

These are one set from a series of emails between Lt Maddock at the Honolulu Police Department and I. In addition, I submitted over 40 police reports with evidence on thumb drives and websites. Videos I delivered as evidence unquestionably proved illegal intrusions into my business network. Everything I submitted was ignored. Law enforcement at all levels refuse to thoroughly investigate any of the cyber crimes I reported. I never received a reply to my emails to the FBI and HPD about the around-the-clock cyber attacks I received.

→ **Information Request/Ricardo Finney Sends**

Raineer 44 <raineer44@lionofjudah808.live>

Wed 5/11/2022 3:46 PM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Aloha, Lt Maddock...

I asked previously but did not receive your reply when I asked:

- if you incurred a problem responding to my encrypted nikon@precisionphotography.live address since I never received your correspondence there.
- for a source from whom I can purchase a secure cellphone of the type used by government officials, politicians, etc.
- if your examination of my computers are limited to those looked at in 2016.

Please advise about the email, the secure cellphone, and the computers. Thank you for your time.

Respectfully,

Ricardo Finney

Precision Photography Hawaii

No reply as of 5/12/22

Unclear why answers refused

Re: HPD Report 22-154047 Referred From Officer Lamug

Raineer 44 <raineer44@lionofjudah808.live>

Wed 5/11/2022 3:39 PM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Aloha, Lt Maddock...

**Irrefutable cyberattack
evidence delivered**

Considering the video evidence and Facebook web site events detailed in my last HPD statement and many emails, I'm unclear why there has been no reply to, or action in response to my last email. The evidence video I provided on the USB thumb drive shows the Post& Email (P&E) Facebook pages reconfigured to a running loop. A second video shows my Windows computer alternating between its Standard and Administrator accounts. The empty Facebook site illegally redirected from my populated cyber crime site. The video content doesn't require a forensic examination. An investment of manpower involves looking at 5 minutes of videos, reading a network diagram, and validating where my stolen website lands.

The visuals show the evidence of hacking you require. Anyone with a reasonable degree of computer proficiency through high-end IT technical and forensic professionals will see the content in the videos presents evidence of hacking. Microsoft will provide the official security determination concerning the incidents I experienced.

Every weekly and bi-weekly cell phone attempt I made over the past 7 months trying to connect personally with Ms. Sharon Rondeau, the P&E editor failed. I submit the same cyber criminals who blocked my Facebook access to Ms. Rondeau are blocking my one-on-one voice connection. No matter what time or day I call including multiple times per day, I get voicemail. I did not make a single successful connection which is identical to my failed attempts to connect to Ms. Odom and others detailed in my Verizon cell phone log.

I ask again that the denial of my phone communication to Ms. Rondeau be investigated without further delay. I ask that the denial of my phone communication with Ms. Odom be investigated without further delay. I ask again that you contact Tyler at Fortinet Cyber Security without further delay about his email send to me that did not arrive.

Cyber attacks and intrusions into my business network have intensified since I delivered my most recent HPD crime statement. I urgently need law enforcement intervention. Standing by for your reply. Thank you for your time.

Respectfully,

No reply as of 5/12/22

Ricardo Finney

Precision Photography Hawaii

From: Raineer 44 <raineer44@lionofjudah808.live>**Sent:** Monday, May 9, 2022 9:45 AM**To:** Maddock, Andrew R. <amaddock@honolulu.gov>**Subject:** Re: HPD Report 22-154047 Referred From Officer Lamug

Aloha, Lt Maddock...

Ref your 4/29/22 comment "Facebook has always assigned their user account using the format with a dot like <https://www.facebook.com/rick.finney.142>. Your explanation to me stating all Facebook addresses require dots is wrong. No where in the documentation Facebook posts is there evidence to support what you told me. Furthermore, Facebook addresses commonly used prove this:

<https://www.facebook.com/lapdhq>
<https://www.facebook.com/SFPD>
<https://www.facebook.com/MayoClinicHealthSystem>
<https://www.facebook.com/Lakers>
<https://www.facebook.com/NASA>
<https://www.facebook.com/create/livehelp>

**The reasons HPD gave
for refusing to investigate
cyber crimes have no merit.**

All of these Facebook addresses and untold numbers more are functional without dots included. My original Facebook address that did not contain periods is no exception. I don't know if the explanation provided was because the HPD website includes a dot and the assumption was that all Facebook addresses did, or if I was told that just to discount what I presented. Regardless, as I explained in 4/29/22 response, my Facebook cyber crime site remains illegally redirected to hide the evidence inside. Apparently, the criminals gained access using the process you identified. My requests to investigate the illegal takedown of my Facebook cyber crime site continue to be ignored.

Concerning the incidents I encountered while at <https://www.thepostemail.com>, your reply attributed everything I encountered to "a misconfigured modem or firewall". There was no acknowledgment of an event that could not possibly be caused by anything other than hacking, that being the video I captured and provided on a thumb drive showing the Post & Email Facebook page changing like a movie. If accessing my thumb drives to view the videos is a concern using your virtual computer eliminates risk.

There was no acknowledgment of the video I captured and provided on a thumb drive proving the intrusion into my Windows PC that caused my Standard and Admin accounts to be active at the same time. This is an event which is impossible to achieve from the user end as it is impossible to log into both accounts at the same time. This event cannot be attributed to anything else but hacking yet it is ignored as if it never happened.

The claim the Verizon call log I submitted is considered normal has no more merit than stating Facebook addresses have always assigned user accounts with a dot. The call log reveal each phone number for every text, call, email, and fax I attempted to send was blocked from being delivered.

Calls and texts I made attempting to reach Anna Odom don't appear even though I saved screen shots proving the tries were made. During the period in question not one of fourteen texts, calls, emails, or fax I sent from my cell phone to media, cyber security firms, and other agencies were answered. An additional 12 emails I have sent to media, cyber security firms, and other agencies using three different email addresses remain unanswered. I submit they are being blocked to prevent communication.

I explained the denial problem was not limited to emails I send. I provided the contact information for Tyler at the security firm Fortinet to verify he sent emails to me about cyber attack security support which I never received. This is a witness who can prove what I claim is true. Again, my request to contact him was ignored as if I never made the reference.

It is wrong to ignore my redirected Facebook cyber crime evidence site, the scrolling Post & Email Facebook site, the Standard and Admin accounts in my PC operating simultaneously, the litany of emails I've sent with zero replies. I asked if incidents such as these are not hacking. I did not receive a reply, yet repeatedly, I am only given reasons why there are no problems instead of investigating obvious illegal intrusions. I ask again for intervention without further delay.

Respectfully,

Ricardo Finney

No reply through 5/12/22

From: Maddock, Andrew R. <amaddock@honolulu.gov>
Sent: Friday, April 29, 2022 12:03 PM
To: Raineer 44 <raineer44@lionofjudah808.live>
Subject: RE: HPD Report 22-154047 Referred From Officer Lamug

Wrong information



Hi Ricardo,

I'm able to view your Facebook page here without any problems. Facebook has always assigned their user account using the format with a dot like <https://www.facebook.com/rick.finney.142>. If the address: <https://www.facebook.com/rickfinney142> worked for you before then Facebook was most likely creating an alias back to the site with the dots in the name. You shouldn't be putting your phone number, address or email on Facebook directly because criminals will use that information to steal your identity. Sites like IPLogger.org are not reliable and cannot be used to determine IP routing. It is normal for Facebook to route traffic through multiple servers around the world for load balancing and for someone to hack your site on Facebook they would need to have control of Facebook servers which would be highly unlikely. I'm able to access the site: <https://www.thepostemail.com> without any problems so your access problem could be due to a misconfigured modem or firewall. The site lists a phone number: 203-987-7948 which you can call to verify if they are receiving your emails. Many of your problems appear to come from over complicating your environment by having a firewall and additional software such as Anti-virus and VPN all running at the same time. These combinations can conflict with each other and cause problems. You can't just assume that a connectivity problem is a cyber-crime or when someone doesn't respond to an email that you sent. If the email is not returned to you then it was sent to the address that you entered, otherwise the server would kick it back.

