A DFIR TRAINING FEATURED BLOG POST

Magnet AXIOM Cyber – Some (awesome) personal observations

I ~~am~~ was not an AXIOM Cyber user.

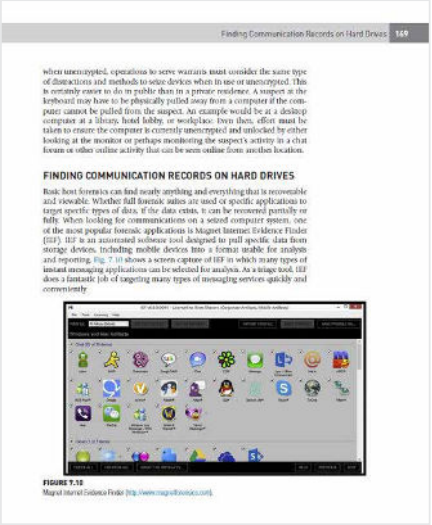
This post is going to give you a few pointers of succeeding in DFIR as an examiner or developer while using Magnet Forensics' AXIOM Cyber application as a case example. These pointers are also self-reminders to me, so everything I say is personal to me as it is potential guidance for you.

Before going any further, **request a trial of AXIOM Cyber** and after reading this post, run it against another tool that you have. You will not regret the time to install, run, and be pleasantly surprised.

MY HISTORY WITH "MAGNET FORENSICS"

I found Jad Saliba's Internet Evidence Finder on the Forensic Focus forum some years ago as freeware. IEF was small and very cool in what it did. I liked it so much that I even donated $25 to Jad to help develop it. I thereby take full credit for where Magnet has gone since. But seriously, I support Magnet as I do now, and as I do with other tools that I use.

During those early years, I used IEF successfully enough in cases, that I choose IEF as an example in one of the books that I wrote to make a point of recovering browser evidence.



Finding Communication Records on Hard Drives 169

when unencrypted, operations to serve warrants must consider the same type of distractions and methods to seize devices when in use or unencrypted. This is certainly easier to do in public than in a private residence. A suspect in the keyboard may have to be physically pulled away from a computer if the computer cannot be pulled from the suspect. An example would be at a desktop computer at a library, hotel lobby, or workplace. Even then, effort must be taken to ensure the computer is currently unencrypted and unlocked by either looking at the monitor or perhaps monitoring the suspect's activity in a chat forum or other online activity that can be seen online from another location.

FINDING COMMUNICATION RECORDS ON HARD DRIVES

Basic host forensics can find nearly anything and everything that is recoverable and viewable. Whether full forensic suites are used or specific applications to target specific types of data, if the data exists, it can be recovered partially or fully. When looking for communications on a seized computer system, one of the most popular forensic applications is Magnet Internet Evidence Finder (IEF). IEF is an automated software tool designed to pull specific data from storage devices, including mobile devices into a format usable for analysis and reporting. Fig. 7.10 shows a screen capture of IEF in which many types of instant messaging applications can be selected for analysis. As a triage tool, IEF does a fantastic job of targeting many types of messaging services quickly and conveniently.

FIGURE 7.10

Magnet Internet Evidence Finder (http://www.magnetforensics.com).

HERE ARE YOUR BENEFITS OF THIS STORY:

- A shareware tool (IEF) became one of the most relevant and impactful forensic applications on the planet in just a few years. **Never discount something that works that may develop into a major tool!**
- Magnet Forensics' tools have been influenced by its users over the years. **When you find a tool that you like, get involved and guide its development for your benefit which then becomes the community's benefit.**
- Support the tools that work for you. Whether financially with donations, licenses, or giving input on what works, what doesn't, and what you'd like to see the tool do, **your input develops tools that do what you need them to do.**
- If you are developing a tool and you have visions of growing it, **you can do it if you do it right**. Jad did it right and I can imagine the struggles, obstacles, pressures, and stress to get to where Magnet is now. Kudos to Jad on his leadership of Magnet.

NOW COMES MAGNET'S AXIOM CYBER

It is an impossibility to give a review on everything AXIOM Cyber can do. **I recently posted a blog on choosing tools** and AXIOM Cyber fits in the area of the kind of forensic app that does practically everything you may need as

a fully featured suite. As much as I miss that little IEF shareware, I am glad to see Magnet progress as it did into what it is today. My $25 went far!

