From: Annon1204
To: conjkhyas@icloud.com
Subject: Re: Hand
Date: Friday, September 7, 2018 6:02:18 PM
Attachments: Schulte_Handwritten_Notes.pdf

Yo you there? Do you want to send me the Russia pieces to email the reporter

Sent from ProtonMail mobile

-------- Original Message --------
On Sep 1, 2018, 10:45 PM, Conj Khyas < conjkhyas@icloud.com> wrote:

> Sent from my iPhone

GOVERNMENT
EXHIBIT
1303-17
S2 17 Cr. 548 (PAC)

79471-ø54

Declaration

Pg. 1

Expert Report 1/29/2018

I am the founder and CEO of my own consulting firm. I was contacted and hired directly by Omar Amanat to provide an expert report in the matter of United States v. Kaleil Isaza Tuzman, et al. 15 Cr. 536 (PGG). I was retained post-verdict on 1/19/18 due to concerns of irresponsible and malicious behavior on behalf of the FBI. Particularly, the expert testimony of Joel DeCapua. I am familiar with the facts in this declaration, from either personal knowledge or from documents that have been provided to me. Insofar as they are within my own knowledge, the facts and matters in this ~~decision~~ declaration are true to the best of my knowledge and belief. I personally examined all the evidence and transcripts myself. ~~The analysis of the evidence~~

My background is in software development and computer engineering. I received my B.S. in electrical engineering from the University of Texas at Austin. I've worked for IBM as a system administrator and at the National Security Agency (NSA) as a systems engineer. I then worked for the Central Intelligence Agency (CIA) as a Technical Intelligence Officer (TIO); for 7 years I worked as a software engineer within the CIA's Engineering Development Group (EDG) where I architected, designed, and developed malware targeting numerous adversaries across the world. Primarily, I worked on Quick Reactions Capabilities (QRCs)

Pg 2

in coordination with the Counter Terrorism Center (CTC) against High-Value Targets (HVTs). My programming expertise includes C, C++, C#, java as well as scripting languages such as python, perl, expect, bash, etc. I've developed covert filesystems and thus obtained an expertise in computer forensics across most major operating systems and filesystems. I also have expertise in network engineering and development including the development of many proprietary communication protocols as well as custom implementations and familiarity with many mainstream communication protocols as a means to probe for vulnerabilities in design and each specific implementation itself. ~~Since everyone~~ In addition to the development and networking expertise, I also possess an expertise in reverse engineering of both criminal and State-sponsored malware. As part of a yearly training program, I've taken numerous SANS courses, most recently in reverse engineering, as well as attended many major conferences including the yearly blackhat/DEFCON. I have a few certifications from various vendors including Cisco's CCNA CCNA routing and switching, and CCNA Security. Finally, I possess an expertise in intrusion detection systems and every major Antivirus (AV) product and vendor in the world.

Pg 3

II. Concerns with FBI as expert witnesses

Although I've had an illustrious engineering career, I'm new to consulting and expert testimony. Quite frankly, most engineers do not gravitate towards the legal system because it involves no engineering — no creation of new programs that gives us such euphoria, and legal work is incredibly boring. However, I began work consulting in the legal system after my involvement in another case where an FBI agent pretended to be a technical expert and gave fabricated and technologically false testimony that inevitably resulted in the loss of liberty to an innocent individual. The federal prosecutor lauded my expertise and made the following statements about me

" Find & insert statements here "

So, on that note, I was given Omar's transcript and read the expert testimony of a Joel DeCapua. Initially, I thought his testimony was a joke and I laughed as I read through his "expert" opinion — but it was not a joke. I was horrified to learn that this unqualified individual was permitted to spread disinformation and fallacious arguments regarding technology, unchallenged, in the court of law. And so, I am here to set the record straight. However, I would first like to present this letter to the courts regarding my concern with FBI expert witness testimony;

Pg 4

I have worked with the FBI throughout my CIA career. We were frequently consulted and contracted to develop their software tools, and I always considered them amateur technical people at best— Even their elite "Cyber" unit rarely included engineers or technical people. In fact, up until recently the FBI has been reluctant to adapt with new technology. Today, the FBI has shifted towards "pseudo expertise" in which they embrace tech but manipulate and extort it for their own purposes. The FBI learn just enough to become dangerous. Literally, the FBI's ignorance of technology has cost civil liberty for innocent people as they spread disinformation as 'expertise'. We are facing a stealth constitutional crisis — a malware of the mind has entered and corrupted the justice system. Technology has advanced so rapidly that the law and law enforcement are 5-10 years behind and are unable to catch up. Into this chasm, defendant, defense lawyers, judges, and juries are increasingly blindsided by the evolution of innovative prosecutorial techniques based on faux forensics which are in turn nothing more than longshot theory and in some cases blatant fabrications analogous to accusations of ~~wizar~~ witchcraft. It is incredibly easy to google concepts and feign expertise to judges, who themselves, know nothing of technology. It is common in the FBI for an agent to enroll in a rudimentary 2-week class on a ~~subj~~ topic and then be labeled the resident subject matter expert (SME) on that topic.

