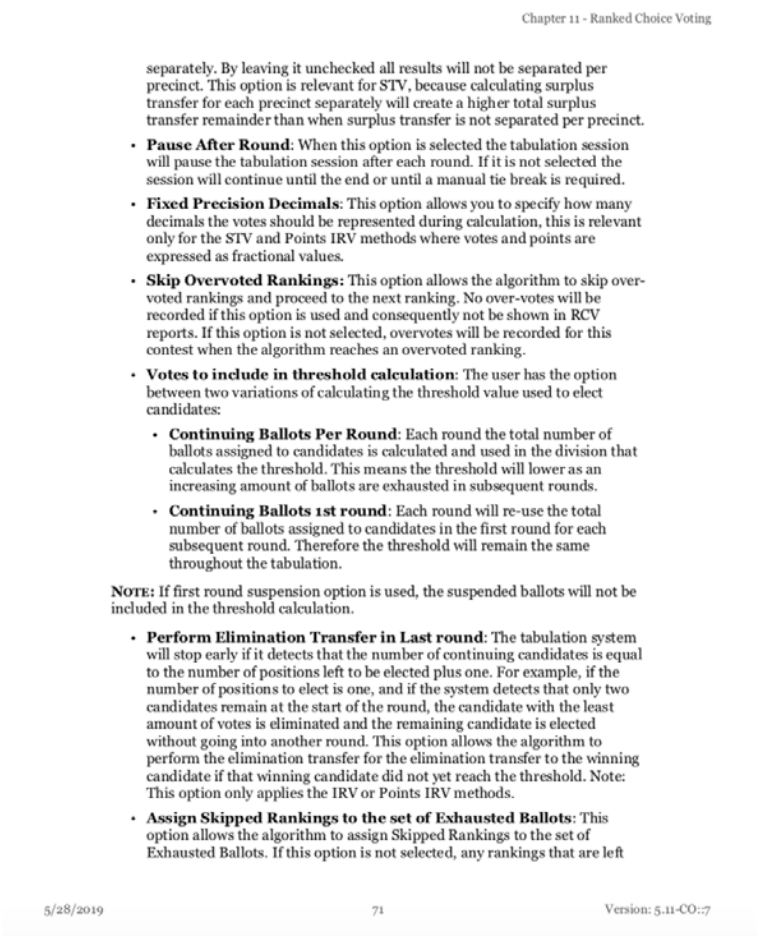

```
"iid": 14271845,
"type": "ip",
"indicator": "13.32.202.112",
"risk": "none",
"risk_recommended": "none",
"manualrisk": 0,
"retired": null,
"stamp_added": "2020-08-16 07:19:05",
"stamp_updated": "2020-09-21 18:57:23",
"stamp_seen": "2020-09-15 01:15:00",
"stamp_probed": "2020-09-21 18:57:23",
"stamp_retired": null,
```


Source code for Dominion can easily be obtained on the dark web so that an attacker knows all the vulnerable points and can plan and plant any malicious code the attacker desires. Here is a small sample of what can be seen on Pirates Bay TORR:


```
"ProductCode","ProductName","ProductVersion","OpSystemCode"
Type"
11818,"OpenElect","1.0","189","1422","English","Voting"
15134,"Hart Voting System Software Files
(BallotNow)","3.3.12","189","2049","English","Voting"
15134,"Hart Voting System Software Files
(BallotNow)","3.3.12","366","2049","English","Voting"
15542,"Open Elect Release","1.2","51","1422","English","Vo
16786,"OpenElect","1.3","51","1422","English","Voting"
17345,"Installed files for D-Suite 4.14-D,WinEDS 3.1.012, \
4.0.175","2016-01-12","786","2530","English","Voting"
17429,"Democracy Suite Election Event Designer (EED) Insta
File","4.14.37","365","2530","English","Voting"
17430,"Democracy Suite ImageCast Central (ICC) Installed
File","4.14.17","365","2530","English","Voting"
17431,"Democracy Suite Adjudication (ADJ) Installed
File","2.4.1.3201","365","2530","English","Voting"
```


2) The use of an algorithm being used in the vote counting is evident from a number of perspectives. First, there is the apparent product of decimal places being used in points instead of whole number votes that can be viewed from the NYT times Edison data. In the two-time series shown below, note the percentages in Series 357 that shows 3 decimal places displayed in the percentage distribution of the 3,616,879 votes. One might argue that the issue is simply due to the fact only 3 decimal places are displayed, and that if 20 or 30 decimal places were displayed, one would see whole numbers appear as votes instead of points with decimal places, and therefore there is no evidence in this illustration that an allocative algorithm was utilized. The problem with this is two-fold. The first is the percentages do not come close to 100% regardless of rounding. But the difference between the 98.2% displayed and 100% might be due to Jo Jorgenson. The presence of Jo Jorgenson as a third-party candidate is exactly the scenario for which RCV was supposedly concocted and contrary to Dr. Rodden assertion that Dominion RCV voting is incapable of producing non-integer vote totals, Dominion's own manual doesn't agree with him. See "Fixed Precision Decimals" in the manual page below:

Source: Democracy Suite EMS Results Tally & Reporting User Guide Version: 5.11-CO::7 May 28, 2019



Chapter 11 - Ranked Choice Voting

separately. By leaving it unchecked all results will not be separated per precinct. This option is relevant for STV, because calculating surplus transfer for each precinct separately will create a higher total surplus transfer remainder than when surplus transfer is not separated per precinct.

- **Pause After Round**: When this option is selected the tabulation session will pause the tabulation session after each round. If it is not selected the session will continue until the end or until a manual tie break is required.
- **Fixed Precision Decimals**: This option allows you to specify how many decimals the votes should be represented during calculation, this is relevant only for the STV and Points IRV methods where votes and points are expressed as fractional values.
- **Skip Overvoted Rankings:** This option allows the algorithm to skip over-voted rankings and proceed to the next ranking. No over-votes will be recorded if this option is used and consequently not be shown in RCV reports. If this option is not selected, overvotes will be recorded for this contest when the algorithm reaches an overvoted ranking.
- **Votes to include in threshold calculation**: The user has the option between two variations of calculating the threshold value used to elect candidates:
  - **Continuing Ballots Per Round**: Each round the total number of ballots assigned to candidates is calculated and used in the division that calculates the threshold. This means the threshold will lower as an increasing amount of ballots are exhausted in subsequent rounds.
  - **Continuing Ballots 1st round**: Each round will re-use the total number of ballots assigned to candidates in the first round for each subsequent round. Therefore the threshold will remain the same throughout the tabulation.

NOTE: If first round suspension option is used, the suspended ballots will not be included in the threshold calculation.

- **Perform Elimination Transfer in Last round**: The tabulation system will stop early if it detects that the number of continuing candidates is equal to the number of positions left to be elected plus one. For example, if the number of positions to elect is one, and if the system detects that only two candidates remain at the start of the round, the candidate with the least amount of votes is eliminated and the remaining candidate is elected without going into another round. This option allows the algorithm to perform the elimination transfer for the elimination transfer to the winning candidate if that winning candidate did not yet reach the threshold. Note: This option only applies the IRV or Points IRV methods.
- **Assign Skipped Rankings to the set of Exhausted Ballots**: This option allows the algorithm to assign Skipped Rankings to the set of Exhausted Ballots. If this option is not selected, any rankings that are left

5/28/2019 71 Version: 5.11-CO::7

Further, from the NYT Edison data displayed below, it is also clear from Series 358 that with only 2 decimals showing in the Biden percentage of 0.45, the total fraction displayed cannot get anywhere near 100% regardless of any truncation in the Trump percentage.
https://static01.nyt.com/elections-assets/2020/data/api/2020-11-03/race-page/michigan/president.json

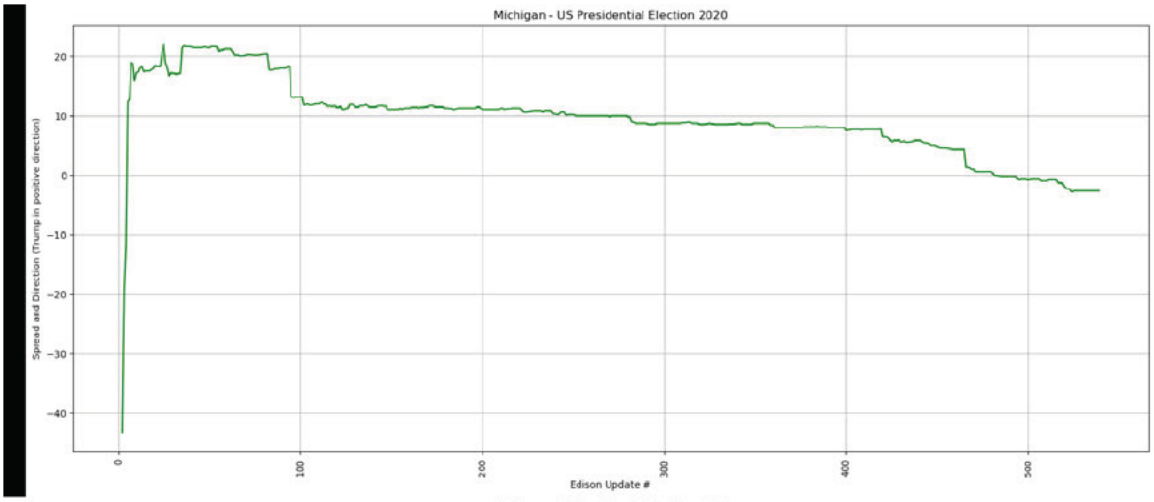
Example:
/data/races/0/timeseries/357/

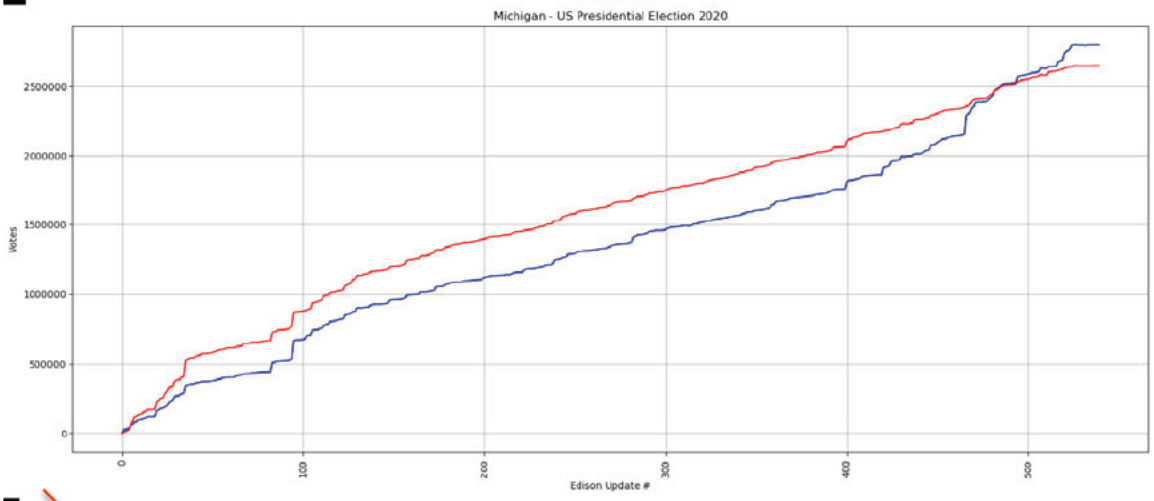

```
▼ 357:
  ▼ vote_shares:
      trumpd:          0.534
      bidenj:          0.448
    votes:             3616879
    eevp:              64
    eevp_source:       "edison"
    timestamp:         "2020-11-04T06:58:47Z"
▼ 358:
  ▼ vote_shares:
      trumpd:          0.533
      bidenj:          0.45
    votes:             3643075
    eevp:              64
    eevp_source:       "edison"
    timestamp:         "2020-11-04T07:00:37Z"
```

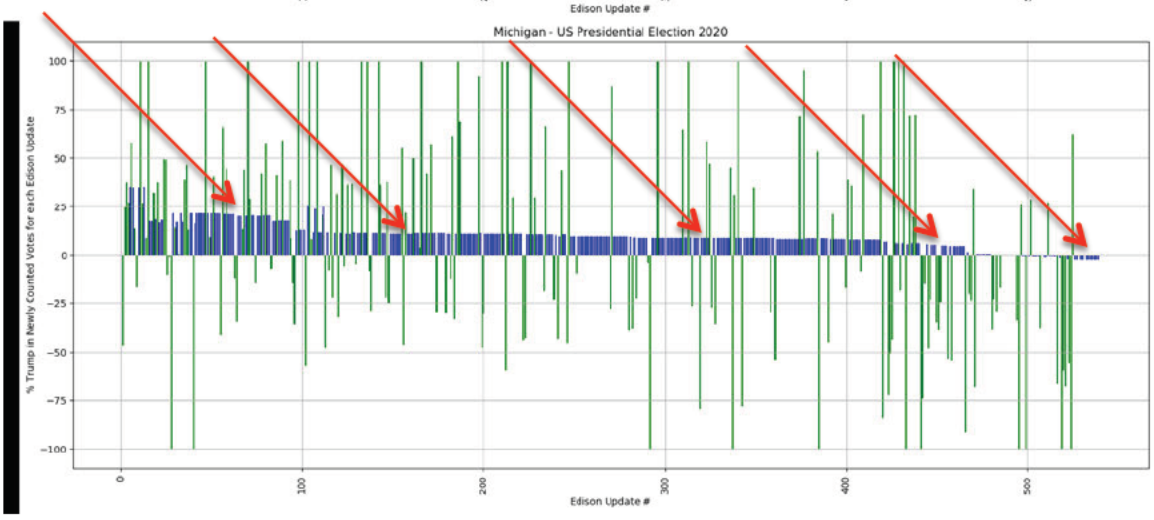
Hence, calculating the "points" for each candidate from the NYT Edison time series by multiplying the votes by the percentage to show the calculated votes/ (TV = Trump Votes) (BV = Biden Votes)

state	timestamp	eevp	trump	biden	TV	BV
michigan	2020-11-04T06:54:48Z	64	0.534	0.448	1925865.66	1615707.52
michigan	2020-11-04T06:56:47Z	64	0.534	0.448	1930247.664	1619383.808
michigan	2020-11-04T06:58:47Z	64	0.534	0.448	1931413.386	1620361.792
michigan	2020-11-04T07:00:37Z	64	0.533	0.45	1941758.975	1639383.75
michigan	2020-11-04T07:01:46Z	64	0.533	0.45	1945297.562	1642371.3
michigan	2020-11-04T07:03:17Z	65	0.533	0.45	1948885.185	1645400.25

3) The second piece of evidence that an algorithm is being utilized comes from our observation that the percentage of the votes submitted in each batch that went towards a candidate remain unchanged for a long series of time and for a number of *consecutive* batches is extremely concerning. Further, the percentage for Trump decreases in a mathematically extremely consistent pattern. The red arrows indicate the impossible consistencies. The statistical impossibility of the consistent percentage reported to Biden approaches zero. This makes clear an algorithm in the election system is allocating votes based on a percentage.







The top graph:
The cumulative spread in percentage between Trump and Biden at any point in time during the vote counting is shown in this graph, where Trump is positive percentage. In other words, a point on the line in this graph represents which candidate is in the lead at any point in time, and by how much. Movement of the line in this graph indicates change in the magnitude a candidate is winning by. If the line slopes up, the votes are moving in a direction that favors Trump. If the line slopes down, the votes are moving in a direction that favors Biden.

The middle graph:
The total accumulated votes counted at any point in time for each candidate is represented in this graph. Red is Trump. Blue is Biden.
The lower graph:
Each bar on this graph represents what percentage of the votes submitted in each batch went towards a candidate, where Trump is positive and Biden is negative.

Analysis:
There are multiple highly anomalous features in this visualization of the Michigan, USA 2020 General Election vote count data. It is important to understand the context of the lower graph and analysis. Every batch of vote counts released represents various groups of people and their votes. These groups of people's votes are expected to have variance, even if multiple batches were produced out of the same geographic area. Large numbers of votes between multiple candidates are unlikely to have the same percentage of going towards a candidate multiple times in different batches.
What we see in the lower graph instead of the expected variance in percentage of votes going to Trump or Biden in each batch are easily distinguishable trends, which are realistically improbable. The statistical probability of that pattern occurring throughout the graph approaches zero.
The observation of these trends not only strongly suggests fraud, but also suggests automated and algorithmic tampering of vote counts.

There is a mechanical correlation between the suspected algorithmically generated vote count releases (labeled in blue on the bottom graph) and the relative difference between the line in the upper graph and zero (an intersection with the line at y=0 in the upper graph indicates a change in which candidate is leading). Furthermore, as soon as the line in the upper graph intersects with y=0, the algorithmically generated vote count releases switch to the opposing side - possibly to either maintain or eek in a Biden victory.
Once the majority of apparent real and organic votes ceased to be counted, we are left with large swaths of released vote counts that repeatedly have the same exact percentage of votes in each release going to Biden. By exact, I mean exact. That is until stray batches of apparent organic votes are released, and then the percentage of votes in each release from the apparent algorithmically generated vote counts going to Biden seem to adjust slightly to account for the change, which then continue to repeat in each release, until the next stray organic batch, and the cycle repeats. It is difficult to come up with a realistic scenario where this described phenomenon is not the result of an algorithm behind the scenes.

4) The suggestion that the information included in the "Spike Chart" of my original affidavit could be simply tabulated votes that were suddenly all reported is erroneous. The spike data came from Edison Research data and Oakland, the largest spike, was for November 7th, well past any "pent up" tabulated vote batches. Later data we found direct from Dominion to the NYT that did not pass through Edison confirms this and even adds further granularity.

