A Forensic Computing Framework to fit any Legal System

SSG Steven W. Wood
US Army, Retired
steven.wray.wood@us.army.mil

"The opinions or assertions contained are those of the writer and are not to be construed as official or reflecting the views of the United States Army."

Abstract: The demand for examinations of digital evidence is on the rise the world over. The majority of the academic work in this field comes from the United States and is heavily geared toward the American legal system. This makes using such a framework very difficult in other countries where the legal system can be fundamentally different. This paper proposes an extended framework that can be used in any jurisdiction in the world. It is our goal to take the existing state of the practice and add a level of abstraction that will increase its usefulness.

1 Introduction

The processing of digital evidence is a relatively young and extremely dynamic scientific field. While great strides have been made in the development of standards and procedures there is still not even an agreed upon name for what it is that we do. The author has come to prefer the term *forensic computing*, which is based on the experiences gained over the last 9 years of doing this work full time. Forensic computing is generic enough of a term to encompass all digital evidence that might need to be examined, yet detailed enough to prevent confusion as to what is being done. Stated in simple terms a computer is used to process evidence that will be used in a court to answer a legal question. Sheldon used the term forensic computing in his look at the diversity of the field. [SH01] Even if we examine a cellular telephone for example, we will need a computer with special software to complete the work. The same could be said for looking at evidence contained on the hard drive of a networked refrigerator.

There are numerous frameworks in the literature of which no single one seems to cover all of the areas that are encountered on a daily basis. The majority of these frameworks seem to be written from the perspective of a single person who is tasked with working an incident from the very beginning to the end. In the real world this is rarely the case, with many people working together to complete the larger task. Current frameworks are further not flexible enough to be applied to differing legal systems, as they seem to be written exclusively for use in the United States. Finally the majority of these frameworks are geared toward purely computer crime incidents when in fact examinations are performed for many other crimes on a regular basis such a rape, murder or terrorism.

This paper will work to define a new framework based on the experiences gleaned from over 1000 cases processed in a government contracted computer crime lab.

1.1 Background

Numerous models have been proposed for digital forensics over the last decade. In a paper written by Pollitt [PO01] there are no less than 15 models that are examined. The common theme between each of these models is that they all appear to be written overwhelmingly for the United States legal system.

It must be noted that many of the biggest names in the traditional forensic fields (Mathieu Orfila and Alphonse Bertillon of France, Hans Gross of Germany and Albert S. Osborn of the United Kingdom to name just a few) were not only non-American, but they performed their work in their respective home countries. A truly universal framework would therefore need to be abstract enough to apply in any country in which it was to be used.

There are numerous scientific principles when dealing with any discipline of forensics that are universally applicable regardless of the country or jurisdiction they are being used in. The difference that we will see is in how these principles are applied, which will be done in accordance with the local legal code and current jurisprudence at that location. While many legal systems are similar in nature, they can vary greatly in content and interpretation. This is evident from the fact that in some countries pictures of children being sexually abused are still not illegal. [ICM01] We cannot take for granted that the way things are done in the United States, or wherever else one lives, is the same around the world.

This paper proposes a new framework for forensic computing professionals that will offer the following:

- International applicability by ensuring enough abstraction to allow any legal system to be supported.
- The framework will give the ability to improve completion times of cases by optimizing the workflow.
- The framework will concentrate on what needs to be done and not how the person should do it.
- The framework will be equally applicable to any type of examination or investigation being conducted whether law enforcement or civil in nature.

1.2 Outline of the Paper

Section 2 of this paper will cover the overarching forensic principles that will surround all of the work being done by the examiner. Section 3 will discuss the framework itself and go into detail on the steps that will need to be taken by the examiner when working a case. Section 4 will touch briefly on the concept of skill levels that are for future work with the framework. Section 5 looks at a test case using the new framework. Section 6 talks about the benefits of the framework. Section 7looks at the future work planned by the author and Section 8 is the conclusion of the paper.

2 Forensic Principles

The model which we are proposing will consist of 6 general scientific principles that can be mapped to anywhere in the world and the corresponding legal code. These principles are not part of the framework itself in that they are not a specific step taken every time the framework is used. Instead they are always present in the background and must be observed by the practitioner at all times. The concept of principles in a forensic framework was proposed by Beebe and Clark. [BC01] These principles are to be thought of as continually running processes that have no clear starting or stopping point. It is fair to say that these principles wrap around the scientific process being performed in the actual steps of the framework. This abstraction shifts the framework from telling the user *how* to do something to telling them *what* they need to do.

We find it important to include these principles to ensure a form of quality control that is always present when the framework is being followed. The principles are not concrete steps that are performed by an examiner but are abstract in nature. How they are carried out, and to what standard, will be decided based on the location of where the work is being performed. The framework however does dictate that the principles are to be used.

