20 QUESTIONS (PLUS 5): THE JOSHUA SCHULTE JURY IS LOST, POSSIBLY HOPELESSLY

According to InnerCity Press (virtually the only press covering the Schulte verdict watch), by end of day today the jurors had sent out 25 notes, most questions but also problems with two of the jurors. At the end of the day they told the Court they "aligned" on two of the charges, but were at an impasse on the other. Given that there's slam dunk evidence that he committed the least serious crimes (false statements and contempt), that suggests at least some members of the jury have reasonable doubt that the guy who wrote a virtual signed confession to committing the most damaging leak in CIA history actually did so.

I wanted to collect the known questions from jurors to give a sense of what issues have driven this uncertainty.

Note 1: A request for a summary of exhibits

Note 2: A request for a transcript of the testimony of David, a CIA Sysadmin, particularly as regards what jurors may have mislabeled 1209-8 (David testified about Schulte's failed attempt to access Altabackups with regards to exhibit 1202-8).

Note 3 asked 7 questions:

1. What is included in Count Three? We aren't sure what the purview is — articles, search warrants, tweets? This pertains to the Espionage Charge tied to posting classified information in one of his

diaries, sending a diagram of CIA's servers to WaPo reporter Shane Harris, and planning to reveal details about how a CIA hacking tool, Bartender, was used in the field (which certainly would expose CIA officers, and probably NOCs).

2. In 2015, when DevLAN went down, was Schulte called to fix the problem? How did he fix it? Schulte's lawyer, Sabrina Shroff, had made much of the fact that when Schulte was at a conference he got called about DevLAN going down. It's not directly related to any of his charges.

3. Can you please reread what was found on Schulte's home computer? This would have focused on deleted materials (and the lack of classified information), but given that Juror 5 almost certainly knew about the child porn allegations and there was a focus on Schulte's hosting of movies, this may have been what they were looking for.

4. Did GX 809 reference Schulte's taking a drug ("took my last piece")? If so, what was it? Was it

regular use? This refers to part of one page of his prison notebook in which he discusses taking his "last piece" and envisioning himself as a Cardinal. It is entirely unrelated to his charges.
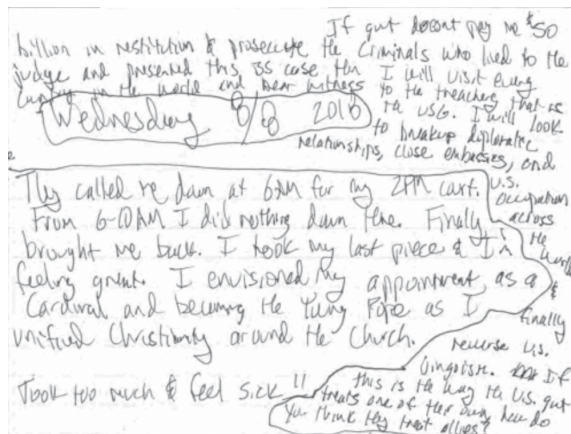
5. Is it confirmed that Schulte's been diagnosed with Aspergers Syndrome? One of the very senior CIA managers suggested to another that Schulte might have Asperbergers. It is entirely unrelated to his charges.

6. For Count One, is Altabackups inclusive of Brutal Kangaroo? Is it inclusive of OSB libraries? The backup that Schulte is alleged to have stolen included both the libraries (which were not leaked) and Brutal Kangaroo (materials on which were leaked), but it included far more, but

the parties did not answer
this because they weren't
sure whether this was a
network question or a
charging one.

7. Where were OSB libraries
housed/where did they live?
They were part of Stash.

Note Four: Can we please have simplified badge
times/formats for Schulte on 4/20/16 in a format
similar to GX 115. One piece of evidence that
Schulte did the reversion during which the
backup sent to WikiLeaks was stolen was that he
was the only one in his SCIF with his computer
during the time the commands doing the reversion
were entered into it. The badge records would
show that. Jurors did get simplified badge
records.