pg.5 The only thing more alarming about DeCapua's testimony is the fact that he is somehow considered a top 'cyber' expert within the FBI. The FBI are incapable of testifying in a court of law as any expert because of the clear bias — you would never permit a defendant to testify as an expert on his own case due to the obvious conflict-of-interest, but somehow it's okay for the FBI? The FBI, who are never impartial, who never tackle an issue as a real scientist observing the scientific method — Research, proposed hypothesis, then tests of that hypothesis that result in a conclusion & advance the respective field. The FBI, on the other hand, write the conclusion first and then seek to manipulate, omit, and cherrypick data that matches their conclusion; they then call this science & claim expertise. This could not be further from the truth. Thus, the legal system must set a precedent and ban all FBI agents from testifying as any sort of expert witness - Force the government to consult an unbiased third party just as the defense. There are now at least two innocent men sitting in prison due to FBI malfesence and the court's failure to recognize this bias. The FBI will do anything and everything to secure a conviction and prison sentence regardless of the facts of the case.

Pg. 6

III Email 1: GX 3553, GX 3549

Let's take a look at the first alleged fabricated email. It's an email chain between the defendant and multiple individuals. DeCapua Speculates that the email from Kaleil Isaza Tuzman on Friday, May 8, 2009 at 5:21 PM is fradulent due to

1.) "Facial abnormalities" including inconsistent "greater than" signs.
2.) Date times within the email appear inconsistent as later emails indicate times sent as before previous emails
3.) Inability to find this email from Tuzman in other recipient's email
4.) Inconsistent message ID in this email with other emails

As I look at GX3549 and the raw email in totality I see nothing alarming or immediately indicative of a forged email. I address each of the agent's concerns below

1.) "Facial abnormalities" — People often look for patterns, but here the psychological and evolutionary need for explanation and relevancy falls short as we find an imperfect, diverse System without symmetry. From my experience, what I see here is ordered chaos that is consistent within the email realm. The internet and email are old and archaic — The RFCs that govern email in particular were never ~~guaranteed~~ intended to guarantee consistency or authenticity to email. For that, you need something like RSA keys and ~~signatures~~ email signing, hashing, etc. But email on its own, was never intended to be introduced in the court of law or stand up to rigorous tests for authenticity. Email was designed to provide virtual communication.

Pg. 7

The differing email clients, providers, and various implementations and GUI designs are just that — incredibly diverse. The 'greater than' sign is a non-issue that can be explained by numerous possibilities including the most likely — That a different email client was used to send this email. Direct user intervention either accidental or purposeful is also possible.; I often times will directly alter replied/forwarded messages to provide a more readible format or concise information. Furthermore, the inconsistent 'greater than' signs actually persist following the 5:21 pm email so are all those emails fake too?

2.) Date-time issue — These people are actually communicating across multiple time zones from the east coast, west coast, and Dubai (according to the transcripts). These time differences will certainly explain the perceived time discrepencies — Note that the time discrepencies aren't from the actual emails but are actually in the body of the email where each client inserts the local time in the response. I would expect these discrepencies to exist and they are consistent with emailing across time zones. Moreover, this time 'issue' exists throughout the email chain not just in the 5:21PM email, which again, is expected. For instance, the first email is claimed to have been ~~sent~~ received at 5/8/09 at 1:33 PM (by Kamal's client, in his local time) and then Kamal responds at 5/8/09 at 10:53 AM (by the next client and so on). Then 7:47PM, 1PM, etc. Clearly, we are seeing people in different time zones. To actually view the real times the emails were sent, you would just have to look at each

Pg. 8

individual email and view the email's received time all relative to a single email client. If you find this all confusing, yes, the Court debates it from 4013-4016 and 4392-4402. I can say from experience that many CIA ~~oper~~ technical operations have failed due to some date, time, or time zone issue. Needless to say, this perceived issue with the email is also refuted.

3.) Inability to find Tuzman email in other recipient accounts – Of the four, this is the only potentially interesting issue. That is, until you realize both other recipients had missing emails during this time – According to Movant exhibit 1B, Kaleil claims on May 9, 09 that his blackberry device wiped emails of several weeks and he attempts to have another individual forward him his own emails. His 5/8 10:21 PM was also amongst the missing emails. Also, on page 6641 its mentioned that Maiden had missing emails between 1/30 to 3/10 of 2009. Finally, all recipients acknowledge that the content of the email was accurate. The final two recipients on the email chain did in fact receive the email in a forward and maintain the email on their accounts according to the defense. And so, I also reject this perceived issue.

GX 3556 4.) Inconsistent Message ID – This differing message ID for Kaleil's 5/8/09 5:21 PM email actually seems to validate my speculation mentioned on issue 1, that Kaleil used a different client to send this email. Each email client generates their own message ID format and so this different message ID indicates that he most likely used a different email client to send it – and thus this explains both

Pg. 9 the different message ID here in issue 4 and the "facial abnormalities" described in issue 1. Also, I'd argue that if someone were to fake an email from Khaleil then they would most likely ~~use~~ re-use one of his legitamite emails as a template which contain the 'MIBNYCMAIL' format. This, of course, is just speculation based on what I would view as a logical step in the email fabrication process. As someone who has spoofed many emails myself, any and all information gleaned from the target account is the most critical step — you don't want discrepencies. Regardless, I find the use of a different email client the most likely scenario, and thus, issue 4 also refuted.

