10 SKILLS YOU NEED TOWARD MASTERING MOBILE APP FORENSICS

ADVANCE YOUR DIGITAL SKILLSET

MAGNET FORENSICS®

10 SKILLS YOU NEED TOWARD MASTERING MOBILE APP FORENSICS

It can be one of the toughest challenges of a forensic examiner's career: the need to locate evidence on a mobile app that isn't fully (or at all) supported by their mobile forensics tools. The reality is, new apps, app features, and versions are introduced at a pace that commercial tool vendors can't possibly keep up with. Added to that, nefarious actors constantly exploit apps in new ways.

To address these challenges, we go back to the basics with the same scientific principles as all forensic methods: question, research, hypothesize, test, analyze—and if necessary, repeat—to guide you toward advancing your skillset.

In the short term, these skills will get you the evidence you need. In the long term, they'll enable you to stay up to date with technology's rapid evolutions and improve your knowledge and value as a forensic examiner.

Skill-building on this level can seem intimidating, but it's grounded in the same scientific principles as all forensic methods: question, research, hypothesize, test, analyze, and if necessary, repeat. Your forensic tools work on the same principles.

Some skills, like writing your own scripts[1], aren't required. Others, though, make you a better investigator. In this paper, we've described ten of these skills, as well as how to make time to follow through on learning them:

1. Document what you find
2. Learn how to acquire the image that will get you the most data
3. Learn what your commercial tools do and don't support
4. Learn how to find and use app parsers
5. Determine and research apps of interest
6. Form and test a hypothesis about the app
7. Create known data
8. Use known data to test app functionality
9. Learn how to find and parse unsupported data
10. Apply your method to case data

Skill 1: Document What You Find

Documentation is the foundation of any forensic process on any test or evidentiary device or data, so it's the first thing to learn to do well. Documenting your work doesn't only help you replicate your results in future tests. It's also useful when you're collaborating with other examiners, or if you want to share your results in a blog or presentation. Finally, documentation can help you justify your interpretation of results when it comes time to testify in court.[2]

[1] Scripting can be a good way to contribute to the digital forensics community, however. For more about how to get started with it, read our blog, "Being Forensically Curious: The Process of Scripting," published December 28, 2017. Find it at https://www.magnetforensics.com/blog/being-forensically-curious-the-process-of-scripting/

[2] Moore, Phill, "Documenting My Work," ThinkDFIR, October 16, 2017, https://thinkdfir.com/2017/10/16/documenting-my-work/ accessed April 9, 2018

Documentation is the foundation of any forensic process on any test or evidentiary device or data, so it's the first thing to learn to do well.

Skill 2: Learn How to Acquire the Image that Will Get You the Most Data

When looking for data from new, unsupported apps, you want as robust a dataset as possible from the device. Before you get to the app, first you must research the device to determine what acquisition method—for example, flashing a custom recovery image to a locked Android device—will work on a given device with a given operating system. Remember, always acquire a test device before using the acquisition method on an evidentiary device![4]

Forensic examiners know that a physical image is the "gold standard". Unlike logical and file system images, which depend on the structure provided to the forensic tool by the device's operating system, a full physical image contains all the data in both allocated and unallocated user space. It goes underneath what the operating system presents.

However, it isn't always possible to acquire a full physical image. The data may be encrypted, or you don't have the tools you need to acquire the image. The next best alternative is a full file system dump, which can provide all data in allocated space. If a file system image isn't possible, a logical image, whether a direct acquisition from the device or from a backup file (which can contain information that isn't available from a logical image), may be necessary.

Recognize that as you take each step down, the likelihood increases that you won't access to all the data necessary to help you find things you've never seen before—the data sources you need to recover information from an unsupported app. Logical and file system images may not include all of the app's data, nor do they offer access to unallocated space.

