CASE STUDY – METROPOLITAN NASHVILLE POLICE DEPARTMENT

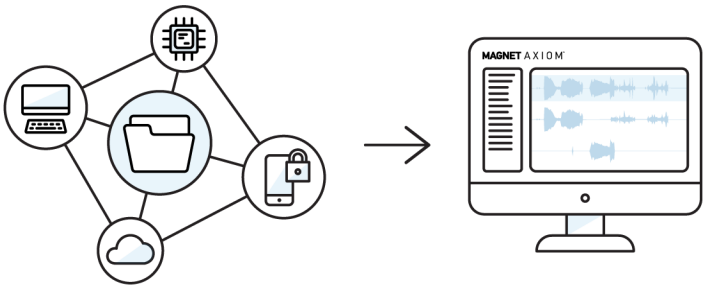
Modern Digital Forensic Tools: How New Tools Cut through the Noise to Find Evidence

> Magnet AXIOM is a great tool when it comes to filtering in and filtering out the important data that investigators need to review, which really reduces the overall time to evidence."
>
> – Detective Chad Gish, CID, SISU, Metropolitan Nashville Police Department

How Chad Gish uses Magnet Forensics' Tools

Magnet AXIOM is one of Detective Gish's go-to tools and it's part of what allows him to create the story of what has happened based on the data collected from digital devices. Today, it's rare, according to Detective Gish, that "we see a crime committed by someone without a computer in their pocket."

With Magnet AXIOM, Gish is able to collect data from multiple sources all-in-one case file, whether it be data from mobile extractions from Grayshift's GrayKey, cloud data from an iCloud backup or a Google warrant return, or vehicle data from Berla iVe. With the geolocation data reviewed in AXIOM, it can also be used to locate likely locations to acquire CCTV footage with Magnet DVR Examiner.



CASE OVERVIEW

- Detective Chad Gish CID, SISU
- Metropolitan Nashville Police Department

PRODUCTS

- Magnet AXIOM
- Magnet OUTRIDER
- Magnet DVR Examiner

PARTNERS

- Grayshift
- Berla

Things Were Simpler in the Good Old Days, Except When it Comes to Digital Forensics

Detective Chad Gish of the Metropolitan Nashville Police Department, digital forensics veteran of 17+ years – with total service time of more than 24 years – has been working cases with digital evidence before the boom of modern digital forensic investigations. When Detective Gish first joined the Cybercrime and Digital Forensics (CID) unit, building a case that included digital evidence with the tools at the time was challenging, even though the devices under investigation were much simpler.

Detective Gish remembers how difficult it was to determine where specific image files came from before forensic tools were able to acquire extended attribute and spotlight metadata. When that data wasn't available, all that could be proven was that a suspect possessed an illicit image. Examiners couldn't always prove how the picture ended up on the device, show how it was airdropped onto that device, or attribute the image to the suspect's account. In some scenarios, this could be the difference between conviction and acquittal based on lack of evidence.

Now, digital forensic tools are benefitting from broader advancements in technology, allowing examiners to streamline their workflows and cut through the digital noise to locate, recover, and collect evidence faster. During the transition from largely computer-based to mobile-first investigations, Detective Gish has witnessed the way officers investigate digital evidence has changed. The advancements in technology have afforded examiners like him new tools to reduce the time it takes examiners and investigators to uncover evidence on digital devices.

The number of digital devices involved in an investigation is growing, averaging around **6 devices per person***, making acquisition, processing and analysis logistically challenging, time-consuming and expensive.

* The 2022 IDC MarketScape

> We need ways to recover data quickly, especially for those high-profile, priority cases, and the technology needs to evolve to allow us to do so."
>
> **– Detective Chad Gish, CID, SISU**
> **Metropolitan Nashville Police Department**

"Even though phones used to be a lot smaller and store less data, it could take 2 or 3 months sometimes to get access to the data," said Detective Gish. "With today's tools, often times we can get the data we need in less than a day. We need ways to recover data quickly, especially for those high-profile, priority cases, and the technology needs to evolve to allow us to do so."

