OCKHAM'S CUT: HOW THE ANDREW MCCABE NOTES WERE DOCTORED

Some weeks ago, I asked for help understanding the irregularities of the Andrew McCabe notes. Among other observations, two people showed that the notes had been created in layers, with the redaction of the protective order footnote seemingly added twice. Since then, longtime friend of the site "William Ockham" has done more analysis (he was the tech expert identified in the second post), and determined that the file must have been made as part of a multi-step process. I share his analysis here. The italics, including the bracket, are mine, the bold is his.

> Here's what I can say about the McCabe notes. The easiest way to explain this is to think about the ancestral tree of the images that are embedded in the documents we have. It all starts with the original page from McCabe's notes *(Generation 0)*.
>
> Someone scanned that page to create an unredacted image file *(Gen 1)*.
>
> That image was printed *(Gen 2)*. {From a technical point of view, this is what happens when a page is copied on a modern copy machine. Based on the evidence I have, I'm fairly sure that a digital image of the original page must exist. If not, it sucks to be the FBI.)
>
> An analog redaction (probably with a black Sharpie or similar instrument) was applied. I strongly suspect that the date was added to the same physical page **before it was rescanned**. It's possible, although I consider it very unlikely, that the date was added after the physical page was rescanned. These original redactions aren't totally black

the way they would be if done with the DoJ's redaction software. In any event, this rescanned image is *Gen 3*.

That physical page with the date was scanned to an image file (*Gen 4*).

At this point, a PDF file that will become 170510-mccabe-notes-jensen-200924.pdf is created by embedding the Gen 4 image and saving the file as a PDF. Then, a separate process adds the words "SUBJECT TO PROTECTIVE ORDER" and "DOJSCO – 700023502" to the metadata inside the file and draws the words in a font called "Arial Black" at the bottom of that page and the file is saved again. ***I am 100% certain that a PDF was created exactly like I describe here***

Update from Ockham to describe how the redaction shows up in the DOJ footnote:

A PDF file is really a software program that has instructions for rendering one or more pages. An image similar to the one above *[Gen 4]* was turned into a PDF file which contained one set of instructions:

1. *Store about 1 megabyte of compressed data.*
2. *Take that data and render an image by interpreting the data as an 8bit per pixel grayscale image 1710 pixels wide by 2196 pixels high (at normal 96 pixels per inch, 17.81 in by 22.87 in, so obviously scanned at a much higher*

    resolution)
3. *Scale that image so it takes up an entire 8 ½ by 11 page*
4. *Render the image*

Then, an automated process adds the footer. The part of the instructions for rendering the Bates number are still in the document and look like this:

Operation	Description	Operands
Dictionary	E.g.: /Name << … >>	/Artifact<</Contents (DOJSCO – 700023502)/Subtype /BatesN /Type /Pagination >>
BDC	(PDF 1.2) Begin marked-content sequence with property list	
q	Save graphics state	
cm	Concatenate matrix to current transformation matrix	1001458.234985434.7999268
gs	(PDF 1.2) Set parameters from graphics state parameter dictionary	/GS0
Tr	Set text rendering mode	0
Tf	Set text font and size	/T1_031.5 [This is a pointer to a font name and size, Arial Black – 18PT]
Do	Invoke named XObject	/Fm0 [This is a pointer to the actual text and location to render it
Q	Restore graphics state	
EMC	(PDF 1.2) End marked-content sequence	

Originally, there would have been a similar set of instructions for the “SUBJECT TO PROTECTIVE ORDER” part as well. They would have looked almost the same except for the “Artifact” operands,

the actual text, and the positioning instruction.

Now, here's the really important part. The DoJ redaction software presents the rendered PDF file to the end user. However, it operates on the actual PDF by rewriting the instructions. When the user drew the rectangle around the words "SUBJECT TO PROTECTIVE ORDER", the redaction software has to find every instruction in the PDF that made changes to the pixels within the coordinates of the rectangle. The redaction software sees two "layers" of instructions that affect the rectangle, the text writing instructions and the image itself. The redaction software removes all the instructions for writing the text and replaces those instructions with instructions to draw a black box in the same place. Then, it also blacks out the pixels in the image itself. It has to do both of those things to ensure that it has removed all of the redacted information, even though in this case it didn't really need to do both.

Then someone at the DoJ opens the PDF and redacts the words "SUBJECT TO PROTECTIVE ORDER" from the page. The redaction does all of the following things:

- *It removes the metadata entry with the words "SUBJECT TO PROTECTIVE ORDER",*
- *It removes the commands that draw the words.*
- *It replaces those commands with commands that draw a black rectangle the same size*

> *as the rendered words.*
> - *It replaces the pixels in the Gen 4 image that correspond to the area of the image that **the words were drawn on top of** with solid black pixels.*
>
> Those last two steps create two very slightly offset redaction boxes. The slight offset is caused by errors caused by using floating point math to draw the same shape in two different coordinate systems. Step 4 creates an image which I'll call *Gen 5* which can be extracted from 170510-mccabe-notes-jensen-200924.pdf.
>
> When someone notices that this file and the Strzok notes have been altered, Judge Sullivan asks for the unaltered versions. Jocelyn Ballantine has a problem. There's no redacted version of McCabe's notes without the added date. She can't use the DoJ's redaction software because that would look even worse (a big black rectangle where the date was added). What's a stressed out assistant US Attorney to do? Here's what she did. She took the unredacted PDF file I mentioned above and converted it to an image. Then she used image editing software to remove the date, which made that rectangle of white pixels. She fires up Microsoft Word on her DoJ work computer and starts creating a new document (likely from a template designed creating exhibit files). The first page just says Exhibit A and on the second page (which has all margins set to 0) she pastes in the image she just created, scaled to fit exactly on the page. Without saving the Word file, she prints the document (using the Adobe

> Distiller print driver) to PDF and submits the printed file as the supposedly unaltered McCabe notes. *[Gen 6]*

It seems like these steps look like this:

Gen 0: FBI had or has McCabe's original notes presumably stored with his other documents.