Video evidence ignored

Lieutenant Andrew Maddock
Honolulu Police Department
Criminal Investigations
Cyber Crimes, Digital Computer Forensics and Crime Analysis
808-723-3586

From: Raineer 44 <raineer44@lionofjudah808.live>
Sent: Friday, April 29, 2022 11:18 AM
To: Maddock, Andrew R. <amaddock@honolulu.gov>
Subject: HPD Report 22-154047 Referred From Officer Lamug

CAUTION: Email received from an EXTERNAL sender. Please confirm the content is safe prior to opening attachments or links.

4/29/22

Aloha, Lt Maddock...

I spoke this morning with Officer Lamug about my HPD report 22-154047 filed on 4/20/22. Not being technically proficient with computers, Officer Lamug agreed it was best he referred my 4/20/22 statement to you. With that said, I return to you again for resolution of HPD report 22-154047.

In addition to my prior request to identify evidence of hacking within my 3/17/22 HPD statement, I ask that you determine if these incidents detailed in report 22-154047 show hacking as well. I provided narratives and visual evidence on a thumb drive:

- My populated Facebook evidence site was redirected twice to a site with no content.
- No email received from a representative from the security firm Fortinet.com, one of 10 addressees who either verified sending emails I did not receive, or an addressee did not receive email I sent,
- Disjointed and disappearing web page content from <https://www.thepostemail.com> captured in screen shots to display.
- Video showing web pages at <https://www.thepostemail.com> flipping in rapid-fire, movie-like fashion with motion that prevented me from posting cyber crime evidence on the media site's Facebook page.
- Takedown of my recently uploaded Dropbox link whereby crime evidence content I uploaded was illegally accessed and erased, The shortened link I used was problem-free but now give an access warning.
- Email alledged from the editor of the Post & Email news site who has been in operation since 2009 but does not have a single media contact.
- Email alledged from the Post&Email editor referring an attorney who as stated successfully sued the federal government for illegal surveillance, yet operates an unsecured/http website. Doesn't pass the common sense test.

The incident with the representative from Fortinet and the editor from the Post&Email news site can be quickly and easily resolved by phone. I ask that a call be made to both individuals to see if my statements check out.

Officer Lamug mentioned he saw your notes which state you inspected two of my computers in December 2021. That did not occur. The only two computers you've inspected were done in 2016 when I asked for the operating system to be examined but the device was checked for malware and spyware. I asked in October 2021 for my compromised desktop computer to be inspected and did not receive a reply. I asked in December 2021 to have my compromised desktop computer inspected and was told no.

As I stated in October and December 2021, a visual inspection of the devices will reveal the compromises I explained occurred.

I continue to receive illegal intrusions into my business network and devices each login every day and night. My attackers have a lot of crimes to hide. That is why they so prolific. As I've noted repeatedly, as a direct result of the incessant cyber attacks, my wife and I cannot operate our computer-based businesses to generate income.

I respectfully request by close of business Thursday, May 5th, you provide your determination if my business devices or business network were hacked as I detailed in my two HPD statements. If you determine yes, please tell me what action(s) you will take to stop the cyber crimes so we are no longer victimized, and when. If you find nothing, please explain why.

Please reply with confirmation you received this email. Thank you for your time. I appreciate it.

Mahalo,

Ricardo Finney
Precision Photography Hawaii



Secured by [Paubox](#) - HITRUST CSF certified

Re: HPD case number 22-161028

Raineer 44 <raineer44@lionofjudah808.live>

Fri 5/6/2022 1:22 PM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Aloha, Lt Maddock... Re: HPD case number 22-161028

**Referred to Lt Maddock
after Officer Peter
closed out my case**

My family and I continue to be stalked online and my devices illegally entered and compromised. I submit this information to add to the list of cyber attack statements I've referred to you since 3/17/22 with requests to investigate and intervene. On 4/25/22 I submitted a HPD statement at the Kapolei Station explaining my iPad and iPhone have been reconfigured to prevent me from connecting to, and corresponding with the Epoch Times news site about my cyber crime cases.

Officer J. Peter assigned my submission to HPD case number 22-161028. On 5/1/22 I filed a follow-on statement providing video evidence of the intrusions.

Officer Peter informed me she documented my submission and stated she will not take further action. I asked Officer Peter to refer my case to your cyber crime division for action, however she expressed an unwillingness to do so.

The evidence in my two statements clearly show the results of illegal intrusions into my two devices that prevent connectivity to a specific source; in this case a repeat incident involving the Epoch Times news outlet stopping me from communicating to them about my cyber attacks and whistle blowing.

I ask that you investigate these intrusions I documented in my two HPD reports 22-161028. Please advise if you will do so, or not. Thank you for your time.

Respectfully,

Ricardo Finney

Precision Photography Hawaii

Response Requested/Ricardo Finney Sends

Raineer 44 <raineer44@lionofjudah808.live>

Thu 5/5/2022 9:00 AM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Aloha,

I checked this morning and after four business days do not see a response to my request to communicate in my SonicWall encrypted email portal, nor replies to the emails I sent from my nikon@precisionphotography.live address.

In my 4/25/22 HPD report 22-154047 I provided proof my populated Facebook evidence site with cyber crime evidence content was redirected to an empty site to hide the proof I uploaded. The redirection had to be accomplished through the Facebook server as you explained, an action far out of my control, and counterproductive to the intent of my Facebook site.

Second, I provided a video on a USB thumb drive attached to the report showing my Windows Standard and Administrator accounts operating at the same time out of my control during an attempted log-on session, an event that was impossible to occur unless my computer was accessed and controlled remotely. The normal Windows logon process for any user will not allow the Standard and Administrator accounts accessed from the desktop to be logged into simultaneously. One or the other must be chosen to operate, not both at the same time.

Third, I provided a video I captured at the Post & Email online news website that shows the site pages rapidly changing in a movie-like fashion. This event was impossible for me to manipulate or control. It did serve to prevent me from posting to the website however.

Fourth, after not receiving a single reply to six emails and one fax sent from three different email addresses I used attempting to correspond with the Epoch Times news outlet, to Anna Odom, and to foxnews.com, my compromised Verizon cell phone network revealed someone (not me) made over 300 calls made minutes and seconds apart while I tried to connect effectively blocking the calls I tried to make.

None of these events are "normal" computer glitches, firewall misconfigurations, or the result of me being paranoid or imagining these illegal intrusions occurred. Instead, each event proves I am stalked and tracked online. My business computers and network are accessed remotely illegally, and that other similar events noting my devices were disabled as I referred are factual.

The hourly stalking and cyber attacks I receive continue and prevent me from operating my computer-based business so I can earn income. I am blocked from seeking secure legal and media help online. I cannot conduct online banking and other secure trade online. I ask again that you investigate the computer crimes I've proven and intervene. Thank you for your time.

Respectfully,

Ricardo Finney
Precision Photography

From: Maddock, Andrew R. <amaddock@honolulu.gov>
Sent: Monday, January 3, 2022 8:31 AM
To: Raineer 44 <raineer44@lionofjudah808.live>
Subject: RE: Response Requested/Ricardo Finney Sends

This message's attachments contains at least one web link. This is often used for phishing attempts. Please only interact with this attachment if you know its source and that the content is safe. If in doubt, confirm the legitimacy with the sender by phone.

Hi Ricardo,

I have reviewed the material in your reports and on your website. I still do not see any sign of actual hacking. The things that you are reporting appear to be normal computer issues or spoofing by scam callers. I have outlined a few of these in the attached Word document.