In summary, I find no evidence at all exists to even suggest that the 5:21PM email is fradulent. My professional opinion is that the email is most likely authentic. I concur with Omar's first expert ~~testimony~~ witness, Modesitt, in his testimony that the email is not fradulent.

IV Decapua demo

DeCapua presents a ~~demo~~ 'technical' demo to the judge and later the jury that amounts to a demo of how to backup and restore emails. I think most people understand the basics of backing up & restoring data so the only 'new' thing here is how it relates to email. In the demo, DeCapua uses Apple Mail and clicks ~~mailbox-export' to~~ ' mailbox--export mailbox" to export his mail to disk then modifies an email and after deleting the originals from yahoo he clicks ~~'file-import' and~~ 'file-import mailbox' and selects the modified mailbox. The emails then appear on yahoo as if they were originals. It was a very simple demo that showed a time-consuming, but simple concept. Personally, I have never seen anything similar to this demo because I have never needed to restore any emails. Also, exploiting something like this is absurd because it doesn't actually accomplish anything to spoof an email to yourself.

Anyway, DeCapua presents no evidence that this is what the defendant did to 'fake' the email that we've already ruled is authentic. DeCapua presents this demo to the Court and speculated the defendant performed the same steps despite no empirical evidence to make such a ~~suggesti~~ hold suggestion. He even suggests that the email would appear exactly ~~like~~ like any real email and thus fradulent emails would be indistinguishable from authentic emails. Essentially, he argues all emails in the world are conceivably fradulent. Now, again, email was never created with a purpose of authenticity. Email & its associated RFCs are designed with the sole functionality of sending and receiving virtual communication. So, the existence of a method for uploading emails to an email ~~Server~~ provider doesn't prove the defendant did anything. That being said, I would personally be shocked to learn that yahoo or ~~another~~ any other email provider would allow a user to upload emails to their server. This seems like an irresponsible feature that never should have been implemented due to many security issues — not really this authenticity issue. But, assuming it does exist — I haven't tried to reproduce the demo and results myself — I would again be shocked if the email provider doesn't somehow flag these emails as foreign or imported. Therefore, I reject DeCapua's statements from page 397-2: When asked what a search warrant would show, DeCapua states matter-of-factly that it would show the altered emails. He never conducted this experiment nor has any evidence to support it but blindly believes it regardless. I find this incredibly irresponsible and I reject his speculation. DeCapua should have at least stated that he would "guess without any evidence that the fake emails would be returned in a search warrant exactly as if they were real." I can make no assessment until his experiment is repeated and the results verified by a real search warrant and comparison of the emails (which only the FBI can do). Based on my expertise, I would speculate that some flag would indicate the emails were foreign. The existence of such a flag would make the government's entire argument moot as the alleged falsified emails clearly contained no such flag. Thus, this is another astounding example of how the FBI and government are biased and incapable of following the scientific method. Fearful of discovering that their hypothesis is false (which is all the experiment could show) and that fraudulent emails ARE somehow differentiated, they did not even ATTEMPT the experiment. Instead, they lazily and unethically just ASSUMED the results matched what they wanted. Incredible. As an engineer, as a scientist, and as a human being I am insulted. The government recklessly touts an incomplete theory to accuse a man of a crime and threaten his liberty. How difficult is it to fully test only a test that you can perform and report your findings? So, with no evidence and no attempts at validation, the government poses an incomplete theory as absolute fact.

Luckily, the court initially rejected DeCapua testimony as pure testimony since he could not definitively state whether the emails were faked. For reference, DeCapua's initial, closed-court testimony was given on 12/5/17 on pages 3933-4031. The defense's expert, Claude Modessit testified to the judge on 12/6 on pages 4371-4416.

Then, on the eve of summation, the prosecutor claimed to have a breaktrough and that DeCapua could testify that three different emails were definitely fake. The three emails had nothing to do with the subject matter of the case—wire fraud, and the content of all three emails were recalled as accurate. In fact the three emails were all final emails in threads and were emails sent from Omar — something unusual to fake.

V Argument from Logic

Prior to discussing the technical arguments from the three emails that DeCapua claimed were falsified I think it's pertinent to look at the non-technical logical issues involved. In addition to my engineering and computer expertise I also have an expertise in basic logic— from the mathematics in discrete math and number theory to the digital logic in computing and broader philosophical discussions. Basically, I see the issue of "fake" emails in this case as the following parallel:

Investigaters see what they assume is a dead body. They search for the murder weapon and begin a vigorous and contentious debate about whether it's the knife or scissors found at the scene. Which is it?! Meanwhile, unbeknownst to anyone, the sleeping 'victim' wakes up and leaves for work.

