Journal of Forensic Sciences And Criminal Investigation
ISSN: 2476-1311

Juniper PUBLISHERS key to the Researchers

Research Article
Volume 17 Issue 1 - February 2023
DOI: 10.19080/JFSCI.2023.17.555951

J Forensic Sci & Criminal Inves

Project Management in Digital Forensic Investigations

Greg Gogolin*, Isaac Gogolin and Seth Gogolin

Center for Cybersecurity & Data Science, Ferris State University, Big Rapids, Michigan, USA

Submission: February 14, 2023; **Published:** March 03, 2023

*Corresponding author: Greg Gogolin, Center for Cybersecurity & Data Science, Ferris State University, Big Rapids, Michigan, USA

Abstract

Digital forensic investigations often occur in crisis mode or with little advanced notice. Digital forensic examiner background and expertise can vary widely, and all too often forensic training is specific to a particular tool set. These factors can limit the ability to manage digital forensic projects. Project management has been used in the Information Technology field for decades, and many of the benefits of this type of structured approach can lead to stronger and more consistent investigation outcomes. This article proposes utilizing project management principles such as developing a project plan with time estimates and dependencies, risk management, and a post case review to improve digital forensic case management. The combination of project management and utilizing best practices in an investigation execution strategy for digital forensic investigations can lead to improved outcomes.

Keywords: Digital Forensics Project Management; Digital Forensics Investigation Plan; Case Management; Forensic Imaging Time Estimation; Incident Response Project Management; Digital Forensic Imaging

Abbreviations: CSAM: Case When Child Sexual Abuse Material; IOT: Internet of Things; NIST: National Institute of Standards and Technology

Introduction

In the 1960s, Project Management was shaped by professional associations and eventually became more formalized by organizations such as the Project Management Institute [1]. Project management has been utilized in the IT and engineering fields for several decades, with more recent adoption of project management into several other fields including marketing and health care because of its ability to help successfully direct projects. Digital forensics began to gain traction as a discipline in the early 2000's, with much of the focus in the law enforcement area. With the rapid rise of cybersecurity incidents, digital forensics became a key aspect of incident response in a broad range of organizations and industries. While digital forensic methodologies have progressed, proper management techniques have lagged the proliferation of digital forensics. This article seeks to raise the awareness of the need for project management in digital forensic cases and to draw a distinction between the use of methodology and the use of project management. In simple form, methodology is how to perform a task whereas project management is when to perform a task.

When an investigator is faced with investigating a case it can be a daunting experience. Identifying the correct steps to follow, what information to look for, and conducting an accurate examination are but a few of the challenges to address. On the surface this may seem rather obvious but in reality, cases are often not that straight forward, particularly for new examiners. In an educational setting digital forensic exercises are often structured and brief. Most of the exercises tend to be focused on a specific competency rather than a full life cycle investigation. Using a methodology for digital forensic examinations is not new [2] nor is the application of the Scientific Method, [3] but using formal project management in digital forensic situations is not common. Project management has been proposed for IT security projects since at least 2006 by Snedaker & Rogers [4] but proposing the use of project management in digital forensic and incident response scenarios is relatively unknown.

An investigation is a project, so project management principles lend themselves well to digital forensic investigations. Developing a project plan helps to ensure the proper steps are performed in the proper order while also providing an overall view of project scope. A project plan can provide the opportunity to integrate organizational policies into the project management process, thus providing a method to help ensure compliance. Developing a customized project charter which includes a project description, identification of limitations, assumptions and risks, as well as budget and potential payback can help determine if a project is viable and what level of resources are appropriate. It should be noted that project payback, also known as return on investment, could take many forms in a digital forensic environment including return of a system to service, conviction, etc.

It should be noted that organizations may develop a threshold on what degree to utilize project management, as digital forensic investigations can vary from a situation that may take minutes to perform to a situation such as the January 6 attacks on the United States Capitol, which was one of the largest digital forensic scenarios in history. This article outlines many of the considerations that should go into creating a digital forensic project plan. Planning for an investigation helps ensure a more thorough and positive outcome. Something that digital forensic investigators are faced with is like what people working in Information Technology often face: the problem is not clearly defined, it is unclear what needs to be done, and there is an assumption that those in the technical field know what to do.

Lack of planning can be easily described using building a house as an example. Requesting that a builder construct a three bedroom range style home is not detailed enough for the builder to know what to do. While the builder knows how to build a house, the details are what is important. Where to locate the house on the lot, color, number of bathrooms…the questions are endless. Similarly, a request for a forensic investigation is often made with little or no background information or investigation objectives provided. “Go through this phone and let me know what you find” is an all-too-common occurrence. A project charter can be used to identify the objective, outline scope, and identify risks and risk response. The charter can also specify which methodologies to utilize and who to involve.

Methodology can explain which procedures to follow from a technical perspective, but methodology can also specify how to obtain background information about a case and tasks such as developing interview templates and conducting interviews. There are a variety of first responder guides and publications such as those from the Department of Justice [5] and many digital forensics investigation books, including Casey [6] and Sammons [7], that can form the basis of digital forensic methodology. However, project management would be a broader perspective and may incorporate many digital forensic cases and methodologies in one case. Case management software is taking hold in some areas, but case management software tends to cover only a portion of project management. This article is focused on identifying the steps that should be taken throughout the entire investigation, not on describing the techniques of how to perform a specific task with a specific tool.

One of the motivators for writing this article originated from reading investigation plans from students. In their plans, students would often write about working alongside law enforcement, seizing the computers, and bringing them back to a lab for processing. While this may occur in some situations, there are many times when this is a fairy tale. If the case at hand is a civil case, then law enforcement may not be involved at all. While criminal cases operate under a search warrant, a civil case often operates under a court order. An investigator may be able to seize equipment in a criminal case, but in a civil case the investigator often schedules time to investigate on the site of the source of information, which may be the opposing counsel’s law office with observers present. Cases that occur in a corporate setting can vary substantially from both criminal and civil cases - at least initially. Corporate cases may or may not develop into criminal or civil cases, and in many situations corporate case pursuit often depends on monetary considerations rather than legal. In all cases, notes should be captured throughout the life of the case.