5) That there are problems in the Dominion System is clear from a visit our team made to Central Lake Township in Antrim Michigan on behalf of a local lawsuit filed by Michigan attorney Robert Marsh. Below is the field report submitted to me by our team.

ASOG Forensics Report on Central Lake Township in Antrim Michigan

Report Date 11/29/2020
Report Version 1.4

On 11/27/2020 the ASOG forensics team visited Central Lake Township in Antrim Michigan on behalf of a local lawsuit filed by Michigan attorney Robert Marsh.

The clerk of Central Lake Township – at around 10:30am – Ms. Judith L. Kosloski, presented to us "two separate paper totals tape" from Tabulator ID 2.

One dated "Poll Opened Nov. 03/2020 06:38:48" (Roll 1)
Another dated "Poll Opened Nov. 06/2020 09:21:58" (Roll 2)

We were then told by her that on November 5, 2020, Ms. Kosloski was notified by Connie Wing of the County Clerk's Office and asked to bring the tabulator and ballots to the County Clerk's office for re-tabulation. They ran the ballots and printed "Roll 2". She noticed a difference in the votes and brought it up to the clerk, but canvasing still occurred, and her objections were not addressed.

Our team analyzed both rolls and compared the results.

Roll 1 had 1,494 total votes
Roll 2 had 1,491 votes (Roll 2 had 3 less ballots because 3 ballots were damaged in the process.)

"Statement of Votes Cast from Antrim" shows that only 1,491 votes were counted, and the 3 ballots that were damaged were not entered into final results.

Ms. Kosloski stated that she and her assistant manually refilled out the three ballots, curing them, and ran them through the ballot counting system - but the final numbers do not reflect the inclusion of those 3 damaged ballots.

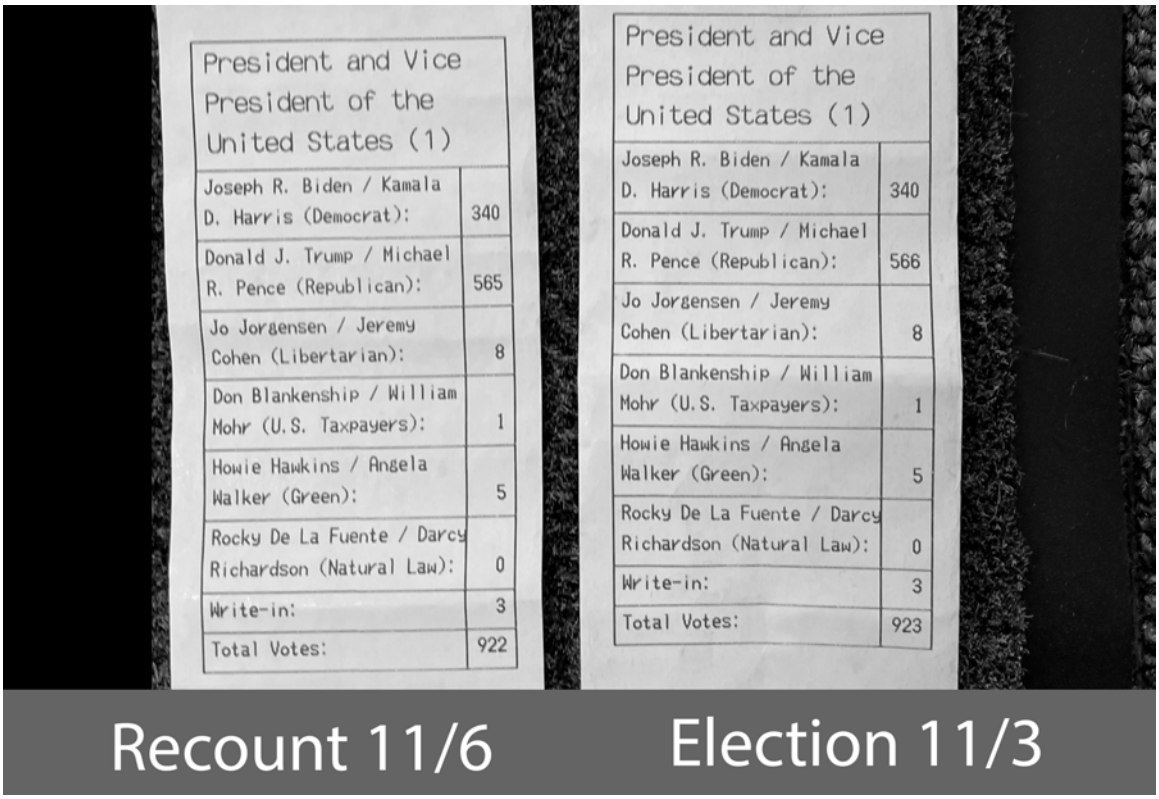
http://www.antrimcounty.org/downloads/official_results_2nd_amended.pdf
Source: http://www.antrimcounty.org/elections.asp

In comparing the numbers on both rolls, *we estimate 1,474 votes changed* across the two rolls, between the first and the second time the exact same ballots were run through the County Clerk's vote counting machine - *which is almost the same number of voters that voted in total.*

The five most significant changes in vote totals are in the screenshots below:

- On Election night, Trump received 566 votes, Biden received 340. On the recount, Trump had 1 less vote at 565 while Biden was unchanged at 340. This is particularly odd since 3 votes less were tabulated. So

potentially Trump could have lost between 3 and 4 votes overall on a very small sample – but that did not happen.



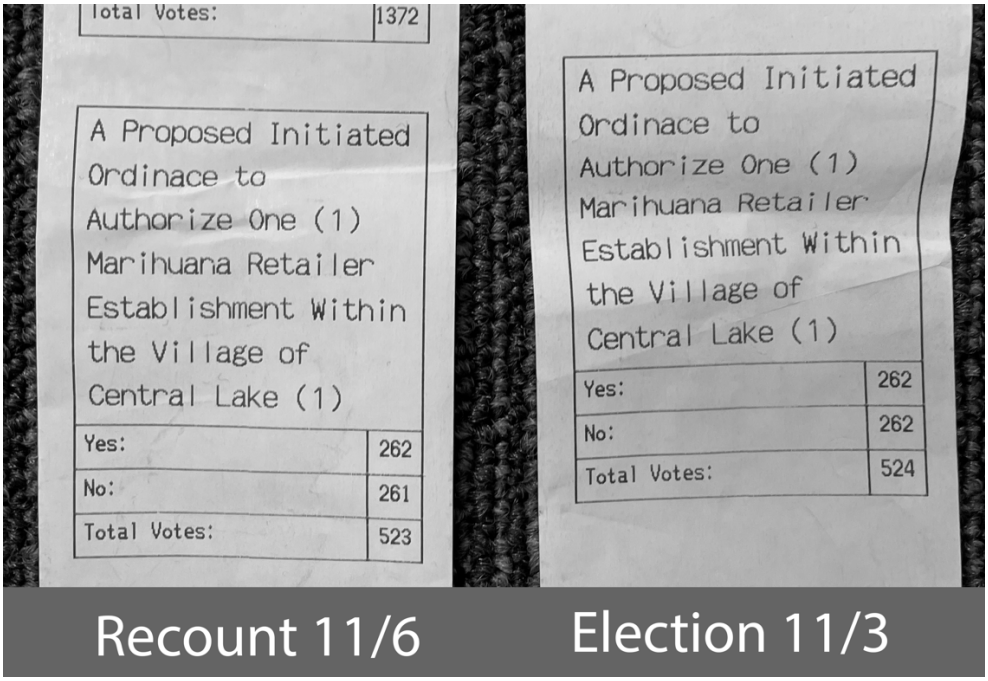
President and Vice President of the United States (1)	
Joseph R. Biden / Kamala D. Harris (Democrat):	340
Donald J. Trump / Michael R. Pence (Republican):	565
Jo Jorgensen / Jeremy Cohen (Libertarian):	8
Don Blankenship / William Mohr (U.S. Taxpayers):	1
Howie Hawkins / Angela Walker (Green):	5
Rocky De La Fuente / Darcy Richardson (Natural Law):	0
Write-in:	3
Total Votes:	922

Recount 11/6

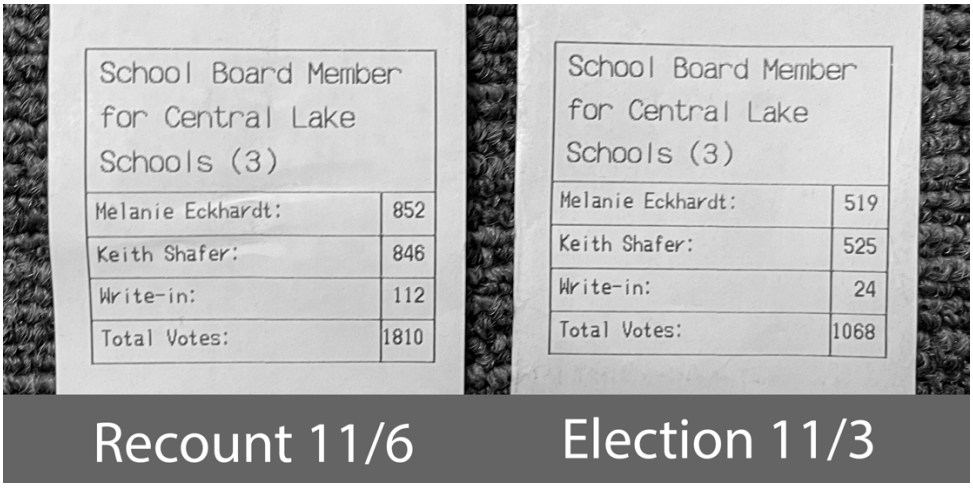
President and Vice President of the United States (1)	
Joseph R. Biden / Kamala D. Harris (Democrat):	340
Donald J. Trump / Michael R. Pence (Republican):	566
Jo Jorgensen / Jeremy Cohen (Libertarian):	8
Don Blankenship / William Mohr (U.S. Taxpayers):	1
Howie Hawkins / Angela Walker (Green):	5
Rocky De La Fuente / Darcy Richardson (Natural Law):	0
Write-in:	3
Total Votes:	923

Election 11/3

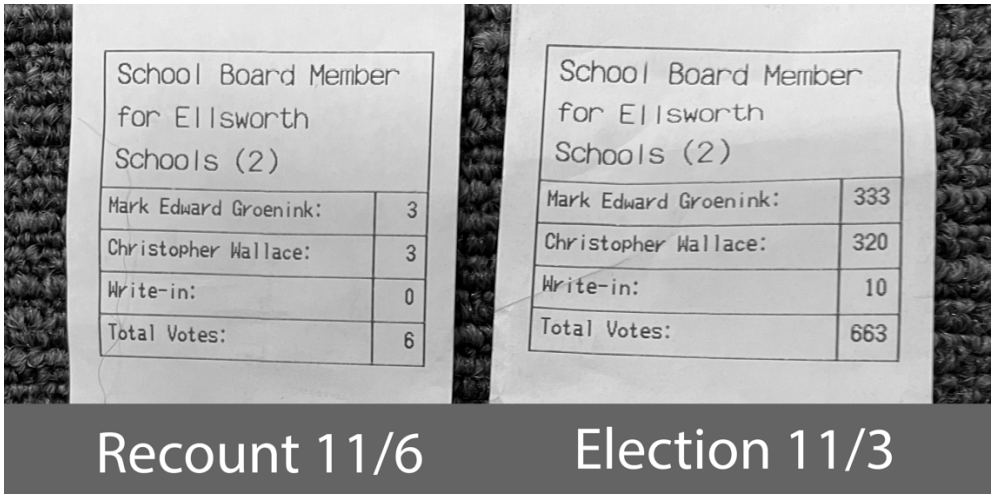
- A Proposed Initiated Ordinance to Authorize One (1) Marihuana (sic) Retailer Establishment Within the Village of Central Lake (1). – On election night, it was a tie vote. Then, on the recount, when 3 ballots were not counted, the proposal passed with 1 vote being removed from the No vote.



- For the School Board Member for Central Lake Schools (3) there were 742 votes added to this vote total. Since multiple people were elected, this did not change the result of both candidates being elected, but you do see a change in who had more votes. If it were a single person election, this would have changed the outcome, but this goes to the fact that votes can be and were changed during the second machine counting.



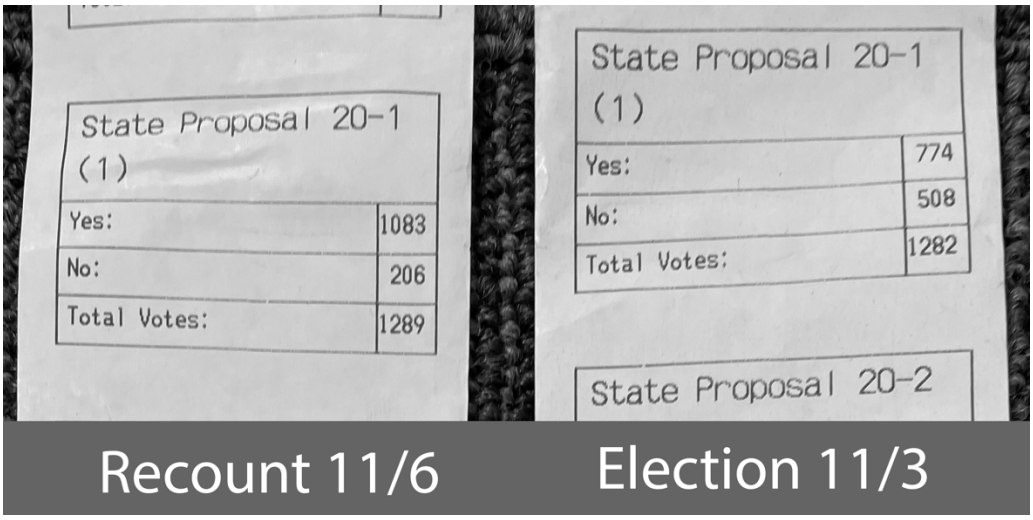
- For the School Board Member for Ellsworth Schools (2) it shows *657 votes being removed* from this election. In this case, only 3 people who were eligible to vote actually voted. Since there were 2 votes allowed for each voter to cast, the recount is correct to have 6 votes. But on election night, there is a major calculation issue:



- In State Proposal 20-1 (1), there is a major change in votes in this category.

Proposal 1 is a fairly technical and complicated proposed amendment to the Michigan Constitution to change the disposition and allowable uses of future revenue generated from oil and gas bonuses, rentals and royalties from state-owned land. There were 774 votes for YES during the election, to 1,083 votes for YES on the recount.

Information about the proposal: https://crcmich.org/publications/statewide-ballot-proposal-20-1-michigan-natural-resources-trust-fund



Process

Our team interviewed Ms. Kosloski on the process of tabulation and how the system works.

Essentially, the Township Clerk is given two Compact Flash Cards and a Security Key. One CF card (also known as ISD Card) goes into the

"ADMINISTRATOR" in the "CF CARD 2" Slot and the other in the "POLL WORKER" in the "CF CARD 1" Slot. The security key is used on the "SECURITY KEY" connector on top.

Pre-election, Ms. Kosloski was given the cards by the County Clerk's office. The County Clerk is Sheryl Guy.

Once the printed ballots are hand-marked by voters, they are run through the machine. At the close of the polls, they run the totals on the print and bring the two CF Cards and security key back to the County Clerk for loading into the server. The cards and keys are not given back to the Township Clerk – these essential technical data sources for the Townships are thereafter held by the County Clerk.

On November 6th, at the request of the County Clerk, and with no explanation, Ms. Kosloski was told to bring the tabulator serial number AAFAJHX0226 and sealed ballots to the Country Clerk's office. There, she was presented with two CF Cards and a security key. Then, they re-ran the original election day ballots. During this process, 3 ballots were damaged and not tabulated on the "Roll 2" results. Again, under the oversight of the canvassing board, Ms. Kowloski cured those ballots, and re-ran them, but they appear to have not been counted in the final vote totals.

Conclusion

The ASOG forensics team believes that a software change loaded into Tabulator ID 2 on November 6th did occur, and this caused the vote totals to change. The change happened on the Tabulator unit, but did so using software configurations from the Country Clerk. The Clear Lake Township Clerk Ms. Kosloski has never been told why they needed to re-tabulate the ballots.

The forensics team would like access to the CF Cards and Security Key for Roll 1 and the CF Cards and Security Key for Roll 2. We also request unrestricted access to the machine that programs the CF Cards, which we believe is called the "Election Event Designer" software of Dominion Democracy Suite – or like-software that was used to program these CF Cards.

We do not believe that the Secretary of State report addresses this, and states the issue at the time was not on the printed totals tape. The Secretary even states "Because the Clerk correctly updated the media drives for the tabulators with changes to races, and because the other tabulators did not have changes to races, all tabulators counted ballots correctly." This is <u>not</u> the case.

We believe this directly contradicts the Sectary of State fact check document. (Link below.)

November 7, 2020 Isolated User Error in Antrim County Does Not Affect Election Results, Has no Impact on Other Counties or States - Jocelyn Benson – Secretary of State of Michigan

https://www.michigan.gov/documents/sos/Antrim_Fact_Check_707197_7.pdf

Excerpt from document:
"These errors can always be identified and corrected because every tabulator prints a paper totals tape showing how the ballots for each race were counted. After discovering the error in reporting the unofficial results, the clerk worked diligently to report correct unofficial results by reviewing the printed totals tape on each tabulator and hand-entering the results for each race, for each precinct in the county. Again, all ballots were properly tabulated. The user error affected only how the results from the tabulators communicated with the election management system for unofficial reporting.

