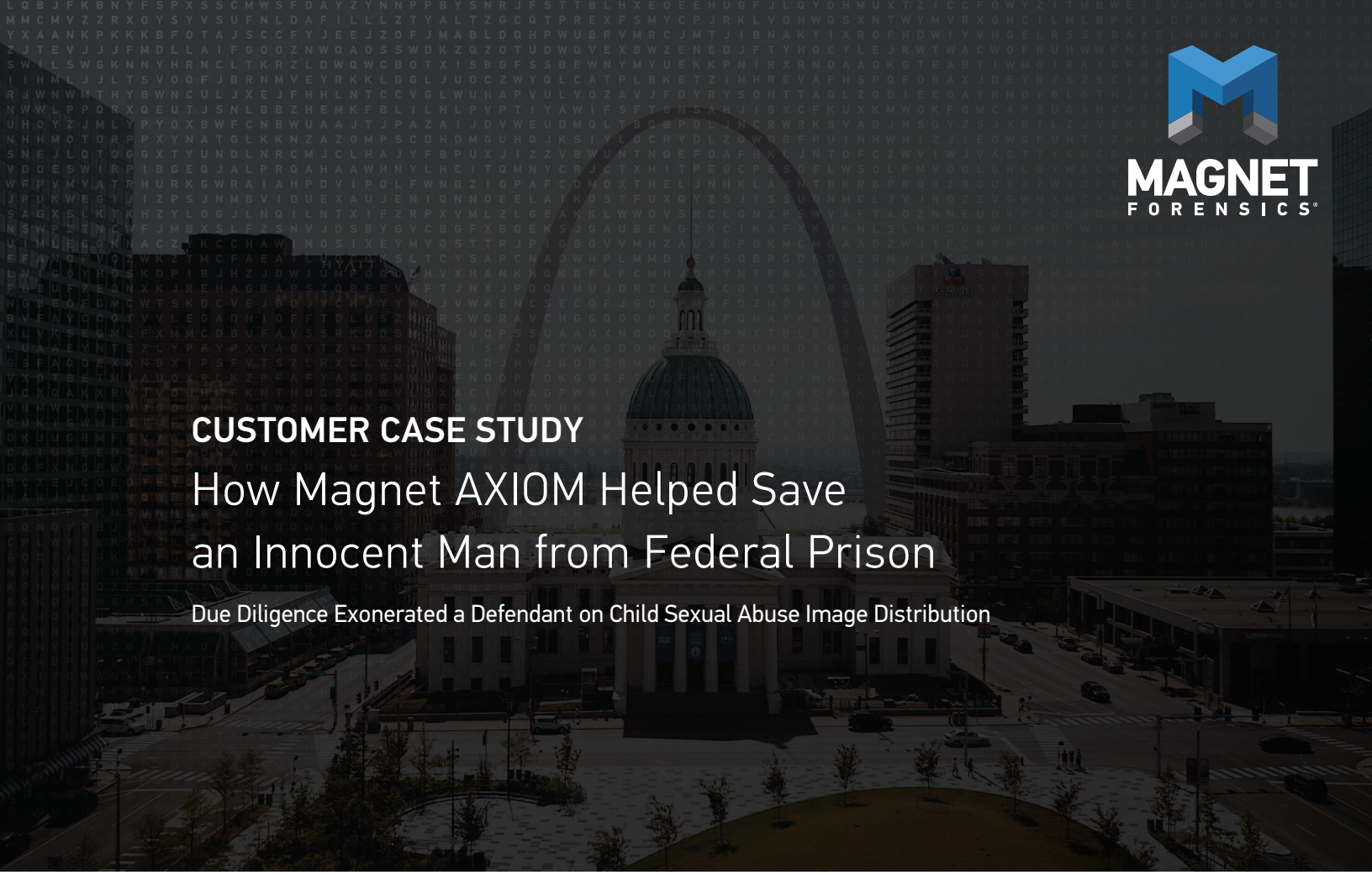

MAGNET FORENSICS®

CUSTOMER CASE STUDY

How Magnet AXIOM Helped Save an Innocent Man from Federal Prison

Due Diligence Exonerated a Defendant on Child Sexual Abuse Image Distribution

THE CHALLENGES

- Complex child sexual abuse cases with multiple systems and devices are time-consuming and painstaking to piece everything together.
- An inaccurate case timeline needed to be reconstructed to account for more than two relevant computer systems.
- A lack of forensic capabilities that could help prove attribution – e.g., jump list parsing.