Let's fully understand what is going on here. The FBI and AUSA are claiming that the defendant directly fabricated entire emails, 3 at least, in which the content of each email was not only entirely innocuous, but furthermore, entirely accurate information that each and every recipient of the email recalls without question. One of the recipients even recognized one of the allegedly fake emails as legitamite in court. OK... Not only that, but the emails have nothing at all to do with the alleged wire fraud that this entire case is based on! Not only THAT, but each of the three emails were final emails in their respective

Pg. 14

email chains, so, the alleged fraudulent emails ~~existed~~ would have existed in only one place- the defendant's Sent box. DOH!
Another parallel:

I call my Grandma to tell her I will be in town for lunch next week. I then, secretly and deceptively, create a fake email in which she is the sole recipient where I copy verbatim what was said over the phone. I then upload the fake email to my Sent box and wait patiently for any inevitable FBI investigation. Once the FBI begin some random, unrelated investigation they will find my fake email to my Grandma and I will have successfully trolled them! Muhahaha!

Step 1: Create fake email regarding real life events and upload to my Sent box and wait patiently...
Step 2: ???
Step 3: Profit!!

It's so absurd. Whether or not 3 random, innocuous emails which were never used as evidence for or against the ~~client~~ defendant in any way whatsoever are fake or not is entirely irrelevant.

Furthermore, is it even illegal for me to create fake emails and upload them to my own email? Maybe I did this for fun or some scholastic purpose before I was ever accused of a crime? Later, I'm accused of a crime and the fake emails I

Pg: 16

VI Attacks of DeCapua as an expert

DeCapua is not an expert of any technological concept by any stretch of the imagination. He does not possess any technical degree in engineering or computer science and has never worked professionally for any tech company or tech role.

The following are a few statements that DeCapua make which invalidates him as a technical expert

~~Page 6300: "Metadata" is a term used only by attorneys.~~

Page 6300: "Metadata is more of a word that's used by attorneys"

This is laughably false. Metadata is commonly used in forensics, email, and many other computing areas where "extra" data is stored along with the main data such as Alternate Date Streams in NTFS or extra data describing videos, pictures, etc.

Page 6332: "And the bes way computers count are, instead of using base 10, it's up to 16, a nice even number. And normally with computers, hexadecimal is represented with ones and zeros, but to make it a little more understandable for us, they designate lettersF to represent values".

— We are all dumber for having read this. It makes no sense & is entirely wrong.

Page 6565: So our counting system has base 10, we count through 10. Computers, because of the way they're built and how they work, it's easier for them to count using a base 16,

Pg 27

of Consistency.

Why does agent DeCapua not notice this very obvious and potentially very critical pattern that I picked up instantly? Bias and ignorance. DeCapua doesn't want to encounter any logical patterns that may legitimately explain the ~~Message ID~~ perceived Message ID anomaly. And therein lies the problem — DeCapua is not only NOT experienced in technology, he is not a scientist. Once again, he does not follow the scientific method that any professional would do. He is clearly not seeking the truth — His confirmation bias overrides all other logic. Maybe he did notice the obvious pattern but consciously chose not to disclose it because it didn't validate his conclusion? Either way this is exactly why amateurs should not testify as experts, specifically FBI agents. They seek guilt and persecution above all else.

At 6317 DeCapua states his assumption that the defendant must have taken a legitamite email from the date of the message ID timestamp and then simply reused the message ID when creating this fradulent email. So, what, 6 months after the end of some email chain the defendant decamped the email. To what end? Look at the content of this email and explain how that makes any sense. DeCapua is just grasping for straws and pulling theories upon theories out of thin air instead of going with the simplest theory — the emails are authentic

$$11000101 = 1\times2^7 + 1\times2^6 + 0\times2^5 + 0\times2^4 + 0\times2^3 + 1\times2^2 + 0\times2^1 + 1\times2^0$$
$$= 128 + 64 + 0 + 0 + 0 + 4 + 0 + 1$$
$$= 197.$$

So, the 8 binary digits of 11000101_2 is equivalent to 3 decimal digits 197_{10}. That is NOT an easy conversion to make — nor is the reverse:

197. Here's our digits in decimal: 128 64 32 16 8 4 2 1

Starting with the highest decimal value, 128 (2^8 is 256 which is too big) If this number 'fits' in our current number (197) ie) less than or equal to, then we place a one in the corresponding digit location (8th digit), subtract then repeat:

$128 \le 197?$ 2^7: Yes $\therefore 2^7 = 1$ $197 - 128 = 069$	$2^6: 64 \le 69?$ Yes $\therefore 2^6 = 1$ $69 - 64 = 5$	$2^5: 32 \le 5?$ No $\therefore 2^5 = 0$	$2^4: 16 \le 5?$ No $\therefore 2^4 = 0$	$2^3: 8 \le 5$ No $\therefore 2^3 = 0$
$2^2: 4 \le 5?$ Yes $\therefore 2^2 = 1$ $5 - 4 = 1$	$2^1: 2 \le 1?$ No $\therefore 2^1 = 0$	$2^0: 1 \le 1?$ Yes $\therefore 2^0 = 1$ $1 - 1 = 0.$		

Always end on 0. So, our number is: 11000101_2 as we would expect.