Even if the error had not been noticed and quickly fixed, it would have been caught and identified during the county canvass when printed totals tapes are reviewed. This was an isolated error, there is no evidence this user error occurred elsewhere in the state, and if it did it would be caught during county canvasses, which are conducted by bipartisan boards of county canvassers."

Summary

If this had been a user setup issue, then the test ballots they run to verify the results they get by comparing them with the test matrix should have caught that. When they made the software change that that used to tabulate the 11/6/20 re-run, there should be a log of the test ballots run through the system and verified against the test matrix. This alone might not show fraud, but it is a crucial part of the software configuration validation process and apparently was not done.

We believe to a reasonable degree of professional certainty that this shows fraud and that vote changing at the local tabulator level has occurred due to a software change in all precincts were Dominion software was used in Michigan. This small sample amplified in a large population area would have major results. Without the explanation of why there was a re-tabulation, why the issue of numbers being off to a significant degree when a vote change was noted, and no further investigation occurred – and when 3 ballots were removed from the totals that changed the final outcome of one proposal, constitutes a definitive indication of fraud.

6) Finally, Dr. Rodden was correct in his noting of excessive turnout figures listed in my affidavit for some precincts in MI based on new data from Michigan. The source of that original data was State level data that no longer exists or some unexplained reason. It existed at
https://data.michigan.gov/
https://mielections.us/election/results/2020GEN_CENR.html

Currently, new data published by the various counties does change. However, at this point we see the current State of Michigan published data as follows:

County	Precinct	Turnout
Ottawa	Spring Lake Township, Precinct 6 - B	120.00%
Allegan	City of South Haven, Ward 3, Precinct 2 (Van Buren County)	100.00%
Alger	Grand Island Town Prec 1	96.77%
Ottawa	Tallmadge Charter Township, Precinct 3 - C	95.24%
Macomb	GROSSE POINTE SHORES-3	94.00%
Oakland	Fenton, Precinct 2	93.33%
Ottawa	Zeeland Charter Township, Precinct 4 - D	90.59%
Muskegon	Ravenna Township Precinct 1	89.72%
Barry	Thornapple Township, Precinct 1	89.23%
Oakland	Novi Township, Precinct 1	89.13%
Kent	Byron Township Precinct 4	89.08%
Ottawa	Jamestown Charter Township, Precinct 2	88.88%
Barry	Thornapple Township, Precinct 2	88.88%
Oakland	Lyon Township, Precinct 8	88.78%
Livingston	Oceola Township, Precinct 5	88.53%
Ottawa	Holland Charter Township, Precinct 4 - B	88.28%
Oakland	Lake Angelus, Precinct 1	88.21%
Ottawa	Port Sheldon Township, Precinct 1 - A	88.19%
Genesee	Grand Blanc Township, Precinct 10	87.96%
Ottawa	Blendon Township, Precinct 2 - B	87.91%
Kent	Vergennes Township Precinct 1	87.75%
Washtenaw	York Township, Precinct 2	87.69%
Oakland	Oakland Township, Precinct 3	87.68%
Livingston	City of Brighton, Precinct 4	87.60%
Sanilac	Flynn Township, Precinct 1	87.37%
Ottawa	Blendon Township, Precinct 1 - B	87.04%
Oakland	Southfield Township, Precinct 4	87.03%
Oakland	Huntington Woods, Precinct 3	87.00%
Washtenaw	York Township, Precinct 3	86.97%
Sanilac	Delaware Township, Precinct 1	86.95%
Sanilac	Wheatland Township, Precinct 1	86.90%
Washtenaw	City of Dexter, Precinct 2	86.84%
Kent	Cascade Charter Township Precinct 8	86.83%
Oakland	Lyon Township, Precinct 6	86.81%
Oakland	Southfield Township, Precinct 3	86.79%

The data shows 469 precincts with voter turn-out above 80%, according to current Michigan county records. Normalizing the current public data votes to 80% turnout (still 15%+/- above normal), the excess votes are at least 27,599 over the maximum that could be expected.

Declaration of NAME {redacted}.

Pursuant to 28 U.S.C Section 1746, I, **{redacted}**, make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I was an electronic intelligence analyst under 305th Military Intelligence with experience gathering SAM missile system electronic intelligence. I have extensive experience as a white hat hacker used by some of the top election specialists in the world. The methodologies I have employed represent industry standard cyber operation toolkits for digital forensics and OSINT, which are commonly used to certify connections between servers, network nodes and other digital properties and probe to network system vulnerabilities.
3. I am a US citizen and I reside at **{redacted}** location in the United States of America.
4. The following link analysis was gathered through open source methodologies and are easily verifiable.
5. As Dominion and Smartmatic makes claims that they are not connected in any way, not only are they connected but their business registration was in the same building on a foreign island to obfuscate their business dealings.

https://offshoreleaks.icij.org/nodes/101732449

ENTITY

DOMINION VOTING SYSTEMS INTERNATIONAL CORPORATION

Connected to **2 addresses**

Connected to **3 officers**

Incorporated: 06-OCT-2009

Registered in: Barbados

Linked countries: Barbados

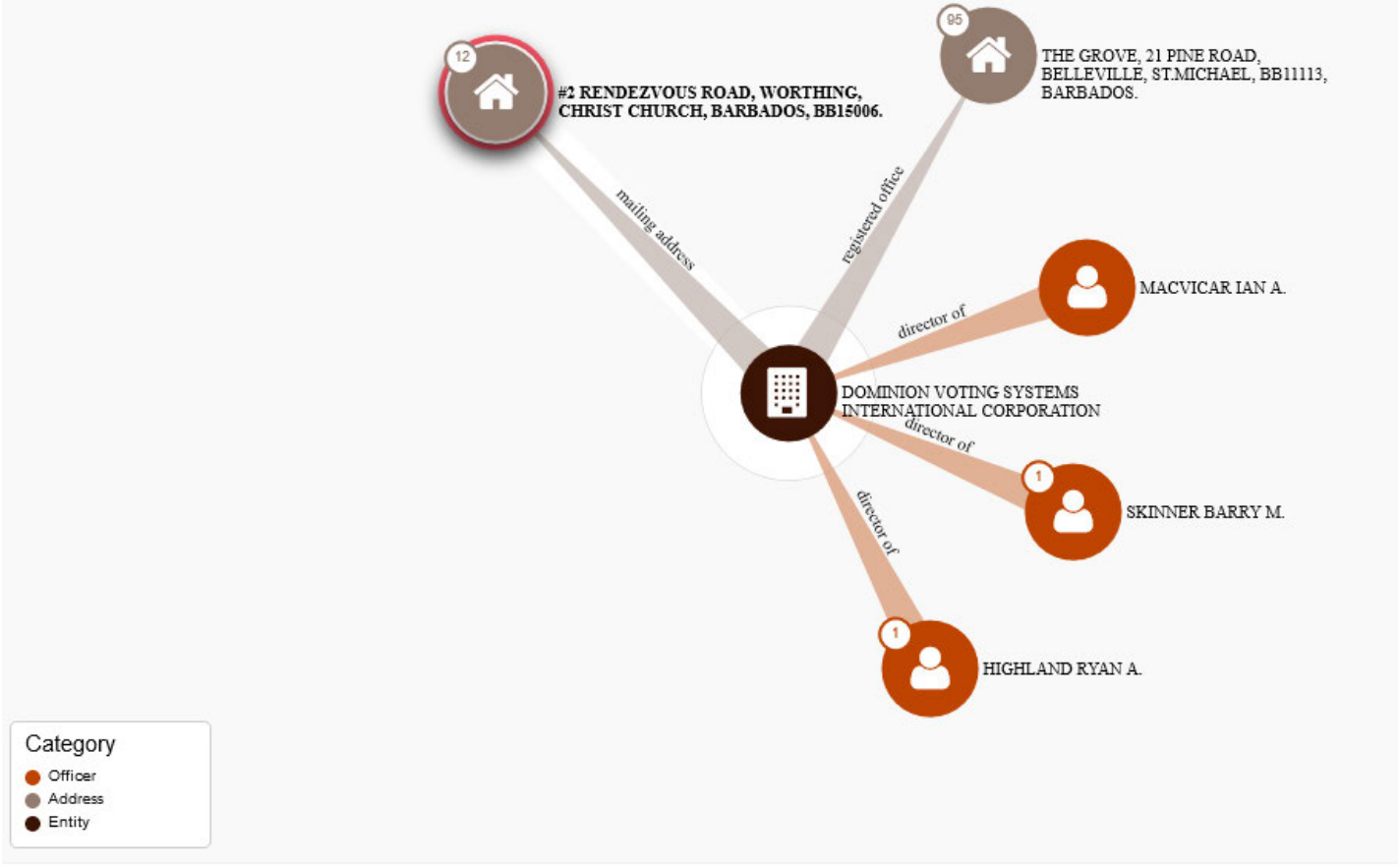
Data from: Paradise Papers - Barbados corporate registry

Barbados corporate registry data is current through 2016

Search in opencorporates

Got a tip? Help ICIJ investigate: contact us or leak to us securely

ICIJ OFFSHORE LEAKS DATABASE



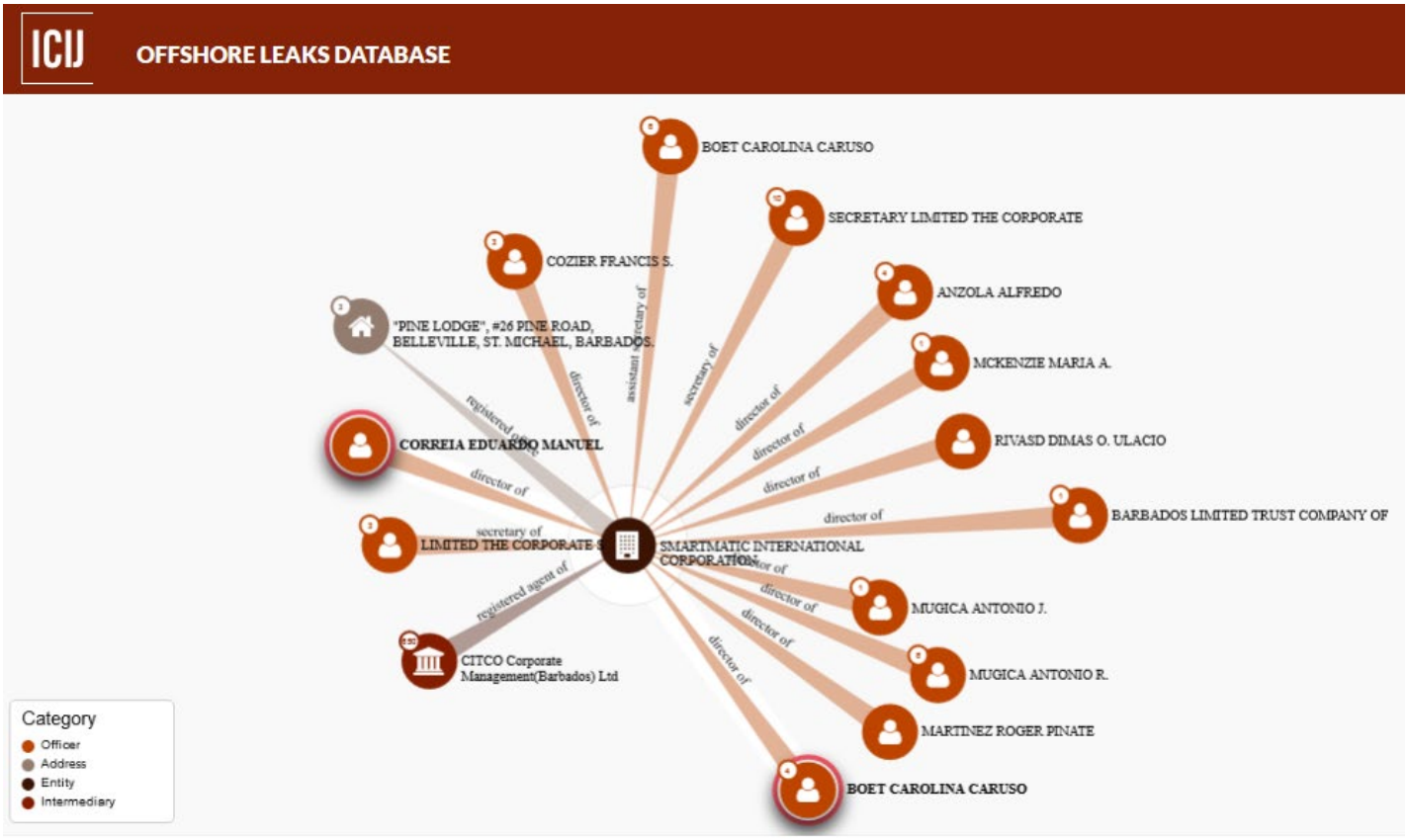
https://offshoreleaks.icij.org/nodes/101724285

SMARTMATIC INTERNATIONAL CORPORATION

Connected to **1 address**
Connected to **13 officers**
Connected to **1 intermediary**

Incorporated: **29-SEP-2004**
Registered in: Barbados
Linked countries: Barbados

Data from: Paradise Papers - Barbados corporate registry
Barbados corporate registry data is current through 2016
Search in opencorporates
Got a tip? Help ICIJ investigate: contact us or leak to us securely



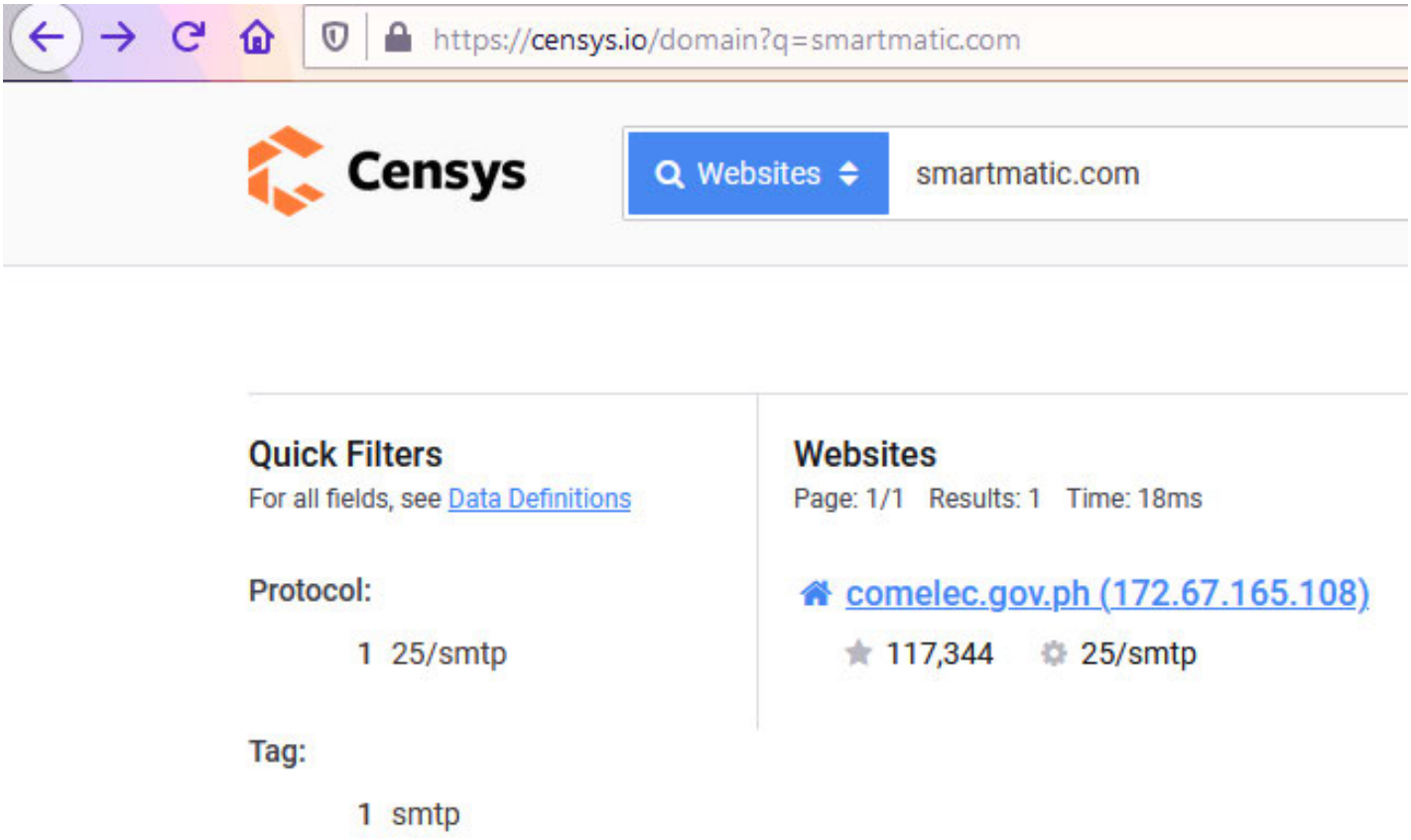
I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge. Executed this November 23th, 2020.

