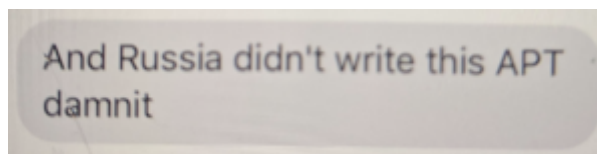


(PART OF) WHAT I SHARED WITH THE FBI

On July 28, 2016, something happened that would eventually lead me to the FBI.

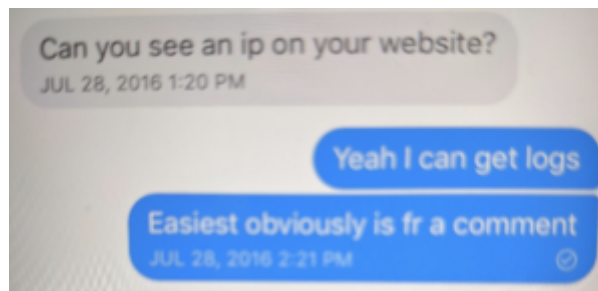
I'm going to explain part of that story now. I'm explaining it for several reasons. I had promised myself I wouldn't let another election pass without sharing what happened. Even now, I can't entirely make sense of it – that was part of the point, confusion. But the release of documents in the wake of the Mueller investigation has provided a great number of public details (some of which I laid out in my Rat-Fucker Rashomon series) with which this story *might* be consistent. I can't prove that this story explains the unanswered questions about the Roger Stone story (and Bill Barr's intervention in the Stone sentencing seems to have shut down some parts of any ongoing investigation to do so). But at least I can share details that may provide an explanation.

It started with a several-day dispute about attribution, starting on July 26, 2016, which included discussions about Guccifer and Crowdstrike. A guy I will refer to by the pseudonym Phil and I were texting on Signal debating that attribution. On the 27th, Phil disputed the Crowdstrike report that APT 28, which had done the hack, was GRU, "Russia didn't write this APT damnit."



I told him, vaguely, that I knew that entities external to both the DNC and Crowdstrike had evidence confirming the GRU attribution. I had a well-placed source who knew Phil was wrong. He seemed not only sure he could convince me otherwise, but intent on learning what I knew, which I didn't share.

The next day, July 28, 2016, Phil made up an excuse for wanting me to tell him what his IP address was—it was a bullshit excuse and doesn't matter for the purpose of this story. "Can you see an ip on your website," he asked. "Yeah I can get logs." I said, "Easiest obviously is fr a comment." (I was wrong about my ability to see the IP address, and he may have known that, because he had been testing how requests to my site worked for months.) "Now," he said, as he left a comment.



I forgot about the request until the next day, July 29, when another of the people who can approve first-time comments at the site emailed me with the comment, which had been posted moments after he had told me, "Now." "I debated about approving that comment by icelanderia in DNC Hack sourcing post," the person said. "But didn't because of the email addy attached to it." To readers of the public site, the comment read, "Just one phrase. Show me the metadata." It was signed "Icelanderia." Visible only to those of us with backstage access, however, it was signed guccifer2@kgb.ru.

Permalink: <https://www.emetvwheel.net/2016/07/28/on-reasonable-sourcing-for-dnc-hack-stories/#comment-704806>

Author

Name

Email

URL

Just one phrase. Show me the metadata.

Much later, Phil told me he liked leaving comments at my site as a, "Great outlet to talk to my usg pals." Until late 2017, we kept getting comments at the site which were consistent with disinformation deliberately left in the first Guccifer 2.0 releases, but which

might or might not have been him.

But I knew that first one, guccifer2@kgb.ru was Phil, purportedly left to find out what IP address his comments would show up as. He never did follow up to ask me whether I could see his IP address. And so I was left trying to figure out why the hell he signed a comment with the name of the persona who was trying to obfuscate what really happened with the DNC hack.