Lieutenant Andrew Maddock
Honolulu Police Department
Criminal Investigations
Cyber Crimes, Digital Computer Forensics and Crime Analysis
808-723-3586

All I reported gave no sign of actual hacking
All "appear to be normal computer issues or spoofing by scam callers"

From: Raineer 44 <raineer44@lionofjudah808.live>
Sent: Wednesday, December 29, 2021 4:39 PM
To: Maddock, Andrew R. <amaddock@honolulu.gov>
Subject: Re: Response Requested/Ricardo Finney Sends

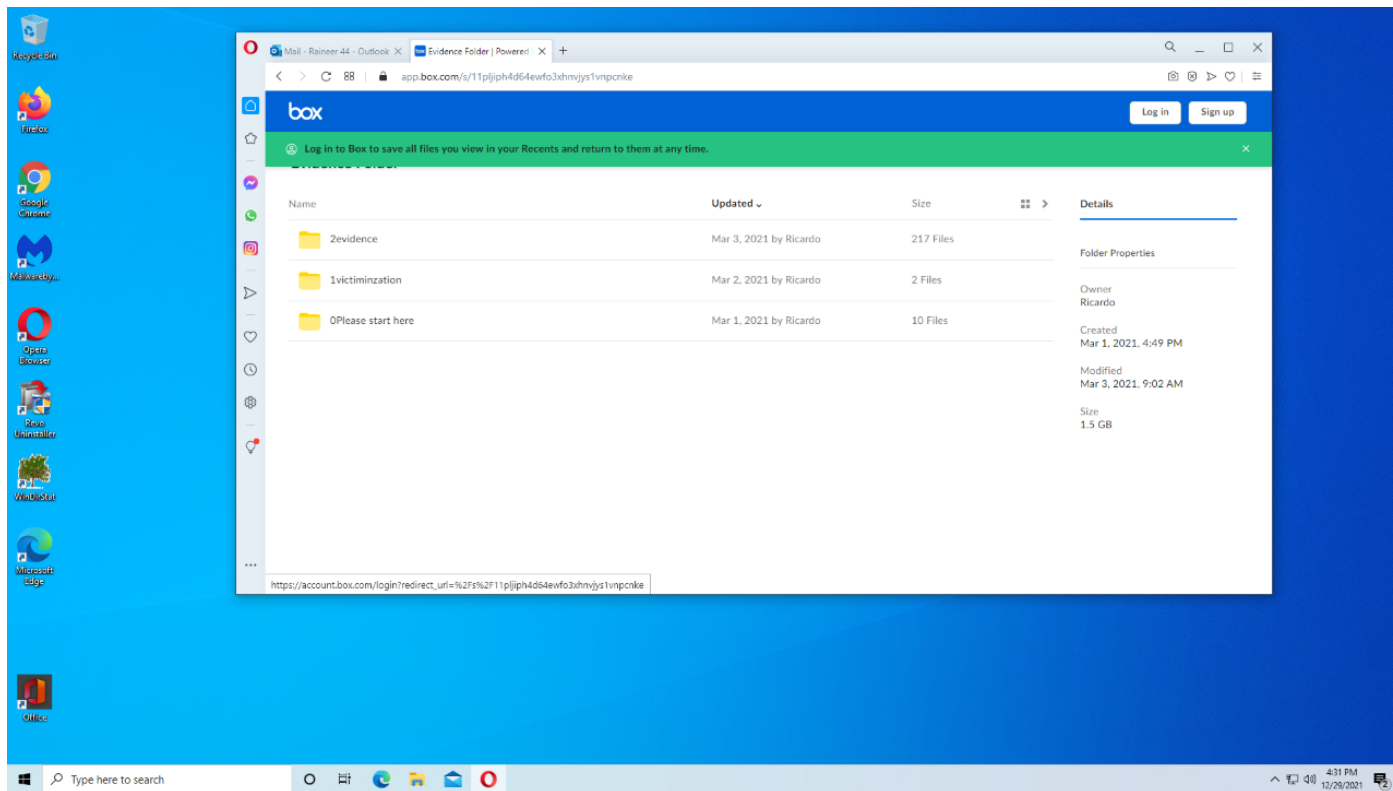
CAUTION: Email received from an EXTERNAL sender. Please confirm the content is safe prior to opening attachments or links.

Aloha, Lt. Maddock...

Thank you for replying. Their appears to be a mistake with the link name. The site is active.

<https://bit.ly/380QUe8>

I will be off-island from 1/06/22 - 1/20/22 attending my granddaughter's christening and birthday.



From: Maddock, Andrew R. <amaddock@honolulu.gov>
Sent: Wednesday, December 29, 2021 1:47 PM
To: Raineer 44 <raineer44@lionofjudah808.live>
Subject: RE: Response Requested/Ricardo Finney Sends

Hi Ricardo,

I haven't had a chance to finish reading all of the reports that you submitted. Once I finish I will give you a call. The link to your website: <https://bit.ly/380QUe8> does not appear to be active.

Lieutenant Andrew Maddock
Honolulu Police Department
Criminal Investigations
Cyber Crimes, Digital Computer Forensics and Crime Analysis
808-723-3586

From: Raineer 44 <raineer44@lionofjudah808.live>
Sent: Wednesday, December 29, 2021 8:34 AM
To: Maddock, Andrew R. <amaddock@honolulu.gov>
Subject: Response Requested/Ricardo Finney Sends

CAUTION: Email received from an **EXTERNAL** sender. Please confirm the content is safe prior to opening attachments or links.

Aloha, Captain Maddock...

To date, I have not received the return phone call concerning my case as you promised at the conclusion of our meeting on 12/17/21. At this point nearly two weeks later I can only conclude there is no intent to call me back. The choice to do so is very disheartening, but even more so is your conclusion that the online harassment, sophisticated cyber attacks, and illegal cellphone wiretapping I've referenced is not factual but instead I am paranoid. While it is a convenient narrative to claim I am paranoid and discount all I have presented, with all due respect sir, as a police officer your assessment of my mental state cannot be qualified as certain. However, what is certain are the facts involved with my case which I have presented that, for whatever reason, are being ignored.

At the end of our meeting I provided an evidence website I had built at <https://bit.ly/380Qus8>. It shows:

- video evidence revealing my cellphone being operated remotely
- forensic evidence proving my cellphone was compromised
- audio evidence proving my voice calls were intercepted and scrambled to prevent clarity and understanding
- proof I was stalked and received cyber attacks while receiving service at the Kahala Mall Apple Store
- proof my keyboard encryption program has been compromised and rendered unsecured
- an example of a malicious file (AGCInvokerUtility.exe) installed in my computer for "backdoor" entry that disabled my computer
- proof I received (and continue to receive) Man-In-The-Middle attacks allowing my emails to be read
- proof my router was reconfigured to block my iPad from connecting

In my many police statement filed in 2021 culminating in my submission on 11/30/21, I presented visual evidence proving my PC had been accessed maliciously during its first startup with a new operating system. I provided irrefutable evidence cyber criminals breached and compromised my email account. I offered saved audio to prove my phone conversation with a Hawaii state office was illegally intercepted and scrambled. I gave contact information for a witness that validated a UPS shipment containing cyber crime evidence I sent to the Epoch Time newspaper was intercepted and stolen to prevent receipt. I provided information to trace and locate the cyber criminal who stole my shipping credentials and harassed me online by using my information to make illegal shipments in my name. These facts cannot reasonably be denied, yet all were found irrelevant.

My request to examine the USB thumb drive I submitted that triggers a scan warning and has the source of computer infection was denied. My request to visually examine a compromised PC that replicates the malicious process used to infect my other devices was denied, along with ignoring the resulting financial losses. My request to examine a laptop that upon examination revealed numerous malicious rootkits had been installed was denied.

