JOHN DURHAM'S LIES WITH METADATA

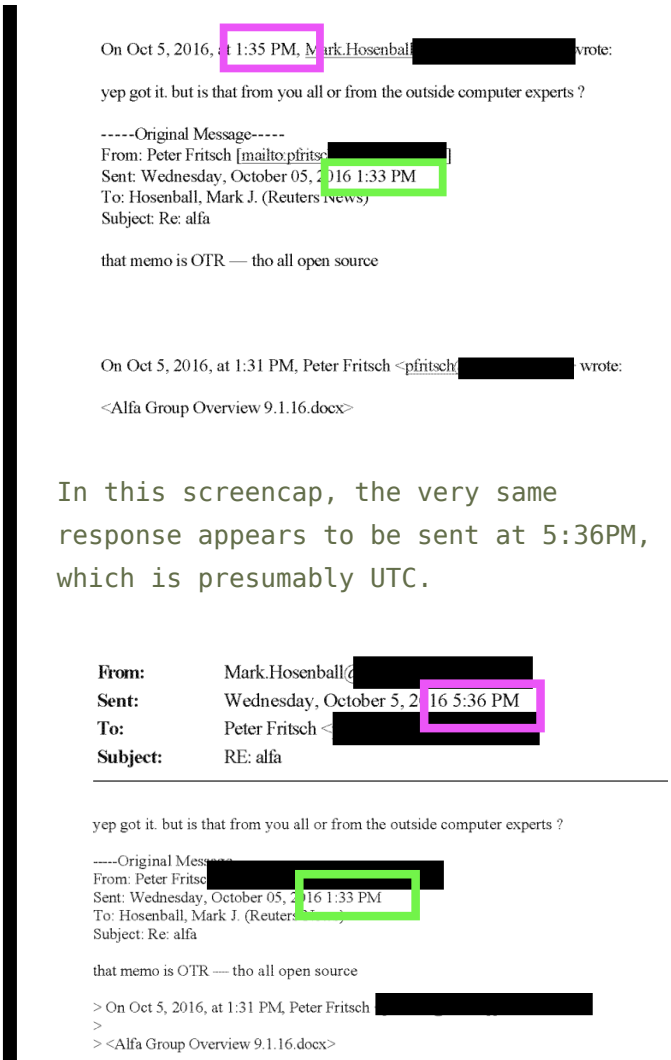
Thanks to those who've donated to help defray the costs of trial transcripts. Your generosity has funded the expected costs. If you appreciate the kind of coverage no one else is offering, we're still happy to accept donations for this coverage — which reflects the culmination of eight months work.

I'd like to thank John Durham for showing us back in April how he was going to mislead the jury with metadata.

He appears to have done just that, yesterday, with several exhibits entered into evidence. And I fear that unless Durham's lie is corrected, he will gravely mislead the jury.

As I pointed out in April, because of the email system at Fusion GPS, the first email in any thread they produced to Durham renders as UTC; the rest render as ET. So, for the emails on which one could check, the first email in every thread they released in April was four hours later than the time the email was actually sent.

> Durham has revealed that his exhibit has irregularities in the emails pertaining to a key issue: whether Fusion sent out a link to April Lorenzen's i2p site before Mark Hosenball sent it to them.
>
> This shows up in the timestamps. In the exhibit, the lead email for each appearance appears to be set to UTC, whereas the sent emails included in any thread appear to be set to ET.
>
> For example, in this screencap, the time shown for Mark Hosenball's response to Peter Fritsch (the pink rectangle) is 1:35 PM, which is presumably Eastern Time.



On Oct 5, 2016, at 1:35 PM, Mark.Hosenball[redacted] wrote:

yep got it. but is that from you all or from the outside computer experts ?

-----Original Message-----
From: Peter Fritsch [mailto:pfritsc[redacted]]
Sent: Wednesday, October 05, 2016 1:33 PM
To: Hosenball, Mark J. (Reuters News)
Subject: Re: alfa

that memo is OTR — tho all open source

On Oct 5, 2016, at 1:31 PM, Peter Fritsch <pfritsch[redacted] wrote:

<Alfa Group Overview 9.1.16.docx>

In this screencap, the very same response appears to be sent at 5:36PM, which is presumably UTC.

From: Mark.Hosenball[redacted]
Sent: Wednesday, October 5, 2016 5:36 PM
To: Peter Fritsch <[redacted]
Subject: RE: alfa

yep got it. but is that from you all or from the outside computer experts ?

-----Original Message-----
From: Peter Fritsc[redacted]
Sent: Wednesday, October 05, 2016 1:33 PM
To: Hosenball, Mark J. (Reuters [redacted])
Subject: Re: alfa

that memo is OTR — tho all open source

> On Oct 5, 2016, at 1:31 PM, Peter Fritsch [redacted]
>
> <Alfa Group Overview 9.1.16.docx>

Both instances of Peter Fritsch's email (the green rectangle), "that memo is OTR—tho all open source," show at 1:33PM, again, Eastern Time.

To be clear: this irregularity likely stems from Fusion's email system, not DOJ's. It appears that the email being provided itself is rendered in UTC, while all the underlying emails are rendered in the actual received time.

That means if you show someone *only* the first email in a thread, you will be misrepresenting what time that email was sent.