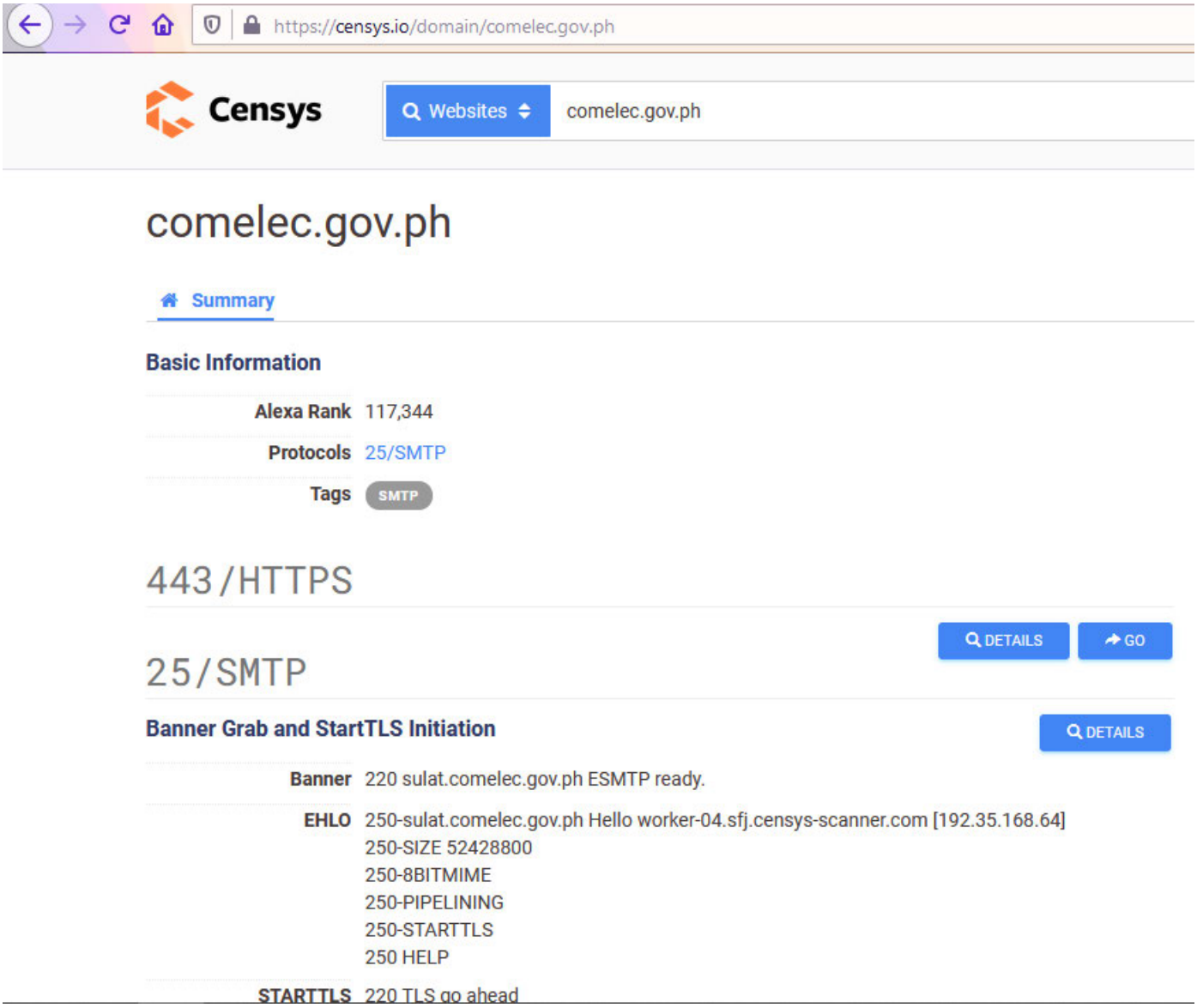
Smartmatic SSL Certificate

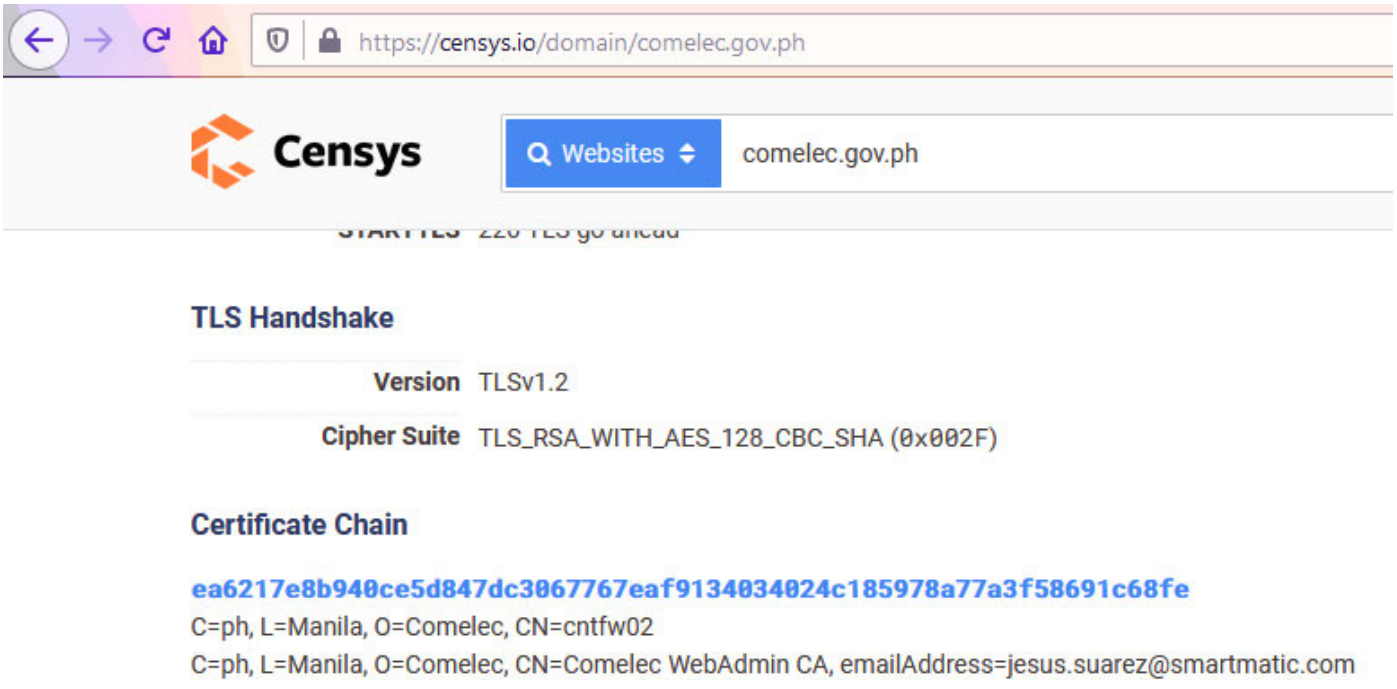
Declaration of NAME {redacted}.

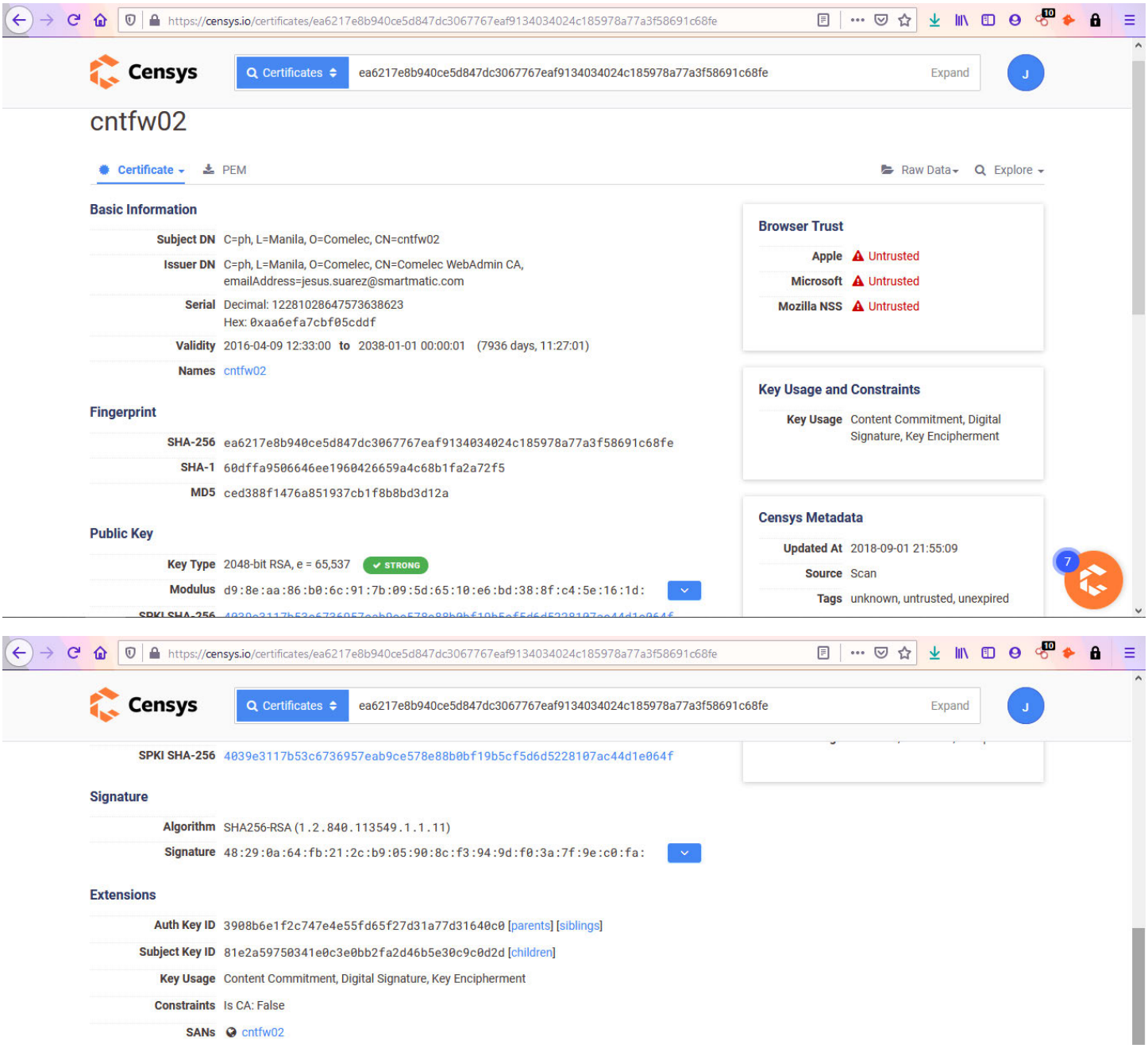
Pursuant to 28 U.S.C Section 1746, I, **{redacted}**, make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I was an electronic intelligence analyst under 305th Military Intelligence with experience gathering SAM missile system electronic intelligence. I have extensive experience as a white hat hacker used by some of the top election specialists in the world. The methodologies I have employed represent industry standard cyber operation toolkits for digital forensics and OSINT, which are commonly used to certify connections between servers, network nodes and other digital properties and probe to network system vulnerabilities.
3. I am a US citizen and I reside at **{redacted}** location in the United States of America.
4. Researching Smartmatic's website and reading their public manuals about the reuse of SSL certificate's, I started to investigate Smartmatic's SSL certificates. Upon searching their website is currently behind Cloudflare yet using the same SSL certificate it made it easy to locate where Smartmatic's website was located. Smartmatic's website is in the Philippine's on their Election commission's server (Comelec.gov.ph).

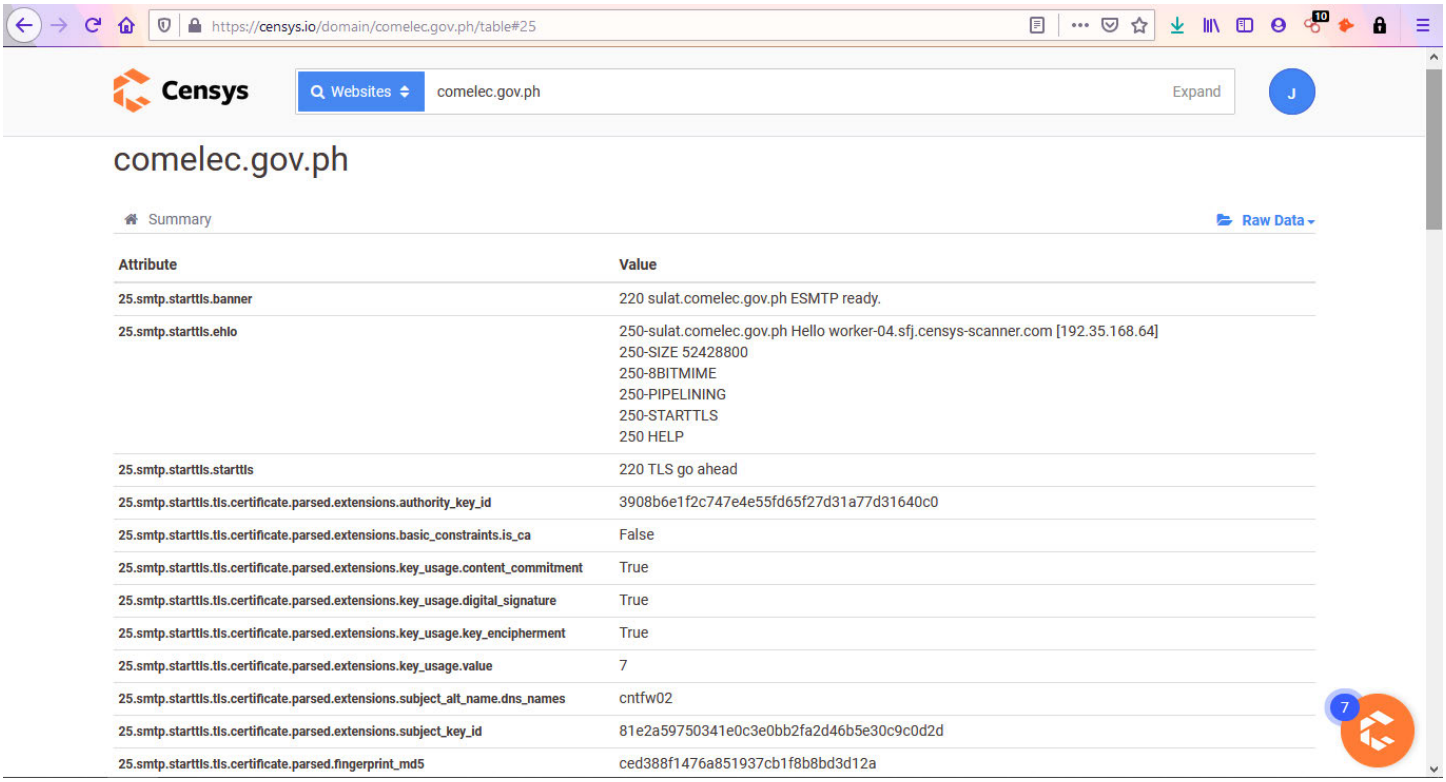


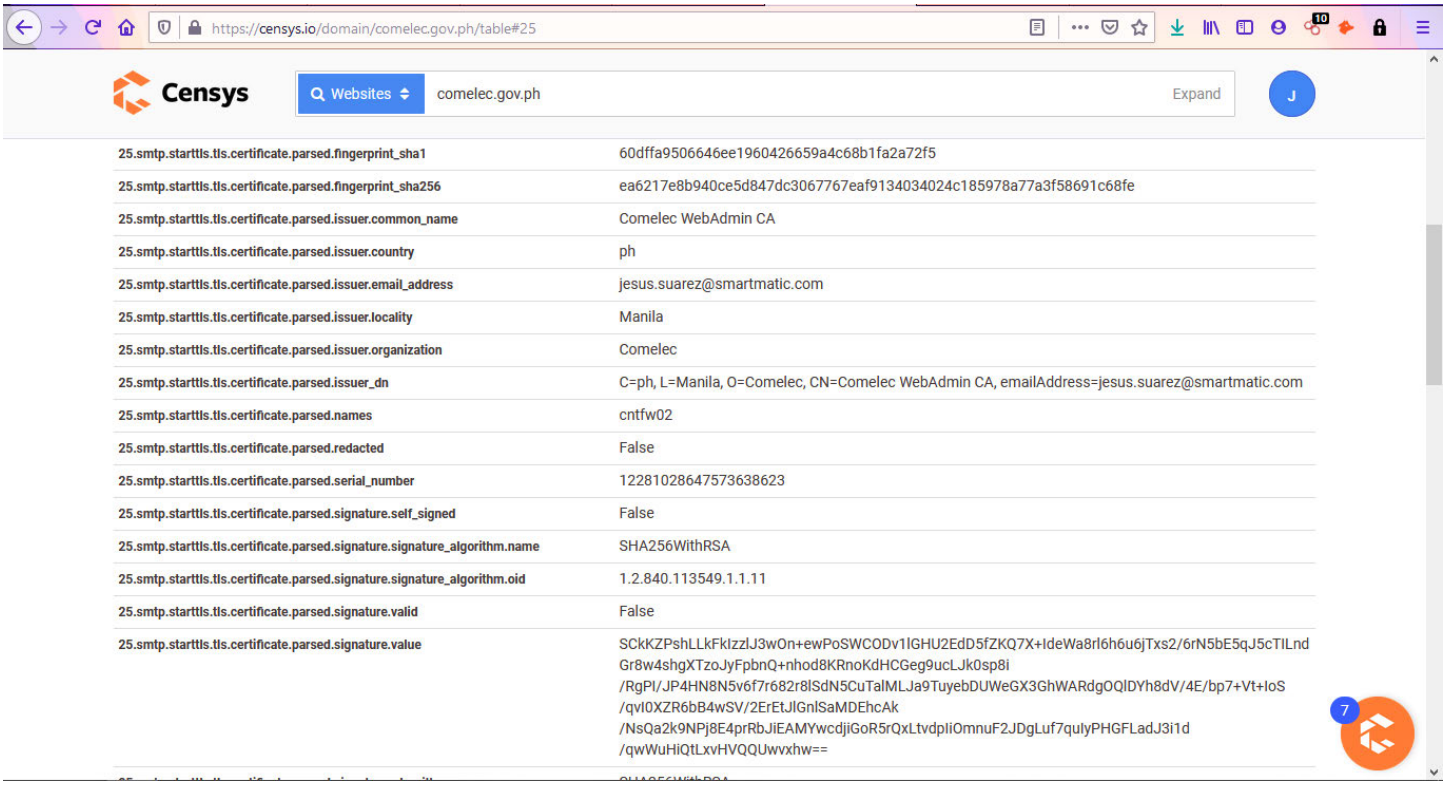

https://censys.io/domain/comelec.gov.ph
Censys
Websites
comelec.gov.ph
comelec.gov.ph
Summary
Basic Information
Alexa Rank 117,344
Protocols 25/SMTP
Tags SMTP
443 / HTTPS
DETAILS
GO
25 / SMTP
Banner Grab and StartTLS Initiation
DETAILS
Banner 220 sulat.comelec.gov.ph ESMTP ready.
EHLO 250-sulat.comelec.gov.ph Hello worker-04.sfj.censys-scanner.com [192.35.168.64]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-STARTTLS
250 HELP
STARTTLS 220 TLS go ahead