An additional focus of this article is to provide a perspective to investigators into how investigations can effectively be conducted. That isn’t to say that everything presented is the only way or best way to conduct every examination, but it will help to ensure that investigations are thorough and follow a set of best practices. Another thing to keep in mind is that digital forensic cases typically involve at least two parties, so there will often be two sets of investigators. The quality of work and expertise of each investigator will become apparent in such situations, so it is important to perform the most complete and accurate examination possible. I have assisted law enforcement in dozens of cases and in some situations have worked with defense. Countless times I’ve seen less than best effort work presented as evidence. All too often an investigator plugs a phone into a tool such as Cellebrite, generates an automated report, and considers that a complete investigation. No keyword searches, no corroborating evidence, and no passion for excellence.

Project Charter

The topics in this section would be incorporated into a project charter. In addition to what is listed subsequently, a project charter would describe the objective and scope, stakeholders, and the approval process for things such as how, when or why to proceed with an investigation.

Obtaining Authorization

The first step in any investigation should be obtaining valid authorization to conduct the investigation. Verbal authorization breeds confusion so it is best to obtain authorization in writing. Written consent is a written and signed authorization for the investigation - email consent may be problematic. A search warrant is an authorization signed by a judge and generally applies to criminal cases. A court order is also an authorization signed by a judge and is generally the search warrant equivalent in civil cases. The legal issues regarding consent to search are covered in detail by Lonardo [8]. These issues should not be taken lightly as the implications for digital forensic experts can be significant [9].

In a corporate setting the computer resources are typically the property of the corporation, so authorization often comes from a corporate officer, or some other person qualified to provide authorization. In many cases the investigation may be confidential or clandestine, which can create a series of challenges to execute the examination in secrecy. Another challenge with a corporate investigation is that the examiner may know the subject of the investigation. It should be noted that authorization for an investigation may have restrictions. Just because an examiner has access to a device doesn’t mean they have full unfettered ac-

How to cite this article: Greg Gogolin, Isaac Gogolin and Seth Gogolin. Project Management in Digital Forensic Investigations. J Forensic Sci & Criminal Inves. 2023; 17(1): 555951. DOI: 10.19080/JFSCI.2023.17.555951

cess. Fishing expeditions are not commonly allowed, particularly in civil cases. Search warrants and court orders may have very specific criteria that must be respected at the risk of contempt of court. These conditions may include certain timeframes, certain areas of a device, and/or keyword and search conditions.

Identify Tools and Resources

The tools that an examiner chooses to use can depend on many factors including what tools are available, the type of media being examined, and what tasks the examiner is trying to accomplish. If the device to be examined was a personal computer, then Forensic Explorer, Axiom, X-Ways or EnCase may be the tool of choice. It is best practice that the forensic software runs on a dedicated machine/virtual machine that ideally is reset for each investigation to help prevent cross-contamination. A field machine may be a laptop with multiple connection ports whereas a specialized forensic workstation would be a great choice for use within a lab. There are imaging tools and dedicated mobile forensic tools that may be used in the field as well. Forensic software licenses are often validated with a dongle or through an Internet connection. Obtaining a stable Internet connection in the field can be problematic, so a dongle option can be helpful. Several imaging software titles don't require license validation for use, so that can eliminate the need for an Internet connection in the field if the primary operation being performed is the imaging process. Incorporating one or more hashing techniques into the imaging process is an important detail that should not be overlooked. If the computer to be examined is powered on it is good practice to image the RAM and potentially perform the imaging process while the computer is powered on. Encryption may be bypassed for a powered-on device while a powered down disk may be encrypted to the point that it isn't possible to examine.

Additionally, cloud storage and other network connected aspects may also be accessible to the examiner while the computer or mobile device is powered on. Ab Rahman and Choo propose a cloud incident handling methodology that describes cloud considerations [10]. If the computer of interest is powered down, then a forensic disk imager can be used. A forensic disk imager is usually the fastest way to take an image and may be able to create multiple copies simultaneously. A second copy may need to be distributed to another legal team or jurisdiction, so forensic disk imagers can be very valuable. They can also be used to forensically wipe and prepare disks to be used as forensic target media or to simply destroy the data on a disk.

For a computer that is powered down the storage should be connected to a write blocker. This would include hard disk drives, solid state drives, and USB/similarly connected drives. Write blockers also have the capability to work with SD and microSD cards and other types of storage media. The capability that a write blocker provides is the ability to access a device without altering its contents. Booting a computer will modify some of the files on a computer but connecting the same drive to a write blocker and then powering up for the imaging process will not modify any files. This can be validated through hashing. If the device to be examined is a mobile device or smart phone the forensic software used is often different than that used for computer forensics. Forensic software such as Axiom can be used for both mobile and computer forensics but software such as Cellebrite or XRY may be more widely used for mobile devices.

Smart phone extraction is different than computer imaging in that a bit for bit copy of the mobile device is typically not taken in the smart phone extraction process. Mobile device extraction may be logical or physical, with physical processing being more precise. However, support for what devices can be physically processed is limited relative to those that can be logically processed, and particularly with iPhones, physical imaging may not be possible. Additionally, the level of support in terms of what can be extracted varies by device, device operating system, applications installed, forensic software vendor, and release of the software. Storage for the imaged drives and device extracts is part of the preparation equation. Having only one target storage device is a gamble because if something doesn't go well with that storage device then the examination process will slow or stop. Having a backup storage device for each target just in case something goes wrong will save the day on occasion.

Having multiple targets drives available can also allow for multiple devices to be imaged and/or processed simultaneously as well. It isn't unusual to have to process multiple devices, and if they can be processed simultaneously a lot of time can be saved. Since this section described the imaging process this would be a good time to point out that images can be encrypted and/or password protected. This may be a requirement of the investigation. Examiners should be aware that if the password to an image is forgotten that password recovery can be difficult to impossible. An additional consideration is image storage. Images can be stored on a network or cloud device, as well as on an external drive. Network and cloud storage needs to be backed up and securely handled in a similar manner that original evidence would be handled.