Decimal is not an easy conversion because 10 is not a power of 2. But, 8 is. So is 16. Base 8 is known as octal and can be used to represent ~~th~~ raw data as well, but it's less concise than say, 16, or hexadecimal. Hexadecimal provides a nice lookup table for each nibble (4 bits). Therefore, we need only break our digits into groups of 4s and transcribe:

0000 - 0	0100 - 4	1000 - 8	1100 - C
0001 - 1	0101 - 5	1001 - 9	1101 - D
0010 - 2	0110 - 6	1010 - 10 - A	1110 - E
0011 - 3	0111 - 7	1011 - B	1111 - F

Easy! So, 1100 0101 becomes C5. & vice versa.

Thus, in hexadecimal we can represent 8 binary digits with only 2 hexadecimal digits. This is an easy compression of data in at

~~DeCapua is not even a begine~~

Forget expert or amateur, DeCapua is not even a begineer yet. He does not understand ~~th~~ very simple computing or basic mathematics of number systems - A prerequisite for any introductory engineering course

Claiming to be an email expert but not knowing base64 is tantamount to claiming to be a pitcrew expert in the field of professional racing, but never seeing or understanding anything about tires. Ludicrous.

Pg. 20

Finally, on pages 6612 and 6613:

Q A UUID doesn't have to be in base 16? Right
A: They have to be in base 16
Q Isn't it a fact that UUIDs can also be created in base 32?
A No.
Q Isn't it a fact that UUIDs can also be created in base 64?
A All UUIDs are in hex
Court: But have you ever seen or do you have experience with either base 32 or base 64?
A No, and I don't see them in practice in digital forensics,

Wow. ~~Again at 6631 he states~~ Base64 is huge on the internet and especially with email & he's never seen it in digital forensics? As oppossed to analog forensics? How is that possible? In fact, base 64 appears in at least government exhibits 3544, 3552, 3549, 3570AZ, and throughout these raw emails. But he doesn't know what it is? Incredible. Based soley on his hexidecimal and base64 testimony it's clear he cannot possibly be taken seriously as any sort of expert. Again, not only is he not an expert but he's not even graduated to the beginner level yet;

at an electric level

Understanding these number systems, encoding, and how computers work is a prerequisite for ~~cs101~~ ee101. So how is it that someone who isn't even a beginner qualifies as an expert? He's incompetent, reckless, and cares nothing of the scientific method and yet he's a top FBI agent. Truly that should

Scare each and every one of us. ~~Claiming to be an~~ With this man considered a "Cyber expert", it's no wonder the incompetent FBI have had So much trouble tracking down leakers, most notably the Vault 7/8 wikileaks perpertrator.

Finally, I want to discuss email spoofing. Spoofing is used as a term to describe the process of creating and sending an email from someone that didn't send it — Essentially all aspects of the email remain constant except changing the "from" field to conceivably any email address of your choice. Email spoofing is common in both phishing and social engineering attacks, of which I am experienced in performing ~~both attacks~~. The purpose of these attacks is to trick the recipient into doing something ~~they~~ malicious or potentially harmful to themselves. ~~Spoofing an email~~ Creating a fake email and uploading it to your sentbox is not Spoofing — it accomplishes nothing. You can't trick someone into clicking on a link in your own sentbox. Therefore, DeCapua has proposed something entirely new which I dub "DeCampua Spoofing" or "Decomping" and is thus defined:

"Decamping" — A self-spoof whereby an individual fakes an email from himself and uploads it to his own sentbox for the purpose of self-trolling or trolling the inevitable FBI investigation by embedding *Rick Astley*(?) in the email & therefore rickrolling all future FBI agents.

Pg 22

Despite the fact that DeCompra is a fraud the judge labels him an expert in "email analysis" on page 6306. Which raises the next question- how does a novice in technology label someone else as an expert? It's too easy today to google a ~~few article~~ topic, read a few articles & pose as an expert. No judge can determine expertise that he himself doesn't possess. And so we are left with ~~the~~ this outbreak of malware of the mind; An epidemic destroying innocent lives.

GX3550 GX 3552

VII Emails 2 and 3 and the "hidden" timestamp

At pg 6253 on the eve of summation, the prosecution claims that DeCapua can now definitively say the emails are fake. Recall earlier that the judge previously ruled on 12/6 that his testimony was pure speculation and would not be presented to the jury. Now, ~~on~~ three days before christmas and the loss of a jury which would result in a mistrial — now there has been a breakthrough. He thinks he discovers something at 1:30AM that morning and wants to present his findings to the judge and jury. Why is all this relevant? It was reckless to ever pursue Decumpua's testimony so late in the trial. As a professional, I find it impossible for him to properly fully vet any theory in such a short time-frame. His actions have real consequences. I've worked in a field within technology where the software I write could mean certain death for assets if not written perfectly. I always took great pride in my work and stressed to ensure my code never cost ~~an~~ a human life. You go above and beyond to ensure safety above all else. If I was ever pushed on a deadline that I could not ensure this safety then I refused and protested its delivery. You don't just take orders - DeCapua was incredibly irresponsible and reckless in his lacksidosical work.

