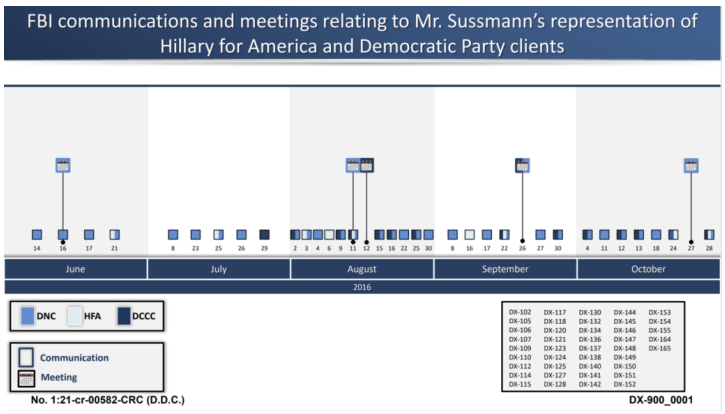
# FBI'S RUSSIAN HACK-AND-LEAK INVESTIGATION AS DISCLOSED BY THE SUSSMANN TRIAL

Now that he has been acquitted, it's easy to conclude the Michael Sussmann prosecution was a pointless right wing conspiracy theory. It was!

But the exhibits that came out at trial are a worthwhile glimpse of both the FBI's investigation into the 2016 Russian hack of Democrats and the Bureau's shoddy investigation of the Alfa Bank anomalies.

I've started unpacking what a shitshow the FBI investigation into the latter was here and collecting technical exhibits pertaining the investigation here (though that post is currently out of date).

As to the Russian hack-and-leak, Sussmann's team facilitated the process with a summary exhibit they included showing a selection of FBI communications pertaining to the investigation that either involve or mention Sussmann. Sussmann introduced these documents to show how obvious his ties to the Democrats would have been to the FBI, including to some people involved in the Alfa Bank investigation. A few of these communications refute specific claims Durham made, showing that meetings or communications Durham argued *must* relate to the Alfa Bank effort could be explained, in one case far more easily, as part of the hack-and-leak response. That is, some of these documents show that Durham was taking evidence of victimization by Russia and using it instead to argue that Sussmann was unfairly victimizing Trump.




Below, I've grouped the communications by topic (though a number of these communications span several topics). Note that Latham & Watkins' paralegal only used the last date on these communications, which I will adopt. But a number reflect a communication chain that extends months and includes dates that are far more important to the Durham prosecution.

Some of these files include topics that have attracted a great deal of often misleading coverage, such as the efforts to get server images from the Democrats. Importantly, by the time the FBI *asked* for server images, according to these communications, the only place to get them was at CrowdStrike.

> I don't believe DNC/DCCC have the images that CS took. Only CS have those. It's like paying ATM fees to your bank to get your cash. DNC/DCCC will be charged to get the images back.

After some discussion about who would pay CrowdStrike to create a second image, the firm offered to do it for free.

These communications also give a sense of the extent to which Democrats faced new and perceived threats all through the election. Given the communications below and some details I know of the Democrats' response to the attacks, I suspect these communications do not include real attempted attacks, either because they were not reported or because the report

went to FBI via another channel. While CrowdStrike attempted to ensure Sussmann was always in the loop, for example, that discipline was not maintained. And we know CrowdStrike found the compromise of the Democrats analytics hosted on AWS in September, a compromise that may only show up in these communications mentioned in passing. Some in the FBI seemed entirely unsympathetic to the paranoia that suffering a nation-state attack during an election caused, which couldn't have helped already sour relations between the FBI and Hillary's people.

Perhaps the most interesting communications — to me at least — pertain to efforts to authenticate the documents that got publicly posted and to identify any alterations to them. At least as laid out in these communications, the Democrats were *way behind* the public in identifying key alterations to documents posted by Guccifer 2.0, and it's unclear whether the FBI was any further ahead. But these discussions show what kind of alterations the Democrats were able to identify (such as font changes) as well as which publicly posted documents the FBI was sharing internally.

# FBI public statements

160614 DX102 A discussion of Jim Trainor's preparation for a meeting with Ellen Nakashima in advance of her June 14, 2016 reporting the hack and CrowdStrike's attribution. Among other things, they note Nakashima's confidence that GOP PACs were also targeted.

160725 DX112 This email chain between Sussmann and Trainor captured Sussmann's frustration that FBI made an announcement of an investigation into the DNC hack without first running the statement by Sussmann.