2.1 Overview

We can see in the below figure what the principles look like. You can see that there is nothing new or earth shattering here. We are simply taking these common concepts out of the physical steps done by an examiner and abstracting them. This makes it possible to adapt to any set of rules or regulations that need to be followed.

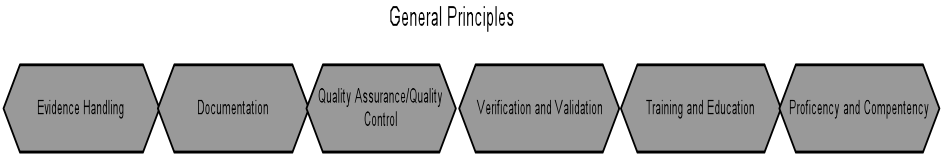
General Principles
Evidence Handling
Documentation
Quality Assurance/Quality Control
Verification and Validation
Training and Education
Proficency and Compentency

Figure 1: The six General Principles.

2.2 Evidence Handling

This is clearly one of the most important parts of any forensic process so why would it be listed under general principles? That is because it is not feasible to cover every possible combination in a framework for every country in the world. It must be the responsibility of the practitioner to make sure they are in compliance with the applicable laws and procedures of their jurisdiction.

What if for example one jurisdiction requires that two copies of all evidence be made on-site? What if another jurisdiction requires simply that the person making the digital copy of the evidence needs to take a picture of what they are doing? What if you are working a strictly intelligence-related case where evidence handling has no bearing at all? Any framework that tried to capture all of these different scenarios would be overly complicated and simply unusable in the real world.

Being a general principle puts the responsibility entirely onto the practitioner to meet the current standards of their jurisdiction. They are the ones who will eventually have to justify their actions in front of a court of law. The standard they will be held to will be the one that is in effect for that jurisdiction and for the type of investigation being performed.

2.3 Documentation

This extremely important part of the forensic process must be considered a principle because how it is done may not only vary between countries, but even between labs in the same jurisdiction. Generally not only must paperwork be accurately filled out and maintained, but the form and content will depend on local requirements. There is no magical “universal forensics form” that has been agreed upon by everyone worldwide that we know of. Information that needs to be recorded at one lab could actually be unnecessary for the next. The examiner will have to follow the rules where they are at and not just make it up as they go along.

The critical requirement here is that the forensic process can be recreated at a later time based entirely upon the documentation that has been kept. A typical forensic lab will not only have hundreds or thousands of cases that they work each year, but it could be many months, or even years, until a case goes to trial. Without the ability to look at the documentation there would be no way to accurately testify as to what was done. The documentation is the only permanent record an examiner will typically have.

2.4 Quality Assurance/Quality Control

Due to the fact that most labs will work differently in performing even the same tasks, there is no single answer for Quality Assurance/Quality Control (QA/QC). The QA/QC program will ensure that the work performed in the lab is in accordance with their documented policies and standards. Results will need to be checked for accuracy and any noted deficiencies will need to be fixed in the processes. This is a very important function needed to maintain the integrity of the entire forensic process.

It is also a responsibility of QA/QC to analyze processes and make recommendations for improvements as needed. Time brings with it new technology which will need to be incorporated into the operating procedures. These will need to be extensively tested and well documented. Experience can also lead to minor changes in certain scientific testing procedures and QA/QC will need to track these and ensure these are put to paper.

2.5 Verification and Validation

This principle differs from QA/QC in that it is not interested in examining policies and procedures but strictly concerns results of tests. If for example a SHA-256 hash value is calculated for a file there must be a way to make sure that it is correct. QA/QC will need to have policies and procedures in place for making that possible. Going through those steps to actually check the results will be the verification.

Validation deals with the results and output of the various tools and procedures being utilized. It is the sole responsibility of the practitioner to make sure that their tools and results are correct. When new versions of software are released they must be validated to make sure changes to them do not produce unexpected results. Validation is an ongoing process and not some single step in performing a forensic examination.

Validation will also need to be conducted on the tools being used to perform the examination. When using any software many events may cause the program to enter an error state in which it can produce unexpected results. These unexpected results may or may not be correct. If the examiner uses these results as the basis for making a finding it is highly possible that it will be wrong. This means that for each new version of Windows for example, tests will have to be conducted to see if the forensic software tool being used produces the same results as before. Changes to the underlying operating system can cause us to see different results even when using the same version of the examination software.

The same validation must be conducted on the forensic tools themselves used by the examiner. Vendors tend to release small updates to their software on a periodic basis. It must be noted that most of these updates are done to address bugs found during the use of the product. Validation will show if the fixes cause any other output to change. During validation it is also possible to determine, by using known sample data, if a new tool is working as it should. No one would want to just open the box of a new tool and jump right into doing casework with it. What if you did and found out later that a flaw made all of your results invalid?