MAGNET AXIOM SOLVES BY

- Allowing the examiner to add more evidence to existing cases.
- Timeline and other filters allowed easy reconstruction of the facts of the case, telling a different story from the one the government presented.
- Artifacts-oriented emphasis uncovered pieces of data that proved intent.

Name: Troy Schnack

State: Missouri, U.S.

Investigation Type: Computer & Mobile

"Without AXIOM, analysis would've taken five times as long...AXIOM made it easier to see that Windows Media Player opened this video on this date and time. You can bookmark that artifact for your summary and move on. No other tool combines all those artifacts like that."

BACKGROUND

The United States Federal Public Defender for the Western District of Missouri provides criminal defense services to people who cannot afford a private attorney. Troy Schnack, a forensic examiner who works for this office, estimates that 85 percent of the cases he's called to assist with involve child sexual abuse material (CSAM)—which can be some of the most complex. "Cases involving drugs or felons with firearms go relatively quick," says Schnack, "but [CSAM] cases tend to be long and drawn out because they frequently involve so many systems."

Most of Schnack's cases are about mitigation rather than whether the client is guilty. "How many original images exist on a device, as opposed to duplicate images, can affect sentencing guidelines," he explains. "My job is to validate that it exists on the client's machine and then to find it the same way the government found it"—in other words, to replicate their forensic process.

At this stage, forensics can also disprove clients' falsehoods. "The evidence shows what they did and what they know," Schnack explains. "We explain that we use the same process as the government and that we can prove whether there was hacking, malware, or some other way the material got on the system."

THE APPEARANCE OF AN OPEN-AND-SHUT CASE

A recent case that Schnack worked seemed, at first glance, to mirror hundreds of other similar cases. A suspect had been arrested and brought up on federal charges of possession and distribution of CSAM. During their investigation, police had focused on the desktop and laptop computers found in the homeowner's bedroom.

The evidence they found on those systems seemed to make for an open and shut case against him: both the CSAM as well as Ares peer-to-peer (P2P) software, commonly used to distribute CSAM, existed on the hard drives. Internet history and other digital artifacts further helped to establish a timeline as to the desktop's usage. "It looked really bad for the client," says Schnack.

Faced with that kind of evidence, in most cases, suspects typically confess. Schnack's job is "mostly to find out how bad the evidence really is, to help determine whether attorneys will take a plea, or proceed with a trial." This time, however, the suspect maintained his innocence.

> "The evidence shows what they did and what they know," Schnack explains. "We explain that we use the same process as the government and that we can prove whether there was hacking, malware, or some other way the material got on the system."

Three other adults lived in the same home. Police had seized 10 computers in all, and also imaged four mobile devices. To begin the fact-finding process that would help attorneys mount an appropriate defense, Schnack's first task was to establish ownership of each of the 14 devices, based on where each was found in the home.

The next order of business was due diligence: to search each computer for Ares P2P software. Schnack started with a quick keyword search for "Ares" across the 10 computers. This search would determine whether the computers that had downloaded the Ares installation program had also attempted to install it.

He found the keyword, and an associated prefetch file—created when the installation executable was run—on a laptop that had no associated forensic reports from the prosecution team. This meant that the laptop belonged to one of the other three residents.

HOW DUE DILIGENCE USING AXIOM REVEALED A DIFFERENT STORY

After Schnack identified the two computers with the Ares keyword match, eliminating the other eight from suspicion, he acquired forensic images and loaded them into AXIOM. "I wanted to compare the dates, times, and downloads from Chrome and Firefox to see when Ares was downloaded and installed," he explains. "I also wanted to see the machines' jump lists to see when the relevant videos were downloaded and viewed. As it turned out, Windows installations also became pertinent to this case."

Those details enabled Schnack to build a timeline across both computers. It showed that the client's desktop had run Windows, email, and Skype across both work and personal accounts for 17 months without a single instance of either CSAM, Ares, or any P2P software until the day it was installed.

The timeline also indicated that in the weeks leading to that installation, the client's roommate had attempted to install the software on his own personal computer with no luck. In fact, AXIOM showed that the Ares executable had been downloaded five times, and that the user had attempted to run that file 15 times before giving up. "AXIOM's parsing made it easy to see the date and time range," says Schnack, "and to filter and sort by times and dates to build the timeline of events. Finding Ares on the [roommate's] computer was the only connection to the file date/time and the download start and finish."

THE TIMELINE

Friday Evening
ROOMMATE COMPUTER

Windows Installation.

