FBI CYBER DIVISION'S ENDURING BLUE PILL MYSTERY

I'm writing a post on the technical analysis John Durham included in his report purporting to debunk the white papers submitted via Michael Sussmann to, first, the FBI and, then, the CIA. But first I'm going to do something even more tedious: Try to track down FBI's persistent blue pill problem — or rather, the FBI's apparent failure to *ever* analyze one of two thumb drives Sussmann shared with Jim Baker in September 2016, the Blue one.

Last year, before Sussmann's trial, Durham had FBI's top technical people review what he claimed were the data Sussmann had shared. He cited those reports in his own report, claiming they debunk the white papers.

Here's how they are described in footnotes.

- 1635 FBI Cyber Division Cyber Technical Analysis Unit, Technical Analysis Report (April 20, 2022) (hereinafter "FBI Technical Analysis Report") (SCO _ 094755)
- 1671 FBI Cyber Technical Operations Unit, Trump/Alfa/Spectrum/Yota Observations and Assessment (undated; unpaginated).

Not only doesn't the YotaPhone report have a date, but it doesn't have a Bates stamp reflecting that it was shared with Sussmann. I'll get into why that is interesting in my follow-up post.

Below is a summary of the materials Sussmann

provided to both agencies. By description, the Technical Analysis Report only reviews the white paper and the smaller of two sets of text DNS logs included on the Red Thumb Drive. By description the Trump/Alfa/Spectrum/Yota Observations only review the Yota White Paper.

The data FBI's technical people reviewed appear to be restricted to what is marked in blue.

Agency	Thumb Drives	Contents	Analysis
FBI	Red	White Paper #1 - Auditable V3	Technical Analysis Report
		White Paper Comments: Time Series Analysis of Recursive Queries	
		Alfa Group Overview	
		19 pages DNS logs (GX 208)	
		62 pages DNS logs (GX 209) [possibly on Blue Drive]	
		6 other documents	
	Blue	Reportedly other DNS logs	
CIA	Two thumb drives	Network Analysis of Yota-Related Resolution Events	Trump/Alfa/Spectrum!Yota Observations and Assessment
		YotaPhone CSV File Collected on December 11th, 2016	
		Summary of Trump Network Communications	
		ONINT on Trump Network Communications	
		6 CSV files: Yota-EOP.csv Yota-CPWest.csv Yota-Spectrum.csv Yota-TrumpOrg.csv Sipper 2016-05-04_2017-01-15_Trump_server.csv	

They did review the actual thumb drives turned over to the CIA, because they found hidden data on one; there's no indication they reviewed the thumb drives provided to the FBI.

In fact, it's impossible that they reviewed the data included on the second thumb drive Sussmann shared, the Blue one.

That's because the FBI analysis claims Sussmann only provided 851 resolutions, which is the 19-page collection of text files included on the Red Thumb Drive, not even the larger set.

> Similarly, the FBI experts told us that the collection of passive DNS data used to support the claims made in the white paper was also significantly incomplete. 1657 They explained that, given the documented email transmissions from IP address 66.216.133.29 during the covered period, the representative sampling of passive DNS would have necessarily included a much larger volume and distribution of queries from source IP

> addresses across the internet. In light of this fact, they stated that the passive DNS data that Joffe and his cyber researchers compiled and that Sussmann passed onto the FBI was significantly incomplete, as it included no A-record (hostname to IP address) resolutions corresponding to the outgoing messages from the IP address. 1658 Without further information from those who compiled the white paper data, 1659 the FBI experts stated that it is impossible to determine whether the absence of additional A record resolutions is due to the visibility afforded by the passive DNS operator, the result of the specific queries that the compiling analyst used to query the dataset, or intentional filtering applied by the analyst after retrieval. 1660
>
> 1659 The data used for the white paper came from Joffe's companies Packet Forensics and Tech Company-I. As noted above, Joffe declined to be interviewed by the Office, as did Tech Company-2 Executive-I. The **851 records** of resolutions on **the USB drive** were an exact match for a file of resolutions sent from University-I Researcher-2 to University-I Researcher- I on July 29, 2016, which was referred to as "[first name of Tech Company-2 Executive-l]'s data." Id. at 7.
>
> 1660 Id. [bold]

There's no way they would have come to this conclusion if they had seen the Blue Thumb Drive, which had millions of logs on it.