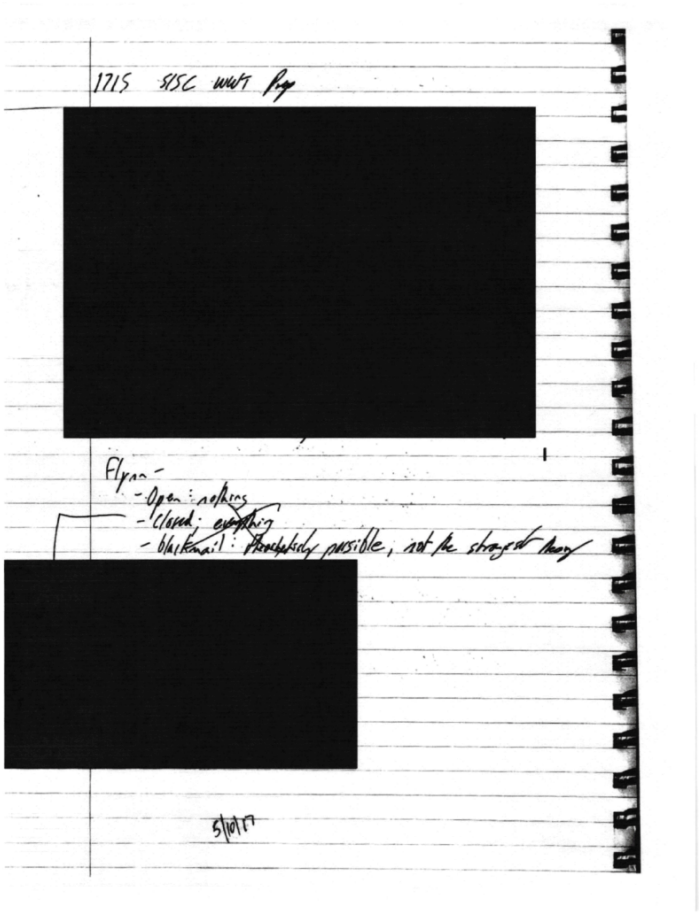
Gen 1: Someone took the notes from there and scanned them, presumably to share with other investigators.

Gen 2: Someone printed out Gen 1 and made notes and otherwise altered them. This is the stage at which the government claims someone put a sticky note with a date on the notes, but it appears they just wrote the date on the notes themselves. If everything had been operating normally, however, when Judge Sullivan asked for unaltered copies of the documents, they could have used the Gen 1 copy to resubmit. They didn't do so, which suggests the chain of custody may have already been suspect. Some possible explanations for that are that Jeffrey Jensen's team received the document from either DOJ IG or John Durham's investigation, not directly from the FBI files. That wouldn't be suspect from the standpoint of DOJ internal workings, but it would be proof that DOJ knew the documents they relied on in their motion to dismiss had already been reviewed by Michael Horowitz or Durham's teams, and found not to sustain the conspiracies that Billy Barr needed them to sustain to throw out Flynn's prosecution (or that DOJ claimed they sustained in the motion to dismiss).

Gen 3: I think Ockham is viewing the creation of the image file in two steps. First, a scan of the file with the note written on it is made, which is Gen 3.

Gen 4: Then, probably before the file is handed off to Jocelyn Ballantine to "share" with Mike Flynn's team (I'm scare-quoting because I suspect there may have been a back channel as

well), the redaction is created for where the protective order stamp would go. Here's what Gen 4 would have looked like:



Gen 5: Gen 4 is then prepared as an exhibit would normally be, by putting it into a PDF and adding the Bates number and protective order stamp, then redacted the latter. Reminder: The protective order footer was also redacted from (at least) the two altered Strzok notes, as I show here.

Gen 6: When Peter Strzok and McCabe tell Sullivan that their notes have had dates added, DOJ re-releases the notes such that the notes are no longer added but the redacted footnote is. As Ockham notes (and as I think everyone who looked closely at this agrees) the date is not removed by taking off a post-it. Instead, it is whited out digitally, leaving a clear mark in the exhibit.

One reason this is so interesting — besides providing more proof that DOJ went to some lengths to make sure a version of these notes

did not include the protective order, freeing Sidney Powell to share it with Jenna Ellis and whomever else she wanted, so they could prepare campaign attacks from it — is that DOJ refused to say who added the date to McCabe's notes. As I noted in my own discussion here, one possible explanation why DOJ kept redacting stuff rather than going back to the original (other than having to submit the file for formal declassification and the post-it hiding other parts of the document) is because the chain of custody itself would undermine the claims DOJ has made in the motion to dismiss, by making it clear that someone had already reviewed this document and found no criminal intent in the document.

The other problem with this multi-generation alteration of Andrew McCabe's notes is, if anyone asks, it is going to be very difficult for anyone involved to disclaim knowledge that these documents were altered. Mind you, Ballantine already has problems on that front: I emailed her to note that the FBI version of Bill Barnett's "302" she shared redacted information that was material to Judge Sullivan's analysis, the positive comments that Barnett had for Brandon Van Grack. So if and when Sullivan asks her why DOJ hid that material information from him, she will not be able to claim she didn't know. Then there's her false claim — which both Strzok and McCabe's lawyers have already disproved — that the lawyers affirmed that no other changes had been made to the notes.

But if this file was prepared as Ockham describes, then both DOJ and FBI will have a tough time claiming they didn't know they were materially altering documents before submitting them to Judge Sullivan's court.

Updated with some corrections from Ockham.