Images that are stored on an external drive can be packaged in the antistatic bag and box that the drive came into and then be placed in a safe or similar secure area when not being used. Thumb drives can be handled in a similar fashion. Proper storage includes considering environmental issues such as heat and humidity as well as access control. Proper storage and cataloging of evidence and the corresponding backups are distinguishing characteristics of a sound investigation. For critical cases it is advisable to also store the version of the forensic software and tools used for the examination. Cases can take years to play out and software changes frequently. Being able to access an image with the tools that were used in the original investigation may be critical to an appropriate resolution.

Identify Potential Risks and Safety Hazards

Identifying risks and safety hazards was an early career point of ignorance. Risks to an investigation can be technical in nature such as a malfunction or lack of support for a particular technology. Attempting a dry run prior to commencing an investigation can help identify risks. Reviewing previous case notes and speaking with other investigators can also provide insight. But the problem is that the very nature of digital forensics involves emerging technologies and dealing with things that may not have a precedent. In the scheme of things, the technical risks can pale when juxtaposed to safety hazards.

An example of safety hazards can be illustrated with this scenario. I was working a civil case that involved a partnership split of a business. The party that engaged my services had a personal protection order out on the other party. The objective was to go into the business in the middle of the night with the owner and image the computers in the business. I asked the owner to notify the local police to make them aware of the situation. As the owner was driving me into the parking lot, she indicated that the partner lived in the apartment above the business. I assumed the personal protection order would ensure an element of safety. As I began working on a computer that was located under a desk, the owner indicated that the partner was approaching the building. He entered, thereby breaking the protection order. I had not met him before and was not interested in a confrontation. His eyes were bloodshot and somewhat glassy. He asked if the computers would be there in the morning, and I informed him that they would be as I was only imagining them. He appeared satisfied and left. Ten minutes later the business partner I was working with indicated that the other business partner was returning. I was immediately concerned that he was returning with a weapon. He entered the building, again breaking the protection order, and began arguing in a very agitated state. I packed up and exited the premises as quickly as possible.

This is one of many types of scenarios an investigator may be faced with. Prior to that situation I had not been concerned with getting shot while performing a digital forensic investigation, but I then realized the importance of developing a risk and safety plan for every investigation. Certainly, there are also health considerations including situations such as the COVID pandemic and other biohazards. Scene specific conditions may include dogs, people with questionable stability, children, drugs, and a host of other safety concerns. Bottom line, safety first.

Identify Actions to Take if Risks Occur

It isn't enough to identify risk and safety issues. One must develop plans of action to take if a risk or safety concern manifests itself. Risks can take many forms and maintaining a risk registry of potential risk factors is an important first step. These lists are meant to be augmented as new risks are discovered. It is important to actively perform risk scanning and awareness. From a safety perspective this may include extra precautions such as not working alone, as well as having a first aid kit and active cell phone service. Risk response should be prudent and responsive. Being indecisive can lead to a less than desirable outcome. While you don't want to be hasty, it is better to err on the side of safety than to risk a situation going bad. This may seem overly dramatic, but it only takes one encounter with someone who is agitated and emotionally charged to find yourself in a very difficult situation.

Specifically, identify possible risks and the possible responses to take should a risk occur. Another risk is losing evidence. This can range from environmental factors or misplacing something. Misplacing something may sound like sloppy work but there can be more to it than that. Cases can drag on for years. I've received calls on cases that were handled several years prior that I thought were completed at that time. Don't underestimate those types of challenges. Be clear on how long it takes to archive case evidence and be consistent with your archiving methodology including a chain of possessions. NIST [11] publishes a sample chain of custody form that serves as a good starting point. I've used locking gun cases that are bolted to the floor to hold many dozens of hard drives containing evidence and case files. Having a case numbering scheme that begins with the year, month and day helps in organization.

Losing evidence can take another form that is more along the lines of evidence access rather than physical loss. With the rapid evolution of technology, the various interfaces also evolve. There are different variations of USB, but remember Firewire? Blackberries and Mini USB? A current forensic tool may not support a legacy format, so investigators need to consider maintaining a software, operating system, and interface archive so that accessibility is not lost.

Limitations and Assumptions

Digital forensic examinations may not be able to be performed in an ideal setting. The exam may be initiated in the field, new techniques may need to be developed, and a host of other issues may arise that impact the examination process. When possible, limitations should be identified as part of the project charter. Similarly, assumptions should also be documented. A case that initially appears to be a straightforward computer exam may turn into a multiple device scenario that involves multiple organizations or jurisdictions. Documenting the initial assumptions and constraints early in the process provides help in scope and overall project decision making.

Budget and Payback

There are several ways to quantify budget and payback (return) on a project. There are the monetary costs - things like licenses, storage, training, and equipment. These alone could make an investigation not feasible. But there are other ways to look at budget and payback, with an important one being opportunity cost. For example, a particular project may consume 500 hours of time and $5,000 of budget. The 500 hours should also be quantified in monetary terms. There are approximately 2,000 hours in a typical work year for one person, so 500 hours would equate to about one-quarter of an annual work year.

Using $100/hour for a loaded cost for illustration purposes would translate into $55,000 of labor and budget. The question should be raised as to whether the investigation will return $55,000 in benefits. Beyond that, since the resources are expended on this project, they aren't available for some other project. If the other project has a higher return or a higher likelihood of achieving the desired outcome, then the $55,000 project maybe shouldn't be pursued as it is currently defined. Perhaps pursuing a smaller portion of the project or combining it with another project makes more sense. These types of decision points are not part of most digital forensic methodologies, but they are very much a part of digital forensic project management.

Project Plan Definition

Topics in this section would include estimating time for tasks, labor considerations, and developing a project plan/work breakdown structure.