You questioned why such an investment of time and resources would be expended to keep me offline and silent. As one of four targeted whistle blowers who were involved in exposing years of abuse of a US Army officer whose family had a presidential inquiry stifled, and whose son and brother ultimately died under mysterious circumstances, those involved in the crimes certainly want all concerned silenced. Dr. Harrell knows the circumstances with her brother intimately. She will validate what the cyber criminals want to stay hidden and vouch for why I am stalked and attacked so incessantly.

Since my visit with you I secured the services of efanicom, a firm that provides secure cell phone SIM cards for protection. For the past four days I have had an iPhone 7 in operation on the efanicom network. After making initial email and text connections to a local contact and a Mainland forensics firm seeking help, I no longer receive communication from either party. Our communication is blocked. This has happened repeatedly as I indicated in my 11/30/21 HPD statement.

My request to examine my compromised cellphone was denied. Now the criminal evidence inside that cellphone cannot be revealed. I woke up today to find that sometime during the night cyber criminals changed the passcode to enter my daily use iPhone 10/Xs on the Verizon network from a combination of seven alpha characters and digits I had set, to a requirement for six digits to be entered which I do not know, thus rendering my phone inaccessible. It is not mere coincidence that the day after I contact a forensics firm about examining my iPhone the passcode for the phone changes overnight locking me out of the device. I don't know how I'm going to restore my cell phone communication as I do not have a secure computer I can use to wipe my phone and resume using it.

You questioned why haven't those who are involved in the criminal act haven't killed me. As much as possible, the criminals want as little attention as possible focused on me. Is it not the case that were I murdered, wouldn't the first question asked by investigators be who would want me dead? My family and others know about the whistle blowing and the desire to keep all hidden. That having been said, I am more concerned for my safety now than I have been at any point during this 5+ year nightmare.

I ask that you assess the totality of the circumstances involved in my case, reconsider your position, and intervene today. It is not just me. My wife and granddaughter have been victimized too. If you will not reconsider, please advise today. I am contacting you from an encrypted email source. Please reply first with an email containing the word "Reply". Once I respond to your email our encrypted loop is closed. Then please send your decision in the second email. Thank you for your time@

Mahalo,

Ricardo Finney

Secured by [Paubox](#) - HITRUST CSF certified

Secured by [Paubox](#) - HITRUST CSF certified

Re: Please Note

Raineer 44 <raineer44@lionofjudah808.live>

Wed 5/4/2022 6:45 AM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Hello, Lt Maddock...

**No reply to my
nikon@precisionphotography.live
address through 5/12/22**

Is there a problem responding to my nikon@precisionphotography.live address? Several days have passed by with no reply. Please advise. Thank you.

Respectfully,

Ricardo Finney

From: Raineer 44

Sent: Saturday, April 30, 2022 5:48 AM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Subject: Please Note

Aloha, Lt Maddock...

I'd like to continue future communication through my SonicWall encrypted email portal. Please reply to the email I sent you from nikon@precisionphotography.live. Those emails you receive from me will first have a notification. Please click on the link provided to proceed to my message.

Mahalo,

Ricardo

Re: HPD Report 22-154047/Facebook Page

Raineer 44 <raineer44@lionofjudah808.live>

Fri 4/29/2022 11:22 AM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Aloha, Lt. Maddock...

The address for Facebook support listed in my HPD report 22-154047 narrative, abuse@facebook.com, has been replaced by disabled@fb.com. I am awaiting a reply.

Best Regards,

Ricardo Finney
Precision Photography Hawaii

From: Raineer 44

Sent: Thursday, April 28, 2022 10:32 AM

To: disabled@fb.com <disabled@fb.com>

Cc: support@gigaisland.com <support@gigaisland.com>

Subject: Support Request/Please Recover My Redirected Facebook Site

From: Ricardo A. Finney
92-1206 Hookeha Place
Kapolei, HI 96707
(808) 255-9701
<https://www.facebook.com/rickfinney142>
User email address: slaopome@gmail.com

**No reply from Facebook
I believe my email was
blocked to prevent receipt**

Aloha,

This message is from Mr. Ricardo Finney in Kapolei, Hawaii. Someone hijacked my Facebook page and replaced it with one with no content. This happened during or after I completed an update sever days ago. My authorized address is <https://www.facebook.com/rickfinney142>. The unauthorized replacment address is <https://www.facebook.com/rick.finney.142>. I did not include any dots . after www. in the authentic/original address line.

Previously the public and I could connect to my site that was populated with photos, graphics, and other content. The site with the dots in the address is barebones/no content.

Please note the illegal redirect and other details in the attached screen shot from a URL checker.

Please help me recover my authorized, original Facebook page. Please include support@gigaisland.com in your reply. Thank you for helping me.

Ciao'

Ricardo Finney

Re: HPD Report 22-154047 Referred From Officer Lamug

Raineer 44 <raineer44@lionofjudah808.live>

Fri 4/29/2022 7:11 PM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Aloha, Lt Maddock...

Thank you for responding with minimal delay. It appears what I explained about my Facebook site and other attacks wasn't clear. I've posted many details for clarity here. Please read all the content carefully. Thank you.

What you viewed at <https://www.facebook.com/rick.finney.142> is not my Facebook page/site. It not the one I designed, posted full of content, and had run online since September 2020. I attached a page from my original site. The site you see is a replacement which I did not install. It is a redirect away from my original site. My site has links to my evidence websites and other related information. The replacement site has only been online since 4/25/22. It appeared sometime overnight on 4/25/22 after I entered my original site to post an update. Cyber criminals posted it to hide my desired site. They did something during the time I was in my site updating it.

Since I built the Facebook site in September 2020, the address has always been <https://www.facebook.com/rickfinney142> with no dots past www. It functioned without dots for the past 18 months. What IPlogger.org did do is validate the address for my original site exists.

By intent whomever posted the replacement site did so purposely to have pages with zero content. The intent of the replacement site is hide the links to my evidence links and other incriminating information related to federal whistle blowing. Per your reference explaining for someone to hack my site on Facebook they would need to have control of Facebook servers, while highly unlikely it obviously is not impossible to do so. The site is changed. What appears I didn't post. All that remains are attacks on the Facebook servers.

I ask that you reconsider discounting what I have explained. Again, the bare Facebook site you see now is not the fully populated one that was in place on 4/24/22 and before. I've written Facebook asking for assistance however I suspect the email I sent has been intercepted and blocked as is the case with selected emails I send of important cyber-relevance.

Concerning the <https://www.thepostemail.com> link, I refer you back to the MP4 file titled "5 PostEmail Facebook Site Scrambled" on the thumb drive I provided. The 15-second video shows a small portion of the view I saw on my monitor and having my mouse to not response to commands. Please look at the video and you will see pages from the Post & Email Facebook site change at approximately 1-second intervals like a movie. Look at the top right to see how fast the tabs change. Watch the tab bars closely and see my cursor unable to click anywhere. Note the cursor moved in jerky motions but was unable to click anywhere while the pages were cycling. Every time I tried to click the Log In button the page would change. Ultimately, the event kept me from posting content at the site. I have had no such problems at any other website.

What I captured on video in real time was not the result of a misconfigured modem or firewall on my end. It was impossible for me to control movements at the Post & Email Facebook site while page after page after page repeated. Someone had to be controlling the rapid, repeated movement of the

Post & Email Facebook page that I captured.

To evaluate, is this another incident of Facebook server control?

My cellphone will only connect to voice mail at Ms. Rondeau (203) 987-7948 number. As I explained in the narrative in my statement, no matter what time I call day or night, whatever day of the week it is year round I am routed to her Magic Jack phone answering service. Correctly, I should get either her directly, or if she's unavailable, I should receive her phone carrier's standard voice mail greeting with the only option to leave a voice message. I have been unable to connect with her via voice for over fourteen months. Every time I leave a voice mail request for a return call, as late as last week, no voice call comes in.

I suspect my phone connection to Ms. Rondeau, who is very literate about the whistle blowing matters, is blocked. To confirm what I claim is true, please ask Det. Pait to make a two-minute voice call to Ms. Rondeau and ask if she received my voice mail messages left this month and if she sent the 5 emails to me I referenced in my 4/25 statement.

