JOSHUA SCHULTE KEEPS DIGGING: HIS DEFENSIBLE LEGAL DEFENSE CONTINUES TO MAKE A PUBLIC CASE HE'S GUILTY

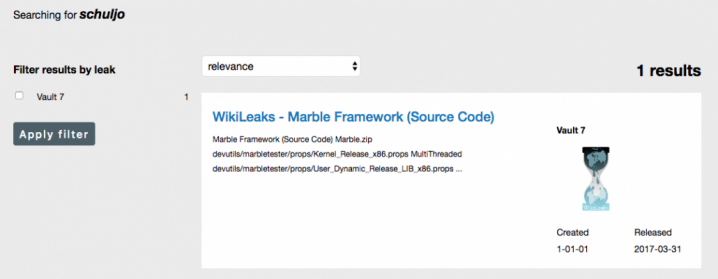
To defend him against charges of leaking the CIA's hacking tools to WikiLeaks, Sabrina Shroff has made it clear that Joshua Schulte is the author of the CIA's lies about its own hacking.

In a motion to suppress all the earliest warrants against Schulte submitted yesterday, Shroff makes an unintentionally ironic argument. In general, Shroff (unpersuasively) argues some things the government admitted in a Brady letter sent last September are evidence of recklessness on the part of the affiant on those earliest warrants, FBI Agent Jeff Donaldson. She includes most of the items corrected in the Brady letter, including an assertion Donaldson made, on March 13, 2017, that Schulte's name did not appear among those published by WikiLeaks: "The username used by the defendant was published by WikiLeaks," the prosecutors corrected the record in September 2018. To support a claim of recklessness, Schroff asserted in the motion that someone would just have to search on that username on the WikiLeaks site to disprove the initial claim.

> Finally, the Brady letter explained that a key aspect of the affidavit's narrative—that Mr. Schulte was the likely culprit because WikiLeaks suspiciously did not publicly disclose his identity—was false. Mr. Schulte's identity (specifically, his computer username "SchulJo") was mentioned numerous times by WikiLeaks, as a simple word-search of the WikiLeaks publication

> would have shown. See Shroff Decl. Exh. F at 7

If you do that search on his username — SchulJo — it only readily shows up in one file, the Marble Framework source code.



That file was not released until March 31, 2017. So the claim that Schulte's name did not appear in the WikiLeaks releases was correct when Donaldson made it on March 13. That claim — like most of the ones in the Brady letter — reflect the incomplete knowledge of an ongoing investigation, not recklessness or incompetence (Schulte has written elsewhere that he believed the FBI acted rashly to prevent him from traveling to Mexico, which given other details of this case — including that he hadn't returned his CIA diplomatic passport and snuck it out of his apartment when the FBI searched his place, they were right to do).

By sending her reader to discover that Schulte's name appears as the author of the Marble Framework, she makes his "signature" that of obfuscation — hiding who actually did a hack.

> Marble is used to hamper forensic investigators and anti-virus companies from attributing viruses, trojans and hacking attacks to the CIA.
>
> Marble does this by hiding ("obfuscating") text fragments used in CIA malware from visual inspection.
>
> [snip]
>
> The source code shows that Marble has test examples not just in English but also in Chinese, Russian, Korean, Arabic

> and Farsi. This would permit a forensic attribution double game, for example by pretending that the spoken language of the malware creator was not American English, but Chinese, but then showing attempts to conceal the use of Chinese, drawing forensic investigators even more strongly to the wrong conclusion, — but there are other possibilities, such as hiding fake error messages.

Marble was one of the files WikiLeaks — and DNC hack denialists — would point to to suggest that CIA had done hacks (including the DNC one) and then blamed them on Russia. In other words, in her attempt (again, it is unpersuasive) to claim that FBI's initial suspicions did not reach probable cause, she identifies Schulte publicly not just with obfuscation about a breach's true culprits, but with the way in which the Vault 7 leak — ostensibly done out of a whistleblower's concern for CIA's proliferation of weapons — instead has served as one prong of the propaganda covering Russia's role in the election year hack.

That's just an ironic effect of Shroff's argument, not one of the details in yesterday's releases that — while they may legally serve to undermine parts of the case against her client — nevertheless add to the public evidence that he's not only very likely indeed the Vault 7 culprit, but not a terribly sympathetic one at that.

Back when FBI first got a warrant on Schulte on March 13, 2017, they had — based on whatever advanced notice they got from Julian Assange's efforts to use the files to extort a pardon from the US government and the week of time since WikiLeaks had released the first and to that date only set of files on March 7 — developed a theory that he was the culprit. The government still maintains these core details of that theory to be true (this Bill of Particulars Schulte's team released yesterday gives a summary of the government's theory of the case

as of April 29):

- The files shared with WikiLeaks likely came from the server backing up the CIA's hacking tools, given that the files included multiple versions, by date, of the files WikiLeaks released
- Not that many people had access to that server
- Schulte did have access
- Not only had Schulte left the CIA in a huff six months before the WikiLeaks release — the only person known to have had access to the backup server at the time who had since left — but he had been caught during the period the files were likely stolen restoring his own administrator privileges to part of the server after they had been removed

But, after it conducted further investigation and WikiLeaks published more stolen files, the government came to understand that several other things that incriminated Schulte were not true.