On page 6309, DeCompua acknowledges that there is no Standard
for generating Message IDs within emails and therefore each
MessageID is undefined per the specification and implementation-
defined. He then claims on page 6310 that blackberry has a "hidden"
timestamp embedded in their Message ID. This is pure speculation
flippant based entirely on inductive evidence from a relatively few emails.
First of all, the timestamp is not hidden at all - it's readily
appearant in the Structure of the Blackberry MessageID. What's
also readily appearant is the term "decombobulater". This term may
X= not be obvious to many, but decombobulator is a reference to X &
Y= fairly Commonly Y in tech culture. We routinely embed little
easter eggs Z= Candies? - Z in the projects we develop and you'll find them in
everything from games to ~~email message IDs to~~ professional software -
Either with or without our management's approval! The use of
'decombobulator' here is highly relevant, not only as a shout out to
the blackberry devs, but also at the flippant attitude of the
devs regarding something as trivial as an email message ID - Blackberry
had some fun with it. Email message IDs are not a serious
XX = matter and at their inception back in XX, never intended to
make a court appearance. I highly doubt developers at Blackberry
every intended their "decombobulater" string to be unveiled ~~here~~ and
highly Scrutinized here in the court of law? Their ~~undefined~~ unpublished
behavior of MessageIDs used to convict a man of wire fraud. No,
email was not designed with authenticity or the FBI in mind. The use
of a UNIX timestamp in addition to numerous other unrecognized
~~data~~ variables is an implementation decision that could be

Created years ago are used against me somehow, for some random, unrelated alleged crime.

Deductive Reasoning:

The government presents the following deductive argument:

1.) If A then B — If evidence exists of wire fraud then wire fraud occurred

2.) C — Fake emails exist

Therefore B — Wire fraud occurred and Omar is guilty.

Whereas I would argue the following:

1.) Generally, people do things for a reason

2.) People perform ~~tedious~~ long, tedious tasks to achieve some end goal

3.) Modifying and fabricating an email is a long & tedious task.

4.) Fabricating 3 random emails out of hundreds or thousands and placing them in your own sentbox and nowhere else does NOT accomplish anything

Conclusion: It's illogical & inconceivable that anyone would fabricate 3 random emails in this manner

Pg. 25

X= Changed at any time, without warning or announcement. For example, Consider Microsoft's undocumented functionality that was changed and Caused poor-practice software issues: X

6315; Q "... offer an opinion as to whether or not this email is authentic?"

— Yes, it's fake.

Q: " Is that simply because the date and time.... don't match the timestamp conversion?"

— "That's correct"

GX $^{3550}/_{3552}$

Wow this is incredible. Let's take a look at these email in ~~GX 3579-A/B~~ This is quite ~~like~~ an astonishing proclamation. Due to a perceived anomaly in an undefined fiedd he claims that the message-ID must be fake. & therefore the email itself frodulent. What does it prove when you find an anomaly with inductively deduced data from an undefined source? Absolutely nothing. Undefined is undefined. No Speculation can ever be stated as a certainty regarding undefined functionality. If you find that 3/0 results in 12 in a given CPU does that mean it will always result in 12? 3/0 is, by definition, undefined. You can make no assumptions of what garbage data resides in any undefined CPU register after a 3/0 operation no matter how many times you get 12 as a result. Any Statement to the contrary is an absurdity. I find agent De Campo's testimony not only false, inconsistent with Computer Science and fundamental engineering principles, but also incredibly reckless.

Pg 26

Why couldn't the message ID combine a random salt with the unix timestamp? ~~Many~~ Perhaps sometimes code flow dictates a secondary method for the messageID generation? Perhaps traffic effects the use of the timestamp? There are any number of variables and deviations unknown to Decompra that could effect the software on blackberry's server and how it constructs an undefined data field. We can't see the source code or logic that dictates what influences these values. What if the time on the server is incorrect or in a faulty state? As a system administrator I've seen many strange network anomalies & software failures due to failing hardware or even specifically servers with wrong dates/times due to NTP desync issues.

Stranger yet, the one real pattern I see from government exhibits GX 3579-A and 3579-B is the specific server ~~bx~~ bxe1141.bisx.prod.on.blackberry. If you look at all the other servers and time information, none of them list this server except for the two emails with the wrong unix time in the message ID. Coincidence? Coincidence that the very 2 emails with inconsistent messageIDs also share only one common trait — The same server sent both. Highly unlikely. Two emails with the same server and the same time issue. Hmm. To me, this is indicative of either a time issue with the server that generates the incorrect unix timestamp for the message ID OR the bisx server is either a test or production machine running different software for generating the message ID — perhaps even a bug in the rollout of new software! Since the algorithm for generating the messageID is ~~random~~ undefined there is no guarantee