For testing purposes, documentation can include screenshots of fake profiles and populated[3] test data, as well as forms or some other way to record types of data you populate. This kind of documentation should include:

- Which apps are installed on the device
- Each test you perform on the app's functionality
- Full file paths
- What your forensic tools can parse, and where they pull data from such as a database/table, plist, xml, etc.

Finally, document a manual review of the same files and whether all or only some relevant tables were parsed.

[3] Test documentation is different from documentation that is discoverable in court.

[4] Read more about the discovery process in our blog post, "Being Forensically Curious: The Process of Discovery," published November 16, 2017 and available at https://www.magnetforensics.com/blog/being-forensically-curious-the-process-of-discovery/

Skill 3: Learn What Your Commercial Tools Do and Don't Support

The purpose of this step is to identify the app data that commercial tools can parse from the mobile device image. You need this step to validate that the parsed data is correct, and to identify installed apps that may be of interest, even if they aren't fully supported by the tool.

Even if a tool supports an app, it's important to verify that all the data was parsed. Typically, whatever the app displays to the user is probably stored on the device. Therefore, it's important to find out if you see all the data you expect or hope to see from an app of interest.

Even if a tool supports an app, it's important to verify that all the data was parsed.

For example, if chat data isn't parsed or was only partially parsed from an app that you know has chat functionality, and you believe the device owner used it, take a screen shot to show that the tool failed to parse those chats. Then you can find the chat data yourself. Keep in mind that in addition to the data tables on the device, it may be possible to find fragments of data stored elsewhere—left by uninstalled apps within unallocated space in the user partition, or saved in a cloud account.

Skill 4: Learn How to Find and Use App Parsers

If an app is unsupported or only partially supported by your go-to commercial tool, then part of due diligence is to find a tool that will offer the parsing support you need. You may try running the same image through other commercial tools in your toolbox.

In some cases, another forensic examiner may have programmed a parsing tool for the particular app. You can find these on GitHub, on the examiner's blog, or repositories such as Magnet's Artifact Exchange.

Even if a parser for that exact app doesn't exist, find out whether the app developer has created other apps, and see if parsers exist for those. Often, developers save time and effort by reusing the same database file for multiple apps, so a parser that works on one can work on others.

As we discuss in Skill 6 below, test your parser of choice to be sure that it works as you expect. Field names may differ between parsers, or the parser may only work for specific functionality that the developer reused code on.

Skill 5: Determine and Research Apps of Interest

You can't test an app if you don't know what you're looking for, so it's helpful to research app capabilities. That way, you can both identify apps of interest and ensure you can thoroughly test that information.

How do you know which apps are of interest? First, find all the installed apps. Their locations depend on the operating system and operating system version, so be sure you know where to look. Then, explore the installed apps' permissions.
Examples of questions you may want to ask include:

- Does this app have chat functionality?
- Does the app collect geolocation data?
- Can the app create video/photos?
- Does the app allow for file sharing or transference?
- Does the app use the current contact database?

Once you've identified the apps you want to dive deeper on, research the apps' features listed in the appropriate app store, including the most recent version and what features were updated or added. Be sure to read description details thoroughly, and compare them to any screenshots or other images of the app. These images may show functionality that's different from the description.

User reviews can offer additional insight into what the app does and why it might be relevant to your case. Be sure to record the permissions the app requires to function, as well as the appropriate path to ensure the permissions on the device are consistent with what you found.

Skill 6: Form and Test a Hypothesis about the App

After reading the app's description and functionality, you can begin to form your own thoughts and opinions about the data you have. Testing allows you to verify how the app actually functions, and ensures that you understand how it stores data. It also shows how your forensic tool (or parser) decodes, parses, and presents the data.

Testing an app properly takes some effort, especially up front, but it's worth it when your findings are well documented. Strong app testing methodology will give you ironclad testimony skills in court and solidify your credibility as an expert witness, because it takes you out of the realm of assumption-making and firmly into the realm of provable facts.