160729 DX117 Before FBI sent out a statement about the DCCC hack, Jim Trainor sent Sussmann their draft statement. In response, Sussmann complained that FBI said they were aware of media reports but not of the hack itself. The

timing of this exchange is important because Durham's team repeatedly described a meeting between Marc Elias and Sussmann that day pertaining to a server as relating to the Alfa Bank anomaly.

# Points of contact

160616 DX105 An email thread sent within FBI OGC (including to Trisha Anderson) discussing an initial meeting between Jim Trainor, Amy Dacey, Sussmann, and Shawn Henry.

160621 DX107 Starting on June 16, Amy Dacey thanked Assistant Director Jim Trainor for meeting with the Democrats about the hack. The thread turned into a confused request from the campaign for a briefing about whether they, too, had been compromised.

160725 DX114 This chain reflects Hawkins' confused response after Sussmann provided the contact information for a Hillary staffer with a role in technical security. Hawkins stated, "Nothing concerning HFA has come up."

160809 DX127 After Donna Brazile replaced Debbie Wasserman Schultz, Sussmann set up a meeting between her and Jim Trainor.

160811 DX128 An email chain among cyber FBI personnel discusses three Secret threat briefings for the DNC, DCCC, and Hillary campaign. Sussmann was scheduled to attend all three briefings, and Marc Elias was scheduled to attend the DCCC and Hillary briefings (though he testified that he did not attend).

160811 DX130 Sussmann sent the FBI notice of a public report of the DNC's establishment of a cybersecurity advisory board. The report was passed on to Jim Trainor.

# DHS outreach

160802 DX106 A Lync chain starting in the initial aftermath of the Nakashima story,

referencing an Intelligence Committee briefing, and discussing how to facilitate DHS assistance to the Democrats through Sussmann.

160802 DX120 With the goal of reaching out to the Democratic victims to offer assistance, DHS asked who the point of contact for both would be.

160816 DX125 This email chain documents DHS' "SitRep" of their understanding of the DNC/DCCC hacks and their efforts to reach out to help. This includes sharing of DNC/DCCC "artifacts" with NCCIC.

# Authentication and venue

160708 DX109 An email chain seeking DNC help authenticating a document released by Guccifer 2.0.

160723 DX110 A discussion starting on July 21 about authenticating and extending after the initial WikiLeaks dump. Hawkins observed, "Looks like there will be multiple releases on that [the WikiLeaks] front."

160802 DX118 After Adrian Hawkins asked CrowdStrike's Christopher Scott a question about a public report that the Democrats' analytics had been hacked, Scott explained that Sussmann had to be involved in any discussions between the FBI and their cybersecurity contractor. Hawkins also asked for specifics about the compromised servers that the FBI could use to establish venue.

160816 DX134 An email chain mentioning but not including Sussmann describes the efforts to establish venue (especially for Field staff who rely on laptops and travel a lot) as well as the efforts to authenticate documents.

160822 DX136 Two Lync messages describing a script that can be used to match WordPress documents with files stolen from the DNC.

160922 DX145 NSD's Deputy Chief of  Cyber, Sean Newell, asks Sussmann to meet to discuss some information requests from NDCA. They set up a meeting for September 26.

160930 DX147 Hawkins follows up on Newell's request for information with a much more detailed request from the San Francisco Division. This request includes details of the forensics NDCA was asking for, generally to include the CrowdStrike reports, network diagrams, logs, and images for the compromised hosts.

161004 DX148 In response to WikiLeaks promises about an upcoming file release, Newell follows up on a September 27 request he made of Sussmann for any files that were altered as well as a list of files that had been released but not circulated outside of the victim organizations first, including some indication whether those had been altered. Sussmann says they would have information available later that week.

161012 DX150 In another chain of responses to Newell's information request, someone at Perkins Coie passes on a description from the DCCC about how an image posted by Guccifer 2.0 differed from the file structure as it appeared on their server, including as it pertained to a file named, "Pelosi Vote Email."

161026 DX154 This chain is a follow-up to the Newell request, though it actually includes Guccifer 2.0 documents about Trump's taxes discussed. It includes description of an altered document published by Guccifer 2.0, in which the font was changed. It also includes a DOJ NSD person asking FBI to print out the document because they don't have any unattributable computers.

161024 DX165 This is yet another continuation of the Newell request, this one included the Trump Report altered by Guccifer 2.0. It includes some discussion of alterations to that document (as compared to unaltered ones released by WikiLeaks). It also describes documents that a

DNC research staffer believes were taken from his local desktop.