That's what Durham did yesterday with a bunch of Fusion-produced emails he submitted during Laura Seago's testimony, including (but not limited to):

- October 5, 2016, 5:23PM: re: so is this safe to look at?
- October 5, 2016, 6:33PM: Fwd: alfa
- October 5, 2016, 6:57PM: Re: Alfa
- October 5, 2016, 7:02PM: Re: Alfa
- October 17, 2016, 4:04PM: memos
- November 1, 2016: What the other side is saying
- November 3, 2016: Foer Follo

Over and over, Andrew DeFilippis showed these to Laura Seago and asked *her* to state what date and time the emails were.

> MR. DeFILIPPIS: Okay. And, Your Honor, if there's no objection from the defense, we'll offer Government's Exhibit 612.
>
> MR. BERKOWITZ: No objection.
>
> THE COURT: So moved.
>
> Q. Okay. So what is the date and time of this email?
>
> A. October 5, 2016, at 5:23 p.m.
>
> Q. And the "Subject" line?
>
> A. "Re: so is this safe to look at" – excuse me – "so this is safe to look at."

While these emails appear to have been produced to Durham at a later time (their Bates numbers *from* Fusion are about 3000 pages off some of the earlier ones), they're from the same series and produced by the same custodian, so we should assume that the same anomaly that existed on the earlier ones exists here.

Seago hasn't seen these emails for years and — because they were treated as privileged — she can only see the first email in a thread, even if there are replies in that thread (and there clearly are, in some of them). She had no way of knowing if she was looking at UTC time!

But Andrew DeFilippis surely does. Indeed, he's prepping an attack on Sussmann for not understanding that Durham turned over Lync files from the FBI without making clear they, also, get produced in UTC. So he's aware of which exhibits he has sent to Sussmann without clarifying the correct time. Yet over and over again, DeFilippis asked Seago what time these emails were sent, even though he likely knows (especially since these are files that are no longer privileged, so he has seen those that are threads) that he was deceiving her.

And the timing of these Fusion emails — and possibly some earlier ones exchanged with Rodney Joffe — almost certainly matter.

As I showed in my earlier post, because Durham didn't fix the anomaly in these emails, they have created the false impression that an October 5 email from Mark Hosenball that shared public links to Tea Leaves' files came in after Fusion sent it out to Eric Lichtblau. They appear to be prepping another deceit, this one conflating a link that Hosenball sent with one Seago found on Reddit.

Assuming the emails released yesterday share this same anomaly, here's how the timeline would work out. I've bolded the ones that would be grossly misleading taken out of order.

5:23PM (could be 1:23?): Seago to Fritsch, Is this safe?

1:31PM: [not included] Fritsch to Hosenball email with Alfa Group overview

1:32PM: Fritsch sends Isikoff the September 1, 2016 Alfa Group overview (full report included in unsealed exhibit)

1:33PM [not included] Fritsch to Hosenball, “that memo is OTR – tho all open source”

1:35/1:36PM: Hosenball replies, “yep got it, but is that from you all or from the outside computer experts?”

1:37PM: Fritsch responds,

> the DNS stuff? not us at all
>
> outside computer experts
>
> we did put up an alfa memo unrelated to all this

1:38PM: [not included] Hosenball to Fritsch:

> is the alfa attachment you just sent me experts or yours ? also is there additional data posted by the experts ? all I have found is *the summary I sent you* and a chart… [my emphasis]

1:41PM: [not included] Fritsch to Hosenball:

> alfa was something we did unrelated to this. i sent you what we have BUT it gives you a tutanota address to leave questions. 1. Leave questions at: tea.leaves@tuta.io

1:41PM: [not included] Hosenball to Fritsch:

> yes I have emailed tuta and they have responded but haven’t sent me any new links yet. but I am pressing. but have you downloaded more data from them ?

1:43PM: [not included] Fritsch to Hosenball, “no”

1:44PM: Fritsch to Lichtblau:

> fyi found this published on web … and downloaded it. super interesting in context of our discussions
>
> [mediafire link] [my emphasis]

2:23PM: [not included] Lichtblau to Fritsch, “thanks. where did this come from?”

2:27PM: [not included] Hosenball to Fritsch:

> tuta sent me this guidance
>
> [snip]
>
> Since I am technically hopeless I have asked our techie person to try to get into this. But here is the raw info in case you get there first. Chrs mh

2:32PM: Fritsch to Lichtblau:

> no idea. our tech maven says it was first posted via reddit. i see it has a tutanota contact — so someone anonymous and encrypted. so it’s either someone real who has real info or one of donald’s 400 pounders. the de vos stuff looks rank to me … weird

6:33PM (likely 2:33PM): Fwd Alfa Fritsch to Seago

6:57PM (like 2:57PM): Re alfa Seago to Fritsch

7:02PM (likely 3:02): Re alfa Seago to Fritsch

3:27PM: [not included] Fritsch to Hosenball cc Simpson: “All same stuff”

3:58PM: [not included] Hosenball to Fritsch, asking, “so the trumpies just sent me the explanation below; how do I get behind it?”

4:28PM: [not included] Fritsch to Hosenball, “not easily, alas”

4:32PM: Fritsch to Hosenball, cc Simpson:

> Though first step is to send that explanation to the source who posted this stuff. I understand the trump explanations can be refuted.

What Durham will completely and utterly misrepresent if it doesn’t clarify this anomaly (and this is the second time they have declined to) is that Seago and Mark Hosenball both accessed different packages of the Tea Leaves materials, one of which then got sent out to Lichtblau. Between 2:33 and 2:57, Seago appears to have compared the files and told Fritsch, who then told Hosenball, that the packages were “all the same stuff.”