In fact, it appears that the FBI *never did review* that Blue Thumb Drive when they were investigating the Alfa Bank anomaly.

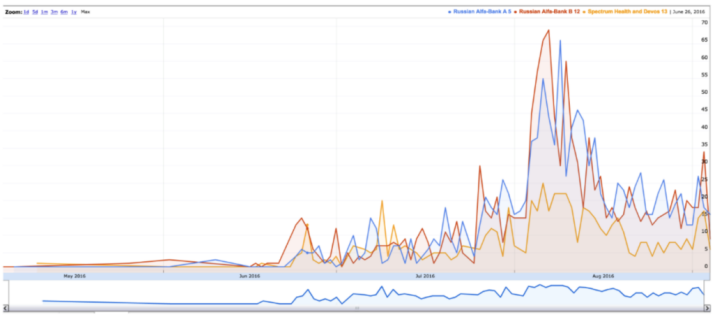
They didn't do so, it appears, because the Cyber

Division Agents who first reviewed the allegations, Nate Batty and Scott Hellman, misplaced the Blue Thumb Drive for weeks.

That may not have been an accident.

Batty and Hellman's initial review, which they completed in just over a day, was riddled with errors (as I laid out during the trial). Importantly, they *could not* have reviewed most of the DNS logs before writing their report, because they claimed, "the presumed suspicious activity began approximately three weeks prior to the stated start [July 28] of the investigation conducted by the researcher."

Even the smaller set of log files included on the Red Thumb Drive showed the anomaly went back to May. A histograph included in the white paper shows the anomaly accelerating in June.



Had anyone ever reviewed the full dataset, the shoddiness of their initial analysis would have been even more clear.

Here's how the FBI managed to conduct an investigation on two thumb drives without, it appears, ever looking at the second one.

As the chain of custody submitted at trial shows, Jim Baker accepted the thumb drives, then handed them off to Peter Strzok, who then handed them off to Acting Assistant Director of Cyber Eric Sporre, who at first put the thumb drives in his safe, then handed them over to Nate Batty.

Within hours (these logs are UTC), Batty and Hellman started mocking the white paper but also complaining about the "absurd quantity of data."

Hellman, at least, admitted at trial that he only knows the basics about DNS.

The next day, Batty told Hellman that their supervisor wanted them to write a "brief summary" of what he calls "the DNC report." Batty appears to have known of Sussmann from other cases and he was informed that Sussmann was in the chain of custody.

From: ncbatty To: jrsmith7	You've got the signatures from all of those people?
From: jrsmith7 To: ncbatty	Sussman to Strzock to Sporre - we can get

In spite of the clear record showing Batty was informed who provided the thumb drives, in 2019, he told Durham that he and Hellman — whose analysis was so shitty — had considered filing a whistleblower complaint because they weren't told what the documentary record shows he was clearly informed. And Durham thought that was sufficiently credible to stick in his report.

Before writing an analysis of this report, Batty admitted, they should first "plug the thumb drives" in and look at the files before they wrote a summary.

ncbatty@fbi.sgov.gov	sjhellman@fbi.sgov.gov	Tim asked if we would write a brief summary of what we think about the DNC report.
ncbatty@fbi.sgov.gov	sjhellman@fbi.sgov.gov	I can do it
ncbatty@fbi.sgov.gov	sjhellman@fbi.sgov.gov	But I'm thinking we should at least plug the thumb drives into Frank's computer and look at the files....
ncbatty@fbi.sgov.gov	sjhellman@fbi.sgov.gov	What do you think?