Computer forensics experts have formally been a part of law enforcement agencies for over 40 years. Specialized computer forensic groups were established in the mid-1980s, such as the FBI's Computer Analysis and Response team and the Met's Computer Crime Department, but the rise of the modern digital forensics lab can be more closely aligned with the emergence of the smart phone. The landscape of policing changed with the launch of the first iPhone in January 2007 and the first Android device, the HTC Dream in 2008. Now, some 15 years later, about 90% of devices entering digital forensics labs are smart phones according to digital examiners.

Adapting to Change

Adapting to changing technology has more or less been a mandate of the role for Detective Gish, necessitated in large part by the need to reduce time to evidence, while leveraging technology to bridge the gap between demand for and the shortage of digital forensic examiners. With today's case backlogs, it's unrealistic to expect that examiners could go through every single detail of every single device on every case.

> Even though there's way more data these days, I only need a small amount of it. Today's tools allow me to go get that data much more easily."
>
> **– Detective Chad Gish, CID, SISU**
> **Metropolitan Nashville Police Department**

"Just this year, we've probably investigated 500 cases, and I'm currently working on one case that has about 50 phones that need to be processed," said Detective Gish.

The storage capacity of mobile devices has also grown exponentially with each passing year and device security has grown in complexity posing significant challenges to investigators. In a recent case, Detective Gish processed two phones that had over 250 gigabytes of data each for a single suspect.

"This is becoming common for almost every case now," said Detective Gish. "It's a lot. Even though there's way more data these days, I only need a small amount of it. Today's tools allow me to go get that data much more easily."

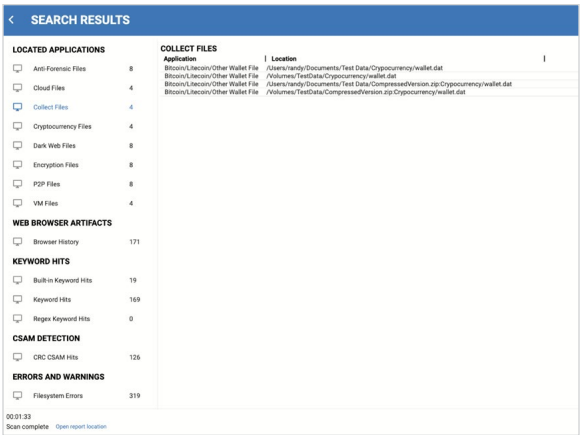
Advancing the capabilities of new tools also helps to offset the experience gap. Detective Gish points out that a lot of the new examiners haven't necessarily grown up in digital forensics or don't have a lot of experience yet, so if the tools can be designed to pick up some of the slack, to be easy to use, and to be reliable now and into the future, it helps to overcome the experience gap as new examiners are onboarded.

For Detective Gish, it's especially important that digital forensic tools continue to develop new solutions to reduce time to evidence, because in the backlog there's evidence that can save a life, that can protect a child. It's even more important when evidence is received for a high priority case and digital forensic examiners are already stretched thin. When the pace of the clock marches forward incessantly, being able to get any advantage is necessary.

How Triaging Tools Reduce the Overall Time to Evidence

"Triage is another tool we have, where we can quickly scan a device before breaking it down," Gish said. "We can review triage reports, so we know where the needle in the haystack is before we even start the search."

Triage reports, provided by tools like Magnet OUTRIDER, become a starting line for Gish, especially when it comes to CSAM cases. When the case includes multiple devices, Magnet OUTRIDER helps to identify some basic but very useful things to reduce the overall time to evidence, such as which device was used most recently and what cloud accounts



have been accessed from that device. Once some of this information has been uncovered, it's easier to prioritize which of those devices to analyze first and then search warrants can also be written right away for the specific cloud accounts identified.

Emerging Data Sources

Not only are new tools changing the way that Detective Gish approaches cases, but so too are emerging sources of data.

"If someone said to me, you could have five unlocked iPhones or you could have the cloud data associated with those phones, if this were 2013, I'd have taken the phones hands down. But, now, I'd have to really think about that. It's a much tougher decision today."