I'll let others write about how to use AXIOM Cyber because I want to give my personal opinion on if you should even try it. In short, the answer is yes. If nothing else, **get a trial version** to take a look at what you are missing if you are not already an AXIOM user.

> "If nothing else, **get a trial version** to take a look at what you are missing if you are not already an AXIOM user."
>
> – DFIR Training

AS FOR AXIOM CYBER, THE SOURCES OF DATA ACCESSIBLE ARE IMPRESSIVE.

- **Computers and mobile devices** – of course.
- **Cloud** – Dropbox, aws, slack, box, Microsoft Team, Office 365, Azure, G Suite!
- **Remote collection** – Including "covert" remote collection from Mac and windows devices, and covert acquisition of employee Office 365, G Suite, and Box accounts.

Quick disclaimer

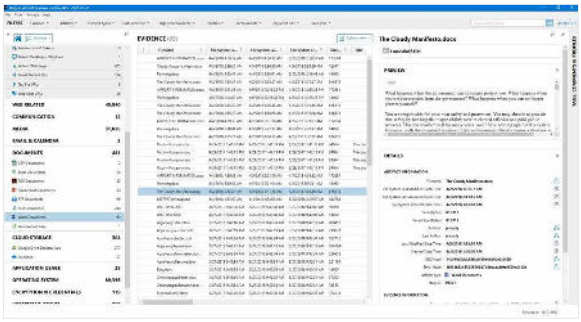
In my experience, no **one** tool does **everything** that you will ever need. Some tools do more and some do less. Some may do everything you need in one or more cases, but there is always something that comes up which requires a different approach or tool. AXIOM Cyber is the type of tool that leans on heavy on being able to do just about everything. If you are looking for that type of capability, then this app fits well.

TODAY'S FORENSIC DASHBOARD

Before you think that I don't believe in or use command line tools and hex editors, slow down a little. I am a firm believer in any tool that does the job I need done. That includes all types of tools, including anything I write for myself.

For the forensic suites, we are in the age of intuitive dashboards where everything is spelled out in front of our eyes. AXIOM Cyber's dashboard, like others, is intuitive to the point that someone without any experience with the application would be able to click and actually find their way around the tool and evidence.

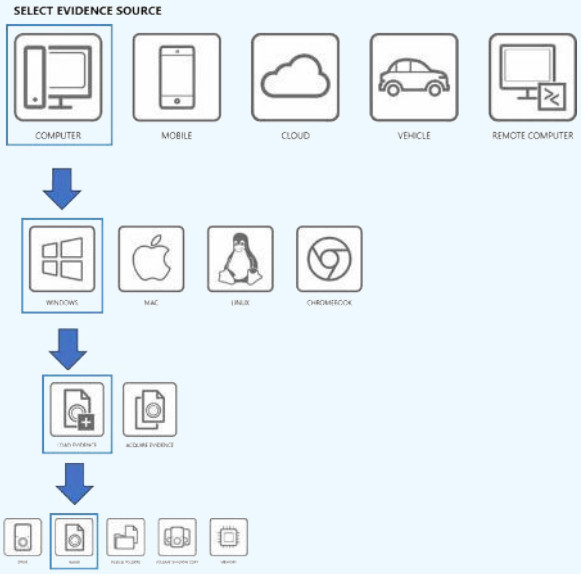
For those coming into the field recently, the current dashboards may not be that much of anything because of not having experience with tools that were counter-intuitive (without anything close to a dashboard). Most of the past applications had poor documentation and hidden (undocumented) features. Getting to the data required knowing A LOT about how to work the tool. Today's dashboard doesn't negate having to know the tool, but it does make accessing the data easier, faster, and less prone to error (ie: missing evidence).



The Basic Stuff

ADDING EVIDENCE

Practically any electronic evidence that you can come across is easily added into a case with AXIOM. From storage devices, images, mobile devices, the cloud, vehicles, and remote machines, it is truly "point-n-click" to add evidence items in an easy-to-follow decision tree.



AXIOM Cyber's remote collection does not mean that it automatically collects everything. That is because it only collects what you want to target. Maybe this is 'everything', but generally, we know what we are looking for and target that data. AXIOM Cyber remote target locations can be **Folders for All Users**, or **Documents for All Users**, or **web browsing data**, or **registry files**, or **event logs**, or the **$MFT**, or **more** (or less)!