Estimate Investigation Time

One of the most frequent questions an investigator is asked is how long the investigation will take. Often this question is posed even before the scope of the investigation is identified. To help with answering this question, a few simple metrics can be useful to provide a response. Some of the time considerations are a matter of physics. It takes a certain amount of time to create a disk image in part because of the limits in I/O. Things like using the fastest device possible for the target medium help but that is just one of several potential bottleneck areas. The state of preparedness that an investigator is in impacts investigation time. For example, if the investigator has forensically prepared target media for images and smart phone processing then that time is saved during investigation execution. This may take a different approach if cloud or network storage is used to hold images, although consideration should be given as to whether it is prudent to use local devices such as external USB drives or cloud storage when in the field. In the lab the connectivity to cloud media is likely faster and more reliable than in the field, thus impacting imaging time less.

Gaining access to a device for the imaging process may be as simple as opening a desktop and connecting the drive to a write blocker. However, laptops and Apple computers can take a significant amount of time to gain physical access to a drive, with potential collateral issues such as voiding product warranties. Also remember the time it takes to access and reassemble the device when calculating imaging time estimates. Images can be taken in a compressed or uncompressed format. While compression may reduce the size of an image it may also impact the time it takes to write an image as less space is consumed. Images can also be taken with various forms of verification including internal hashing during the imaging process and a second pass at the image to verify hashes. Encrypting an image can also impact imaging time.

At the time of this writing the rule of thumb that I use is about eight hours per terabyte for a physical bit for bit image. The number of files on a device and amount of free space may influence imaging time, but eight hours per terabyte is a helpful metric for estimation purposes. When given the option, I have generally found that compressing while imaging provides a time benefit. This is contrary to what is often noted in forensic training manuals and methodologies, where they often state that use of compression will reduce the size of a forensic image but increase the time it takes to perform the imaging process. Time spent compressing files can be offset by the time it takes to write an uncompressed (larger) file. (Table 1) provides a summary of imaging test results using FTK Imager, which is commonly used in the imaging process (Table 1).

Table 1: Imaging times.

Image Iteration	USB Type	Source	Target	Device	Imagein Technique	Compression	Encryption	Elapsed Time	# Files	Image size
Comp0-Run1	2	Seagate 250	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 3.4.2.6	0	no	2:20:39	160	232 GB
Comp0-Run2	2	Seagate 251	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 3.4.2.6	0	no	2:18:54	160	232 GB
Comp0-Run3	2	Seagate 252	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 3.4.2.6	0	no	2:18:50	160	232 GB
Comp6-Run1	2	Seagate 253	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 3.4.2.6	0	no	2:05:15	90	130 GB
Comp6-Run2	2	Seagate 254	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 3.4.2.6	0	no	2:06:34	90	130 GB
Comp6-Run3	2	Seagate 255	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 3.4.2.6	0	no	2:05:47	90	130 GB

Comp9-Run1	2	Seagate 256	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 3.4.2.6	0	no	2:21:29	90	130 GB
Comp9-Run2	2	Seagate 257	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 3.4.2.6	0	no	2:20:30	90	130 GB
Comp9-Run3	2	Seagate 258	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 3.4.2.6	0	no	2:20:46	90	130 GB
Comp0-Run1	2	Seagate 259	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 4.2.1.4	0	no	2:19:59	160	232 GB
Comp0-Run2	2	Seagate 260	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 4.2.1.4	0	no	2:17:18	160	232 GB
Comp0-Run3	2	Seagate 261	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 4.2.1.4	0	no	2:19:36	160	232 GB
Comp6-Run1	2	Seagate 262	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 4.2.1.4	0	no	2:04:59	90	130 GB
Comp6-Run2	2	Seagate 263	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 4.2.1.4	0	no	2:05:09	90	130 GB
Comp6-Run3	2	Seagate 264	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 4.2.1.4	0	no	2:05:13	90	130 GB
Comp9-Run1	2	Seagate 265	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 4.2.1.4	0	no	2:17:43	90	130 GB
Comp9-Run2	2	Seagate 266	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 4.2.1.4	0	no	2:17:39	90	130 GB
Comp9-Run3	2	Seagate 267	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	FTK Imager 4.2.1.4	0	no	2:17:06	90	130 GB
Comp-Run1	2	Seagate 267	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	EnCase Imager 7.10	enabled	no	3:03	67	133 GB
Comp-Run2	2	Seagate 267	WD Passport 1TB	HP Intel i7-5600U cpu @ 2.6GHz	EnCase Imager 7.10	enabled	no	2:15	67	133 GB

A 250 GB Seagate drive was imaged three times using FTK Imager 3.4.2.6 using no compression (compression 0), default compression (compression 6), and full compression (compression 9). The sequence was repeated using FTK Imager 4.2.1.4. An external 1TB Western Digital Passport was the target drive and wiped each iteration. With these limited runs, the results were that default compression was the fastest and created an image size consistent with full compression. A single comparison run using EnCase Imager 7.1 using encryption was also performed. The 3:03 run included image verification, while the 2:15 run did not include verification. There are several variables that can impact imaging times including the amount of free space on a drive, the connection technology utilized, and the imaging technology utilized.

These tests used USB 2 for both the Tableau write blocker and the target storage device. However, these tests show that a baseline estimate of 8 hours for 1TB of imaging is reasonable. Something to keep in mind is that not all computer investigations require that an image of the driver be taken. Hooking the drive up to a write blocker and previewing the drive allows an investigator the opportunity to perform a review of its contents to determine if it is of interest. Depending on the situation and the custody of the computer, it may be possible to perform the entire investigation while in preview mode. If a computer is powered on, then consideration should be made to image RAM. There are various ways to accomplish this, but the importance of a RAM image should not be discounted as many types of activities and malware are RAM resident only. Failure to image RAM could mean the loss of RAM resident artifacts. The time it takes to imagine RAM depends on factors such as the size of RAM, method used, and target media. If the RAM in question is part of a virtual machine, then a snapshot of the virtual machine may be the preferred approach.