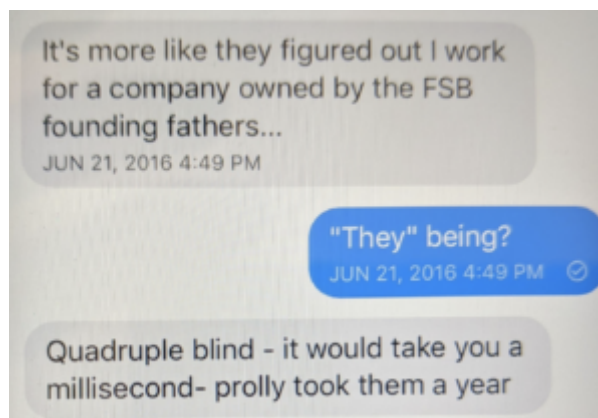
Normally, I don't think twice about comments left at my site under obviously fake names. Lots of people choose not to use their real email addresses when leaving comments at this site. Unsurprisingly, we've had a ton of comments claiming to use NSA email addresses. And from time to time – though, given how chummy and long-established emptywheel's comments section is and how closely we moderate obvious trolls, not all that often – people try to get funny with their log-in names.

In this case I did take notice. I did so, partly, because of how he had left it, giving me a heads up that it was him, but doing so in such a way that only I would know it was him (as noted, he never did ask me what IP he had come in under and, as I said, I was never able to determine that). But it also made me rethink stuff that had happened between us going back to fall 2015 and earlier, especially because of what had happened starting on June 14, 2016, the day that the Democrats publicly announced they had been hacked by the Russians, when he tried to get me to change my operational security even as he seemed to be debating about going forward with something, which he referred to in terms of "tapping out."

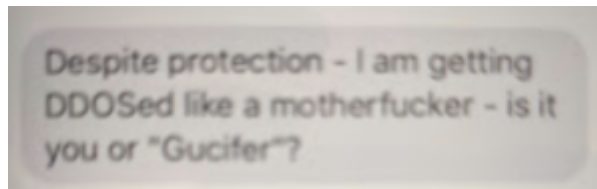
On June 14, 2016, the same day the Washington Post reported that the DNC had been hacked by Russia, Phil called me up and asked me to delete notes of conversations we had had going back to December 2015, notes telling a story about his life and motivations for being angry with the government that he had wanted me to tell after he died, which he claimed – starting in December

2015 – was going to be imminent. The next day, he claimed he believed he was being investigated by the FBI for the way he had narked out some people in April, which was his explanation for escalating levels of paranoia. That same day, he asked me to shift our comms to the Silent Circle text service, which would have put the texts beyond the reach of US law enforcement. This was at least the fourth effort he had made to shift to more secure comms than Signal and PGP email with me, including a highly inappropriate suggestion earlier that spring; each time, including this one, I blew off the request, because I didn't believe these conversations were that sensitive or interesting.

Starting at 3:12PM on June 21, the weirdness resumed. He asked me to change my PGP key, inventing a bullshit excuse, while explaining he was flipping his own keys. He showed me a traceroute on my site he had done, reflecting my recent addition of Cloudflare to protect the site (he had concocted an earlier traceroute in May 2016 that—I'm certain—was designed to make me paranoid). He advised me that when using a VPN, one should always choose a Swiss or even a Russian server. He told me he worked for a company owned by FSB's founding fathers.



Around 8:12PM on June 21, he claimed, "I am getting DDOSed like a motherfucker—is it you or 'Gucifer'?"



As far as I knew, he had no website to be DDOSed. As he surely knew, I didn't have the capability to DDOS anything. It was just word salad invoking the newly unveiled GRU persona, but amid the other weirdness I didn't make too much of it.

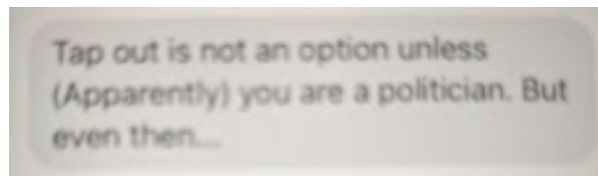
He then called me and repeated much of the story he had told me over the past six months, the story the notes of which he had, just a week earlier, asked me to destroy. In that retelling of the story, he would include several details about Russia (on top of the FSB founding fathers comment). He described a meeting he attended months before, overseas, one that (he claimed) members of Russian intelligence had also attended, where he had been physically beat up. Before that June 21 conversation, he had told me a version of that overseas meeting story at least 6 times, including telling me about the meeting in real time (in just two of those tellings do I remember him mentioning Russian intelligence, and precisely who in Russian intelligence he said attended was inconsistent). I'm not attesting that his claims about the meeting were true, I'm describing that he kept telling me about the meeting over the course of more than six months.