In the last 7 or 8 years, as more data has moved to the cloud, Gish has been impressed by the amount of evidence you can collect from cloud packages that are acquired with a warrant return or things like iOS backups from iCloud. In some cases, Gish suggested, albeit rather facetiously, that if you hand that data to an investigator, they may think they have the data from the phone itself.

> "The case came together by using data from different sources to layer the evidence together, which gave us the story of what was happening."
>
> **– Detective Chad Gish, CID, SISU**
> **Metropolitan Nashville Police Department**

Nevertheless, with the data that's being stored by cloud service providers, such as Google, WhatsApp, Microsoft O365, etc., not only can you get data from the different messaging apps, but you can also get additional data for the user, like waypoint data. Gish shared an example where in one homicide investigation he could see the exact moment the trigger was pulled. The victim was murdered while driving, so Gish was able to see waypoint data that was registering consistent speed until the time the victim was shot and then he could see the speed immediately drop until the car stopped where it was found on the side of the highway.

Leveraging cloud data to identify the moment that the car began to slow was a critical discovery for Detective Gish. Doing so allowed him to quickly establish time of death, expediting the investigative process, and reducing the overall time to evidence. In this case, it allowed Detective Gish to quickly understand that by the time he had arrived at the scene, the victim had already been there for a few hours. In turn, this afforded his team more information for when they were canvassing the area for witnesses.

As new data sources become available, being able to correlate data between sources becomes increasingly important, as is capitalizing on new data sources that become available to find not only more evidence, but also more pertinent evidence.

According to Gish, on one case where there were several car-jackings, he and his team we were able to acquire data from the vehicles once they were recovered, plus they were able to recover the phones from the suspects. What they did to piece the sequence of events together was acquire the waypoint data from the suspect's cloud accounts, correlate that with the route data from the vehicles, and then they used that to identify where the best locations would be to recover video from CCTV.

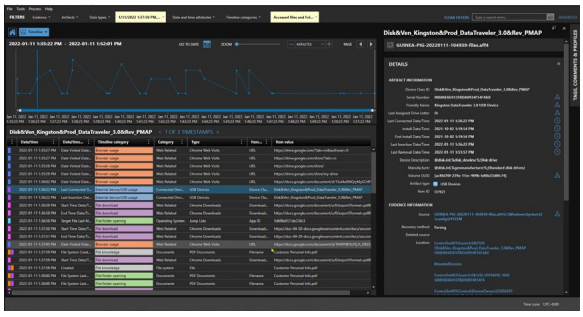
"The case came together by using data from different sources to layer the evidence together, which gave us the story of what was happening."

Turning Data into a Cohesive Story

Magnet AXIOM is one of Detective Gish's go-to tools and it's part of what allows him to create the story of what has happened based on the data collected from digital devices. Today, it's rare, according to Detective Gish, that "we see a crime committed by someone without a computer in their pocket."

With AXIOM, Gish is able to collect data from multiple sources all-in-one case file, whether it be data from mobile extractions from Grayshift's GrayKey, cloud data from an iCloud backup or a Google warrant return, or vehicle data from Berla iVe. With the geolocation data reviewed in AXIOM, it can also be used to locate likely locations acquire CCTV footage with Magnet DVR Examiner.

According to Detective Gish, "Magnet AXIOM is a great tool when it comes to filtering in and filtering out the important data that investigators need to review, which really reduces the overall time to evidence."



Some Final Notes

As technology evolves, investigators must adapt to get the best data possible to conduct efficient investigations and to reduce the overall time to evidence. The next stage of technological advancement is underway as cloud infrastructure is offering examiners and investigators automated workflows to churn through backlogs of digital evidence and new tools to share evidence between the lab and non-technical stakeholders.

> "If you can get to the evidence quickly, and reduce the time it takes to get there, it just makes sense,"
>
> **– Detective Chad Gish, CID, SISU**
> **Metropolitan Nashville Police Department**

While Detective Gish notes that these new technologies certainly require updated regulatory oversight and new legal precedents to be set, given the option to return to the 'good ol' days' of digital forensics or to press forward with new tools, he'll take the latter.

"If you can get to the evidence quickly, and reduce the time it takes to get there, it just makes sense," said Detective Gish.

Learn more at **magnetforensics.com**

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

MAGNET FORENSICS®