# HUNTER BIDEN'S MATRYOSHKA CELL PHONE: HOW THE IRS AND FROTHERS GOT HUNTER'S ENCRYPTED IPHONE CONTENT

Believe it or not, what sent me down the rabbit hole of Hunter Biden's "laptop" was not the laptop itself.

It was a cell phone.

Or, more specifically, it was two details in purported IRS whistleblower Gary Shapley's testimony. First, after introducing summaries from some Hunter Biden WhatsApp chats — summaries that, Abbe Lowell claimed, got the most basic details wrong — Shapley explained that the chats didn't come from the laptop itself, they came from a warrant served on Apple for the iCloud backup to which they were saved.

> Q Could you tell us about this document, what is it, and how was it obtained —
>
> A Sure. So there was an electronic search warrant for iCloud backup, and these messages were in that backup and provided —
>
> Q Okay.
>
> A — from a third party, from iCloud.

This appears to be the search warrant return obtained — again, per Shapley's testimony — in August 2020.

> For example, in August 2020, we got the results back from an iCloud search warrant. Unlike the laptop, these came to the investigative team from a third-party record keeper and included a set

> of messages. The messages included material we clearly needed to follow up on.

Shapley's disclosure that there were WhatsApp texts saved to iCloud stunned me. That's because, for all the material produced from the laptop itself — which even frothers have treated as all the content in Hunter Biden's iCloud account — I had never seen WhatsApp texts.

Plus, there's a technical issue. WhatsApp texts, like Signal texts, don't automatically back up to iCloud. If one really wants to use their end-to-end encryption to best advantage, one doesn't store them in the cloud, because then the only easy way to get the texts would be directly from someone's phone. These texts purported to involve a Chinese national (though, as noted, Lowell says that's false) whose phone would presumably be inaccessible overseas. And at the time the IRS obtained these texts, Hunter Biden didn't know about the investigation into himself. They hadn't seized *his* phone.

For Shapley's description to be true, then, Hunter Biden would have had to back up the texts to his iCloud. But if he had, they should have shown up on the laptop itself, right along with every other scrap of the President's son's private life.

There were crumbs of an explanation for this in Shapley's notes from the October 22, 2020 meeting on the government's treatment of the laptop attributed to Hunter Biden.

In the meeting, Whistleblower X — who by his own description saw things online that he hadn't obtained via the laptop directly, even though DOJ warned the agents not to do that — kept prodding about whether the investigative team had been provided all the messages on the laptop.

> 29. SA [Whistblower X] asked if all information on the hard drive had been reviewed…the answer is that they did not

> look at all of that SA [Whistleblower X] questions if Dillon reviewed all iMessage's that wore relevant and not privileged. They would find the answer.

As Shapley recorded, on February 27, 2020, the forensics people provided all messages from the hard drive of material John Paul Mac Isaac restored from the laptop.

> 30. 2/27/2020 DE3 with all messages from the hard drive were provided by computer forensics– via USB Drive

That production included iPad and MacBook messages, but *no iPhone messages*.

> 32. 227 Productions
>
> DE3 USB containing exported messages (ipad and macbook messages) No iphone messages

They didn't get messages off any iPhone until they found a password, conveniently written on a business card, and with that password, were able to get into encrypted iPhone content on the laptop.

> Laptop – iphone messages were **on the hard drive but encrypted** they didn't get those messages until they looked at laptop and found a business card with the password on it so they were able to get into the iphone messages [my emphasis]

This still didn't answer my question – how was the IRS able to get WhatsApp texts from iCloud when they weren't on the iCloud content that appears on the Hunter Biden laptop.

But a detail on the fourth of Guy Dimitrelos' reports on Hunter Biden's laptop may explain it.

In his first report, Dimitrelos explained that the 5 million artifacts found on the hard drive

were connected to Hunter Biden's iCloud account, which he says was tied to the email rhbdc@icloud.com.

