

Josh Duggar Trial: Prosecution Expert Details What He Saw on Office Computer at Center of the Case

Forensic analysis found that a partition and secondary operating system (“a separate computer on a computer”) hid the illicit material on the desktop in Duggar’s office

By [Adam Carlson](#)

December 03, 2021 12:30 AM

[Josh Duggar](#) and his wife and kids still stand beaming out from the desktop background of the HP office computer that, until Nov. 8, 2019, sat on the desk in the office at his Wholesale Motors car lot.

Now, two years later and three days into the former *19 Kids and Counting* star's [trial on child pornography charges](#), the computer sits sheathed in wrapping and red tape — signs it has been turned into evidence against him.


The HP desktop is central to federal prosecutors' case against Duggar, 33, who has pleaded not guilty to the charges of knowing receipt and possession of child pornography.


For more on Josh Duggar's child pornography trial and other top stories, listen below to [our daily podcast on PEOPLE Every Day](#).



iHeart 📶

The latest from Josh Duggar’s child pornography trial, plus inside Meghan Mar...

PEOPLE Every Day





Duggar's attorneys argue investigators ignored other leads, saying, "This is the equivalent of a trail of blood from a murder scene ... they [the prosecution] didn't follow it. It does not lead to Josh Duggar."

But the government claims the evidence and computer analysis led them to no other conclusion except that he was responsible.

On Thursday, the trial's third day in Fayetteville, Arkansas, the prosecution witnesses explained more of what they meant.

James Fottrell, director of the Department of Justice's High Technology Investigative Unit, spoke the longest and spoke last. Over several hours on Thursday afternoon, with testimony continuing Friday, Fottrell detailed his personal forensic investigation of the three of Duggar's devices that investigators seized: a personal MacBook, an iPhone and the HP desktop in his office.

No evidence of child sexual abuse material has ever been found on Duggar's personal laptop or cell phone — a fact his defense repeatedly highlights in arguing that someone else, someone nefarious, was secretly using the computer in his office — but that HP machine was riddled with illicit material, Fottrell testified.

On the stand, with the aid of a series of screenshots taken during his forensic analysis (and recreated via a visualization tool that draws from a copy of the HP hard drive), Fottrell walked through some of what he saw and learned in exploring the machine.

RELATED: Audio Revealed from When Josh Duggar Learned He Was Being Investigated for Child Pornography

Building on the prosecution's case, Fottrell said a program to install a Linux operating system was downloaded onto the HP just days before the computer was found to be sharing child sexual abuse material in May 2019. And while the main or public-facing portion of the computer appeared to be mostly business-related, with files and programs connected to financial transactions and auto inventory and a work email inbox, the hard drive had in fact been split in two that May, with the other side using Linux — what another expert on Thursday described in testimony as "a separate computer on a computer, if you will."

What's more, Fottrell said from the stand, switching the desktop from its default Windows operating system to the Linux side required a user to be physically present both during initial installation and every time a user wants to access the Linux side of the hard drive, which had a separate password. (The defense has theorized someone may have hacked or remotely accessed the machine when the child pornography was accessed.)

RELATED: Anna Duggar Attends Court with Husband Josh Duggar on Day 1 of His Child Porn Trial

After touring through his inspection of the Windows side of the HP – including noting that Covenant Eyes, an "accountability" program to monitor and block objectionable Internet use such as adult pornography, was set to auto-run when the computer was logged on – Fottrell then switched to the Linux side of the hard drive, where the sexual abuse material was found.

He reiterated the password for the Linux side: intel1988, which prosecutors argue was used by Duggar for some of his personal accounts (and also includes his year of birth). A former employee and distant Duggar relative suggested on the stand earlier Thursday they might also be aware of it – something prosecutors ridiculed as a convenient ploy.

In his testimony, Fottrell told the jury how he had gone deeper into the hard drive and found evidence or remnants of dozens – if not more than 100 – images of child sexual abuse material, as well as several videos.