Practicing the various RAM imaging techniques prior to deployment to a case will provide confidence and time metrics with which to base estimates. Estimating the time, it takes to process a smart phone can vary. I've had phones take 15 minutes and then when processing a similar smart phone had it take a few hours. There are several estimating techniques such as PERT and Delphi, and these techniques may provide more precise estimates. Similarly, including a safety factor in either task estimates or a safety factor for the overall project is a typical project management consideration. Safety factors should incorporate both time and budget. Smart phones and mobile devices are typically handled differently than computers in that a bit for bit image generally isn't taken with a smart phone.

The terms logical and physical processing are used when describing the smart phone forensic process. Physical is typically the more definitive process but the ability to perform physical processing lags the ability to perform logical processing. In other words, physical processing lagging logical processing is often explained in that vendors may provide the ability to perform logical processing but not provide the ability to perform physical processing. This is an important aspect of mobile forensics: often the result of the processing is a report, not an image. This means that to be able to reproduce the same report the device should remain unused. Another important difference with smart devices is that their settings may need to be altered to be able to initiate forensic processing. While this doesn't necessarily mean that evidence will be altered it does mean that the device is not the same.

Altering the settings for processing is not going to create photographs, text messages, or Internet activity, but the investigator should note what was done to the device for processing so that the question of altering a device is documented upfront. Some cases may involve one device whereas other cases may involve multiple devices. If you have the technical capability to perform multiple imaging processes simultaneously your total time spent imaging can be dramatically reduced. Some mobile forensic tools such as XRY can process multiple smart devices simultaneously. Another aspect is that some cases necessitate creating two images as multiple parties may be performing investigations. In situations such as these there are hardware imaging devices that can create multiple copies at the same time. The actual investigation itself depends on the objectives and reasons for the investigation. Simple cases can be analyzed within a few hours whereas complex investigations may require 100 or more hours. Cumulative cases such as January 6 would run into the tens of thousands of hours.

It is in the investigation phase where complicated factors that weren't anticipated are uncovered. This may include challenges such as encryption or finding things that expand the scope of the investigation. This is another reason why assumptions and limitations should be stated in the project charter, and why a safety factor is necessary for estimates. Writing the report may take as much as 30% or more of the time it takes to perform an investigation. A report tends to take considerable time in complex cases, those involving multiple devices, and those where fine detail is needed. A good investigation should be complemented with a good report. Too often reports are unclear and incomplete, which can give the impression that the investigation itself was not conducted with appropriate care. There are other intangibles to include in time estimates including the expertise of the investigator, transportation time to/from the scene, postage time, documentation time, court and/or procedural delays, and archiving a case. While there may be other things to consider when estimating how long a case will take, what has been outlined in the subsequent sections is a good starting point for what goes into creating accurate estimates. Note that time estimates should be included for each task in an investigation project plan.

Approaching the Case with a Project Plan

A project plan typically includes a work breakdown structure composed of the tasks in the project. The sequence of tasks includes dependencies that dictate the order in which they can occur, and this can be influenced by resource availability. Resources include both people and the tools necessary to perform the tasks. The project plan with task time estimates provides a potential picture into how long a project will take and how much it will cost. There are various project management methodologies including Waterfall, Agile and Scrum, but determining which project management technique to use is beyond the scope of this article.

An example of how quickly an investigation can turn is a case involving unauthorized access to a corporate computer. The objective was to find out who logged in and then take corrective action. The case quickly turned into a criminal case when child sexual abuse material (CSAM) was found on the computer. It is important to involve law enforcement when a non-criminal case becomes a criminal case. An investigator may be a corporate employee or a private investigator. As such they do not have immunity from handling certain types of evidence including material involving child exploitation. There is an obligation to immediately involve law enforcement. There may be confusion with how to begin that actual investigative process and what constitutes evidence, particularly with new investigators or with new technology. There are a variety of publications that describe potential digital forensic evidence such as those at NIST [12].

For the purposes of this discussion, the investigative process is focused more on the point to which a device is connected to forensic software and the examination begins. Different tools handle things in different ways and potentially in a different order. This is particularly true with mobile forensic software. Commercial tools that are primarily focused on computer forensics include EnCase, Axiom, Forensic Explorer, and X-ways. Open-source tools include tools such as Autopsy and The Sleuth Kit. Commercial mobile forensic tools include Cellebrite, MSDB XRY, and Oxygen. There are commercial computer forensic tools that support mobile forensic investigations, but generally they are not as strong in the mobile space as the dedicated vendors. Axiom is an example of a strong tool in both the computer and mobile forensic spaces.

Beginning a computer investigation includes connecting the image to the forensic workstation utilizing software or hardware write blocking technology. This ensures that the evidence is not modified during the investigation process. A good practice is to take hashes before and after an investigation to verify that the evidence hasn't changed. Computer forensic tools tend to be menu-driven. Some include suggested configuration options for the evidence case processor, which is often the first step. The art is determining which configuration options to pursue and in which order. In other words, project management. It is common as cases become more complex for an investigator to employ techniques beyond the menu-driven approach. This is where experience and creative thinking come into play.

Being able to think like the subject of the investigation is a valuable trait. For example, menu-driven evidence processors may be preconfigured to find artifacts relative to commonly used tools such as Firefox, Chrome and Google. A more sophisticated user that is being investigated may utilize tools that are more on the fringe and may not be supported by the menu-driven evidence processors. Artifacts left behind by these fringe tools may be overlooked unless the examiner performs some research and develops some unique approaches. Taking it a step further, these fringe tools may not reside on the device in question. They may reside on an external drive or in a cloud account which may not be part of the image. Therefore, the examiner may need to account for the various devices that were connected to the computer in question.

It may be appropriate to process multiple devices simultaneously in an investigation. If this direction is chosen, it is important to provide proper naming and documentation in order to attribute your findings correctly within the report. Processing multiple devices simultaneously is often a time saving consideration. Processing evidence can take several hours so it is common practice to run the evidence processor over night or through a weekend. Processing multiple devices helps reduce idle time. It can also provide consistency in approach, eliminate the need to run common operations multiple times, and help amalgamate reporting. One of the most common operations that an investigator performs is a keyword search. This may be to look for actual words, parts of words, or even patterns. Credit cards are often searched by pattern. For example, an American Express credit card number may start with a 3 and be 15 digits in length that may or may not have dashes or spaces within the 15 numbers. Patterns are commonly searched for using GREP.