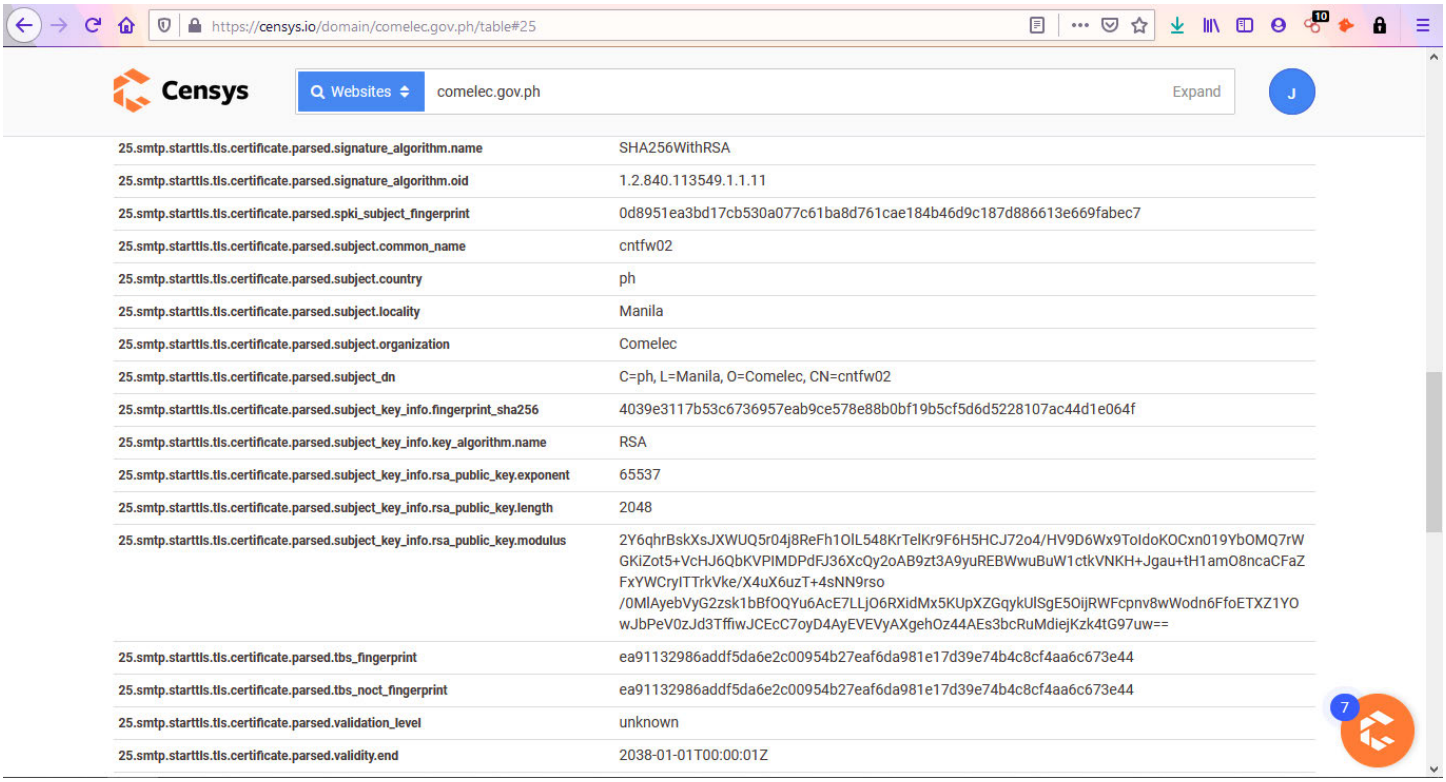

https://censys.io/domain/comelec.gov.ph
Censys
Websites
comelec.gov.ph
TLS Handshake
Version TLSv1.2
Cipher Suite TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
Certificate Chain
ea6217e8b940ce5d847dc3067767eaf9134034024c185978a77a3f58691c68fe
C=ph, L=Manila, O=Comelec, CN=cntfw02
C=ph, L=Manila, O=Comelec, CN=Comelec WebAdmin CA, emailAddress=jesus.suarez@smartmatic.com



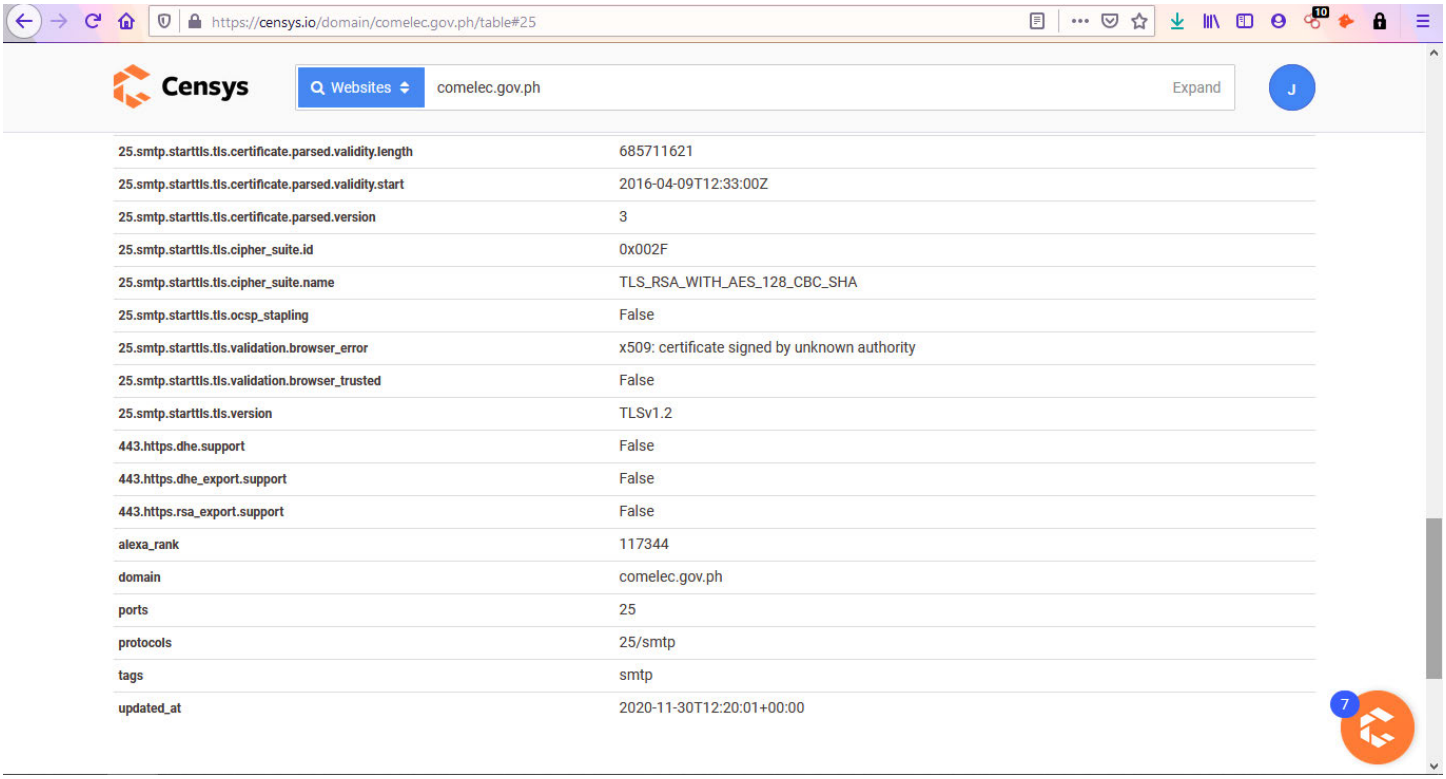
5. As can be seen in the images above the SSL certificate used was registered by the email address jesus.suarez@smartmatic.com on the 9th of April 2016.


https://censys.io/domain/comelec.gov.ph/table#25
Censys
Websites
comelec.gov.ph
Expand
J
comelec.gov.ph
Summary
Raw Data
Attribute
Value
25.smtp.starttls.banner
220 sulat.comelec.gov.ph ESMTP ready.
25.smtp.starttls.ehlo
250-sulat.comelec.gov.ph Hello worker-04.sfj.censys-scanner.com [192.35.168.64]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-STARTTLS
250 HELP
25.smtp.starttls.starttls
220 TLS go ahead
25.smtp.starttls.tls.certificate.parsed.extensions.authority_key_id
3908b6e1f2c747e4e55fd65f27d31a77d31640c0
25.smtp.starttls.tls.certificate.parsed.extensions.basic_constraints.is_ca
False
25.smtp.starttls.tls.certificate.parsed.extensions.key_usage.content_commitment
True
25.smtp.starttls.tls.certificate.parsed.extensions.key_usage.digital_signature
True
25.smtp.starttls.tls.certificate.parsed.extensions.key_usage.key_encipherment
True
25.smtp.starttls.tls.certificate.parsed.extensions.key_usage.value
7
25.smtp.starttls.tls.certificate.parsed.extensions.subject_alt_name.dns_names
cntfw02
25.smtp.starttls.tls.certificate.parsed.extensions.subject_key_id
81e2a59750341e0c3e0bb2fa2d46b5e30c9c0d2d
25.smtp.starttls.tls.certificate.parsed.fingerprint_md5
ced388f1476a851937cb1f8b8bd3d12a
7


https://censys.io/domain/comelec.gov.ph/table#25
Censys
Websites
comelec.gov.ph
Expand
J
25.smtp.starttls.tls.certificate.parsed.fingerprint_sha1
60dffa9506646ee1960426659a4c68b1fa2a72f5
25.smtp.starttls.tls.certificate.parsed.fingerprint_sha256
ea6217e8b940ce5d847dc3067767eaf9134034024c185978a77a3f58691c68fe
25.smtp.starttls.tls.certificate.parsed.issuer.common_name
Comelec WebAdmin CA
25.smtp.starttls.tls.certificate.parsed.issuer.country
ph
25.smtp.starttls.tls.certificate.parsed.issuer.email_address
jesus.suarez@smartmatic.com
25.smtp.starttls.tls.certificate.parsed.issuer.locality
Manila
25.smtp.starttls.tls.certificate.parsed.issuer.organization
Comelec
25.smtp.starttls.tls.certificate.parsed.issuer_dn
C=ph, L=Manila, O=Comelec, CN=Comelec WebAdmin CA, emailAddress=jesus.suarez@smartmatic.com
25.smtp.starttls.tls.certificate.parsed.names
cntfw02
25.smtp.starttls.tls.certificate.parsed.redacted
False
25.smtp.starttls.tls.certificate.parsed.serial_number
12281028647573638623
25.smtp.starttls.tls.certificate.parsed.signature.self_signed
False
25.smtp.starttls.tls.certificate.parsed.signature.signature_algorithm.name
SHA256WithRSA
25.smtp.starttls.tls.certificate.parsed.signature.signature_algorithm.oid
1.2.840.113549.1.1.11
25.smtp.starttls.tls.certificate.parsed.signature.valid
False
25.smtp.starttls.tls.certificate.parsed.signature.value
SCkKZPshLLkFkIzzlJ3wOn+ewPoSWCODv1lGHU2EdD5fZKQ7X+IdeWa8rl6h6u6jTxs2/6rN5bE5qJ5cTILnd
Gr8w4shgXTzoJyFpbnQ+nhod8KRnoKdHCGeg9ucLJk0sp8i
/RgPI/JP4HN8N5v6f7r682r8lSdN5CuTalMLJa9TuyebDUWeGX3GhWARdgOQlDYh8dV/4E/bp7+Vt+IoS
/qvI0XZR6bB4wSV/2ErEtJlGnlSaMDEhcAk
/NsQa2k9NPj8E4prRbJiEAMYwcdjiGoR5rQxLtvdpIiOmnuF2JDgLuf7qulyPHGFLadJ3i1d
/qwWuHiQtLxvHVQQUwvxhw==
7



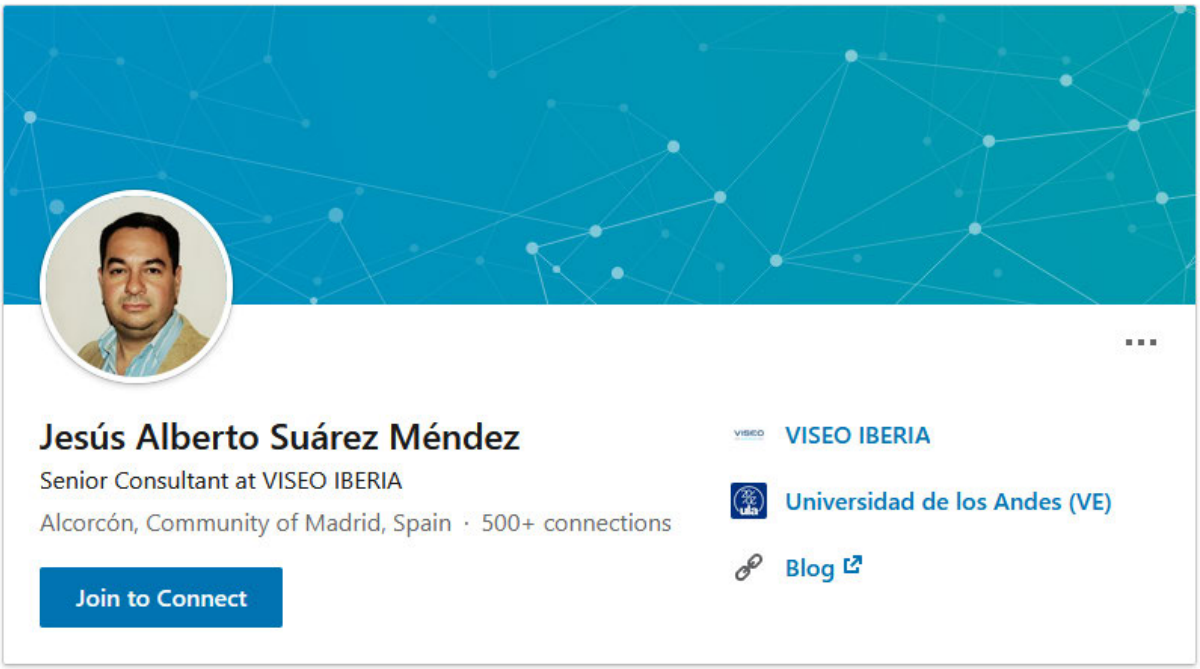
25.smtp.starttls.tls.certificate.parsed.signature_algorithm.name	SHA256WithRSA
25.smtp.starttls.tls.certificate.parsed.signature_algorithm.oid	1.2.840.113549.1.1.11
25.smtp.starttls.tls.certificate.parsed.spki_subject_fingerprint	0d8951ea3bd17cb530a077c61ba8d761cae184b46d9c187d886613e669fabec7
25.smtp.starttls.tls.certificate.parsed.subject.common_name	cntfw02
25.smtp.starttls.tls.certificate.parsed.subject.country	ph
25.smtp.starttls.tls.certificate.parsed.subject.locality	Manila
25.smtp.starttls.tls.certificate.parsed.subject.organization	Comelec
25.smtp.starttls.tls.certificate.parsed.subject_dn	C=ph, L=Manila, O=Comelec, CN=cntfw02
25.smtp.starttls.tls.certificate.parsed.subject_key_info.fingerprint_sha256	4039e3117b53c6736957eab9ce578e88b0bf19b5cf5d6d5228107ac44d1e064f
25.smtp.starttls.tls.certificate.parsed.subject_key_info.key_algorithm.name	RSA
25.smtp.starttls.tls.certificate.parsed.subject_key_info.rsa_public_key.exponent	65537
25.smtp.starttls.tls.certificate.parsed.subject_key_info.rsa_public_key.length	2048
25.smtp.starttls.tls.certificate.parsed.subject_key_info.rsa_public_key.modulus	2Y6qhrBskXsJXWUQ5r04j8ReFh1OlL548KrTelKr9F6H5HCJ72o4/HV9D6Wx9ToIdoKOCxn019YbOMQ7rW GKiZot5+VcHJ6QbKVPIMDPdFJ36XcQy2oAB9zt3A9yuREBWwuBuW1ctkVNKH+Jgau+tH1amO8ncaCFaZ FxYWCryITTrkVke/X4uX6uzT+4sNN9rso /0MlAyebVyG2zsk1bBfOQYu6AcE7LLjO6RXidMx5KUpXZGqykUlSgE5OijRWFcpnv8wWodn6FfoETXZ1YO wJbPeV0zJd3TffiwJCEcC7oyD4AyEVEVyAXgehOz44AEs3bcRuMdiejKzk4tG97uw==
25.smtp.starttls.tls.certificate.parsed.tbs_fingerprint	ea91132986addf5da6e2c00954b27eaf6da981e17d39e74b4c8cf4aa6c673e44
25.smtp.starttls.tls.certificate.parsed.tbs_noct_fingerprint	ea91132986addf5da6e2c00954b27eaf6da981e17d39e74b4c8cf4aa6c673e44
25.smtp.starttls.tls.certificate.parsed.validation_level	unknown
25.smtp.starttls.tls.certificate.parsed.validity.end	2038-01-01T00:00:01Z



