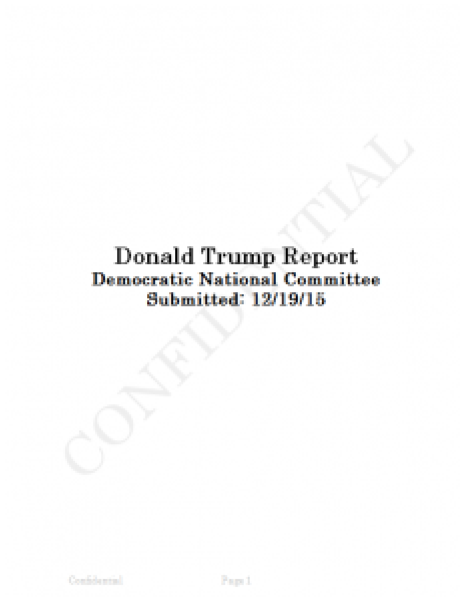
ON METADATA AND MANIPULATION: THE FIRST GUCCIFER 2.0 DOCUMENTS

In the AP's (very worthwhile) coverage of the data it obtained from Secureworks it reveals at least the fifth piece of deception pertaining to the first documents released by Guccifer 2.0 on June 15, 2016. It revealed that Guccifer 2.0 added the word "confidential" (possibly as both the watermark shown on the front page and in the footer) to this document.

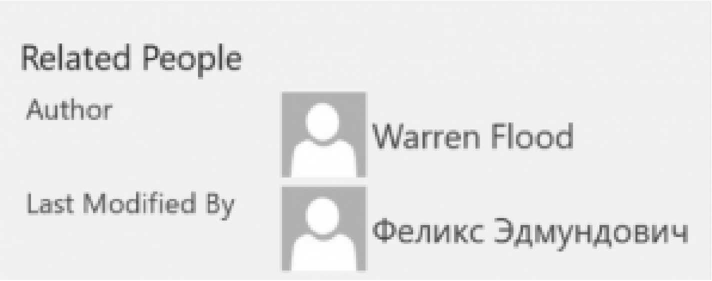
> But there were signs of dishonesty from the start. The first document Guccifer 2.0 published on June 15 came not from the DNC as advertised but from Podesta's inbox, according to a former DNC official who spoke on condition of anonymity because he was not authorized to speak to the press.
>
> The official said the word "CONFIDENTIAL" was not in the original document.
>
> Guccifer 2.0 had airbrushed it to catch reporters' attention.

Here's that watermark, which would have made reporters obtaining the document to ascribe it more value than it had.



Donald Trump Report
Democratic National Committee
Submitted: 12/19/15

On top of that change, we know that Guccifer 2.0 deliberately used the name Felix Edmundovich, invoking Iron Felix, the founder of the KGB (though another document invoked Che Guevaro in the same way) in the metadata of the document.



Related People

Author	Warren Flood
Last Modified By	Феликс Эдмундович

This analysis and this analysis compellingly shows, in my opinion, that the other Russian metadata in the documents was also deliberately placed there.

Finally, I believe that the addition of Warren Flood as author was *also* deliberate.

In addition, Guccifer 2.0 released these documents as DNC documents when in fact they are either Podesta documents or have not yet been sourced.

GUCCIFER 2.0 DNC'S SERVERS HACKED BY A LONE HACKER

Now, Guccifer 2.0 in fact didn't hide some of these alterations. Some were identified the same day the documents were released. But at the time they were interpreted as OpSec failures, rather than intentional deception. To this day, skeptics try to argue that the intentional deception of the rest of the metadata is somehow different than the tribute to Iron Felix (which is a mirror to the assumption in the early days that the Iron Felix was deliberate but the other Russian metadata was not, which I criticized here), without explaining why that would be the case.

In this post, I talked about how some of the other deception — pitching these Podesta (and other) documents as DNC documents — would have been a way to taunt the DNC and Crowdstrike for their false claims downplaying the hack. (Note, in the post, I ask why Guccifer 2.0 harped on VAN so much; the AP piece reveals that VAN officials and those working on voter registration were targeted, which suggests maybe the Russians did get VAN data and we simply don't know about it.)

So contrary to the belief of some commentators, it has long been known *that* Guccifer 2.0 altered these documents. But I don't think there has been a full accounting of all the ways that it worked (it's not even clear we know the full extent of the deception).

For now, I'm going to leave these multiple layers of deception laid out (I'd add, that whatever cutout led Julian Assange to believe — or at least to claim — the documents were sourced to Americans is another layer of deception, a different kind of metadata.)

There were multiple layers of deception built into these first documents, alternately taunting the Democrats who would have known them to be deception, the analysts who mistook them as mistakes, and the press who took them to indicate real value. I suspect there are at least two more layers of deception here.

But it's worth noting that *no one* was immune from this deception, and it's likely there are still a few layers that we’re missing here.

Update: As Thomas Rid notes on Twitter, one of the first five documents Guccifer 2.0 released is a version of one that Guccifer 1.0 had released.