Table 2: Classroom slang.

Phrase	Meaning
Airpods	Wireless headphones
And I oop	Oops
Bet	I'll do it
Boi	Boy
Bruh	Dude
Bye Felicia	Aggressive/slightly offensive way to say bye to somebody
Catch the woah	The dance of 10th graders
Clown	Fool, to make a mistake
Cop that	I'd take that (steal that)
Dank	Cool, awesome
Dead	Ridiculously funny
Delish	Yum
Drip	Flex
Eskettit	(es-kett-it) Let's get it
F	To pay respect
Fam	Short for family
Finna	I'm going to
Flex	To show off
Full send	You BETTER do it

G.O.A.T or GOAT	Greatest of all time
Glow up	To become more attractive
Gucci	Cool
Hahah Saaah dude	what's up dude
Hot tea	Spicy gossip
Ice	Expensive jewelry
Jo	Your momma
Karen	Woman that complains and wants to speak to the manager
Kobe	Make a good shot
Left on red	To be ignored; big insult
Let's get this bread	Let's get it, just do it
Lit	Sweet; cool
Mood	To express that something is relatable
No send	DON'T DO IT
Obtain this grain	Variation of «let's get this bread»
Ok Boomer	Ok old person
On fleek	To be perfect
On point	To be perfect
Oof	Ouch
RIP	(Not R.I.P) that's too bad
Salty	To feel bitter about something
Send it	Synonym for «let's do it»
Shade	A dis
Ship	To support a relationship
Shook	To be shooken up/surprised by something
Shooketh	To be shooken up/surprised by something
SickNasty	Rad
Sis	A female friend
Slaps	This burger slaps.
Slay	To have looks hot enough to kill
Smash it	To eat something quickly
Spill the tea	To share spicy gossip
Spoilt	Alternative spelling to «spoiled»
Swerve	Stay clear of the drama
Thick	Curvy
Thirsty	Craving approval/attention
Throw hands	To be upset
Throw shade	To diss somebody
To flame someone	To roast someone
Tothed	To get blocked by Tom Toth
Tryna	Trying to
Vibe	Mood
Vibe Check	To tell someone to check their attitude
VSCO girl	Basic girl who wears srunchies and owns a hydroflask
Woke	To be aware of current events
Y'aint	Y'all ain't
Yeet	A word used to express excitement or as a battle cry

Yote	Past tense of «yeet»
You've been had	You've been served/caught
That's an L	That's a loss/ bad tyr
I'm vibing	I'm chillin'/hangin'
Roger that artifact	Ok boomer
10-4 Dinosaur	Ok boomer

Keywords can be locations, names, objects, or anything that helps identify people, places, actions or things. Interviews are a good way to identify keywords. Different languages, slang, and writing styles that are common in texting are considered when developing keyword searches. Erin Gogolin developed a list of commonly used slang phrases that she hears in the classroom. The terms are in (Table 2) and illustrate how examiners need to consider the environment beyond proper English when creating keyword search terms. Searching for other languages is also a consideration (Table 2). The background just presented illustrates that there are many variables to consider. There may be similarities between cases, but cases can also be unique. Keeping that in mind, the following additional considerations for developing a case investigation project plan.

Darknet and Internet Case Considerations

If the case at hand is a Darknet case or has Surface Web integration, these are some considerations in addition to the more typical digital forensic subsequent steps following this section. A Darknet or Surface Web situation is usually quite a bit different from a typical digital forensic case in that a lot of background work can be involved. Some common steps:

1. Utilize policy and procedure reviews in part for legal and ethical considerations. This should include managerial reviews to provide a second set of eyes and oversight.

2. Equipment setup and security that reduces or eliminates tracking.

3. Budget review - probably involving crypto.

4. Persona building.

5. Establishing the identity of the target to the degree possible and incorporate OSINT.

6. Document when you see it as it may disappear - screen shots, download webpage source code and images, hash files, note time and domain registration. Video screen capture software can be very useful, perhaps with microphone capabilities for narration.

7. Consistency is your friend - same folder structure, same/similar report format.

Pre-Examination Steps

If not a Darknet or Surface Web case, this is where the pre-examination process usually starts. Prior to starting the actual investigation, these are some of the things to keep in mind realizing that there may be extenuating circumstances such as safety factors, compromised environment, or other considerations:

1. Review authorization (warrant/court order/statements)

2. Prepare interview questions and conduct interviews

3. Determine what equipment and techniques may be needed

4. Establish if there are DNA contamination protocols

5. Photograph evidence, document scene and scenario

6. Register serial numbers, etc.

7. Establish custody procedures.

8. Determine if a device is powered on, image RAM if it is a computer, document accounts, active processes and applications, network connections, cloud connections. If mobile, disable lock/timeout/screen saver. Strongly consider imaging the full device even if you have the credentials.

Sequencing Tasks

The sequence of tasks varies by objectives and circumstances of an investigation, as well as dependencies and resource requirements as previously noted. Some situations necessitate getting in and out as quickly as possible and some cases may allow for a more abbreviated approach. Investigators should assume that their findings may end up in court even if that isn't the initial thought. It is a much better practice to perform all steps properly rather than attempt to backfill robustness into an investigation. Which steps to take and in what order depends on several factors. After obtaining authorization, user login/account/device access information is usually first on the list. When starting an investigation, sitting on your hands so that you don't start playing around with things before your plan is set may be a prudent next step. Take a moment to visualize the investigation process.

