“UR SUBMISSION FORM IS TOO FUCKING SLOW, SPENT THE WHOLE DAY UPLOADING 1 GB.”

As I noted, one of the Roger Stone-related warrant applications released last week includes more details on the communications between the Guccifer 2.0 persona and WikiLeaks leading up to the DNC release. Emma Best examines the filing from a perspective of how someone, purportedly with no prior relationship to WikiLeaks, would go about transferring even a marginally significant submission to WikiLeaks. Almost a month of back-and-forth transpires between the first contact with Guccifer 2.0 and the successful transfer of the DNC files.

A key exchange, however, happened on July 6, 2016. After Guccifer 2.0 inquires whether WikiLeaks received some documents Guccifer 2.0 sent, the persona gets cranky because it took so long to upload a 1 GB file to WikiLeaks submission system. [I’m using Best’s conversion of this filing into a nifty transcription.]

> Guccifer 2.0: “fuck, [I] sent 4 docs on brexit on jun 29, an archive in gpg[.] ur submission form is too fucking slow, [I] spent the whole day uploading 1 gb”
>
> WikiLeaks: “We can arrange servers l00x as fast. The speed restrictions are to anonymise the path. Just ask for custom fast upload point in an email.”
>
> Guccifer 2.0: “will u be able to check ur email?”
>
> WikiLeaks: “We’re best with very large data sets. e.g. 200gb. these prove themselves since they’re too big to fake”

Almost two weeks into this exchange, WikiLeaks

says they can arrange for a custom server to transfer larger data sets — of around 200 GB.

These exchanges should, to a significant extent, be considered theater. Both sides of this conversation knew that the FBI would be watching all DMs between WikiLeaks and the Guccifer 2.0 persona. So it can't be taken as a definitive indication of how any files get sent.

Still, it shows how WikiLeaks would respond, using the public communication accounts, to a request to submit data in July 2016.

That's significant because it shows how things might have proceeded, two months earlier, when Joshua Schulte allegedly sent 1TB of data to WikiLeaks on May 1, 2016.

While the prosecution in Schulte's case provided forensic evidence to explain when he stole the CIA files and sent them to WikiLeaks, key gaps remain (perhaps most notably, how he got the files out of his building, though that may be because of certain classification decisions). And because Schulte used Tails and wiped his devices afterwards, there's no record of him actually sending the files.

Here's how prosecutor Matthew Laroche described that process in his closing arguments.

> Just as a general matter, you know this information was transmitted to WikiLeaks because they posted it on the internet. They obviously got it, and the question is when did he send it?
>
> And that's answered by what he did on the 30th and May 1. Let's look at the evening of the 30th.
>
> At 6:47 p.m., he is searching for Google history and Google view browsing history. He is concerned about what he's been searching for. On the evening, that night, he is searching for digital disk-wipe utility on several occasions, and at 10:52 p.m., he visits a website Kill

> Your Data Dead With These Tips and Tools. The defendant is interested in finding out how to securely delete information that might connect him to the leak, anything that he might've brought home with the leak on it, anything that he might've used to transfer it.
>
> And at 10:55 p.m., he runs a similar search for SSD wipe utility. And you'll remember all those hard drives that were recovered from his home. He was wondering how to wipe them to make sure that there was no evidence of his activities.
>
> Now, overnight, he continues working.
>
> At 12:19 a.m., the defendant mounted his D drive onto his virtual machine, the same D drive that had those encrypted files, data2.bkp through data6.bkp. They're in his D drive. He mounts his D drive.
>
> Then, overnight, he is constantly looking at his computer. On at least four occasions, he is unlocking his virtual machine in the middle of the night: 1:57 a.m.; 2:34 a.m.; 2:56 a.m.; 3:18 a.m. He is doing that because he is transferring data and he wants to make sure it's happened correctly. And you know that is the case because of the Google searches he runs at of the end the night and the early morning.
>
> At 3:18 a.m., just after he unlocks his screen saver, the defendant searches for How Long Does It Take to Calculate MD5?
>
> Remember, calculating an MD5 is a way to confirm that what you transferred from one place to another is the same, that it went correctly, that there were no errors. You calculate an MD5 to confirm that what you transferred transferred correctly, and that's what he's looking

> for at 3:18 a.m.
>
> Then at 3:21 a.m., the defendant visits a website, How Can I verify That a 1TB File – one terabyte file – transferred correctly?

That description is based off this forensic testimony from Michael Berger.

Prosecutors described this as happening overnight. Overnight transmission of a 1TB file using WikiLeaks' public submission site would be utterly impossible given the state of it at the time and the volume of data Schulte was transferring, and probably impossible regardless of how much time someone spent. Overnight transmission of 1TB of data using Tails, even to a dedicated server, would be difficult enough. Best describes that, "1 TB over Tor in one night is unlikely."

The government timeline does have Schulte in possession of the data earlier than that, potentially giving him a week to transfer the data, with this process describing just the end of the process.

Still, the way this would happen, normally, would be for WikiLeaks to set up a dedicated server to accept the files. And that would take prior communication. Such communication likely would have happened over Jabber, not Twitter (Schulte's opsec was piss poor in many ways but he did use Jabber).

Such a prior conversation is entirely consistent with testimony provided elsewhere, where prosecutors focused on the website's alternative submission process.

But the seeming necessity for prior communication before this transfer happened suggests Schulte's alleged theft and transfer of the files might not have been as reactive a decision as portrayed in his prosecution.

It would take premeditation to send WikiLeaks a 1TB file, whatever the timing. Prosecutors may

know that, and have an explanation for when such prior communications happened, but they're withholding those details for any of a number of reasons. Or it may be a big hole in this story. Schulte insists he didn't do it and a jury failed to convict.

One way or another, however, the state of the WikiLeaks' submission system as it existed in 2016 presents a big gap in prosecutors' current story.

Update: Two important details for those trying to figure out how long this transfer would really take. First, Schulte ran a commercial server specifically focused on video streaming at the time, so his upload speeds would not limit the transfer time at all. Second, Schulte at least claimed that hiding data for exfiltration was his speciality. That by itself wouldn't help him send stuff to WikiLeaks, at least not without prior contact. But it does mean that the means by which he transferred this file relied on tools he has developed at CIA.