THE DANCE BETWEEN JOSHUA SCHULTE AND WIKILEAKS

Way back when Joshua Schulte was first charged for leaking the CIA's hacking tools to WikiLeaks, I noted a loose coincidence between WikiLeaks' release, for the first time, of some of CIA's hacking source code rather than just development notes and the activity on Tor that led to Schulte getting his bail revoked. Since then, however, court documents have laid out a number of other interactions between Schulte and WikiLeaks. This post lays all of those out.

The government currently maintains that Schulte stole the CIA's hacking tools in late April 2016 and sent them (it's unclear whether they believe he sent them directly to WikiLeaks or not), using Tails, in early May. In court documents (the most informative warrant affidavit starts at PDF 129, though the FBI would revise some of its understanding of events after that time), that timeline is based off the searches Schulte did in Google (!!!) mapping out his actions.

> April 24, 2016: Schulte searches for a SATA adapter (which lets you connect a computer hard drive via a USB connection); Schulte searches how to partition a drive
>
> April 28, 2016: Schulte searches, for a second time, on how to restrict other admins from seeing parts of a LAN
>
> April 30, 2016: Schulte researches how to delete Google history, Western Digital disk wipe, and Samsung ssd wipe (the search of Schulte's apartment would find both Western Digital and Samsung drives)
>
> May 1, 2016, 3:20AM: Schulte searches on "how can I verify that a 1 tb file transferred correctly?"

> May 4, 2016: Schulte searches on “can you use dban on ssd,” referring to a wiping software called Darik’s Boot and Nuke
>
> May 6, 2016: Schulte researches Tor
>
> May 8, 2016: Schulte researches how to set up a Tor bridge

In August 2016, Schulte for the first time started tracking WikiLeaks coverage via a number of Google searches, but without visiting the site. He also researched Tails for a second time, as well as throwaway email.

Schulte’s first trackable visit to the WikiLeaks site itself was on March 7, 2017, the day of the first Vault 7 release (though WikiLeaks had started hyping it earlier, starting in February 2017).

From that first release on March 7 through September 7, WikiLeaks would release another Vault 7 release fairly regularly, often every week, other times at two week intervals and, at one point in June, releasing files on consecutive days. WikiLeaks then released the one and only Vault 8 file — source code rather than development notes — on November 9.

In general, that rhythm of releases is not obviously remarkable, though of course it took place against the background of serial efforts to get Julian Assange a pardon in the US.

But it intersects with the investigation of Schulte laid out in search warrant applications and other filings in a few key ways. As I’ll show in a follow-up, it’s clear that Schulte provided WikiLeaks with a story about the files to offer a rationale for their publication, so it’s clear that he did more than provide the files as a dead drop. After the first files dropped, he realized he’d be the prime suspect. Court filings reveal that he contacted a number of his former colleagues (using Google!), trying to find out what they knew about the

investigation, acknowledging that he would be a key suspect, and denying he had done the leak.

Then, between the first and the second Vault 7 release, on March 15, the FBI interviewed Schulte as they were searching his apartment. As part of that interview, Schulte lied to the FBI so as to be able to leave his apartment with the CIA diplomatic passport he had never returned (he had plane tickets to leave the country the following day). When he left his apartment, he told FBI Agents he'd be back in roughly an hour. He went to Bloomberg (where he still worked), stashed his passports there, and got on his work computer. 45 minutes after the time he said he'd return, the FBI found him leaving the lobby of Bloomberg, and on threat of arrest, got him to surrender his passports. After all this happened, Bloomberg did an analysis of what Schulte had done on his work computer and phones in this period; FBI seized his work hard drive in May 2017. If Schulte had on-going communications with WikiLeaks, this would have provided an opportunity to reach out to them to tell them he was under imminent threat of arrest.

From that point forward, the FBI asked Schulte new questions based off what had been released by WikiLeaks. Most notably, on June 29, they asked Schulte whether he altered Brutal Kangaroo, a file released by WikiLeaks just a week earlier, outside the CIA.

The rhythm of WikiLeaks' regular releases continued through August 24, when Schulte was arrested for child porn, with a file released that day, and another file released on September 7, while he was in jail. But after Schulte was released on bail after a September 13 hearing, WikiLeaks released no more Vault 7 files.

An April 2019 Bill of Particulars released last month strongly suggests there may be a tie between Schulte's Tor activities starting on November 16, 2017. The document suggests that Schulte *may have met with someone* on November 8, 2017, then lied to the FBI or prosecutors about

it 8 days later. Among the four lies the government described to substantiate False Statements and Obstruction charges in his indictment, it explains,

> On or about November 16, 2017, Schulte falsely described his trip to a court appearance from the vicinity of Grand Central Terminal to the vicinity of the courthouse, and also falsely claimed to have been approached on the way to that court appearance by an unknown male who allegedly stated, in substance and in part, that he knew that Schulte had been betrayed and bankrupted by the U.S. Government.