Skill 7: Create Known Data

Creating known data helps with decoding, later in the process. Known data gives you a sense for how data is stored and how the device interprets it. For example, when you take a screen capture of a text message with a date and time stamp, it can help you understand the device's date/time format as a reference point.

Since you've already researched app functionality, you can script your test ahead of time. In addition, to save time, build a research profile using fake contact information, chats, location data, etc. that you can store in test iTunes and Google accounts. That way, the data will auto-populate from profile to test device (or emulator) when you log in.[5]

Once you have a profile building plan, the correct app and operating system versions, and you know what you want to test on each app, start recording profile data using a test reference device of the same make/model/OS version/app version as the exhibit.

Skill 8: Use Your Known Data to Test App Functionality

After you've recorded the fake profiles, it's time to test the data you've created. If possible, test the app across Android, iOS, and any other relevant platforms. It's important to know how an app developed for Android stores and displays data it receives from the same app on an iOS device, and vice versa.

In addition, cross-platform functionality can be different. An app's iOS version may have features that its Android version doesn't. If you only focus on one and not the other, you may never know what happens when the iOS app with geolocation sends data to the Android without, and what the Android does with the data when it receives that feature.

As you go, be sure to capture screens and record timestamps to document the test.

THE PRACTICAL BENEFITS OF CREATING KNOWN TEST DATA

Although creating known data can take time, it can be fun if you work with others to create it. If you're a student, you can collaborate with other students or find a mentor. If you're a professional, you can mentor students or junior forensic examiners.

Creating known test data has multiple benefits:

- You avoid using your own or someone else's personal data.
- You can include "distractor" data that has nothing to do with a "case" your fake profiles are the subjects of, such as contacts the "suspect" never actually communicated with.
- Creating known data using a scenario gives you knowns, as well as making it easier to record accurate timestamps and any oddities.
- It will be easier to reuse the data to test the next app—including if you end up lending or borrowing someone else's test device, you can make testing easier for them in the future, too.
- You'll have built relationships with other examiners for future research. Build your playbook as you go. You may only have time to focus on case-related research.

[5] Learn what to do before you create data in our blog, "Being Forensically Curious: The Process of Testing," published November 30, 2017 and accessible at https://www.magnetforensics.com/blog/being-forensically-curious-the- process-of- testing/

Skill 9: Learn How to Find and Parse Unsupported Data

Test smartphone images can be large, so it may be difficult to find where the app stores the applicable test data. Unfortunately, it isn't as easy as looking in data/<packagename> for the app's storage because associated files (e.g., attachment data), might be stored in media/0. Also, different apps store data in different paths, so evidence could potentially be located in multiple places.

Once you find the files and locations where the app stores data, it's time to parse—to decode, or break down—the data into human readable format. This may mean using a SQLite or plist viewer, which can help determine how apps use those data files. Remember, some data may have been stored in proprietary formats, encoded, or encrypted, adding a level of complexity.

After you've reviewed that data, ensure you look for any other applicable databases that could contain data such as attachments. (If you can't easily see the data, it may be stored in a proprietary format.) You can also look for applicable files and databases based on test data.[6]

To do this well, learn to differentiate:

- App metadata from user data, especially as the two can be intertwined
- Probative or responsive data from "distractor" data
- Structured from unstructured data

For example, just because a device recorded WiFi hotspots doesn't mean the user actually visited the location. Likewise, just because the app used permissions to record data such as a contacts list, doesn't mean the user actually contacted those people using the app. Your testing skills will help you determine how much or how little data bleeds over from permissions and other functionality into databases.

Keep in mind that many apps that advertise "end-to-end" encryption only cover data in transit, not data at rest. Since the data at rest remains unencrypted, it is readily available to be interpreted and examined. Search for scripts or papers to help you find unencoded stored data, or see if a vendor can help. If you can't obtain some content because it's encoded, you can still obtain metadata or other content to correlate.