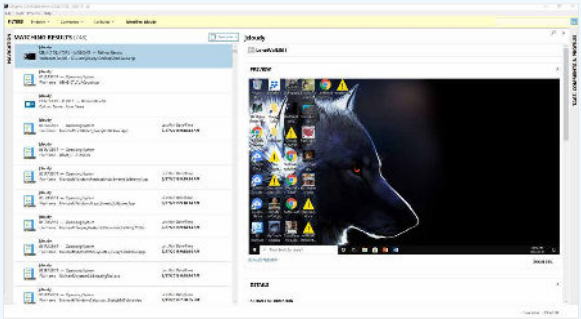
This is so easy that you might get spoiled.

PROCESSING EVIDENCE

Like many tools, AXIOM Cyber cleanly displays the options for what you want to process. And like any tool, the more you ask it to process, the longer it will take (or shorter if you ask for just the evidence that you need). And like many tools, processing is processing. It is the result of the processing that sets tools apart from each other. That's when AXIOM Cyber's dashboard really comes into play.

The dashboard is completely self-explanatory. Everything fits well with adjustable panes. Files are categorized in neatly and orderly. Drilling down to a file of interest is simply selecting the category, the file type within that category, and then the file of interest. Your file's metadata and preview are cleanly displayed. Each time that I see something this easy to use, I know that a lot of development time was spent to take a complicated feature and make it simple.

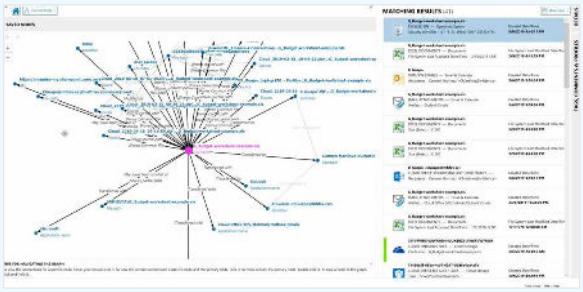
THE MAGIC



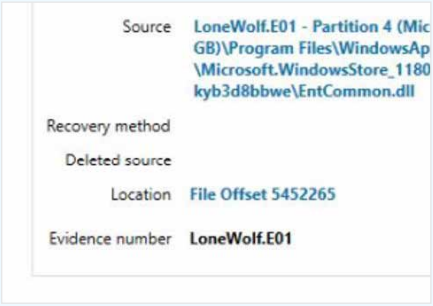
I'll admit, remote collection has always been magic to me. This is not something new, but I am happy to be able to access remote devices

and collect targeted data. Some of the other things that AXIOM does might actually be magic because these major features are wrapped up in one application. Things like 'rebuilding desktops' is a powerful visual feature that is practically done automatically, yet if you've manually rebuilt web pages or booted problematic images in virtual machines, then you know how cool this is as part of AXIOM.

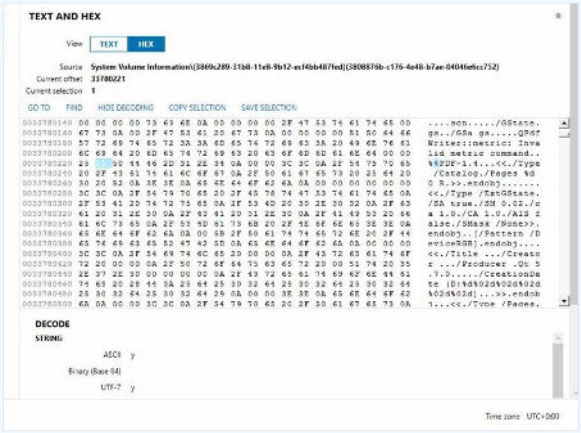
Visual for saved nodes is quick with relevant file data plainly listed.



As a point of convenience, knowing the file location makes it easy to validate findings with other tools. As I have seen some tools not easily give the file location, this is always a nicety that should be norm (but isn't for some tools for some reason...).

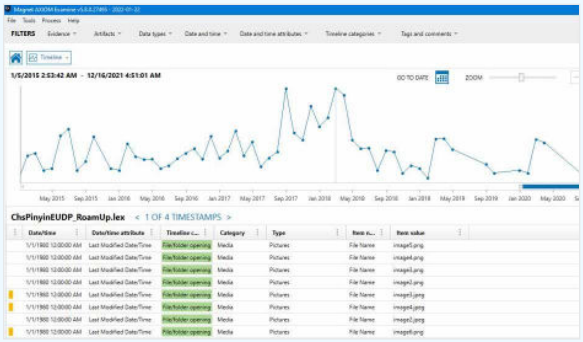


A click on the offset does what you think it does. It takes you to the offset to see the data for yourself.