Another detail in that June 21 conversation was the way he insisted to me, as he had at least once before June 14, almost plaintively, that he hates Russia. Phil told me that two of his most cherished possessions were trophies from interactions with Russia. At the time, I didn't understand why he felt it was so urgent to convince me he really did hate Russia, but after the fact it seemed to be an effort to excuse himself, like emphasizing that he had been physically beaten.

There was a third story, too, another story

about an interaction with Russia more alarming than the others, another one he had told me once prior to June 14. The story involved a moment when Russians held "a gun to [his] head." I believe the story, as he told it to me, was a well-rehearsed lie, one he had told others. But if the lie served to explain away something else, it would be the kind of thing that might mean his comment might not be a joke, that he might have a role in the Guccifer 2.0 operation.

In June, this felt somewhat stalkerish. I still had no idea why he was telling me this, aside from the fact he wanted me to tell the story of his grievances with the government, but he was also in a bad place and I was trying to make sense of it. The next day, June 22, between 12 and 5PM ET, we spoke again on and off. When I suggested I might be under surveillance to see how he'd react, he said there were no rules, saying that no one could back out of a deal (I had no idea what deal he was talking about). "360 degrees of no rules, tap out is not an option unless (Apparently) you are a politician. But even then..."



The next day, June 23, just after 5PM, he told me he had been contemplating a line from a Cormac McCarthy screenplay: "The world in which you seek to undo the mistakes that you make, is different from the world where the mistakes were made." He added, within that same hour, "I'm done. I don't re-decide." Phil was, obviously, a mess, but he was also done talking about ways out of whatever mess he was in.

I broke off communication at that point for a period, but a week later, at 6:51PM on June 30, he was back. He told me he had "unfucked his problems."

As weird as all this was, in those days in June,

I was just observing, trying to figure out what had caused the sudden bout of paranoia, and honestly trying to figure out what he wanted out of me. I sure as hell didn't think, at the time, there was a tie between all that and the DNC hack (remember, he was claiming – probably another lie – that the FBI was investigating him, which I assumed was what all the weirdness was about).

But when I remembered all this on July 29, it made me reconsider whether there was a tie. As I've alluded to publicly in the past, it is why I spent six months on my part to test the Russian attribution for myself, to decide for myself whether the IC and CrowdStrike, along with people in tech companies and individuals who fought this hack personally with whom I'd spoken – were correct, that it had been the Russians, or whether what I took to be Phil's suggestion that he or people he knew, without the Russians, may have been involved. Absent such an effort, I assume that certain other people who've interacted with Phil have, instead, taken the existence of an American body claiming to have been involved as enough to deny Russian involvement. That may be what happened with Roger Stone.

Once I was convinced about the Russian attribution in December 2016 and given a growing certainty I couldn't test key parts of this story myself, I began to consider sharing it with the government in a way that protected both my identity and Phil's.

As I noted in the title, these events were just one part of the reason I went to the FBI in 2017, and not actually the most urgent reason at the time, nor the one I had most confidence in. There's another part of the election year attack – one few people know is related – that I believed (and still believe) he may have had a role in, too. Those other parts of this story were, in 2017, an escalating, ongoing threat, which is part of why I ultimately chose to meet with two FBI cyber agents and a prosecutor from

DOJ's National Security Division, to stop ongoing damage if I was right.

Now, four years later, it's clear the details Phil shared with me in 2016 might be consistent with several details discovered in the Roger Stone investigation. Indeed, starting in August 2018, Mueller's team appears to have investigated whether Stone had been co-present, in the US, with someone involved in this operation, and they also appear to have confirmed, after the Mueller team shut down, that Stone met with someone face-to-face at the RNC who gave Stone advance warning of the DNC drop. On July 15, 2016, Phil described to me flying east from the West Coast.

More interesting still is the way that Phil's activities over a key weekend in August 2016 overlap with Roger Stone's. I won't yet lay out how this timeline looks (I'll return to it). For now, compare the one I did in this post to the timeline I lay out here.