25.smtp.starttls.tls.certificate.parsed.validity.length	685711621
25.smtp.starttls.tls.certificate.parsed.validity.start	2016-04-09T12:33:00Z
25.smtp.starttls.tls.certificate.parsed.version	3
25.smtp.starttls.tls.cipher_suite.id	0x002F
25.smtp.starttls.tls.cipher_suite.name	TLS_RSA_WITH_AES_128_CBC_SHA
25.smtp.starttls.tls.ocsp_stapling	False
25.smtp.starttls.tls.validation.browser_error	x509: certificate signed by unknown authority
25.smtp.starttls.tls.validation.browser_trusted	False
25.smtp.starttls.tls.version	TLSv1.2
443.https.dhe.support	False
443.https.dhe_export.support	False
443.https.rsa_export.support	False
alexa_rank	117344
domain	comelec.gov.ph
ports	25
protocols	25/smtp
tags	smtp
updated_at	2020-11-30T12:20:01+00:00

https://es.linkedin.com/in/jesusalbertosuarez

LinkedIn People Jesús Alberto Suárez Méndez



Jesús Alberto Suárez Méndez

Senior Consultant at VISEO IBERIA

Alcorcón, Community of Madrid, Spain · 500+ connections

Join to Connect

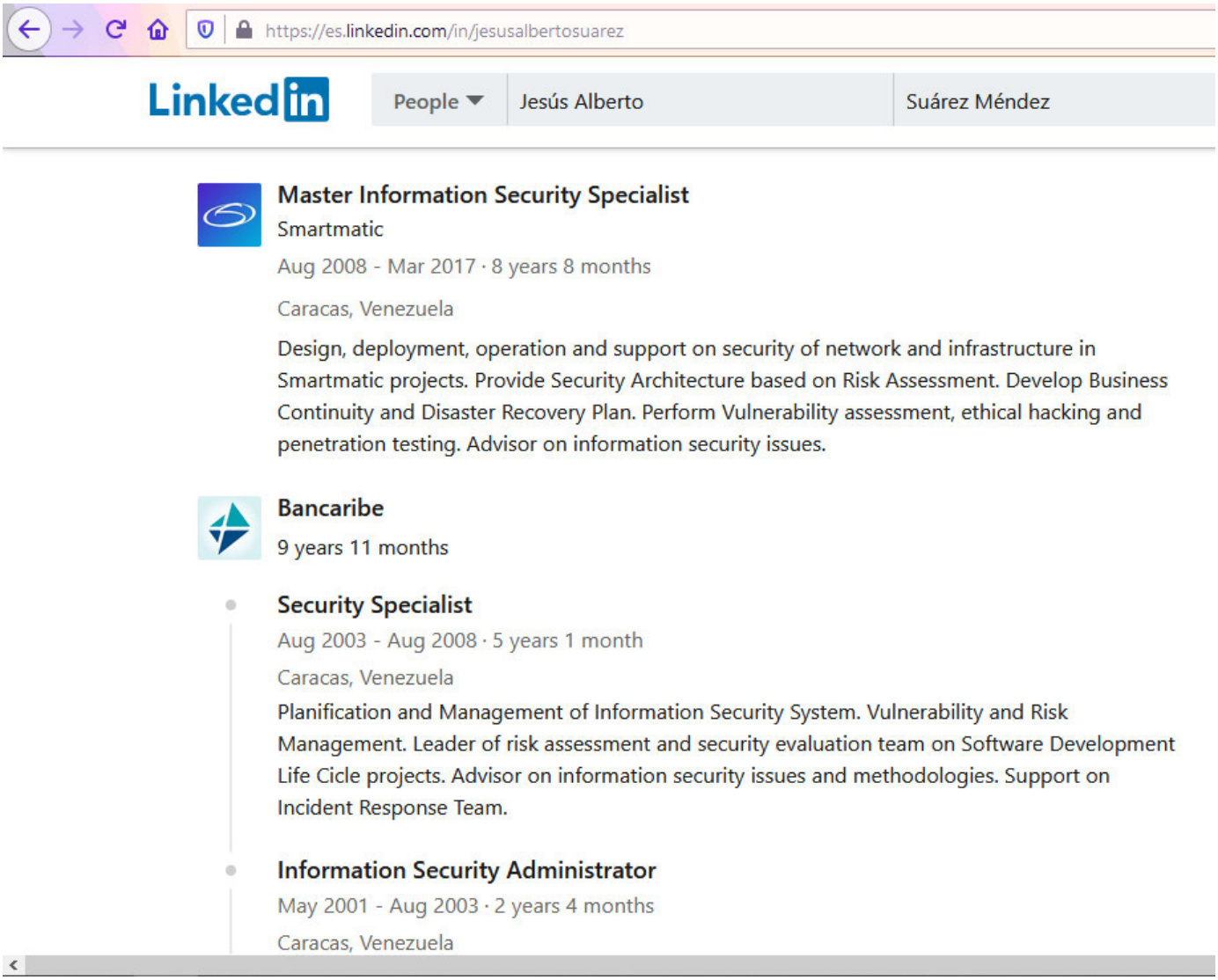
VISEO IBERIA

Universidad de los Andes (VE)

Blog

About

DevOps SysAdmin and Information Security Professional with more than 20 years of experience. Specialized in Security and IT Management, IT Risk Assessment and Management, IT architecture, automatized deployments on Linux environment and cloud using DevOps tools. Very interested in



6. As seen from Jesus' LinkedIn profile, he was employed by Smartmatic as their Master Information Security Specialist from August 2008 – March 2017, within the time frame of the registered SSL certificate for Smartmatic and within Venezuela.
7. This evidence shows that Smartmatic was indeed connected to Venezuela as well as shows that their dealings with the Philippine's is still on-going as their website is in their election commission servers with matching and current SSL certificates.

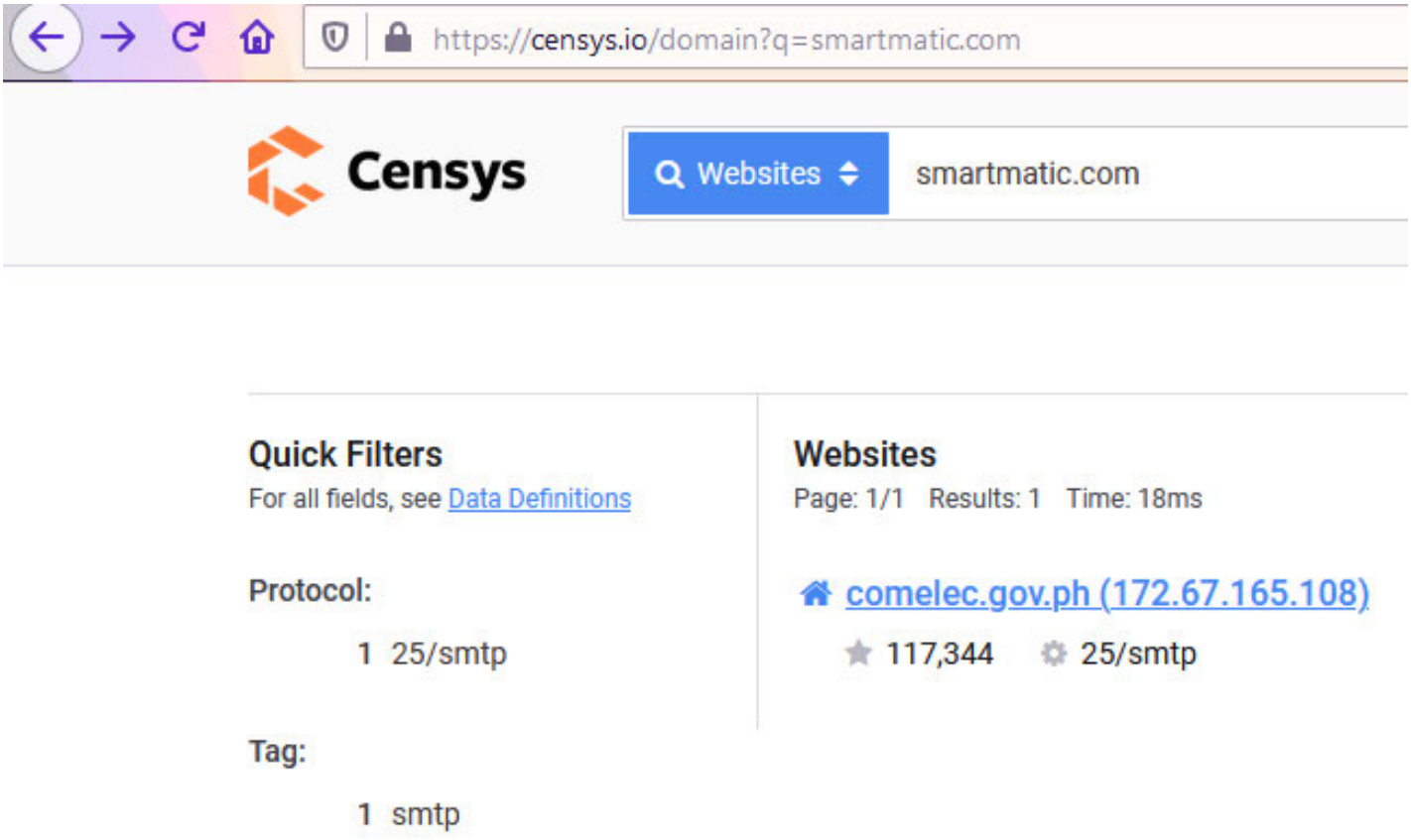
I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge. Executed this November 23th, 2020.

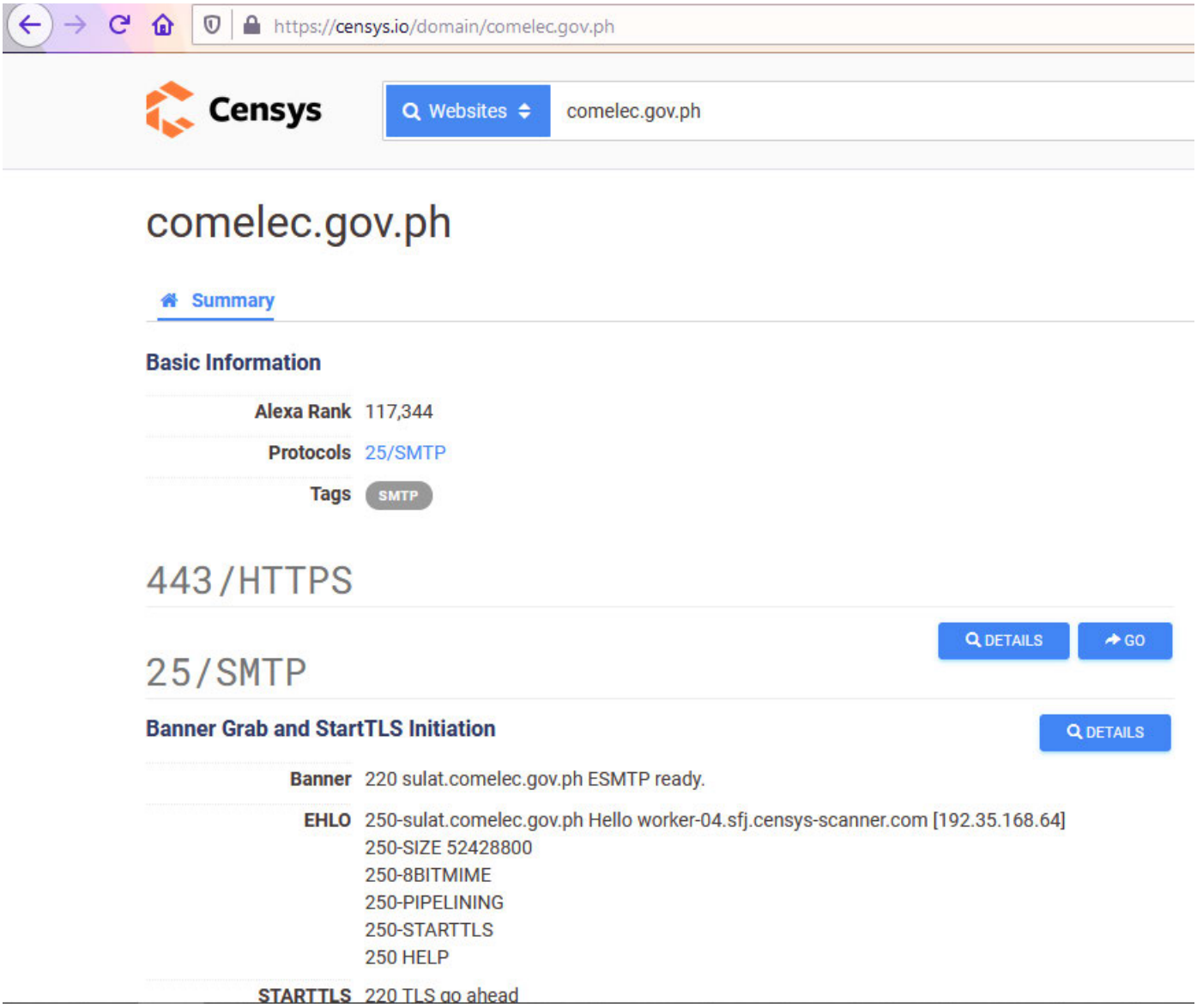
Smartmatic SSL Certificate

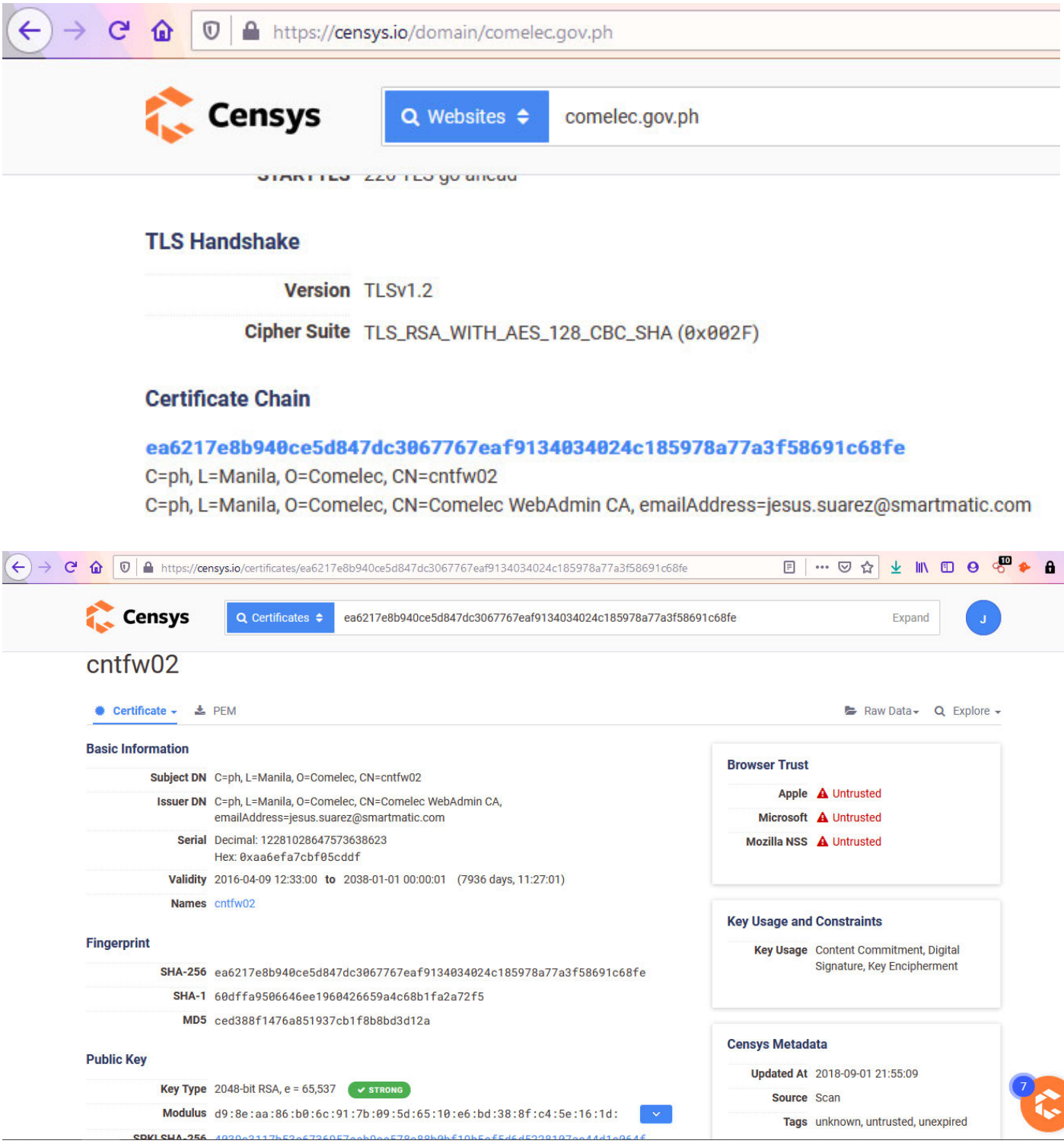
Declaration of [redacted]

Pursuant to 28 U.S.C Section 1746, I, [redacted], make the following declaration.