Concerning conflicts and additional software, as I've explained many before, my attempts to use VPN software has been, and continues to be defeated each time I try to go private. I used a single VPN program that always received interference and connectivity blocks. Not only that, but as I indicated in my 12/29/21 HPD report, my computer was infiltrated and a block was installed to prevent me from installing new VPN software. I've resubmitted a screen shot to prove what I claim is true.

It is not just my outbound email that I do not received replies. As detailed in my statement, the Fortinet cyber security representative validated he sent email to my nikon@precisionphotography.live address. He sent his email to me, I did not receive it, and it didn't get kicked back to him. Please also call Tyler at Fortinet who will validate his failed email to me. I have dozens of other failed email contacts, all either media or cyber security personnel. Tyler and Mrs. Rondeau will only take a few minutes to accomplish. Please call them to check my claims.

Please understand that those who stalk me online are acting at a very high level of sophistication. Blocking my VPN use is absolutely essential to stalk and track my online activites so actions I take can be overcome and inbound communication can be intercepted and blocked. Those who stalk me online have done everything outside of physical harm to prevent what has happened to me and the circumstances with the whistle blowing from being exposed. As one example, the Verizon phone log I secured from the cyber protection firm Efani reveals hundreds calls per day made in some cases a minute apart causing failed connections to not only voice and text calls I sent to Mrs. Odom and others who could help me, but caused a series of emails I tried to send from my affected iPhone to Fox News, the Epoch Times, and other reporters and news agencies to fail. Out of nearly twenty emails I sent to various sources, I did not receive a single reply.

Between being subjected to MITM attacks, redirects, IP placement on blacklists, emails with "Blast" in the beginning of the address forcing redirects, scrambled cellphone audio, connectivity blocks in my tablets, and no VPN allowed, I am unable to communicate out or in with anyone in private to coordinate help and relief from my circumstances. I have compromised computers that don't require a forensic examination to see the operating system has been modified maliciously to prevent me from printing, safely using USB thumb drives, or prevent unwanted remote access, all of which I've asked repeatedly to be examined so you can see I'm telling the truth and not imagining the incidents.

Maj Beckley told me long ago that if I provided sound evidence of intrusion after what your cyber crime division didn't resolve he would submit a formal request to the FBI to investigate my case. In addition to the video showing pages from the Post & Email Facebook site running like a cartoon while I'm connected, I have other visual proof such as my Windows Standard and Admin account active and running on the desktop at the same time while malicious activity was going on in the background. I have simultaneous http and https connections at the same website that allowed damaging unsecured script and malicious rootkits to be written to the operating system in one of my laptops. These intrusions and many others were not caused overcomplicating my environment or software conflicts. Instead, the cause of these events and others that cause me harm is facilitated by others connecting to my devices remotely and inside my network illegally.

I've detailed these and many other compromises in the HPD statements I've posted since Mar 2021.

While you consider what I have offered here, I have a request. Please send me a source to purchase a secure cellphone identical to those used by politicians, intelligence agents, etc. Thank you again for your time. I'm very grateful.

Respectfully,

Ricardo Finney
Precision Photography Hawaii

From: Maddock, Andrew R. <amaddock@honolulu.gov>
Sent: Friday, April 29, 2022 12:03 PM
To: Raineer 44 <raineer44@lionofjudah808.live>
Subject: RE: HPD Report 22-154047 Referred From Officer Lamug

Hi Ricardo,

I'm able to view your Facebook page here without any problems. Facebook has always assigned their user account using the format with a dot like <https://www.facebook.com/rick.finney.142>. If the address: <https://www.facebook.com/rickfinney142> worked for you before then Facebook was most likely creating an alias back to the site with the dots in the name. You shouldn't be putting your phone number, address or email on Facebook directly because criminals will use that information to steal your identity. Sites like IPLogger.org are not reliable and cannot be used to determine IP routing. It is normal for Facebook to route traffic through multiple servers around the world for load balancing and for someone to hack your site on Facebook they would need to have control of Facebook servers which would be highly unlikely. I'm able to access the site: <https://www.thepostemail.com> without any problems so your access problem could be due to a misconfigured modem or firewall. The site lists a phone number: 203-987-7948 which you can call to verify if they are receiving your emails. Many of your problems appear to come from over complicating your environment by having a firewall and additional software such as Anti-virus and VPN all running at the same time. These combinations can conflict with each other and cause problems. You can't just assume that a connectivity problem is a cyber-crime or when someone doesn't respond to an email that you sent. If the email is not returned to you then it was sent to the address that you entered, otherwise the server would kick it back.

Lieutenant Andrew Maddock

Honolulu Police Department
Criminal Investigations
Cyber Crimes, Digital Computer Forensics and Crime Analysis
808-723-3586

From: Raineer 44 <raineer44@lionofjudah808.live>
Sent: Friday, April 29, 2022 11:18 AM
To: Maddock, Andrew R. <amaddock@honolulu.gov>
Subject: HPD Report 22-154047 Referred From Officer Lamug

CAUTION: Email received from an **EXTERNAL** sender. Please confirm the content is safe prior to opening attachments or links.

Aloha, Lt Maddock...

I spoke this morning with Officer Lamug about my HPD report 22-154047 filed on 4/20/22. Not being technically proficient with computers, Officer Lamug agreed it was best he referred my 4/20/22 statement to you. With that said, I return to you again for resolution of HPD report 22-154047.

In addition to my prior request to identify evidence of hacking within my 3/17/22 HPD statement, I ask that you determine if these incidents detailed in report 22-154047 show hacking as well. I provided narratives and visual evidence on a thumb drive:

- My populated Facebook evidence site was redirected twice to a site with no content.
- No email received from a representative from the security firm Fortinet.com, one of 10 addressees who either verified sending emails I did not receive, or an addressee did not receive email I sent,
- Disjointed and disappearing web page content from <https://www.thepostemail.com> captured in screen shots to display.
- Video showing web pages at <https://www.thepostemail.com> flipping in rapid-fire, movie-like fashion with motion that prevented me from posting cyber crime evidence on the media site's Facebook page.
- Takedown of my recently uploaded Dropbox link whereby crime evidence content I uploaded was illegally accessed and erased, The shortened link I used was problem-free but now give an access warning.
- Email alledged from the editor of the Post & Email news site who has been in operation since 2009 but does not have a single media contact.
- Email alledged from the Post&Email editor referring an attorney who as stated successfully sued the federal government for illegal surveillance, yet operates an unsecured/http website. Doesn't pass the common sense test.

The incident with the representative from Fortinet and the editor from the Post&Email news site can be quickly and easily resolved by phone. I ask that a call be made to both individuals to see if my statements check out.

Officer Lamug mentioned he saw your notes which state you inspected two of my computers in December 2021. That did not occur. The only two computers you've inspected were done in 2016 when I asked for the operating system to be examined but the device was checked for malware and spyware. I asked in October 2021 for my compromised desktop computer to be inspected and did not receive a reply. I asked in December 2021 to have my compromised desktop computer inspected and was told no.

As I stated in October and December 2021, a visual inspection of the devices will reveal the compromises I explained occurred.

I continue to receive illegal intrusions into my business network and devices each login every day and night. My attackers have a lot of crimes to hide. That is why they so prolific. As I've noted repeatedly, as a direct result of the incessant cyber attacks, my wife and I cannot operate our computer-based businesses to generate income.

I respectfully request by close of business Thursday, May 5th, you provide your determination if my business devices or business network were hacked as I detailed in my two HPD statements. If you determine yes, please tell me what action(s) you will take to stop the cyber crimes so we are no longer victimized, and when. If you find nothing, please explain why.

Please reply with confirmation you received this email. Thank you for your time. I appreciate it.