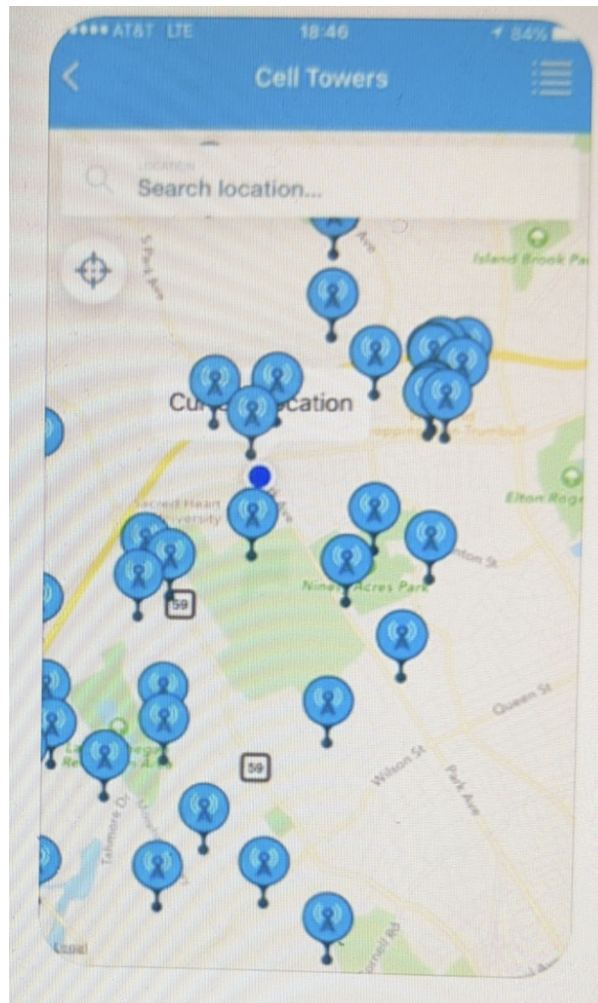
On August 12, 2016, the night that Guccifer 2.0 released DCCC documents the timing of which Jerome Corsi had predicted, Phil texted me at 11:32PM and told me he was thinking of going to the Trump rally that was scheduled – inexplicably, from a campaign strategy standpoint – in Roger Stone and Paul Manafort's home state of Connecticut the next day. "Should I stay or should I go..." he said, but he already had a ticket. At 9:46 AM the next morning, he said it again. "Trump rally [in CT] tonight, thinking of swinging by."

He did go, and made sure I had abundant contemporaneous record of it. At 4:21PM he told me he was close to the protest venue. At 4:33PM he told me he had put together an IMSI catcher for the event to track where the Secret Service had Stingrays.

Amid those texts, I told him that I had freed up the Guccifer comment at my site; I wanted to see how he'd react. "Haha-the mouthpiece," he responded. "'they' are clueless as I'm fond of

saying..." he added, which I took not only as confirmation that he did leave the comment, but also to mean that he believed the authorities misunderstood the Guccifer persona.

It was an hour, though, before the calls started. From 5:57PM to 6:58PM, he kept calling me and sharing video of what he was doing at a protest close to the rally (as well as a screenshot of the IMSI catcher).



At the time, I thought he was hoping to film himself picking a confrontation with the cops that would go viral. I thought it was really stupid and started ignoring his calls. It was actually years before I reviewed all these videos. When I did, I realized that he was not interacting with any of the protestors. He was, instead, just badgering the cops, in really controlled fashion. He was filming the confrontations so as to catch their name badges. And then, each of several times he did this, he would back off and thank the cops for what they

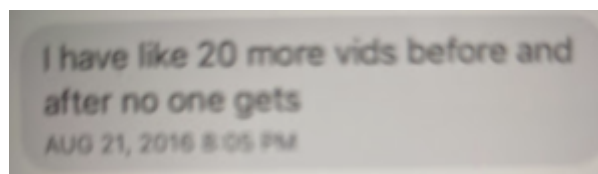
were doing. Those interactions would have left a handful of cops, whose names I'd have, who would have remembered him as the obnoxious guy at an event protesting Donald Trump.

At 9:59PM, he told me the rally itself was done, he was not in jail, and his phone was intact. He showed me a document that he had picked up at the rally.

The next morning, August 14, at 7:22AM, he texted me a picture to let me know he was in NYC. That was the day Jerome Corsi claims he started a file named "Podesta," that would eventually become posts that integrated documents publicly released in October.

Again, I didn't make much of this, as I didn't make much of earlier events.