Following are important things to identify and document in most forensic cases - may vary for computer forensic cases to mobile forensic cases:

1. Document scene, assign team duties if multiple people involved

2. Determine type of evidence capture and processing - imaging, live box, etc.

3. Device identifiers
4. Operating system and version
5. Installed applications and versions
6. Accounts
7. Startup Applications
8. Cloud
9. Logs
10. Connected devices
11. Networks
12. Timeline of activities including file MAC times
13. Administrative tools such as antivirus
14. Scan for malware
15. File signature/hash analysis
16. For mobile

a) Place in airplane mode, utilize Faraday, review battery life/maintain power

b) Carrier and SIM

c) Determine if provider information such as tower traffic reports and subscriber activity is needed, and if so, request immediately

Other Important Initial Steps

1. Identify social media accounts and presence
2. Identify email
3. Internet history
4. Search engine history
5. Cookies
6. Gaming presence
7. Time Zone
8. Cache
9. Recent Files
10. Account Change Event
11. Review graphic files

Identifying Sources of Information

Information can come from many different sources. We've already discussed computers and mobile devices but that barely scratches the surface. There are cell carrier records maintained by service providers. There may be cloud vendors providing various services including servicing applications installed on a device. There may be data being captured that nobody is aware of. Geofencing information could fall into this classification. Vendors such as Google, Apple, and a host of other organizations can passively gather information related to someone's location and application usage habits. Geofencing would be gathering information from the various sources related to a particular geographic area to gain insight into what has been occurring in that specific area.

An application of Geofencing involves trying to tie a particular person to a specific geographic location at a given point in time. Sources of information can also include cars, Internet of Things (IoT) devices, vendors that support IoT devices, security cameras, dashboard cameras, doorbell cameras, and many other types of network-connected or electronic devices. Something as complex as an automobile could have multiple sources of information including car computers, radio - which is often paired and synchronized with a smart phone, and the black box event recorder. Obtaining as much information from as many sources as possible generally provides the best opportunity to complete the most accurate investigation.

Note that retention of potential evidence by various parties may be brief. This is particularly true of cell phone service providers, so pursue the information early. Companies capture an incredible amount of detail through someone's online habits and use of digital technologies. The combination of zip code and birth date can be enough to identify a person based on activities. Everyone has received various types of contacts from companies based on their online activity profile. Cookies can be used to identify organizations that track individuals, which means that these organizations may have relevant information for a case. If organizations are going to assemble massive databases about individuals, investigators should be able to make these organizations pay a price similar to what cell phone carriers, who are frequently asked to provide information on customers.

Validate Findings

An investigation is only as strong as the information it is based on. Findings that cannot be validated should not be reported as fact. Validation can be accomplished in many ways including repeating the steps in an investigation - ideally with another tool. Consistent results produced from two tools are much more reliable than if only one tool is used. Part of the reason is that forensic tools include software, and software can contain bugs. Most vendors release a maintenance release periodically to correct the bugs, but having two different tools reduces the chance that forensic findings are influenced by bugs. Remember, not finding something is every bit as contributory to an investigation as finding something. As such, this should be noted in the final report. Another validation method is to utilize an external review. This is like the academic peer review process when conducting research.

An external reviewer can confirm that reasonable methods were employed, and the results are consistent with what one would expect. There is great value in experience as it can provide a feel for the reasonableness of the results. It also can help confirm if a behavior or finding is an outlier, which is an important characteristic. If results are not validated then they should be described as such, which would not carry the same weight as results that have been validated. The density of findings is also an important part of validation. Finding one image or one example of a Google search does not prove a pattern of activity. It may be coincidental, a typo, or other easily explained reason. However, finding dozens of examples over time, particularly on multiple devices, produces a more conclusive result.

A good investigator strives to produce facts and report all of them. Particularly in a criminal case, it is not the function of the investigator to determine guilt or innocence. Determining guilt or innocence is a function of the judge and jury. Reputations can be irreparably damaged by reporting weak, inaccurate, or inappropriate findings. Lives can be irreparably altered. An investigator must validate their findings and report all of them accurately and appropriately. Only reporting findings that support a particular objective while ignoring findings that may be contrary to the objective are unethical and potentially criminal. Reputations may be irreparably damaged by reporting of weak, inaccurate, or inappropriate findings; this also refers to the investigative team. Verify, verify, verify.

Report Writing

A well written report is one that concisely conveys information in a clear and unambiguous manner. The report writing process can take as much as a third of the time of the investigation. Report writing is every bit as important of a skill as the investigative process itself because the report represents the work involved and conveys the product of the investigation. Most people only see the report, so if the report is poorly written they not only may not understand the findings, but they might also perceive that the investigation was as poorly conducted as the report appears to indicate. Information can come from many different sources and many different forensic tools.

Most investigators tend to submit each report individually rather than take the time to try and integrate the information into one report. Submitting multiple reports leaves the reader to attempt to pull things together, which they may not be equipped to do. Investigations frequently have a time element to them. They focus on a particular date and time. Assimilating information from multiple sources into one integrated report can often be effectively accomplished by constructing a temporal report, which includes a timeline that describes a set of activities, behaviors or events from each information source in one report. Reports should include a title, date, investigator, case number and report version as the title page or report header. Version numbers are important as reports frequently have revisions.

An executive summary/abstract can provide an effective overview of the investigation methods and findings that lays foundational knowledge that may be necessary to understand the rest of the report. A copy of the authorization, whether it be an engagement letter, court order or search warrant should also be included. Larger reports may be organizationally assisted by utilizing appendices for exhibits, and the authorization may logically fit within the appendix. The body of the report documents the findings. This should include documenting the hashes where possible for any device that is part of the investigation. A suggestion is to include the hashes from the beginning of the investigation and the hashes after the investigation is complete to verify that no evidence has changed.

Findings should be supported with artifacts from various sources as well as references so that the artifacts can be easily validated. References can be file name and path, sector location, or similar addressing information. While it is important to note that one artifact or behavior does not prove a pattern of activity, there are times when that is all there is to report. On the other end of the spectrum, child exploitation cases may involve thousands of images. Including these images in a report is not appropriate, and in fact may be the distribution of child exploitative material even if you are a law enforcement officer. This should be handled in consultation with the judge and prosecutor.