Mahalo,

Ricardo Finney
Precision Photography Hawaii



Secured by [Paubox](#) - HITRUST CSF certified

Re: Request For Your Reply/Re HPD Case 22-154047

Raineer 44 <raineer44@lionofjudah808.live>

Thu 4/28/2022 1:51 PM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Aloha, Lt Maddock...

Please reply to my request as detailed in the attached message sent this past Monday. Thank you for your time.

Respectfully,

Ricardo

From: Raineer 44

Sent: Monday, April 25, 2022 5:25 AM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Subject: Request For Your Reply/Re HPD Case 22-154047

Aloha, Lt Maddock...

On 4/22/22 I submitted a HPD statement under cyber crimes that is assigned report number 22-154047. Among other incidents detailed in the report, I provided a screen shot proving a Facebook site which displayed crime evidence I uploaded had been replaced with one with no content and a different, redirected website address. An abuse report I sent to Facebook remains unanswered as do 10 other addresses I contacted in the past three weeks..

I contacted one of the 10 intended recipients by phone who confirmed he sent emails to my address. I received nothing.

A site with crime evidence I uploaded to <https://bit.ly/383CRJU> and verified to be active was taken down and replaced with access warning from bitly.com.

I included visual evidence on a thumb drive showing Facebook pages for the Post&Email news site rapidly changing in a movie-like fashion after I landed on it. This action which I could not possibly have initiated would have prevented me from posting cyber crime evidence to the Facebook site.

In my report I detailed six more incidents I attribute to cyber attacks. Do you consider any of the events I explained to be caused by hacking or do you consider them normal computer issues?

Respectfully,

Ricardo

Re: 3/17/22 HPD Statement

Raineer 44 <raineer44@lionofjudah808.live>

Wed 3/23/2022 7:53 AM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Aloha, Lt. Maddock...

I did not receive your reply verifying you received the details I sent in support of my HPD statement submitted on 3/17/22. Since then I discovered cyber criminals have hacked my business email again blocking correspondence essential for me to make a living. I attached evidence my business email address bounces. This has been done repeatedly. Each time I get my business email operational it is hacked and disabled again.

Most recently, my Wi-Fi has been hacked resulting in no connectivity to seven devices previously linked to one home office and three personal networks. I am working with my network engineers who after extensive investigation cannot determine so far why the channels that should be working suddenly aren't.

In my 3/17/22 report the cell phone logs I presented proved hundreds of calls occurred minutes apart all day for several weeks, none of which I made while calls I made to Ms. Odom would not connect. I presented proof calls I made before and after I failed to reach Ms. Odom were successful. I provided an example proving my cellphone made an unsecured connection and secured connection at the same time at a website.

In my statement I referred a 9th incident whereby my VPN was hacked with my claim supported by witness verification. Also I submitted proof my laptop computer was illegally accessed to block four VPN software applications from being installed.

I provided visual proof the printer function in my desktop computer was hacked and disabled. I added that my Windows firewall settings has been hacked to bypass the required password freely allowing malicious inbound connections. Both these events are readily evident upon visual inspection.

I am progressively being cut off from cell phone and Internet connectivity by cyber criminals. I urgently need law enforcement intervention now so the cyber attacks against me will stop and I can recover and resume business operations.

Are you going to investigate these cyber crimes reported in my 3/17/21 HPD statement or not? If not, why not? Thank you for advising.

Respectfully,

No reply received

Ricardo Finney

Precision Photography Hawaii LLC

From: Maurice Soque <msoque@dialogix.net>

Sent: Tuesday, March 22, 2022 8:40 AM

To: Raineer 44 <raineer44@lionofjudah808.live>

Subject: Fwd: Delivery Status Notification (Delay)

----- Forwarded Message -----

Subject: Delivery Status Notification (Delay)

Date: Sun, 20 Mar 2022 14:50:57 -0700 (PDT)

From: Mail Delivery Subsystem <mailer-daemon@googlemail.com>

To: msoque@dialogix.net



Delivery incomplete

There was a temporary problem delivering your message to **ricardo@precision.photography**. Gmail will retry for 21 more hours. You'll be notified if the delivery fails permanently.

The response was:

DNS Error: DNS type 'mx' lookup of precision.photography responded with code NOERROR
DNS type 'aaaa' lookup of precision.photography.snwlhosted.com. responded with code NXDOMAIN
DNS type 'a' lookup of precision.photography.snwlhosted.com. responded with code NXDOMAIN

This is my inoperable commercial photography business email address repeatedly compromised by the Army cyber criminals. It remains unusable.

Re: New HPD Report #21-151824/Ricardo Finney

Raineer 44 <raineer44@lionofjudah808.live>

Thu 3/17/2022 3:03 PM

To: Maddock, Andrew R. <amaddock@honolulu.gov>

Aloha, Lt. Maddock

My Verizon cell phone log with more than 300 calls spaced a minute or seconds apart was deemed normal. Texts, calls, emails and a fax I sent failed.

I continue to be harassed and stalked through hourly cyber attacks that disable my software and hardware. I delivered hard copies of the attached HPD report and attachments to the Kapolei Station at 1310 today. I attached a merged Adobe Acrobat .pdf to this email containing the entire report and 10 attachments.

Attachment 1-5 are screen shots with the dates, times and details revealing calls, texts, and voice mail messages I attempted to send to Ms. Anna Odom failed. Calls, texts, and voice mails I sent to other parties before and after my attempts to reach Ms. Odom were successful. As I indicated in my last HPD report, my communication with Ms. Odom was blocked to prevent our interaction and resulting criminal disclosures.

Attachment 6 is an Excel cell phone log for my cell phone received from Verizon. The Excel file reveals over 300 calls flooding my network which I did not dial made minutes apart day and night for over a month. Selected calls I made did not connect nor did I receive replies to emails sent from my phone. My HPD report only has the first page of the phone log. I was unable to print the entire phone log after my computer's printer function was disabled. I attached an email and the original phone log I received from my phone network host.

Attachments 7 validates cyber criminals attacked and disabled my VPN programs again to prevent me from logging on privately and not being stalked.

Attachment 8 validates my computer was illegally accessed and reconfigured to block VPN software from being installed.

Attachment 9 shows the operating system in my computer has been changed so a password is not required to unblock the Windows firewall. This is how my other computers reported in prior HPD reports have been illegally accessed and their operating systems and proprietary and third-party software programs has been damaged or disabled. I captured a 21-second video that shows evidence of the intrusion.

Attachment 10 shows the software installed to operate my Brother LaserJet printer has been hacked causing the printer to be disabled in an attempt to prevent me from printing crime evidence.

Attachment 11 shows a portion of recent expenses I've been forced to incur as a direct result of the cyber attacks. The funding in the form of a 4th cash-out home refinancing cycle is necessary to stay financially solvent and to try to reinstate my three computer-based small businesses.

I am unable to earn a living because of the because of the incessant harrassment, surveillance, and hacking. Each time I get my equipment repaired the devices are attacked and compromised. I cannot communicate with certain persons and agencies because I am stalked online, my VPN's are

repeatedly blocked, and because seen through Man-In-The-Middle and other cyber attacks, my communication is followed and canceled by the malicious third parties who stalk me online around the clock.

Please investigate the events detailed in this report. Please protect me from further criminal acts so I can communicate across the Internet without being subjected to criminal stalking stalked or interfered with.