Pg 28

Winchester house

At 6320 DeCarla acknowledges his theory regarding the July email does not apply to the email with the 2087 unix timestamp in the message ID. Yet, even with zero theories as to how this message ID was derived let alone why any of these emails were decamped, he is unyielding in his assertion of fraudulence. Zero proposed theories, but absolute confidence that it must be fake. I can honestly say I don't think a single technical person in the entire world would ever say with absolute certainty that this email must be false based entirely on the undefined message ID implementation. Not one. It should be noted that the discussion of the unix timestamp seemed to confuse the court enough that at 6579, the notion of a unix timestamp in the message ID field appears to merge with the datetime field of the email itself as if the email itself showed a future date — it does not. Both emails show a correct date. It is only in ~~two of these~~ the undefined message ID field where the speculated discovery of a unix datetime stamp exists. Nowhere else. No other abnormalities & with no theory about the 2087 message ID he still states for the record that both emails are absolutely false — I just can't process this idiocracy. His theory has devolved into the Winchester house with all these special cases and uncertainties. Was the value randomly generated? That's the only other real possibility if it wasn't taken from a real message ID? ~~Or perhap~~ How did the ~~user~~ person know it was a 32-bit value? What if it were a 64-bit value? If you're not going to use an existing header why even keep the same structure? There are a million questions

Pg 29

but no answers from DeCapua. Let's assume it was a random Value — If a randomly-generated 64-bit number is generated ~~that~~ then that gives us a one in a hundred billion probability of any given year and one in a billion for any 200 year span. Given that $2^{64} \approx 10^{18}$ & there are $\simeq 3 \times 10^{7}$ seconds per year then $\frac{10^{7}}{10^{18}} = 1/10^{11}$. A ~~couple hundred year~~ 200 year range would be $\simeq \frac{10^{2}}{10^{11}} \simeq 1/10^{9}$.

On Cross-examination at 633T: ~~DeCapua acknowledges~~

Q: You haven't confirmed with blackberry about what other possibilities exist within their computer infrastructure that could potentially explain this, have you?

A: No.

Weighing the evidence of undefined messageIDs alone should have been sufficient to dissuade any technical expert from ever testifying that the emails ~~was~~ were definitively fake. It's unfathomable. This fact combined with the simple observation I noted regarding the two emails processed by the same blackberry server & my own speculation of something different most likely occurring on this server that directly caused the messageIDs AND the fact, again, that the content of those emails was recognized as authentic I can state with a very high degree of accuracy that ~~the emails~~ no evidence suggests ~~[illegible]~~ these emails are fradulent, and in fact, that they are most likely authentic.

VIII Email 4 and UUIDs GX3351

Pg 6309: Message-ID, there's no standard for what it's supposed to look like; it just has to be unique, but every company has their own twist or spin.

6589:

Q: Based on your review of this message-ID and your familiarity with hex characters, are you able to offer an opinion as to whether or not this message ID was fabricated?

A: It's fake.

Q Based on testimony that this message ID was fake, are you able to offer an opinion as to whether or not this email was sent on 3/26/2012?

A: It was not.

Wow. Once again, incredible confidence based on an undefined field. This message ID, which appears to be of a UUID format, is declared fradulent due to a 'U' in the field and therefore the entire email a fake. Absolute confidence, but wait:

6331:

Q. It's also possible that a message ID could use a format that looks like what you're describing, but not actually use hex?

A: It's possible

Pg 31

Yet: 6334:

Q: What is the fact that a message ID is different from what you would expect for a hex ID can't definitively show you that this particular email was never created, right?

A: "It's so far outside the realm of possibility that that is why I say definitively this is a fake email"

"So far outside the realm of possibility" - That is quite a statement to make about software you know nothing about and an undefined data field. I can state the following, to my knowledge as a software engineer, the C compiler does not fail to compile because a 'U' exists in a UUID nor does it crash. A ~~computer does no~~ program does not halt at runtime if a UUID is displayed with a 'U' nor does it kernel panic (well I guess unless you program it to do so). I can also state that many GUIDs I have used ~~and interacted with~~ in, say, named mutexes or other synchronization objects used ~~across~~ for multi-process communication have contained non-hexadecimal characters. Now, I don't recall if I ever used a 'U' specifically, but it is certainly within the realm of possibilities for a 'U' to exist in a string, and thus, his assertion is ridiculous.

Finally, in open court Delapena once again presented his demo. He also acknowledged that in the past two weeks since his first demo for the judge he still has not attempted to contact Yahoo and verify his baseless assumption that uploaded emails are not flagged.

DeLoqua's demo of the backup and restore of emails in which you can ~~emulate~~ manipulate the emails and then ~~restore them~~ upload them to the server is like announcing to the world that you've discovered a new way to sit in a chair: You turn it on its side and then sit laying across the ground. Ok, congrats I guess? It's new sure, but like decamping, it's not in anyway useful. Why in the world would you sit in a chair in this manner? Why in the world would you spoof yourself or modify emails in your inbox about real events and conversations? Perhaps you must do it in tandem while laying across the floor in the chair? Have at it.