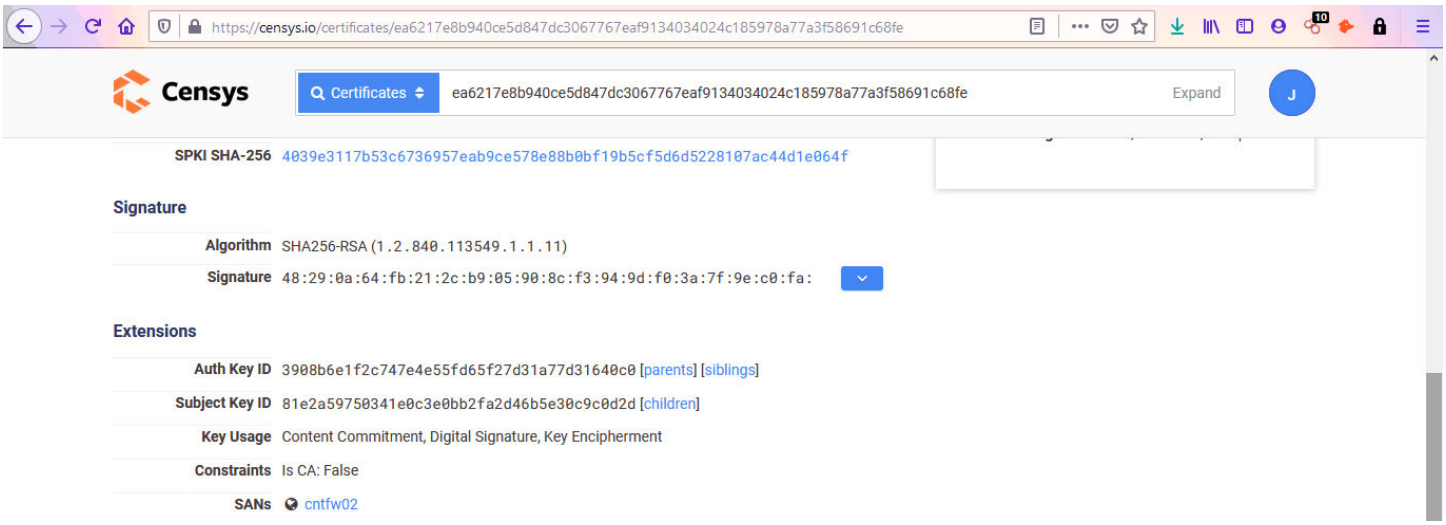
1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I was an electronic intelligence analyst under 305th Military Intelligence with experience gathering SAM missile system electronic intelligence. I have extensive experience as a white hat hacker used by some of the top election specialists in the world. The methodologies I have employed represent industry standard cyber operation toolkits for digital forensics and OSINT, which are commonly used to certify connections between servers, network nodes and other digital properties and probe to network system vulnerabilities.
3. I am a US citizen and I reside at [redacted] location in the United States of America.
4. Researching Smartmatic's website and reading their public manuals about the reuse of SSL certificate's, I started to investigate Smartmatic's SSL certificates. Upon searching their website is currently behind Cloudflare yet using the same SSL certificate it made it easy to locate where Smartmatic's website was located. Smartmatic's website is in the Philippine's on their Election commission's server (Comelec.gov.ph), as seen below:



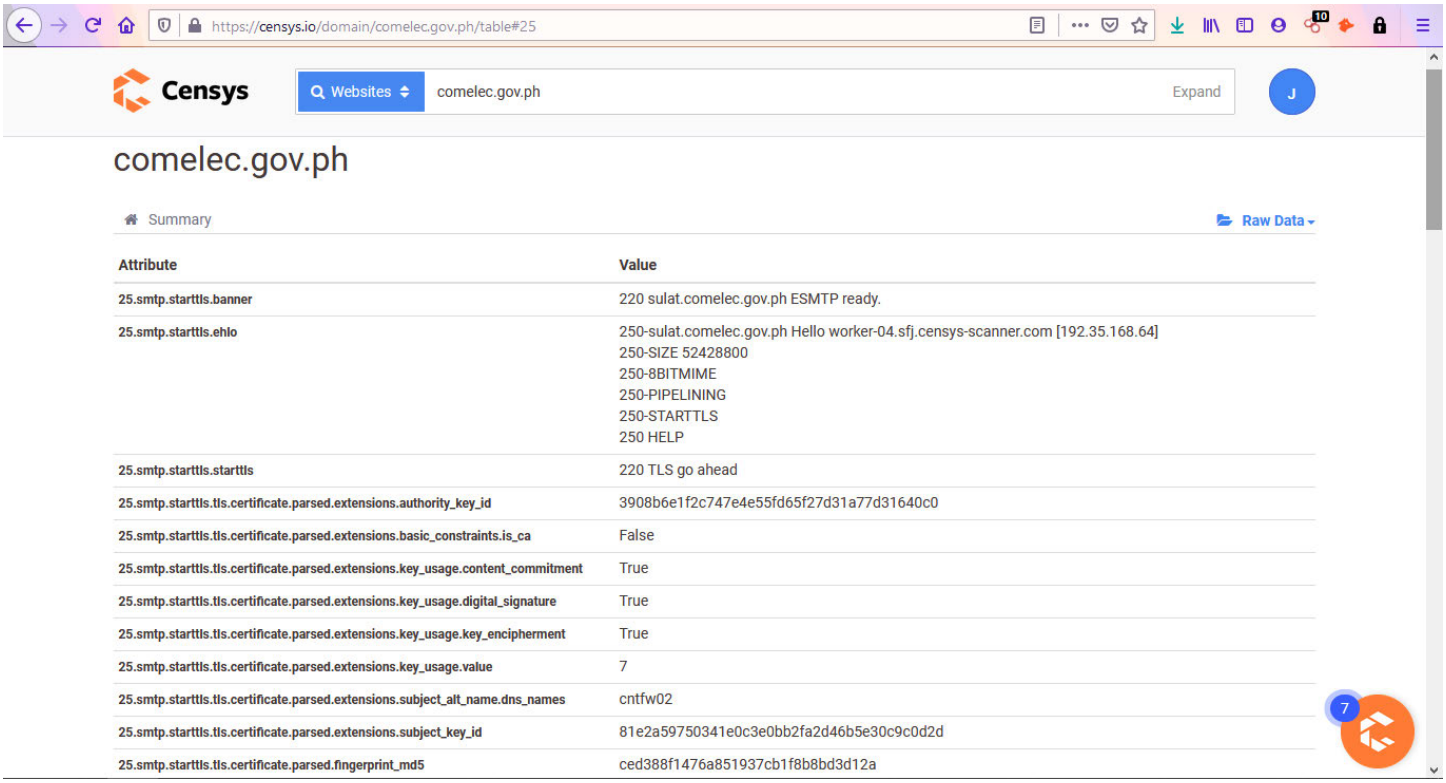

https://censys.io/domain/comelec.gov.ph
Censys
Websites
comelec.gov.ph
comelec.gov.ph
Summary
Basic Information
Alexa Rank 117,344
Protocols 25/SMTP
Tags SMTP
443/HTTPS
DETAILS
GO
25/SMTP
Banner Grab and StartTLS Initiation
DETAILS
Banner 220 sulat.comelec.gov.ph ESMTP ready.
EHLO 250-sulat.comelec.gov.ph Hello worker-04.sfj.censys-scanner.com [192.35.168.64]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-STARTTLS
250 HELP
STARTTLS 220 TLS go ahead

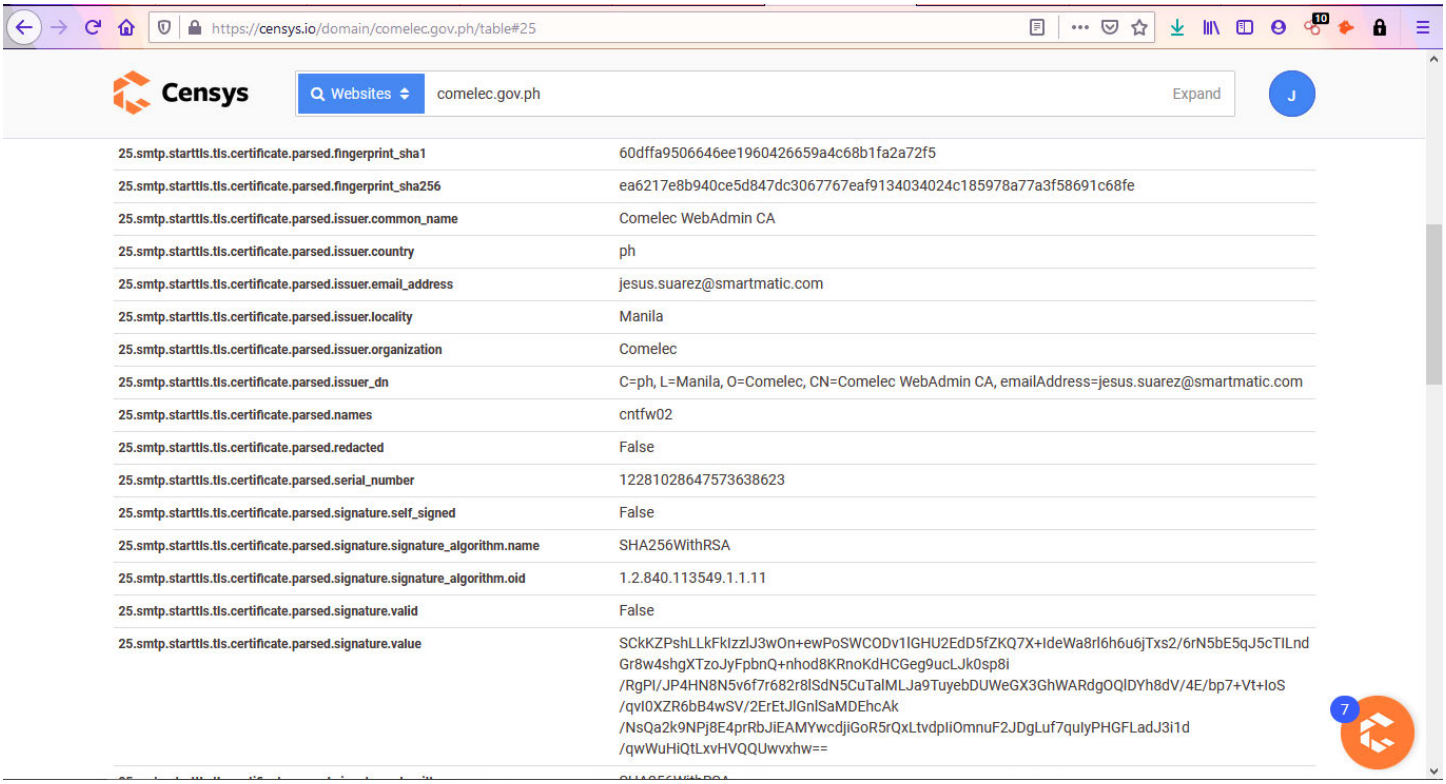

https://censys.io/domain/comelec.gov.ph
Censys
Websites
comelec.gov.ph
TLS Handshake
Version TLSv1.2
Cipher Suite TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
Certificate Chain
ea6217e8b940ce5d847dc3067767eaf9134034024c185978a77a3f58691c68fe
C=ph, L=Manila, O=Comelec, CN=cntfw02
C=ph, L=Manila, O=Comelec, CN=Comelec WebAdmin CA, emailAddress=jesus.suarez@smartmatic.com

https://censys.io/certificates/ea6217e8b940ce5d847dc3067767eaf9134034024c185978a77a3f58691c68fe
Censys
Certificates
ea6217e8b940ce5d847dc3067767eaf9134034024c185978a77a3f58691c68fe
Expand
J
cntfw02
Certificate
PEM
Raw Data
Explore
Basic Information
Subject DN C=ph, L=Manila, O=Comelec, CN=cntfw02
Issuer DN C=ph, L=Manila, O=Comelec, CN=Comelec WebAdmin CA, emailAddress=jesus.suarez@smartmatic.com
Serial Decimal: 1228102864757363862 3 Hex: 0xaa6efa7cbf05cddf
Validity 2016-04-09 12:33:00 to 2038-01-01 00:00:01 (7936 days, 11:27:01)
Names cntfw02
Fingerprint
SHA-256 ea6217e8b940ce5d847dc3067767eaf9134034024c185978a77a3f58691c68fe
SHA-1 60dffa9506646ee1960426659a4c68b1fa2a72f5
MD5 ced388f1476a851937cb1f8b8bd3d12a
Public Key
Key Type 2048-bit RSA, e = 65,537 STRONG
Modulus d9:8e:aa:86:b0:6c:91:7b:09:5d:65:10:e6:bd:38:8f:c4:5e:16:1d:
Browser Trust
Apple Untrusted
Microsoft Untrusted
Mozilla NSS Untrusted
Key Usage and Constraints
Key Usage Content Commitment, Digital Signature, Key Encipherment
Censys Metadata
Updated At 2018-09-01 21:55:09
Source Scan
Tags unknown, untrusted, unexpired

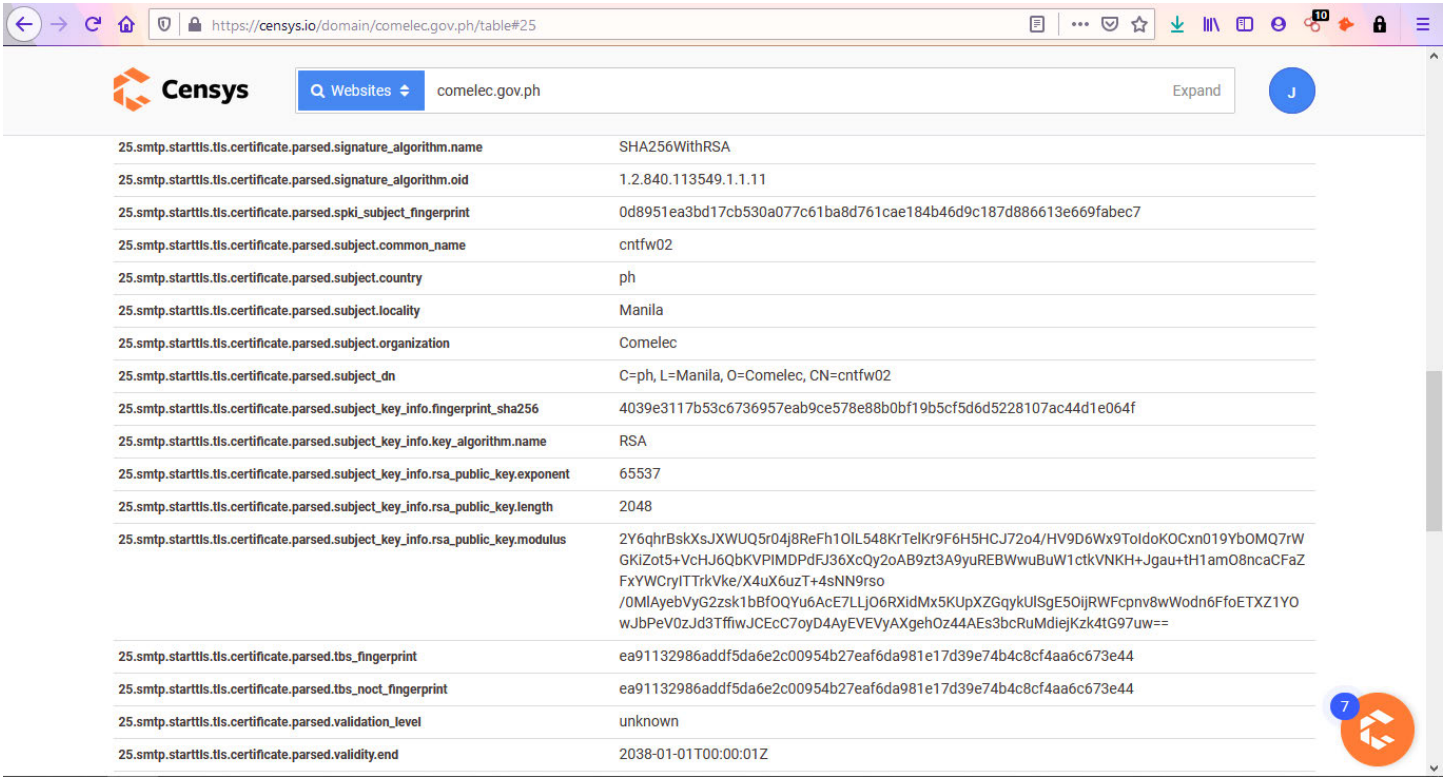


5. As can be seen in the images above the SSL certificate used was registered by the email address jesus.suarez@smartmatic.com on the 9th of April 2016.