Except that just over a week later, as part of a conversation from 7:56 to 8:28PM on August 21 (and so hours after Stone's famous "time in the barrel" comment), he emphasized to me that I was the only one whom he had sent videos from the August 13 protest. Then he said there were more. "I have like 20 more vids before and after no one gets," he told me. Something was interesting enough, both from before and after he attended the protest of the Trump rally, that was not only worth filming, but that was more sensitive than these protest videos.



Even as Stone and the persona Guccifer 2.0 were chatting away on Twitter over the weekend of August 12, a guy who'd just covertly signed his name "Guccifer2" on my site was at the Trump rally, taking videos of ... something.

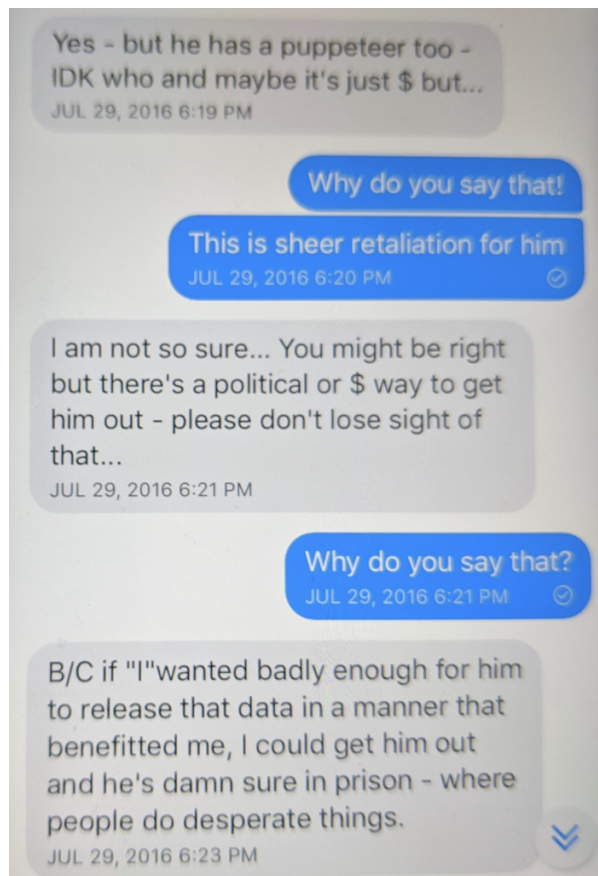
Not immediately, but over time, I've wondered what might be on those videos.

On January 1, 2017, in the wake of Trump boasting that, "I also know things that other

people don't know," about the Russian hack, I did a post wondering if what Trump thought he knew was the same thing that Craig Murray believed – that there was an American involved in this operation. I wrote, "I have a suspicion that Trump's campaign did meet with such a person (I even have a guess about when it would have happened)." I had the rally in mind. Within 30 minutes after I published the post, after having not spoken to me in weeks (he later told me he had been overseas), Phil called me, but hung up before we spoke.

Indeed, events that the investigation have since made public – including the confirmation that Roger Stone set about getting Julian Assange a pardon no later than 7 days after Trump won the election – made me revisit additional texts from July 29, ones I hadn't even paid attention to in real time.

On July 29, 2016 – the same day I was trying to figure out why this guy had just made a big deal of signing a comment guccifer2 – we had another conversation, one I believed at the time was unrelated, a discussion about what motivated Julian Assange. Revenge, I argued: the guy hates Hillary, going back to 2010. "Yes" Phil conceded, "but he has a puppeteer too – IDK who and maybe it's just \$ but." Again, I was sure this was "sheer retaliation for him." "You might be right," Phil responded, "but there's a political or \$ way to get him out – please don't lose sight of that..." I still didn't buy it, and asked again why. "B/C if 'I' wanted badly enough for him to release that data in a manner that benefitted me, I could get him out and he's damn sure in prison – where people do desperate things."



On that day in July 2016, no one in public knew there'd be a second dump. Certainly, no one knew that, on that day and the next, Roger Stone was in conversations with Trump's campaign manager planning how to optimize the next dump. "Good shit happening," Stone told Manafort just over an hour before this exchange, before the old friends spent 67 minutes on the phone together on July 30, their longest conversation of the year. No one knew that Stone would turn immediately to getting Assange out of the Embassy at least as early as November 15, probably even before.

But Phil, who had just made sure I knew he signed a comment Guccifer2, seemed to be sure of it before it all started.