The documentary evidence shows that these guys formed their initial conclusion about the white paper without ever reviewing the data first.

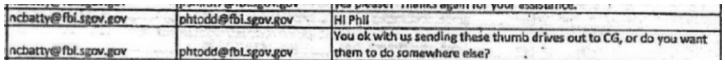
A day later, Curtis Heide texted from Chicago and asked them to upload the thumb drives, plural, so they could start looking at them.

caheide@fbi.sgov.gov	ncbatty@fbi.sgov.gov	nate, can we toss the contents of those thumb drives on opwan so we can review them today?

They only uploaded one, the Red Thumb Drive.

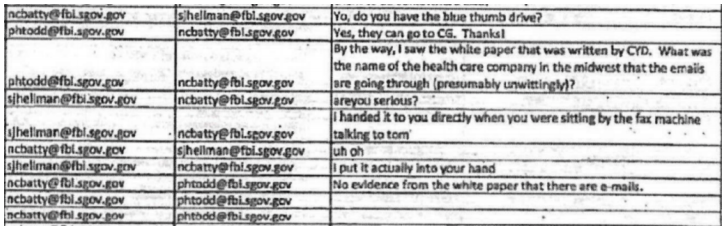
That's clear because when Kyle Steere documented what they had received on October 4, he described that his report is, "a brief summary of the contents of the USB drive," singular. The contents match what were on the Red Thumb Drive.

Two hours and 16 minutes later, after uploading the Red Drive, Batty asked if he should send the actual thumb drives to Chicago.



ncbatty@fbi.sgov.gov	phtodd@fbi.sgov.gov	Hi Phil
ncbatty@fbi.sgov.gov	phtodd@fbi.sgov.gov	You ok with us sending these thumb drives out to CG, or do you want them to do somewhere else?

48 minutes later, Batty asked Hellman if he had the Blue Thumb Drive.

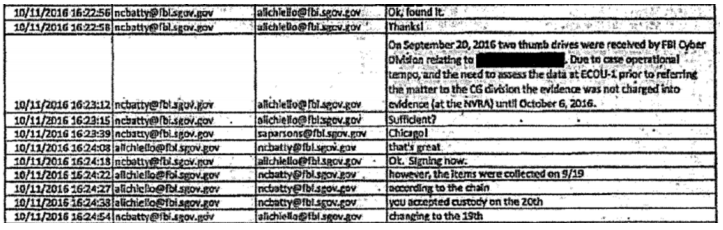


ncbatty@fbi.sgov.gov	sjhellman@fbi.sgov.gov	Yo, do you have the blue thumb drive?
phtodd@fbi.sgov.gov	ncbatty@fbi.sgov.gov	Yes, they can go to CG. Thanks!
phtodd@fbi.sgov.gov	ncbatty@fbi.sgov.gov	By the way, I saw the white paper that was written by CYD. What was the name of the health care company in the midwest that the emails are going through (presumably unwittingly)?
sjhellman@fbi.sgov.gov	ncbatty@fbi.sgov.gov	areyou serious?
sjhellman@fbi.sgov.gov	ncbatty@fbi.sgov.gov	I handed it to you directly when you were sitting by the fax machine talking to tom
ncbatty@fbi.sgov.gov	sjhellman@fbi.sgov.gov	uh oh
sjhellman@fbi.sgov.gov	ncbatty@fbi.sgov.gov	I put it actually into your hand
ncbatty@fbi.sgov.gov	phtodd@fbi.sgov.gov	No evidence from the white paper that there are e-mails.
ncbatty@fbi.sgov.gov	phtodd@fbi.sgov.gov	
ncbatty@fbi.sgov.gov	phtodd@fbi.sgov.gov	

The chain of custody shows that Batty didn't send anything on September 22, when he and Hellman were panicking about the missing Blue Thumb Drive. Instead, he put something in storage on October 6, two weeks later. That he put them in storage makes no sense, because when he wrote an Electronic Communication explaining why he was sending the thumb drives to Chicago on October 11 (by that point, 19 days after saying they would send the thumb drives to Chicago that day), he claimed,

> Due to case operational tempo, and the need to assess the data at ECOU-1 prior to referring the matter to the [Chicago] division the evidence was not charged into evidence (at the NVRA) until October 6, 2016.