I continue to have critical emails blocked or bounce. Please confirm you received this email and the attachments in legible order. I await your reply. Thank you for your valuable time@

Best Regards,

Ricardo Finney
Precision Photography Hawaii, LLC

From: Efani <support@efanimobile.zohodesk.com>
Sent: Wednesday, February 23, 2022 12:56 PM
To: Raineer 44 <raineer44@lionofjudah808.live>
Subject: Re:[## 1881 ##] Additional Information

Ricardo,

I've attached the call logs below

Please let me know if you need anything else

---- On Tue, 22 Feb 2022 16:07:17 -0500 "Raineer 44"<raineer44@lionofjudah808.live> wrote ----

Aloha,

I'm going to file a report with law enforcement about the blocked number I receive. Please ask Verizon to send a copy of the cellphone logs for the dates listed in my submission to my email address. Thank you for helping me. This will be of immense help. Thanks again@

Ciao'

Ricardo

From: Efani <support@efanimobile.zohodesk.com>
Sent: Tuesday, February 22, 2022 4:45 AM
To: Raineer 44 <raineer44@lionofjudah808.live>
Subject: Re:[## 1881 ##] Additional Information

Ricardo,

Nothing is appearing on their logs as well but we've reprovisioned the line. Please turn the phone off and on and try again.

---- On Mon, 21 Feb 2022 18:15:35 -0500 "Raineer 44"<raineer44@lionofjudah808.live> wrote ----

Hi, Will...

Thanks for your reply. I understood you have an interface with the carrier Verizon. Please check with them to see what their logs reveal about the phone number in question. Something is blocking my access to that specific phone number while others connect.

Many Thanks,

Ricardo

From: Efani <support@efanimobile.zohodesk.com>
Sent: Monday, February 21, 2022 6:54 AM
To: Raineer 44 <raineer44@lionofjudah808.live>
Cc: support@efani.com <support@efani.com>
Subject: Re:[## 1881 ##] Additional Information

Hi Ricardo,

As stated previously, everything on our end looks fine. I see that the account is active with no blocks on the account.

If the service isn't working for you we can do a few things;

1. We can try switching you to our AT&T service or
2. We can move you off of the service onto the carrier of your choice

Please let me know how you'd like to proceed

Best,

Will Rose
Customer Service Manager
---- On Mon, 21 Feb 2022 01:57:06 -0500 "Raineer 44" <raineer44@lionofjudah808.live>
wrote ----

Hi,

Please confirm you received my two emails sent at 10:45 a.m. and 12:41 p.m. on 2/20/22.

Many Thanks,

Ricardo

From: Raineer 44
Sent: Sunday, February 20, 2022 10:41 AM
To: support@efanimobile.zohodesk.com <support@efanimobile.zohodesk.com>
Subject: Additional Information

Aloha,

Using my iPhone with the number (808) 688-4897, I began phone communication to (808) 824-9725 from 12/22/21 through 1/29/22. Connectivity stopped on 1/29/22. I attached additional information about this problem.

Please investigate and advise if the calls in question are being blocked from connecting.

Standing by for your assessment in coordination with the carrier. Thank you@

Best Regards,

Ricard



Secured by [Paubox](#) - HITRUST CSF certified



Secured by [Paubox](#) - HITRUST CSF certified



Secured by [Paubox](#) - HITRUST CSF certified

RE: Response Requested/Ricardo Finney Sends

Maddock, Andrew R. <amaddock@honolulu.gov>

Mon 1/3/2022 8:31 AM

To: Raineer 44 <raineer44@lionofjudah808.live>

1 attachments (965 KB)

21-504872.docx

This message's attachments contains at least one web link. This is often used for phishing attempts. Please only interact with this attachment if you know its source and that the content is safe. If in doubt, confirm the legitimacy with the sender by phone.

Hi Ricardo,

I have reviewed the material in your reports and on your website. I still do not see any sign of actual hacking. The things that you are reporting appear to be normal computer issues or spoofing by scam callers. I have outlined a few of these in the attached Word document.

Lieutenant Andrew Maddock
Honolulu Police Department
Criminal Investigations
Cyber Crimes, Digital Computer Forensics and Crime Analysis
808-723-3586

From: Raineer 44 <raineer44@lionofjudah808.live>
Sent: Wednesday, December 29, 2021 4:39 PM
To: Maddock, Andrew R. <amaddock@honolulu.gov>
Subject: Re: Response Requested/Ricardo Finney Sends

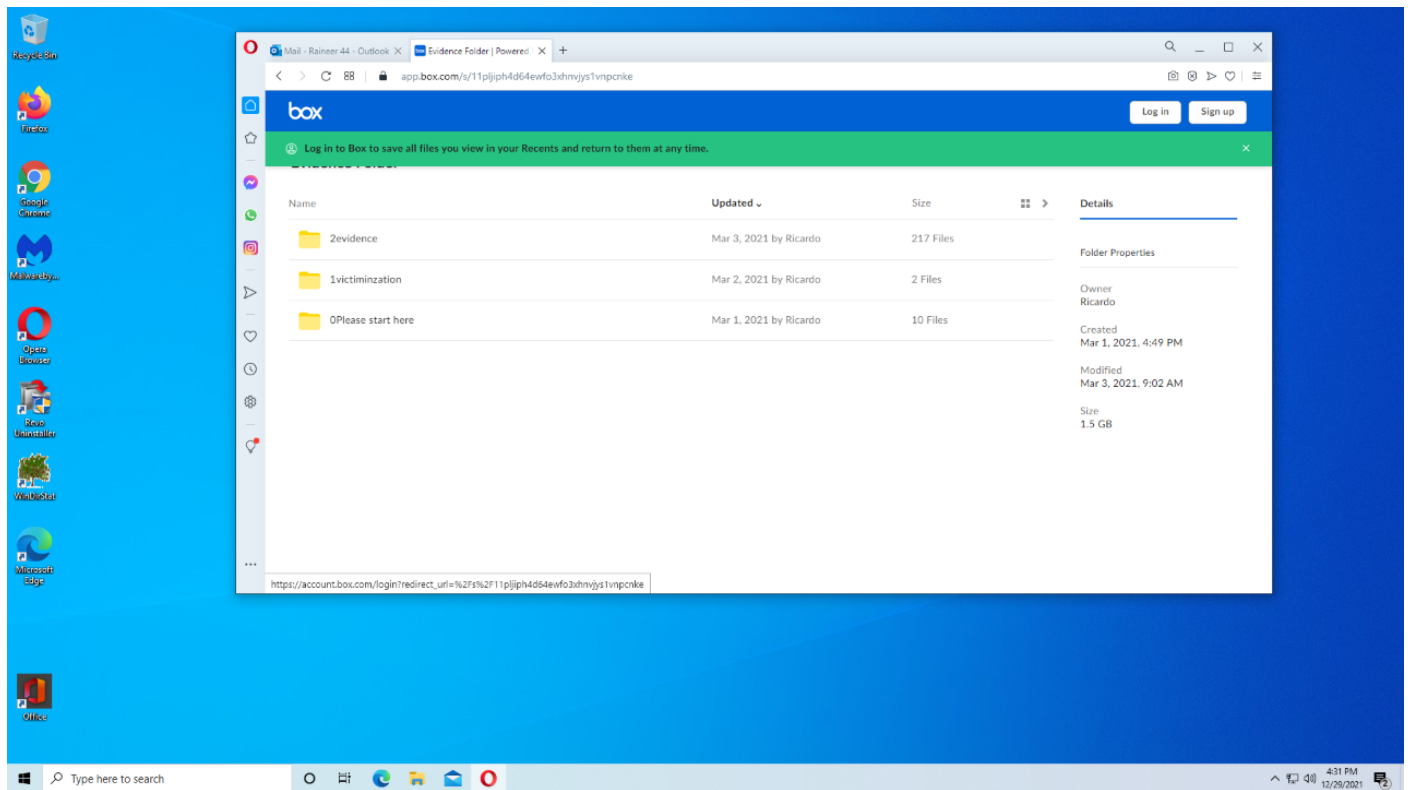
CAUTION: Email received from an **EXTERNAL** sender. Please confirm the content is safe prior to opening attachments or links.

Aloha, Lt. Maddock...

Thank you for replying. Their appears to be a mistake with the link name. The site is active.

<https://bit.ly/380Qug8>

I will be off-island from 1/06/22 - 1/20/22 attending my granddaughter's christening and birthday.