Pg. 17

This statement makes me cringe. No, computers don't "count in hex". Hex isn't used because it's a "nice, even number" — so is 10. Computers are not built with 16 different possibilities for an electron — If he has designed a computer that uses spin, charge, and other quantum properties of an electron then that's called a quantum computer, and we would love for him to please gift society with his invention & claim the nobel prize. But otherwise, computers use voltage, charge, and power related via $V=iR$, $R=Vi$. Thankfully, Einstein was wrong and quantum mechanics have thus far held up as valid otherwise transistors would not work — nor would any modern technology. Anyway, computers are binary: On or off, 1 or 0. DeCapua doesn't seem to fully understand very basic computing and mathematics. Hexadecimal is just a different way to represent data. It's a data format like ascii, unicode, base 64; All encoding schemes. The easiest representation of raw binary data for humans to ~~read~~ easily convert back & forth & which is reasonably concise is hexadecimal. Let's see why:

Binary can be converted to base-10 as such: [11000101] Each binary bit represents a power of 2, from right to left. Thus, 8 digits would have the following values: ~~2^8 2^7 2^6 2^5 2^4 2^3 2^2 2^1~~

$$2^7 \; 2^6 \; 2^5 \; 2^4 \; 2^3 \; 2^2 \; 2^1 \; 2^0$$

IX Conclusion

I conclude that no evidence suggests any of Omar's emails were fabricated. I also conclude that they were all most likely authentic.

DeCapua's testimony should have been the following:

DeCapua: I speculate based on undefined fields in the message ID that these emails could possibly be fabricated.
Court: Thank you, very special agent DeCapua. Here's a participation trophy and a pat on the back — You can go back to your little sandbox now and let the grownups finish talking.

Unfortunately that isn't how it transpired. People's lives are at stake and DeCapua has made erroneous and fallacious statements with some presumption of knowledge or intelligence that isn't there. He has decided to take the haphazard approach in which he neither seems to care about the consequences of his actions nor the people he's hurt. He never should have taken the stand at such a short notice. He was irresponsible and reckless and his eggregious mistake has cost an innocent man severely. If DeCapua worked for any self-respecting entity he would be held responsible for his own actions and fired immediately. Fortunately, he works for the FBI so they are likely to give him another 'Investigator of the year!' award and promote him for a job well done.

These FBI agents possess no technical abilities. They learn the smallest bits and pieces to become dangerous — They learn enough to be able to google search and even recognize what may appear to be a Unix timestamp — but not enough to analyze what they are seeing in context, how it relates to the issue at hand, or the background and experience to professionally understand applicable technical concepts. They can shoot a gun but they can't think critically. Essentially, the agent sees increasing numbers and makes the simplest of observations that he then applies erroneously to a misunderstood concept and then draws a fallacious conclusion that he recklessly pursues never once realizing his own extraordinary ignorance of the subject matter at hand. ~~We refer to~~ Dumb people are blissfully unaware that they're dumb — which is perfectly fine until they are granted dominion over other people & influence of their lives.

It's important to note the self-imposed timeline here. This entire testimony was sprung on the defence on the eve of summation — the prosecution had long since rested. In fact, the case seemed to be highly in Omar's favor according to multiple individuals that I've spoken — The government had literally provided no evidence at all of any wire fraud in a wire fraud case. DeCapua was a last-ditch effort to thwart the law and save the prosecution, Although he previously only speculated one email was potentially fabricated, on 2AM days before the jury would have been lost, he decides that he can now testify with a certainty that three separate emails are fradulent — Emails with nothing to do with the case whose content was recognized and even in at least one incident, some of the emails were even recognized. Whereas the CIA takes precautions to ensure ~~the~~ innocent lives aren't lost, the FBI seems content to shotgun a last-second theory on a whim — No time for testing and validation. And so, DeCompra gave misleading, and fallacious testimony with reckless disregard for the law, ~~professional~~ engineering professionalism, and human life. — And all to confuse and confound the jury; The defendant was accused of witchcraft — sending emails from the future. The defense had no time to find an expert and refute the FBI's testimony and so the judge and jury were successfully infected with the malware of the mind & found the defendant guilty.

As I stated at the onset, this is the second case I've found in the past several months in which 1.) An unqualified, incompetent FBI agent claimed technical expertise that he obviously did not possess and 2.) The FBI agent used his power, & authority, to claim expertise and make misleading, malicious, and false technical assertions with a reckless regard for the law or consequences; these baseless claims then directly resulted in the loss of liberty to the defendants. Despite no actual, legitamite evidence and no technical expert in the world who would back their claims, these FBI agents have discovered that they can corrupt, distort, and manipulate technical data to influence the court. Finding one case is perhaps an anomaly, but two is a trend — How many innocent people are in prison today due to FBI malfesence? This is an abomination that must be stopped.

I swore an oath to protect and defend the Constitution from enemies both foreign and domestic. To date, the greatest existential threat to the American people and the United States Constitution is the United States government itself. Namely, the FBI and justice system, which assaults ~~and~~ its own people. Armed with a rudimentary misunderstanding of technology, the FBI have finally embraced technology & perverted it as a powerful medium through which it can spread its malware of the mind and destroy innocent lives.

Pg 37

References

GX 3553 - 1st email Chain
GX 3549 - Raw email
GX 3550 - 2nd email 3/10/09 from omar
GX 3552 - 3rd email 12/2/08 from omar
GX 3551 - 4th email 3/26/12 from omar
GX 3579A - email 2 with timestamp Conversion
GX 3579-B - email 3 with timestamp Conversion
GX 3556 - Kaleil Sent emails Message ID RE: Email 1