Saturday
ROOMMATE COMPUTER

Windows updates complete; Chrome and antivirus downloaded and installed.

Sunday
ROOMMATE COMPUTER

Chrome runs for the first time; first search for Ares; three seperate downloads attempted, installation failed.

The Following Weekend
ROOMMATE COMPUTER

Windows Explorer delivers error messages; user recreates their username with a-2 appendage; Ares is downloaded from Chrome twice more.

Third Consectutive Weekend
HOMEOWNER COMPUTER

Ares downloaded and installed on the clients' desktop; this is followed by the download of a "bad" filename.

However, Schnack still needed to find hard evidence that the roommate had used the homeowner's desktop for nefarious purposes. AXIOM's Relative Time Filter showed everything else that was happening on the computer at the time of installation, including form fills for webmail, credit cards, and bank account validations on Chrome and Firefox that had not been made on that machine for the 17 months before the Ares installation.

Schnack then turned to the roommate's mobile device. Police had seized and imaged the phone, but prosecutors had not provided its report. Once the defense team obtained that, Schnack saw that the roommate had downloaded the RedTube custom app—not found on the Google Play Store—and that the phone contained a folder with multiple videos downloaded over six months with filenames containing "indicative" keywords such as "teens." On the morning police served their search warrant, in fact, pornography had been downloaded to the phone as police entered the residence.

> "AXIOM's parsing made it easy to see the date and time range," says Schnack, "and to filter and sort by times and dates to build the timeline of events."

The defense team's investigators dug deeper. They validated police interviews which had revealed that "everyone in the house" used the homeowner's desktop and laptop computers because they were "the fastest." (Schnack says no other usernames or partitions were created on these systems.) They also found that the roommate had a prior history of abuse-related claims made against him.

The final piece of evidence needed to exonerate the suspect were call detail records from the day the Ares software had been downloaded and used on his desktop. Those showed that the homeowner had been 10 miles away at a casino.

"The roommate wasn't intentionally trying to incriminate our client," says Schnack. "He admitted that he 'always messed up' computers"—a result of the malware which his activities resulted in. Photos of his bedroom, taken during the search warrant execution, showed a number of DVD jewel cases with "barely legal," "hardcore" XXX-rated movies. The defense team was able to tie these to the roommate because they were in the same photographic frame as an electric bill in the roommate's name. No one had pinpointed this because of the preponderance of evidence pointing to the homeowner. "We would never have found any of this stuff without the due diligence of looking at all the machines, not just the two that had been highlighted by the government report," Schnack says.

SAVING TIME WITH AXIOM SEARCH AND FILTER CAPABILITIES

AXIOM ended up saving significant time for Schnack with some key capabilities. "Without AXIOM, analysis would've taken five times as long," he explains. "Other tools don't parse jump lists, so AXIOM made it easier to see that Windows Media Player opened this video on this date and time. You can bookmark that artifact for your summary and move on. No other tool combines all those artifacts like that."

> "We would never have found any of this stuff without the due diligence of looking at all the machines, not just the two that had been highlighted by the government report," Schnack says.

The government had assumed that the download date/time was when the download started—not when it finished. As Schnack wrote in his blog post on the topic, however:

> "The download [date/time] in these [databases] is actually when the download completed. The P2P programs record this information once the download has finished.... The only reliable way to determine when the file download was initiated is based on the files Creation [Date/Time]."

"When I realized that I was looking at the finish date, that meant I had to search for new dates and times to re-match activity to those," Schnack says. "What those finally pointed to was that the client was not on his machine at those times."

Out of the hundreds of child exploitation cases Schnack says he has worked, this is only the second in which a man was exonerated. That AXIOM was instrumental not just in clearing his name, but also in identifying the true guilty party, reinforces how its emphasis on artifacts and robust filtering tools are necessities for investigators in every case.

"When I realized that I was looking at the finish date, that meant I had to search for new dates and times to re-match activity to those," Schnack says. "What those matches finally pointed to was that the client was not on his machine at those times."

SEE MAGNET AXIOM IN ACTION FOR YOURSELF

If you'd like to learn more about Magnet AXIOM and how it can help find evidence you may be missing with other solutions, visit magnetforensics.com/magnet-axiom. While you're there, you can learn more about the product, request an in-depth personal demo from an AXIOM expert, and request a free 30-day trial version.

Learn more at magnetforensics.com

For more information call us at 1-844-638-7884
or email sales@magnetforensics.com

MAGNET FORENSICS®