Note Five: In Exhibit GX 107, what does
lock/unlock computer mean in columns Source and
Type? Is the computer locking itself? What is
someone unlocking? This pertains to something
tracked on CIA badge records and was not
explained in testimony.

Note Six includes four questions:

1. Is there evidence that April
18 and 20 were the only two
times in 2016 that Schulte
left the vault last? April
18, the day Schulte
allegedly conducted
reconnaissance on the backup
files, and April 20, the day
he allegedly stole him were
the only two days he was the
last person in his SCIF at
RDB (the time period for
which may include just the

last seven months he worked at CIA).

2. What does mount the Altabackups mean? This refers to how the CIA networks were set up, and Schulte's role in doing that.

3. What does create data store mean? This pertains to testimony about one attempt Schulte made to regain access to files he had been booted from.

4. When someone logs out of a virtual machine, what happens to the log files from that session? There was no testimony on this point (jurors likely asked it to try to assess whether Schulte's buddy Michael could have stolen the files).

Note Seven (Exhibits 16-17, I think) asked for the transcripts of Michael Berger (the FBI forensics expert who presented evidence of Schulte's efforts to wipe evidence at home) and Michael (Schulte's buddy who took a screen cap of him deleting logs).

Note Eight: Jurors complained that one of the jurors, Juror 4, was not deliberating with the rest of the jury and coming in late.

Note Nine included two questions:

1. Can we please have testimony from Richard Evanchec. Evanchec is one of the FBI

agents that interviewed Schulte and searched his home, and so is central to the false statements charges.

2. What testimonies covered GX 1305-8 and GX 1305-9. Can we please have transcripts about that. These are Schulte's Google records, which Evanchec also testified about.

Note Ten: Juror five has prior information, probably including details of Schulte's child porn charges. She also looked up one of the lawyers. It became clear in a later sidebar that this is the juror who had said something inappropriate to another juror, possibly about deliberations, on February 13, during the trial.

Note Eleven included two questions:

1. What happened to Schulte's computers and workstation after he went to Bloomberg (after November 10)? This is likely a question testing a theory about whether someone — possibly Michael? — could have altered logs on Schulte's computer after he left on November 10, 2016.

2. When and where was Rufus's SSH key found? Was it found in the home directory or was it found forensically? Schulte had stored the key of someone, Rufus, who had had Admin access but left,

on his home directory. He used it when he was deleting logs on April 20. Sabrina Shroff had gotten one witness to testify that it was very easy to access other people's home drives, so this is likely another effort to test an alternate culprit theory.

There were two more questions today (which I'll update on Monday when that transcript is released):

- Something about the CFAA charge, suggesting jurors are *not* treating the reversion as a hack, but might be treating Schulte booting his colleague off Brutal Kangaroo as one.
- Something about unanimity on charges, possibly relating to the leaks from jail.

And then jurors told the court that they're only in agreement on two charges, but stuck on the others.

For the reasons I laid out here — as well as the two problem jurors — I'm not surprised about that. And given the questions, it seems clear that the extended focus on Schulte's employment disputes at the CIA made at least some of the jurors sympathetic to the idea that someone at CIA framed Schulte. Keep in mind, too, that Schulte adopted the moniker Jason Bourne in prison, so he fed that idea. And — as Shroff noted in her close — there was no good reason to focus on the continued employment disputes that extended two months after Schulte allegedly

stole the files.

When the CIA puts its formers on trial, in my opinion, it believes the general population will be as outraged by a violation of CIA's sacred trust as they themselves are. That may be why prosecutors aired that entire nasty employment dispute. But that's generally not the case outside of EDVA, especially not in SDNY.

Between that, and the forensic complexity of this case, it appears the jury is lost.

Reminder; Calyx Institute and other donors sprung for the transcripts of this trial.