> [T]he government appears to have abandoned the central themes of the March 13 affidavit: namely, that the CIA information was likely stolen on March 7–8, 2016, that Mr. Schulte was essentially "one of only three people" across the entire CIA who could have taken it, and that WikiLeaks's supposed effort to conceal his identity was

> telltale evidence of his culpability

There's no indication, however, that Donaldson was wrong to believe what he did when he first obtained the affidavit; Shroff claims recklessness, but never deals with the fact that the FBI obtained new evidence. Moreover, for two of the allegations that the government later corrected — the date the files were stolen and the number of people who had access to the server, Donaldson admitted those were preliminary conclusions in his initial affidavit (which Shroff doesn't acknowledge):

> It is of course possible that the Classified Information was copied later than March 8, 2016, even though the creation/modification dates associated with it appear to end on March 7, 2016.
>
> [snip]
>
> Because the most recent timestamp on the Classified Information reflects a date of March 7, 2016, preliminary analysis indicates that the Classified Information was likely copied between the end of the day on March 7 and the end of the day on March 8.
>
> [snip]
>
> It is, of course, possible that an employee who was not a designated Systems Administrator could find a way to gain access to the Back-Up Server. For example, such an employee could steal and use—without legitimate authorization—the username and password of a designated Systems Administrator. Or an employee lacking Systems Administrator access could, at least theoretically, gain access to the Back-Up Server by finding a "back- door" into the Back-Up Server.

Between the two corrections, the revised

information increases the number of possible suspects from two to five, out of 200 people who would have regular access to the files. A footnote to a later affidavit (PDF 138) describes that on April 5, 2017, FBI received information that suggested the number might be higher or lower. (I suspect Schulte argued in a classified filing submitted yesterday that even more people could have accessed it, not least because he has been arguing that in his various writings posted to dockets and other things,)

But, even though the Brady letter corrects the dates on which Schulte reinstated his administrator privileges for the Back-Up server slightly (he restored his own access on April 11, not April 14, which is when his managers discovered he had done so), Shroff only addresses his loss of privileges as innocent, without addressing that he got that access back on his own improperly.

More importantly, the motion doesn't address, at all, that Schulte kicked everyone else off one of his programs, the Brutal Kangaroo tool used to hack air gapped networks using thumb drives. Nor does it address allegations against Schulte made in August 2016 as part of his clearance review, including that his demeanor changed for the worse around February 2016, he might be "subject to outside coercion," and he tended not to abide by "guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems." There are other details in the affidavit — such as Schulte's attempt to learn what his former colleagues knew of the investigation — that support probable cause too (these may be among the things Shroff addresses in a classified filing).

That is, the probable cause that Schulte was the culprit was pretty strong even with the errors in the original affidavit, and none of the errors suggests malice or incompetence or even the recklessness Shroff alleges.

Shroff is right that the March 13 affidavit

doesn't offer as much probable cause to tie Schulte's home to the crime; but that's the magistrate's fault and fairly standard for computer crimes, not the FBI's. Shroff obscures the effect of FBI obtaining a second warrant to actually search the 150 storage media and computer devices they found in his home (a list of what they seized starts on PDF 116), as well as a second warrant to obtain child porn.

It is also true, as the defense argues, that the evidence to search for child porn was thin. But given that the government had a warrant to search the computer in question, and given precedents about child porn, that may not matter (though I think it is more likely to succeed than the rest of this). In any case, by the time of the main searches on child porn, three different magistrates had signed off on these searches.

This is a totally understandable attempt to get some of this evidence suppressed. But along the way the affidavits released yesterday provide a slew of damaging new details such as:

- Schulte conducted a ton of searches on Google in April 2016 about detecting USB insertion, copying big files, deleting files, preventing other admins from seeing what someone was doing on a LAN
- Schulte made a snapshot of (part of?) the LAN on April 20, 2016
- In early May, Schulte researched how to use Tor and Tails, which the government alleges he used to send the files
- On August 4, 2016 — the day

after Snowden sent this tweet — Schulte did a Google search for WikiLeaks for the first time ever (note, I believe the Snowden tweet may have been preparation for the misleading IG report on him released the following month)

- Between then and March 7, Schulte searched on WikiLeaks over 20 more times, reading hundreds of articles on it; but he didn't visit WikiLeaks for the first time until March 7, 2017, the first day the files posted; he also searched for that Snowden tweet

In short, just Schulte's Google searches alone provide very strong evidence that he's the Vault 7 leaker. Which explains why his attorneys are making what will probably be an unsuccessful attempt to claim the Google searches were overly broad and lacked probable cause (something Schulte wrote elsewhere seems to reflect that he has been told this will be treated under a Good Faith exception).

Schulte has been trying to disclose all these materials for over a year. But they really don't help his case.