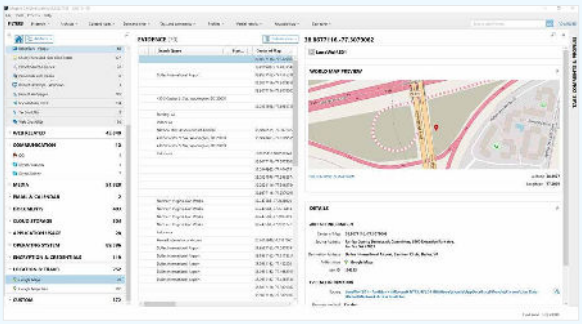
TIMELINES? YEA. WE GOTS DEM TIMELINES.

Again, something in one application that many times requires putting together using multiple tools. For what artifacts to put on the timeline.... take your pick! Maybe you want a timeline of PDF files or audio files, or both PDFs and audio files. Or maybe a timeline of deleted files! Check the boxes for artifacts of interest and your timeline updates to your needs.



MAPPING

Sometimes locations are important. Actually, most times locations are important, and mapping is a decently developed feature.



EXPORTING FILES AND REPORTING

One of the benefits of a forensic suite is that of exporting files and creating reports. When using a potpourri of tools, it takes extra effort to merge various types of reporting into one cohesive report. The same goes with exporting files in a manner that is consistent.

AXIOM gives just about every option you may or may not need. CSV, Excel, HTML, KML, XML, load files, and more. Again, the more you can stay in one app, the more cohesive the final reporting will be. I am not advocating to only use one tool, but AXIOM Cyber does put things together nicely.

The advanced

The advanced is nothing more than the basics done well and being skilled to the point that the difficult things look easy and the impossible things taking a little bit longer to complete.

THE POINT OF MAKING THESE THINGS EASY

Some forensic tools are difficult to use, which means you are slower to get to the data that you need. Intuitive applications allow you to get to the data fast, sort and combine data in order to see the big picture, and ultimately help you to find the problem/evidence/solution. The less time spent on filtering massive amounts of data from multiple machines gives you time and flexibility to analyze data.

AXIOM Cyber gives you access to acquiring remote sources plus forensic analysis in every aspect, including diving into hex, because sometimes that is needed or maybe it is the only thing needed. Being able to stay 'inside' one tool as much as possible reduces human error when moving between tools to accomplish tasks. Multiple tools are most always needed, but AXIOM Cyber helps minimize external apps.

THE "HOW TO USE"

There are plenty of writings on how to use any tool, including Magnet's online manual. AXIOM is no different than most tools in having plenty of sources in showing how to use the tool. I rarely get into the "how to use" aspects of tools when writing because my point of writing is to give my personal opinion of if a tool is worth the effort to try. In this case, it absolutely is **worth the try**.

If you want to have a tool that should be able to handle the unexpected, then this is certainly **worth the buy**.

A TIP ON BEING SUCCESSFUL IN DFIR

You need to be able to see the forest through the trees aka see the big picture aka **know and be able to tell the story of what happened**. The one thing that AXIOM Cyber does is show you the forest in a visual manner. Sometimes you need to peek your head out of the hex to see the big picture, then dive back in again with a better targeted focus. Being able to quickly and accurately tell the story of what you know shows decision makers that you know what you are doing. Knowing the story gives you confidence to make good decisions.

Conclusion

Get the trial. Even if you have no plans to get aboard the Magnet train, it behooves you to (1) see what is available because you might need it and not know it, (2) keep up with the capabilities of tools as compared to other tools that you use, and (3) be wary of what other examiners are using who may end up in an opposing side that pits you and your tool against the opposing expert and their choice of Magnet AXIOM.

Is AXIOM Cyber pretty? Oh yes. Pretty easy to see the big picture while being able to drill down to the bits.

Does AXIOM Cyber do everything? It certainly does a lot, and although I make it a point to never say that one tool does it all, this comes close.

> "If you want to have a tool that should be able to handle the unexpected, then this is certainly **worth the buy**."
>
> – DFIR Training

Learn more at **magnetforensics.com**

Speak to an expert today, call us at **1-844-638-7884**
or email **sales@magnetforensics.com**

MAGNET FORENSICS®