One way to handle reporting of artifacts when there is considerable volume is to include a few as a representative sample and to note that the artifacts represent five of the five hundred found or something similar. Another way is to include the voluminous artifacts in an appendix. It is appropriate to include a table of contents and page numbering, particularly in the case of long reports. This can help identify the relative location of information and what is contained in each entry within the appendix. An investigator typically takes notes as they work a case. Including the case notes or a summary of the case notes can be useful in driving the narrative within the report. Notes can also help explain why various methods and techniques were utilized. Reports are often signed, and it isn’t unusual to have each report page initialed. Make sure when you put your name on something that you are comfortable with the product. In most cases an investigator’s report will be challenged, and this challenge often comes from another investigator. If their report is more precise and complete than your report, you likely be viewed as less competent. If you put your name on a report that was not accurate and that is successfully challenged by another expert your reputation will be impacted. Verify, verify, verify.

Preparing for Court

An exercise that is particularly useful in the classroom is to give the students a case to investigate and have them perform an analysis from both the defense/prosecution and plaintiff/defendant perspective. Looking at the case from each perspective provides insight into strengths and weaknesses, while also helping to anticipate possible questions during court examination. Going through the various forensic reports with the team that you are working with is important so that everyone understands the facts in the case. It is critical that the forensic examiner presents facts, and that they are accurate, appropriate, and not one-sided. This is maybe best described using a case.

Forensic tools often designate a text message as read or unopened. I have seen text messages being presented in court in this manner. However, just because a forensic tool notes a text message as read doesn't mean that it has been read. In the case of an iPhone, if someone has an open iMessage channel with someone else, the messages will automatically be marked as read because the channel is open. The iPhone could be in the glove box when the message was received, but it the iMessage channel is open the message will be marked as read. Similarly, if the screen is locked, if an iMessage comes in and the person simply swipes it away it will be marked as read. There are many ways an iMessage can be marked as read by the forensic tool when in fact it wasn't.

In the discovery process the parties to the case may become aware of strategies. Be prepared to question everything, including a critical review of the methodologies involved. Cases where cell phone tower traffic is used to pinpoint someone's location at a particular time are an example. Readings from one tower are not sufficient. At its best, a single cell tower may be able to provide a circle of area around a tower, but multiple towers are necessary for more precise location. Time to tower readings, tower traffic, weather conditions, geography and signal skip are but a few of the things that can impact accuracy. Corroborating evidence is very helpful in this type of situation. Often the legal representation is peripherally familiar with the details of digital forensics.

Developing a list of questions to ask the opposing team may fall on the forensic examiner. This would include reviewing the processes utilized to ensure they were appropriate, chain of custody, and the skill set of the examiner. A question that should be anticipated in any case is if the examiner is aware of any other evidence and if the findings were validated. Validation can be performed by using a second tool and obtaining the same result. Corroboration would be another way to confirm something. In a car accident scene, the event data recorder can provide useful information as to time sequence and potentially accident reconstruction. I've seen cases where only one vehicle's event data recorder was analyzed in a multi-vehicle crash. This is an example of evidence being left in the field and an indication of less than thorough work.

Summary

Digital forensics is stressful and can lead to many sleepless nights. Following procedures that reflect best practices and focusing on facts over emotion can help examiners maintain a clear head and produce positive outcomes. Using project management techniques that incorporate a standard methodology that is updated as experience and situations dictate can provide for a much smoother case experience. Project management is commonly used for Information Technology projects to improve project outcomes, and digital forensic examinations should seek to leverage the same benefits. Creating a project charter includes defining the objective and scope, stakeholders, and the approval process for things such as how, when or why to proceed with an investigation.

Further aspects include obtaining authorization, identifying risks and safety hazards, risk response, limitations and assumptions, budget and payback. A project plan includes time estimates, a work breakdown structure composed of appropriately sequenced steps and procedures for organizing an investigation, and time and budget safety buffers. The last step in the process is to evaluate how the examination went and to update the methodology and project plan templates accordingly. Follow up reviews of investigations can take many forms such as the format suggested by Grispos [13]. The most important thing is to consistently review and refine investigative processes to provide the best possible investigative outcomes. Utilizing project management appropriately will help an examiner provide consistent results.

References

1. Garel G (2013) A history of project management models: From pre-models to the standard models. International Journal of Project Management 31(5): 663-669.
2. Carroll O, Brannon S, Song T (2008) Computer Forensics: Digital Forensic Analysis Methodology.
3. Gogolin G (2012) Digital Forensics Explained. CRC Press/Taylor and Francis, New York.
4. Snedaker S, Rogers R (2006) IT security project management handbook. Syngress. Rockland, Massachusetts, USA.
5. US Department of Justice (2008) Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition.
6. Casey E (2009) Handbook of Digital Forensics and Investigation. Academic Press. Amsterdam, Netherlands.
7. Sammons J (2012) The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress. Amsterdam, Netherlands pp. 313.
8. Lonardo T, White D, Martland T, Rea A (2011) Legal Issues Regarding Digital Forensic Examiners Third Party Consent to Search. Journal of Digital Forensics, Security and Law 6(4).
9. Liles S, Rogers M, Hoebich M (2009) A survey of the legal issues facing digital forensic experts. In IFIP International Conference on Digital Forensics, Springer, Berlin, Heidelberg pp. 267-276.
10. Ab Rahman NH, Choo KKR (2015) A survey of information security incident handling in the cloud. Computer Security 49: 45-69.
11. (2017) National Institute of Standards and Technology | NIST.
12. (2022) National Institute of Standards and Technology | NIST.
13. Grispos G, Glisson WB, Storer T (2017) Enhancing security incident response follow-up efforts with lightweight agile retrospectives. Digital Investigation 22(1): 62-73.

How to cite this article: Greg Gogolin, Isaac Gogolin and Seth Gogolin. Project Management in Digital Forensic Investigations. J Forensic Sci & Criminal Inves. 2023; 17(1): 555951. DOI: 10.19080/JFSCI.2023.17.555951