This incident almost certainly happened on November 8. As noted, he was arrested on August 24, 2017. He was denied bail at first (so remained in jail). But when he was arraigned on the first (child porn) indictment on September 13, he was granted bail, including house arrest. While he would have had to check in with Parole Officers, the next "court appearance" he had (because the first status hearing got delayed a few times) — and the only court appearance before November 16 — was on November 8. He'd have gone to his first and second arraignment from jail; he was only out on bail to travel to a court appearance from his home for that first status conference.

It seems likely that an FBI surveillance team tracked Schulte on that day doing *something* suspect between the time he left his home and arrived at the courthouse. The mention of Grand Central suggests he may have met someone there, though that's not dispositive because his apartment was just a few blocks away. But Schulte's description of meeting a man he didn't know, which the government alleges is false, seems like the kind of lie you'd tell if you were covering for meeting a man you *did* know. As noted, that probably happened on November 8.

On November 9, WikiLeaks released their single Vault 8 file.

Then, Schulte was asked, by some "law enforcement agents and/or prosecutor[] at the U.S. Attorney's Office" about the incident on November 16.

That same day that he was interviewed about the incident on the way to the courthouse, November 16, he got on Tor for the first of five times, as laid out in his detention memo.

> Separately, since the defendant was released on bail, the Government has obtained evidence that he has been using the Internet. First, the Government has obtained data from the service provider for the defendant's email account (the "Schulte Email Account"), which shows that the account has regularly been logged into and out of since the defendant was released on bail, most recently on the evening of December 6, 2017. Notably, the IP address used to access the Schulte Email Account is

> almost always the same IP address associated with the broadband internet account for the defendant's apartment (the "Broadband Account")—i.e., the account used by Schulte in the apartment to access the Internet via a Wi-Fi network. Moreover, data from the Broadband Account shows that on November 16, 2017, the Broadband Account was used to access the "TOR" network, that is, a network that allows for anonymous communications on the Internet via a worldwide network of linked computer servers, and multiple layers of data encryption. The Broadband Account shows that additional TOR connections were made again on November 17, 26, 30, and December 5.
>
> [snip]
>
> First, there is clear and convincing evidence that the defendant has violated a release condition—namely, the condition that he shall not use the Internet without express authorization from Pretrial Services to do so. As explained above, data obtained from the Schulte Email Account and the Broadband Account strongly suggests that the defendant has been using the Internet since shortly after his release on bail. Especially troubling is the defendant's apparent use on five occasions of the TOR network.

When it ultimately came time to explain away this use of Tor, Schulte pointed to a series of posts that would form part of what the government claims Schulte called an "information war" attempting to discredit the US government. That was first made broadly available when WikiLeaks posted it on June 19, 2018, the day after Schulte was charged with leaking the Vault 7 files.

The government alleges that a copy posted to Facebook later that year, on September 25, 2018, was posted by Schulte from his jail cell himself, using a contraband cell phone, which makes the WikiLeaks tweet part of Schulte's deliberate information campaign from jail.

And around the same time Schulte posted his diaries from jail, the government claims, Schulte was prepping to send Wikileaks materials from a fake FBI agent attesting that the Bureau had framed Schulte by planting child porn on his computer.

> iii. A document that appears to be an article for release by WikiLeaks.org ("WikiLeaks"), in which a purported FBI "whistleblower" claimed to have provided the discovery in this case to WikiLeaks and that the FBI had planted evidence of child pornography on Schulte's computer to frame him (the "Fake FBI Document").
>
> [snip]
>
> What appears to be a "to-do" list dated September 12, 2018, in which Schulte wrote that on September 17 and 18, he

> would “DL Disc. UL WL,” and.that on September 19, 20, and 21, he would “schedule tweets[.]” I believe that here, “DL Disc. UL WL” means that Schulte planned to download his discovery (”DL Disc.”) from the Schulte Laptop and upload that discovery to WikiLeaks (“UL WL”). As noted above, in another place in the Schulte Cell Documents, Schulte drafted the Fake FBI Document, a purported statement by a supposed FBI “whistleblower” who provided Schulte’s discovery to WikiLeaks and claimed that the FBI had planted evidence of child pornography on Schulte’s computer.

As I’ll show, Schulte gave WikiLeaks several claims it used to introduce the series in March 2017.

Then, several key events — an incident that probably occurred on November 8 which the government accuses Schulte of trying to cover up, WikiLeaks’ sole release of source code from the CIA, the interview at which Schulte allegedly lied about the November 8 incident, and some activity on Tor — makes it more likely the events are more than a coincidence.

And then WikiLeaks contributed early to Schulte’s “Information War,” and Schulte may have expected he could get WikiLeaks to cooperate again, with even more blatant disinformation.

That’s a fairly remarkable degree of coordination at a time when WikiLeaks was trying to coerce an Assange pardon and Schulte was (according to the government) trying to lie his way out of a great deal of legal trouble.