Not a shred of evidence in the available record supports that claim and a great deal shows it to be false.



10/11/2016 16:22:56	ncbatty@fbi.sgov.gov	alichiello@fbi.sgov.gov	Ok, found it.
10/11/2016 16:22:58	ncbatty@fbi.sgov.gov	alichiello@fbi.sgov.gov	Thanks!
10/11/2016 16:23:12	ncbatty@fbi.sgov.gov	alichiello@fbi.sgov.gov	On September 20, 2016 two thumb drives were received by FBI Cyber Division relating to [redacted]. Due to case operational tempo, and the need to assess the data at ECOU-1 prior to referring the matter to the CG division the evidence was not charged into evidence (at the NVRA) until October 6, 2016.
10/11/2016 16:23:15	ncbatty@fbi.sgov.gov	alichiello@fbi.sgov.gov	Sufficient?
10/11/2016 16:23:39	ncbatty@fbi.sgov.gov	saparsons@fbi.sgov.gov	Chicago!
10/13/2016 16:24:08	alichiello@fbi.sgov.gov	ncbatty@fbi.sgov.gov	that's great
10/13/2016 16:24:18	ncbatty@fbi.sgov.gov	alichiello@fbi.sgov.gov	Ok. Signing now.
10/13/2016 16:24:22	alichiello@fbi.sgov.gov	ncbatty@fbi.sgov.gov	however, the items were collected on 9/19
10/13/2016 16:24:27	alichiello@fbi.sgov.gov	ncbatty@fbi.sgov.gov	according to the chain
10/13/2016 16:24:38	alichiello@fbi.sgov.gov	ncbatty@fbi.sgov.gov	you accepted custody on the 20th
10/13/2016 16:24:54	ncbatty@fbi.sgov.gov	alichiello@fbi.sgov.gov	changing to the 19th

But he didn't send the physical thumb drives until October 12, FedEx instead of internal BuMail.

Signature: [illegible]	10/6/16 1626	Signature: [illegible]	OCT 0 6 2016	
Printed Name/Agency: N.C. Batty		Printed Name/Agency: Annamarie Lichiello - FBI		4:20p
Reason: To CCC		Reason: Storage		
Relinquished Custody	**Date and Time**	**Accepted Custody**		**Date and Time**
FED EX # 5916 5139 9400				
Signature: [illegible]	OCT 12 2016	Signature: [illegible]		10-14-16
Printed Name/Agency: Annamarie Lichiello - FBI	12:15pm	Printed Name/Agency: [illegible]		
Reason: TO CG per Serial 12		Reason: Rec. Transfer		10:15 A

By October 12, the FBI had decided there was nothing to these allegations.

Somewhere along the way, there was some confusion as to whether there was one or two thumb drives. At the time the case ID was added — the case was opened on September 23 — it seems to have been understood there was just one thumb drive.

Case ID: 105H-CG-2083487 1B: 1 2 Barcode: E5541017

This form is incomplete without reference to the FD-1087.

Batty does seem to have sent two thumb drives, one Red and one Blue, to Chicago after that 20-day delay, though.

At trial on May 23, Alison Sands dramatically pulled two thumb drives — a Red Thumb Drive and a Blue Thumb Drive — out of the evidence envelope where she put them years earlier.