For example, he said, his analysis showed the computer had thumbnail versions of the photos while he was able to also recover some deleted files and, through further examination, found evidence of downloaded and/or streamed videos like "pedomom" and "Daisy's Destruction" as well as viewed lewd images of an 8-to-12-year-old girl.

Fottrell said "Daisy's Destruction" was notorious: It includes an infant being tortured and was among the "most offensive" he had seen in his career. (At the request of the defense, the judge ordered the jury to disregard that characterization because it was a subjective opinion, not a fact.)

RELATED: Derick Dillard Attends Day 2 of Josh Duggar Child Porn Trial amid News Jill Duggar May Testify

Certain of the images obtained from the HP hard drive were shown to the jury after being described in open court, but they were withheld from the gallery.

Fottrell said the various associated timestamps with the computer use showed a pattern: The hard drive was partitioned and the Linux side booted up on May 13, 2019, after which Tor — a widely used but controversial Internet browser that preserves anonymity — was downloaded within 20 minutes.

A peer-to-peer file-sharing program, uTorrent, was also installed as was a media player. (It was a peer-to-peer program on the IP address at Duggar's car lot that first caught the police's attention in May 2019.)

And even as the defense has sought to desensationalize the use of Tor and peer-to-peer programs — which Duggar has previously said he was aware of or had used — Fottrell showed that his work linked the Tor on Duggar's work desktop to the so-called "Dark Web," which is only accessible on Tor's "hidden services": a network of anonymous websites.

"It's mostly criminal activity," Fottrell said. Credit card and financial schemes; drugs; guns; sexually exploitative material and murder-for-hire. "All kinds of crazy stuff," he said.

The Tor browser on Duggar's HP had bookmarked two sites that kept lists of these anonymous websites on the Dark Web.

Fottrell didn't stop his testimony with the May 2019 activity. In June, he said, the user had gone in and set up a new background — a mountain range crowned with blue sky — and created the sole document file he was able to find. It was a sale document from June 22, 2019, and the salesman listed was "Josh."

Fottrell's testimony continues Friday after which he will be cross-examined by the defense.

RELATED: Prosecution Gets Heated Questioning Josh Duggar Relative and Colleague: 'You Were Hiding Something'

Other Testimony from Day 3

Elsewhere in court on Thursday, the defense finished its cross-examination of Homeland Security Investigations Special Agent Gerald Faulkner who executed the search warrant of Duggar's business in 2019. Attorney Justin Gelfand continued to press Faulkner on certain decisions such as why they didn't seize other digital devices on the property that day like the office router.

Faulkner said the team was not advised by their analysts to take the router and any other device not seized was cleared beforehand and didn't check three boxes that authorities were looking for (including sex abuse material and evidence they were on the car lot in May 2019 when other child porn was accessed).

Gelfand also singled out that Faulkner made two errors, inadvertent or not, when executing the warrant. He wrongly indicated to people at the scene that investigators were looking for illicit activity late at night. (Faulker mistakenly converted the time zone on a report about when the sex abuse material was shared from the car lot's IP address in May 2019.) And he believed a car lot employee who said he hadn't started working there until mid-June when it was several weeks earlier.

Jeffrey Pryor, another special agent, testified briefly about the steps in seizing material during the 2019 search and Jeff Wofford, an executive with Covenant Eyes, testified about Duggar's use of the program (with his content filter set for the standard "mature teen") and how the monitoring could be evaded with a Linux partition. The defense pointed out a user could also simply not download the program on their hard drive to evade it.

RELATED VIDEO: Josh Duggar Trial — Evidence, Witnesses and Looming Arguments Become Clearer as Jury Is Seated

Matthew Waller, a former employee and distant relative of Duggar, also testified — sparking a back-and-forth with the defense and prosecutors over his statement that the "intel" in the Linux partition password "intel1988" was vaguely familiar.

Before Fottrell, forensic analyst Marshall Kennedy, who did the initial examinations of Duggar's devices, took the stand.

Duggar's trial is expected to carry into mid-week.