# CrowdStrike Reports

160815 DX132 Burnham to Farrar explaining there are two CloudStrike reports, one for the DNC and the other for the DCCC. The former is done, while the latter will be done soon.

160825 DX137 Hawkins asks Sussmann about the DNC CrowdStrike report, Sussmann explains it's still a few days away, but then the next day says he's reading "it" (which may be the DCCC report). Sussmann's response gets forwarded to a few more people.

160830 DX 138 A Lync chain conveying that Sussmann had alerted the FBI that the CrowdStrike report was done and asking if WFO should pick it up.

# Server images

161013 DX151 In another chain of responses to Sean Newell's information request, the discussion turns from Sussmann's effort to make sure the Democrats respond to all the FBI's data request to how to obtain images (whether to have CrowdStrike spend 10 hours to do it or let FBI onsite to do it themselves). As part of this chain, Sussmann says that "in theory" the Democrats would be amenable to letting the FBI onsite to image the serves themselves, but then checks to see whether the data is at CrowdStrike or the DNC.

161013 DX152 This chain is follow-up to the request for server images. Sussmann connects the FBI and CrowdStrike, CS offers to image the servers for free, and the FBI provides the address where to send them.

161028 DX153 A Lync that starts with Newell requesting someone attend the October 11 meeting with Sussmann, continues through a discussion about how to get images of the compromised

servers (including whether Sussmann may have misinterpreted the ask), and includes a discussion about a re-compromise.

# Lizard Squad ransomware threat

160803 DX121 Late night on August 2, Sussmann reported a ransomware threat from the Lizard Squad. This email discusses the various equities behind such a threat and involves a guy named Rodney Hays, whom the Durham team would at one point insist must be Rodney Joffe.

160806 DX124 This chain reflects more of the response to Sussmann reporting a ransomware threat from Lizard Squad. As noted, it involves a guy named Rodney Hays that Durham's team insisted must be Joffe.

160922 DX144 Over a month after the Democrats reported the Lizard Squad threat, Eric Lu wrote up the intake report, including the bitcoin address involved and Sussmann's email to Rodney on August 9 thanking him for his assistance.

# Other threats

160726 DX115 Sussmann set up a meeting with Hawkins and others so someone could report "some offline activity related to the intrusion." This was around the time when Ali Chalupa believed she was being followed, though nothing in this chain describes the threat.

160908 DX140 On August 26, EA Hawkins wrote Sussmann directly alerting him to a new phishing campaign targeting Democrats. On September 7, he wrote back with three accounts that may have been targeted.

160916 DX141 Moore emailing Josh Hubiak – a cyber agent in Pittsburgh – asking for contact information for Michael Sussmann so she can obtain the contact information for a DNC bigwig whose Microsoft Outlook account was compromised,

apparently by APT 28. Hubiak is one of the agents also involved in the Alfa Bank investigation.

160917 DX142 The day after the request for contact information for the DNC bigwig, there's further discussion about how to contact him. The FBI also shares new files reflecting the network share for a different DNC person, a former IT staffer, that was uploaded to Virus Total.

160927 DX146 In response to public reports that some Democratic phones may have been targeted and a potential compromise of Powell's phone (probably Colin, whose communications were posted to dcleaks), there's some chatter about what information is available from Apple and Google. One of the key agents involved complains that, "it would be awesome if Google helped out, as I know they are at least 2 steps ahead of me and I'm in a sad, losing game of catchup."

161011 DX149 This seems to be a collection of Lync notes from October 11, showing three different issues pertaining to Sussmann happening at once: the transfer of custody of the thumb drives to the Chicago office, a reference to a meeting with Sussmann, and a report of a new Democratic concern about exposed Social Security numbers.

161230 DX155 A Lync chain that goes from October 28 through December 30 covering the concern about a bug at DNC HQ, the response to the NYT article naming Hawkins, and another compromise alert.

161017 DX164 This may be a summary prepared for Mother Jones. Whatever the purpose (there is no date), it describes the timeline of FBI's response to a request for a sweep of DNC headquarters in response to some anomaly. Sussmann permitted the sweep but asked that it be done covertly, so as not to alert DNC staffers.

# Crossfire Hurricane

160804 DX123 On August 4, Joe Pientka forwarded the original June 14 Nakashima story to the agents who had just been assigned to the Crossfire Hurricane team with the explanation, “Just going through old – possibly pertinent emails.”