> Q. Ms. Sands, I'm showing you what's been marked for identification as Government's Exhibit 1. Do you recognize that?
>
> A. Yes.
>
> Q. What is that?
>
> A. This is the la envelope.
>
> Q. Do you know what this envelope contains?
>
> A. Yes, it contains the thumb drives. So I basically took them out of evidence and put it into this envelope.
>
> [snip]
>
> Q. Now, Ms. Sands, do you recall how many thumb drives there were?
>
> A. Yes, there's two.

> Q. Do you recall if they had any particular colors?
>
> A. One is blue and one is red.

On the stand, Sands also introduced Steere's memo, the one that documented the contents of the Red Thumb Drive. In doing so, though, she falsely claimed (at least per the transcript) that the memo described both thumb drives.

> Q. Do you recognize what Government's 206 is?
>
> A. Yes.
>
> Q. What is that?
>
> A. It is the EC documenting what information was on the **thumb drives** that were provided.

She also introduced the items included on the Red Thumb Drive, one after another, into evidence.

Except for the 19-page set of text files used for technical analysis.

When prosecutor Brittain Shaw got to that file in Steere's memo, she tried to move it into evidence, but both Judge Cooper and Sussmann attorney Michael Bosworth noted it was already in evidence.

> MS. SHAW: Could we go back to Government's Exhibit 206, please? Moving down the list –
>
> BY MS. SHAW:
>
> Q. The second item, what is that?
>
> A. It is data that was provided as alleged evidence of these DNS lookup tables.
>
> Q. After number 2, is that the title that was given to the file or is that something you assigned?

> A. I believe that's something we assigned.
>
> Q. Okay.
>
> MS. SHAW: And if I could have Government's Exhibit 208, please. If you'd just blow that up a little bit. Thank you.
>
> BY MS. SHAW:
>
> Q. And, Ms. Sands, do you recognize what that is?
>
> A. Yes, these are the DNS lookups that I just described.
>
> MS. SHAW: All right. I would move Government's Exhibit 208 into evidence.
>
> MR. BOSWORTH: It may be —-
>
> THE COURT: I think it's probably in.
>
> MS. SHAW: All right.

It was already in.

Almost a week earlier, Scott Hellman introduced what he called "a portion" of the data included with the exhibit. It was the 19-page text file of DNS logs that reviewed in the Technical Analysis included on the Red Thumb Drive. He didn't describe it as one stand-alone document included on the thumb drive. He seemed to imply this was a selection the FBI had made.

> Q. And if I could show just to you on your screen what's been marked Government Exhibit 208. And Agent Hellman, this is about an 18- or 19-page document. But you just see the first page here. Do you recognize this?
>
> A. It appears to be a portion of the technical data that came along with the narrative.
>
> MR. DeFILIPPIS: All right. Your Honor, the government offers Government Exhibit

> 208.
>
> MR. BERKOWITZ: No objection.
>
> THE COURT: So moved.
>
> Q. And if we look at that first page there, Agent Hellman, what kind of data is this?
>
> A. It appears to be — as far as I can tell, it looks to be — it's log data. So it's a log that shows a date and a time, a domain, and an IP address. And, I mean, that's — just looking at this log, there's not too much more from that.
>
> Q. And do you understand this to be at least a part of the DNS data that was contained on the thumb drives that I think you testified about earlier?

All the while, he and DeFilippis referred to this as "a part" of the DNS data and referred to the thumb drives, plural.

And that, it appears, may be all the data anyone at the FBI ever analyzed.

Update: I erroneously said there were texts between Batty and Hellman that may have gotten deleted. I've corrected that error.

Update: I added details from the Lync files showing Batty provided a claim that conflicts with all public evidence about why he didn't check the thumb drives into evidence until after the investigation was substantively done.

Update: I've updated the table to show what Sussmann shared. Particularly given FBI's shoddy record-keeping and Durham's obfuscation, it's not clear on which drive GX209 was, nor is it clear whether there was a separate set of CSV DNS logs on the Blue Drive and if so how many logs they included.