> 30. *The hard drive contained approximately 5,791,819 files and system artifacts and was connected to and authenticated on an Apple iCloud account of rhbdc@icloud.com which is owned by Robert Hunter Biden (RHB).*
>
> [snip]
>
> 36. *Since this Apple MacBook Pro model was not released until 2017, all data prior to 2017 was stored (backed-up) to the rhbdc@icloud.com account and then downloaded to the MacBook Pro hard drive Downloads folder as illustrated in paragraph 30.*

In his fourth report — basically 133 pages into his sequential reporting — Dimitrelos noted that Hunter Biden had another iCloud account, one tied to one of the emails he identified on page 4 of his report: RHB@RSPDC.COM.

In fact, at least according to the unreliable emails released at BidenLaptopEmails dot com (AKA MarcoPolo), *that's* the account to which the

laptop believed to be the one that ended up at Mac Isaac's shop was registered to, *not* the rhbdc@icloud.com account.


Dear Robert Hunter,

Your Apple ID (**rhb@rspdc.com**) was used to sign in to iCloud on a MacBook Pro 13".

Date and Time: October 21, 2018, 5:50 AM PDT

At the Marco Polo site, there are 453 pages of emails from the rhb@rspdc.com account (so around 22650). They include some of the most interesting in the collection, the ones directly with the Biden family and others indicating sensitive travel. There are 269 from the rhbdc@icloud.com account (so around 13,450) — but it's the latter that seems to have been taken over in early 2019. I've described that the droidhunter88 gmail account effectively took over control of the iCloud account in that period (though I need to go back to the timeline and distinguish which events happened on one iCloud account and which on the other), and I think that's right. But importantly, at times, the RosemontSeneca email is linked into it. That is, a RosemontSeneca email was used on both iCloud accounts.

As to the phone, Dimitrelos describes that he found a phone registered to the rhb@rspdc.com account in an encrypted container in an iTunes backup.

> I identified an encrypted container located within Apple's MobileSync iTunes default backup folder.
>
> [snip]
>
> I identified the iOS backup to be an iPhone with the phone number below and Apple id of
>
> rhb@rspdc.com which is one of Robert Hunter Biden's iCloud accounts.

Part two of Dimitrelos' report described finding passwords for the iTunes account in two places.

First, a picture of a partly rumpled lined piece of paper stored in a Hidden Album. This picture included Amazon, WiFi, iTunes, GMail, and Apple ID passwords, all registered to a different Gmail account. And then, associated with an iPad registered to still a third iCloud account, registered to a Gmail account.

The latter shows that *Hunter Biden's iTunes password was changed on January 30, 2019*, solidly in the middle of the period I've argued that his account was taken over by the DroidHunter gmail account.

And screencaps in parts two and four of Dimitrelos' report show that both the iPad and the iPhone were backed up during this same period, on February 6, 2019. Someone changed the iTunes password, and backed up these two devices, where they were found on the laptop. All in this same period where Hunter Biden seems to have lost control over his laptop.

In part four of Dimitrelos' report, he describes that there were, indeed, WhatsApp messages on the iPhone, registered to that entirely different iCloud account, seemingly backed up to iTunes on the rhbdc@icloud.com account.

I can't be sure about this, because I'm not a forensics expert, both Shapley and Dimitrelos are deliberately unreliable narrators, and even they don't have all the data to understand what went on here. But it appears that the reason why there were no WhatsApp texts on the laptop itself, which had all the content in the rhbdc@icloud.com iCloud account, is that they weren't used by a device registered to the rhbdc@icloud.com iCloud account. They were used by a device registered to the rhb@rspdc.com account, which was (as Shapley's notes reflect) stored in encrypted fashion on the laptop.

There's one more very important point about this.

The government had a warrant. If they really did find a business card (one not described anywhere I've seen in Dimitrelos' report) with a

password, they were able to get the encrypted content (though oftentimes prosecutors will recommend you go back and get a second warrant for that). From there, it seems, the IRS got another warrant for the *other* iCloud account, the rhb@rspdc.com one. That's how they got a legally sound copy of the WhatsApp texts in August 2020.

But for people like Rudy Giuliani or Garrett Ziegler or John Paul Mac Isaac, taking a laptop they purport to have been abandoned, and then using a password found on that laptop to access an encrypted container — especially one of a different iCloud account — is legally another level of conduct.

Update: I screwed up the number of emails; I've corrected that now.