10 STEPS TO MAKING TIME FOR FORENSIC SKILL-BUILDING

Even using a clearly defined method can challenge your time and energy. How can you make the time to perform the critical validation your cases need, and still have enough time to devote to your other cases? Here are 10 steps toward making forensic research part of your everyday workday.

- Sometimes the low hanging fruit will be enough, or will have to be enough, because other cases take precedence.
- When it isn't enough, prioritize your research by whether one or more artifacts seem to be missing or need to be proved, or simply seems out of context.
- Validation—research to prove what a result means or how the artifact came to exist—counts as forensic research. That's important when there isn't published research to explain something you don't understand, your go-to tools don't support the artifacts, or if the device is being submitted as evidence in a case.
- Use your forensic tools to automate as much of your process as you can, so you can spend more time validating to understand the results from your tools.
- Make it a point to learn something new each week, whether it's a new fact about an artifact, file or operating system, by reading forensic blogs and doing your own research. You could also learn these new things during your workout or commute to work by listening to forensic podcasts.
- Get your lab manager's buy-in by stressing that verifying and validating your findings will give you confidence in your conclusion(s).
- Demonstrate the value of your research, not only to your case, but also what it means for other investigations down the road: time savings, or some other key performance indicator.
- If something is really interesting, but you can't find existing research about it, consider taking personal time to figure it out.
- Seek ways to make forensic research more rewarding: submit a proposal paper to a conference or a guest blog, partner with someone else on a research project, or participate in a challenge like a Capture the Flag competition.
- Build your playbook as you go. You may only have time to focus on case-related research.

[6] Get additional details on what to look for in our blog, "Being Forensically Curious: The Process of Finding and Parsing" published December 14, 2017 and accessible here: https://www.magnetforensics.com/blog/being-forensically-curious- finding-and- parsing/

Skill 10: Apply Your Method to Case Data

After creating and parsing test data to understand where and how the device stores it, it's time to apply that method to the same stored data in the case evidence. Compare your evidentiary data to your known data. By noting how, for example, two simultaneous conversations, their time stamps, and their user IDs are stored, you can use the knowledge you gained from testing to explain how it works with the evidence.

Bear in mind that sometimes evidentiary data doesn't parse out the same way test data does, even with the same app/OS/versions/models. Results depend on several factors, including the acquisition method and whether the test is on a jailbroken or rooted device.[7] Be sure to examine the files manually within the directory to be sure you don't miss anything.

Following these ten steps will enable you both to recover mobile device evidence that isn't supported by commercial tools, and to validate the evidence those tools do recover. Having a better understanding of the scientific principles that underpin your forensic tools enables you to evaluate those tools more thoroughly, to be sure they're effective and will deliver their money's worth.

FIND UNSUPPORTED MOBILE DEVICE EVIDENCE WITH MAGNET AXIOM

Magnet AXIOM was built with an artifacts-oriented approach that can help you find more evidence from unsupported apps, giving you a stronger foundation for your manual validation. AXIOM's Dynamic App Finder enables users to discover chat, geolocation, contact information, and web data applications that aren't yet supported by a native artifact.

AXIOM also enables you to build custom artifacts of your own using extensible markup language (XML) or Python scripting. With custom artifacts, you can recover data—messaging, location, browser interactions, etc.—from across an app. When your custom artifact is complete and you've tested it to be sure it works, share it on the Magnet Artifact Exchange so that other AXIOM users can benefit.

In addition, AXIOM can acquire physical images. It also integrates and analyzes images acquired from third-party tools and other methods, such as JTAG and chip-off techniques, for a more comprehensive examination.

[7] For more on how this can happen, read our blog "Being Forensically Curious: The Process of Finding and Parsing" published December 14, 2017 and accessible here: https://www.magnetforensics.com/blog/being-forensically-curious-finding- and-parsing/

If you'd like to learn more about Magnet AXIOM and how the Dynamic App Finder, custom artifacts, and other capabilities can help you support otherwise unsupported data, visit magnetaxiom.com. 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