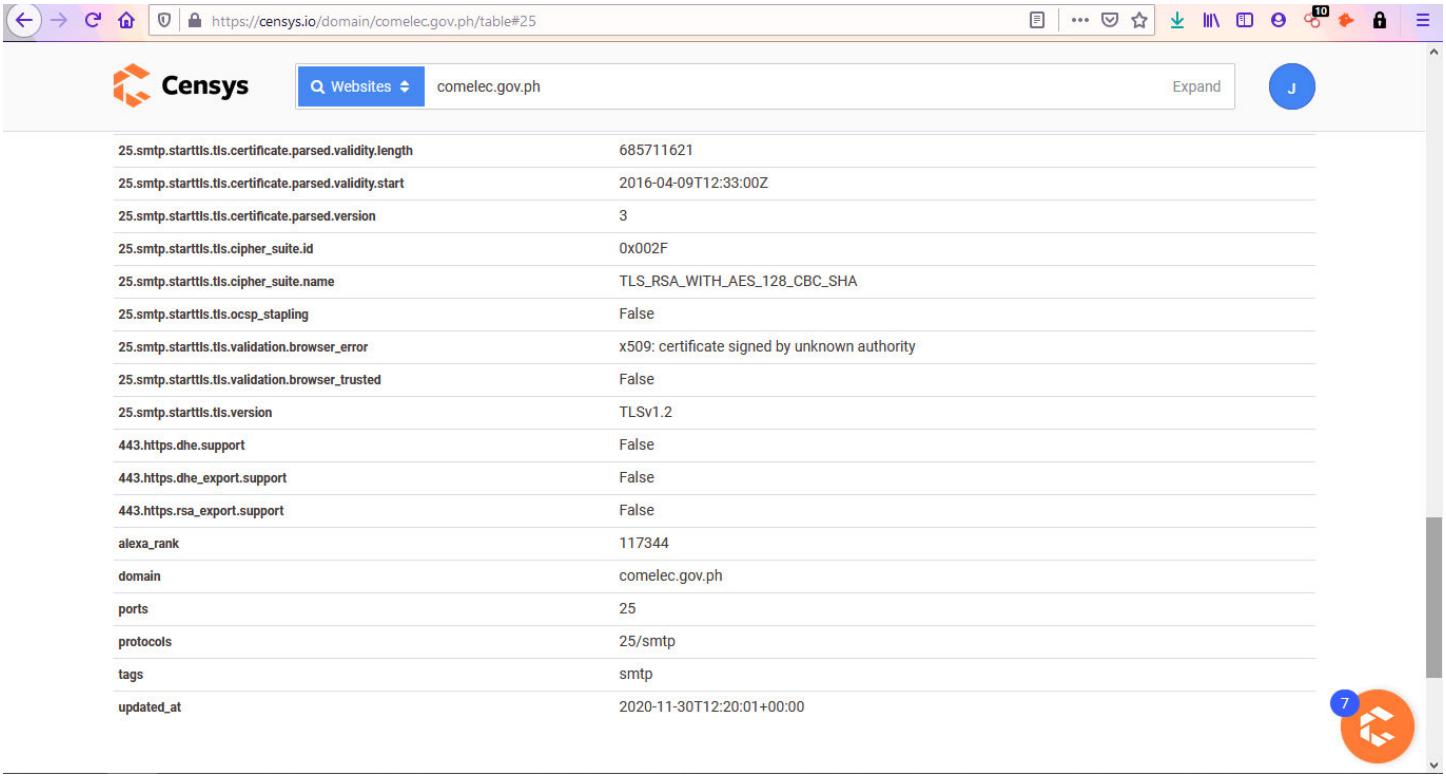




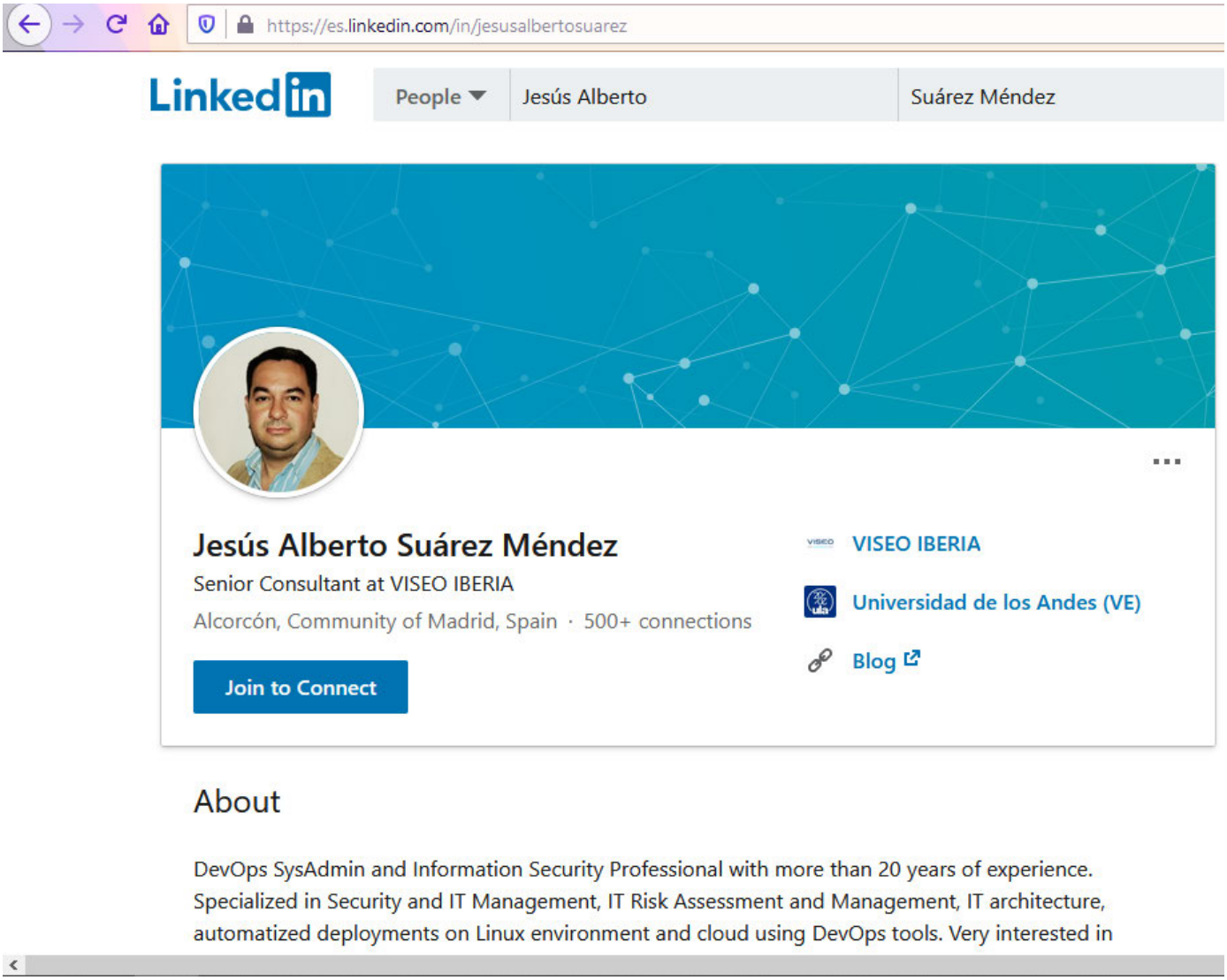
25.smtp.starttls.tls.certificate.parsed.fingerprint_sha1	60dffa9506646ee1960426659a4c68b1fa2a72f5
25.smtp.starttls.tls.certificate.parsed.fingerprint_sha256	ea6217e8b940ce5d847dc3067767eaf9134034024c185978a77a3f58691c68fe
25.smtp.starttls.tls.certificate.parsed.issuer.common_name	Comelec WebAdmin CA
25.smtp.starttls.tls.certificate.parsed.issuer.country	ph
25.smtp.starttls.tls.certificate.parsed.issuer.email_address	jesus.suarez@smartmatic.com
25.smtp.starttls.tls.certificate.parsed.issuer.locality	Manila
25.smtp.starttls.tls.certificate.parsed.issuer.organization	Comelec
25.smtp.starttls.tls.certificate.parsed.issuer_dn	C=ph, L=Manila, O=Comelec, CN=Comelec WebAdmin CA, emailAddress=jesus.suarez@smartmatic.com
25.smtp.starttls.tls.certificate.parsed.names	cntfw02
25.smtp.starttls.tls.certificate.parsed.redacted	False
25.smtp.starttls.tls.certificate.parsed.serial_number	12281028647573638623
25.smtp.starttls.tls.certificate.parsed.signature.self_signed	False
25.smtp.starttls.tls.certificate.parsed.signature.signature_algorithm.name	SHA256WithRSA
25.smtp.starttls.tls.certificate.parsed.signature.signature_algorithm.oid	1.2.840.113549.1.1.11
25.smtp.starttls.tls.certificate.parsed.signature.valid	False
25.smtp.starttls.tls.certificate.parsed.signature.value	SCkKZPshLLkFkIzzlJ3wOn+ewPoSWCODv1lGHU2EdD5fZKQ7X+IdeWa8rl6h6u6jTxs2/6rN5bE5qJ5cTILnd Gr8w4shgXTzoJyFpbnQ+nhod8KRnoKdHCGeg9ucLJk0sp8i /RgPl/JP4HN8N5v6f7r682r8lSdN5CuTalMLJa9TuyebDUWeGX3GhWARdgOQlDYh8dV/4E/bp7+Vt+IoS /qvI0XZR6bB4wSV/2ErEtJlGnlSaMDEhcAk /NsQa2k9NPj8E4prRbJiEAMYwcdjiGoR5rQxLtvdpIiOmnuF2JDgLuf7qulyPHGFLadJ3i1d /qwWuHiQtLxvHVQQUwvxhw==

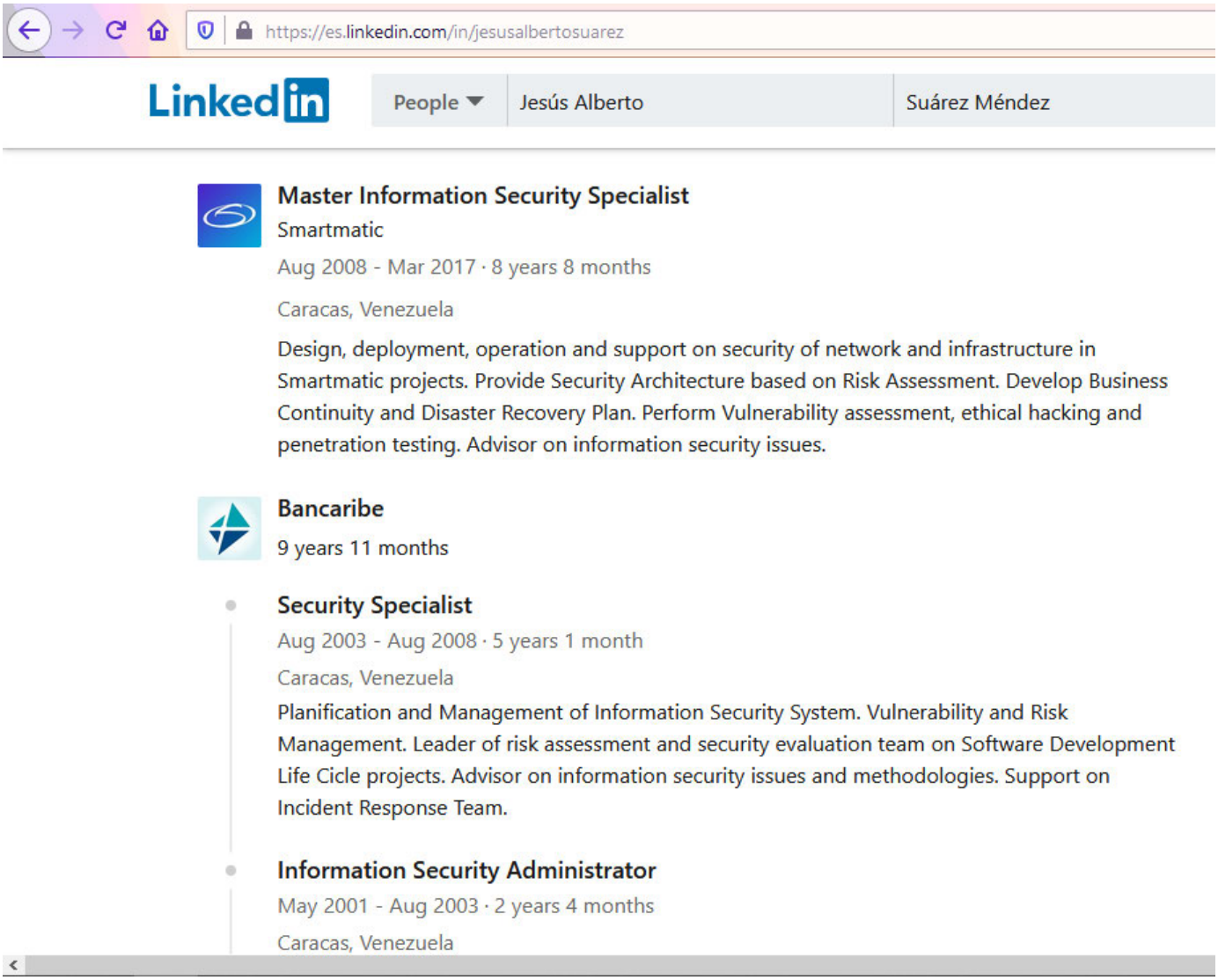


25.smtp.starttls.tls.certificate.parsed.signature_algorithm.name	SHA256WithRSA
25.smtp.starttls.tls.certificate.parsed.signature_algorithm.oid	1.2.840.113549.1.1.11
25.smtp.starttls.tls.certificate.parsed.spki_subject_fingerprint	0d8951ea3bd17cb530a077c61ba8d761cae184b46d9c187d886613e669fabec7
25.smtp.starttls.tls.certificate.parsed.subject.common_name	cntfw02
25.smtp.starttls.tls.certificate.parsed.subject.country	ph
25.smtp.starttls.tls.certificate.parsed.subject.locality	Manila
25.smtp.starttls.tls.certificate.parsed.subject.organization	Comelec
25.smtp.starttls.tls.certificate.parsed.subject_dn	C=ph, L=Manila, O=Comelec, CN=cntfw02
25.smtp.starttls.tls.certificate.parsed.subject_key_info.fingerprint_sha256	4039e3117b53c6736957eab9ce578e88b0bf19b5cf5d6d5228107ac44d1e064f
25.smtp.starttls.tls.certificate.parsed.subject_key_info.key_algorithm.name	RSA
25.smtp.starttls.tls.certificate.parsed.subject_key_info.rsa_public_key.exponent	65537
25.smtp.starttls.tls.certificate.parsed.subject_key_info.rsa_public_key.length	2048
25.smtp.starttls.tls.certificate.parsed.subject_key_info.rsa_public_key.modulus	2Y6qhrBskXsJXWUQ5r04j8ReFh1OlL548KrTelKr9F6H5HCJ72o4/HV9D6Wx9ToIdoKOCxn019YbOMQ7rW GKiZot5+VcHJ6QbKVPIMDPdFJ36XcQy2oAB9zt3A9yuREBWwuBuW1ctkVNKH+Jgau+tH1amO8ncaCFaZ FxYWCryITTrkVke/X4uX6uzT+4sNN9rso /0MlAyebVyG2zsk1bBfOQYu6AcE7LLjO6RXidMx5KUpXZGqykUlSgE5OijRWFcpnv8wWodn6FfoETXZ1YO wJbPeV0zJd3TffiwJCEcC7oyD4AyEVEVyAXgehOz44AEs3bcRuMdiejKzk4tG97uw==
25.smtp.starttls.tls.certificate.parsed.tbs_fingerprint	ea91132986addf5da6e2c00954b27eaf6da981e17d39e74b4c8cf4aa6c673e44
25.smtp.starttls.tls.certificate.parsed.tbs_noct_fingerprint	ea91132986addf5da6e2c00954b27eaf6da981e17d39e74b4c8cf4aa6c673e44
25.smtp.starttls.tls.certificate.parsed.validation_level	unknown
25.smtp.starttls.tls.certificate.parsed.validity.end	2038-01-01T00:00:01Z



25.smtp.starttls.tls.certificate.parsed.validity.length	685711621
25.smtp.starttls.tls.certificate.parsed.validity.start	2016-04-09T12:33:00Z
25.smtp.starttls.tls.certificate.parsed.version	3
25.smtp.starttls.tls.cipher_suite.id	0x002F
25.smtp.starttls.tls.cipher_suite.name	TLS_RSA_WITH_AES_128_CBC_SHA
25.smtp.starttls.tls.ocsp_stapling	False
25.smtp.starttls.tls.validation.browser_error	x509: certificate signed by unknown authority
25.smtp.starttls.tls.validation.browser_trusted	False
25.smtp.starttls.tls.version	TLSv1.2
443.https.dhe.support	False
443.https.dhe_export.support	False
443.https.rsa_export.support	False
alexa_rank	117344
domain	comelec.gov.ph
ports	25
protocols	25/smtp
tags	smtp
updated_at	2020-11-30T12:20:01+00:00


https://es.linkedin.com/in/jesusalbertosuarez
LinkedIn
People
Jesús Alberto
Suárez Méndez
Jesús Alberto Suárez Méndez
Senior Consultant at VISEO IBERIA
Alcorcón, Community of Madrid, Spain · 500+ connections
Join to Connect
VISEO IBERIA
Universidad de los Andes (VE)
Blog
About
DevOps SysAdmin and Information Security Professional with more than 20 years of experience. Specialized in Security and IT Management, IT Risk Assessment and Management, IT architecture, automatized deployments on Linux environment and cloud using DevOps tools. Very interested in



6. As seen from Jesus' LinkedIn profile, he was employed by Smartmatic as their Master Information Security Specialist from August 2008 – March 2017, within the time frame of the registered SSL certificate for Smartmatic and within Venezuela.
7. This evidence shows that Smartmatic was indeed connected to Venezuela as well as shows that their dealings with the Philippine's is still on-going as their website is in their election commission servers with matching and current SSL certificates.

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge. Executed this December 3rd, 2020.

[redacted]