From: Maddock, Andrew R. <amaddock@honolulu.gov>
Sent: Wednesday, December 29, 2021 1:47 PM
To: Raineer 44 <raineer44@lionofjudah808.live>
Subject: RE: Response Requested/Ricardo Finney Sends

Hi Ricardo,

I haven't had a chance to finish reading all of the reports that you submitted. Once I finish I will give you a call. The link to your website: <https://bit.ly/380Qug8> does not appear to be active.

Lieutenant Andrew Maddock
Honolulu Police Department
Criminal Investigations
Cyber Crimes, Digital Computer Forensics and Crime Analysis
808-723-3586

From: Raineer 44 <raineer44@lionofjudah808.live>
Sent: Wednesday, December 29, 2021 8:34 AM
To: Maddock, Andrew R. <amaddock@honolulu.gov>
Subject: Response Requested/Ricardo Finney Sends

CAUTION: Email received from an **EXTERNAL** sender. Please confirm the content is safe prior to opening attachments or links.

Aloha, Captain Maddock...

To date, I have not received the return phone call concerning my case as you promised at the conclusion of our meeting on 12/17/21. At this point nearly two weeks later I can only conclude there is no intent to call me back. The choice to do so is very disheartening, but even more so is your conclusion that the online harassment, sophisticated cyber attacks, and illegal cellphone wiretapping I've referenced is not factual but instead I am paranoid. While it is a convenient narrative to claim I am paranoid and discount all I have presented, with all due respect sir, as a police officer your assessment of my mental state cannot be qualified as certain. However, what is certain are the facts involved with my case which I have presented that, for whatever reason, are being ignored.

At the end of our meeting I provided an evidence website I had built at <https://bit.ly/380Qug8>. It shows:

- video evidence revealing my cellphone being operated remotely
- forensic evidence proving my cellphone was compromised
- audio evidence proving my voice calls were intercepted and scrambled to prevent clarity and understanding
- proof I was stalked and received cyber attacks while receiving service at the Kahala Mall Apple Store
- proof my keyboard encryption program has been compromised and rendered unsecured
- an example of a malicious file (AGCInvokerUtility.exe) installed in my computer for "backdoor" entry that disabled my computer
- proof I received (and continue to receive) Man-In-The-Middle attacks allowing my emails to be read
- proof my router was reconfigured to block my iPad from connecting

In my many police statement filed in 2021 culminating in my submission on 11/30/21, I provided visual evidence proving my PC had been accessed maliciously during its first startup with a new operating system. I provided irrefutable evidence cyber criminals breached and compromised my email account. I offered saved audio to prove my phone conversation with a Hawaii state office was illegally intercepted and scrambled. I gave contact information for a witness that validated a UPS shipment containing cyber crime evidence I sent to the Epoch Time newspaper was intercepted and stolen to prevent receipt. I provided information to trace and locate the cyber criminal who stole my shipping credentials and harassed me online by using my information to make illegal shipments in my name. These facts cannot reasonably be denied, yet all were found irrelevant.

My request to examine the USB thumb drive I submitted that triggers a scan warning and has the source of computer infection was denied. My request to visually examine a compromised PC that replicates the malicious process used to infect my other devices was denied, along with ignoring the resulting financial losses. My request to examine a laptop that upon examination revealed numerous malicious rootkits had been installed was denied.

You questioned why such an investment of time and resources would be expended to keep me offline and silent. As one of four targeted whistle blowers who were involved in exposing years of abuse of a US Army officer whose family had a presidential inquiry stifled, and whose son and brother ultimately died under mysterious circumstances, those involved in the crimes certainly want all concerned silenced. Dr. Harrell knows the circumstances with her brother intimately. She will validate what the cyber criminals want to stay hidden and vouch for why I am stalked and attacked so incessantly.

Since my visit with you I secured the services of efani.com, a firm that provides secure cell phone SIM cards for protection. For the past four days I have had an iPhone 7 in operation on the efani.com network. After making initial email and text connections to a local contact and a Mainland forensics firm seeking help, I no longer receive communication from either party. Our communication is blocked. This has happened repeatedly as I indicated in my 11/30/21 HPD statement.

My request to examine my compromised cellphone was denied. Now the criminal evidence inside that cellphone cannot be revealed. I woke up today to find that sometime during the night cyber criminals changed the passcode to enter my daily use iPhone 10/Xs on the Verizon network from a combination of seven alpha characters and digits I had set, to a requirement for six digits to be entered which I do not know, thus rendering my phone inaccessible. It is not mere coincidence that the day after I contact a forensics firm about examining my iPhone the passcode for the phone changes overnight locking me out of the device. I don't know how I'm going to restore my cell phone communication as I do not have a secure computer I can use to wipe my phone and resume using it.

You questioned why haven't those who are involved in the criminal act haven't killed me. As much as possible, the criminals want as little attention as possible focused on me. Is it not the case that were I murdered, wouldn't the first question asked by investigators be who would want me dead? My family and others know about the whistle blowing and the desire to keep all hidden. That having been said, I am more concerned for my safety now than I have been at any point during this 5+ year nightmare.

I ask that you assess the totality of the circumstances involved in my case, reconsider your position, and intervene today. It is not just me. My wife and granddaughter have been victimized too. If you will not reconsider, please advise today. I am contacting you from an encrypted email source. Please reply first with an email containing the word "Reply". Once I respond to your email our encrypted loop is closed. Then please send your decision in the second email. Thank you for your time@

Mahalo,

Ricardo Finney

Secured by [Paubox](#) - HITRUST CSF certified

Secured by [Paubox](#) - HITRUST CSF certified

Response Requested/Ricardo Finney Sends

Type here to search



From: Maddock, Andrew R. <amaddock@honolulu.gov>
Sent: Wednesday, December 29, 2021 1:47 PM
To: Raineer 44 <raineer44@lionofjudah808.live>
Subject: RE: Response Requested/Ricardo Finney Sends

Hi Ricardo,

I haven't had a chance to finish reading all of the reports that you submitted. Once I finish I will give you a call. The link to your website: <https://bit.ly/380Qug8> does not appear to be active.

Lieutenant Andrew Maddock
Honolulu Police Department
Criminal Investigations
Cyber Crimes, Digital Computer Forensics and Crime Analysis
808-723-3586

From: Raineer 44 <raineer44@lionofjudah808.live>
Sent: Wednesday, December 29, 2021 8:34 AM
To: Maddock, Andrew R. <amaddock@honolulu.gov>
Subject: Response Requested/Ricardo Finney Sends

CAUTION: Email received from an **EXTERNAL** sender. Please confirm the content is safe prior to opening attachments or links.

Aloha, Captain Maddock...

To date, I have not received the return phone call concerning my case as you promised at the conclusion of our meeting on 12/17/21. At this point nearly two weeks later I can only conclude there is no intent to call me back. The choice to do so is very disheartening, but even more so is your conclusion that the online harrasment, sophisticated cyber attacks, and illegal cellphone wiretapping I've referenced is not factual but instead I am paranoid. While it is a convenient narrative to claim I am paranoid and discount all I have presented, with all due respect sir, as a police officer your assessment of my mental state cannot be qualified as certain. However, what is certain are the facts involved with my case which I have presented that, for whatever reason, are being ignored.

At the end of our meeting I provided an evidence website I had built at <https://bit.ly/380Qug8>. It shows:

- video evidence revealing my cellphone being operated remotely
- forensic evidence proving my cellphone was compromised
- audio evidence proving my voice calls were intercepted and scrambled to prevent clarity and understanding
- proof I was stalked and received cyber attacks while receiving service at the Kahala Mall Apple Store
- proof my keyboard encryption program has been compromised and rendered unsecured
- an example of a malicious file (AGCInvokerUtility.exe) installed in my computer for "backdoor" entry that disabled my computer