2.6 Training and Education

There is no end to the learning process regardless of the forensic specialty being practiced. Researchers find new ways of performing existing tests while new technology will bring with it new possibilities. DNA testing is a prime example of this concept. Without continued training in the newest techniques a practitioner will not learn about the changes in the science. Attending training from a variety of providers can give the practitioner a broader knowledgebase from upon which to draw.

Under this principle would also fall the attendance of conferences related to the practitioners primary forensic specialty as well as general forensic-themed gatherings. These events are a great way of exchanging ideas with peers and learning what others are doing. The open exchange of information is a wonderful way of getting ideas looked at by other professionals in the community as well as getting their opinions to any questions you might have.

In forensic computing it is best to attend training covering general subjects as well as specialized courses covering software suites. This gives the student a solid foundation on which they can build their knowledge for using the individual tools. The Certified Computer Examiner Bootcamp would be a good choice for the general requirements. [CCE01] This weeklong class covers basic forensic practices as well as showing the student what is happening at the lower levels of the computer. Guidance Software offers numerous classes that will give a candidate the deeper understanding of how the tools being used work. [GUI01] These classes are geared toward the EnCase line of products but the knowledge gained can be applied to other tools as well.

2.7 Proficiency and Competency

This section is designed to ensure that the person doing the forensic work is skilled and able to perform to standards. What this means will vary from jurisdiction to jurisdiction. Be it a requirement for government licensing or mandatory yearly training, it would be captured under this principle.

There are numerous vendor-specific as well as vendor-neutral certifications available in the market. These certifications show that a person has the knowledge and ability to use a specific tool correctly. While not a perfect solution they are what we have available to us at the moment. Until something better does come along we will need to use these forms of skill measurement to their fullest potential. It is best for a practitioner to have a variety of certifications from multiple sources.

The examiner will need to keep documentation current that proves what they know and how well they are at doing their job. Many people have years of practical experience yet have never obtained a certification or college degree to prove it. This does not mean however that they are not highly qualified. Alternate evidence will need to be gathered in accordance with where the person is working. A comprehensive list of all work preformed is a prime example of such proof.

3 A Process Framework for Forensic Computing

The framework consists of 8 distinct steps that will cover the actual work that is to be performed. These steps will map more to what needs to be done and worry less about how it must be done. If a framework dictates how an examiner is to do their work they have no flexibility to adapt to the situation they find themselves in. This could make a framework unusable in an entire country if it is contradictory to the prevailing laws. Concentrating on what needs to be done, and letting the principles of the framework guide the how, makes it possible to overcome these limitations.

No investigation is conducted in a vacuum and the forensic examination of a computer is no different. There are steps that will need to be taken to ensure a complete, fair and reproducible examination. Most examiners will say they are afraid of missing information that might prove a person's guilt. We see it slightly different and think it would be worse if an exam was stopped too soon and evidence of a person's innocence was missed.

It should be obvious to most readers that there is no incident response phase included in this new framework. It was decided to leave this out because by far the majority of examiners will not ever be involved with this. Generally a victim detects that one of their systems has been compromised and then report it to the Police. The Police will get all of the necessary legal paperwork together and make a copy of the affected system. Once that is done the image of the system will be turned over to the lab for examination. Alternatively the victim could contact a third party vendor who then comes on-site to examine what happened. Either way the examiner will first become involved well after the incident occurs.

The steps which are detailed below are designed to be performed in the order in which they appear. This does not mean that in special situations some steps will change order or that some may even be left out completely. Each investigation is unique in the evidence it holds, what the person is accused of doing and what facts are being looked for. A case where we are trying to find pictures of abused children stored on a camera is very different from one where we need to find a deleted email on a server sitting in another country. That being said we still want to try and cover as many eventualities as we can without overly regulating what is happening. Forensic computing is much too fluid of a process to try and use any type of checklist to measure progress.

The below steps are similar to the process outlined by Carrier and Spafford. [CS01] In forensic computing we may be dealing with bits and bytes stored as either a 0 or a 1, but the actual work truly is no different than a traditional crime scene. Similar rules and procedures will need to be observed.

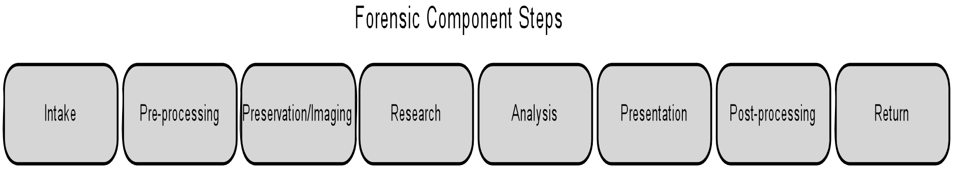

Figure 2: The eight Forensic Component Steps.

3.1 Intake

This is a step that will be taken before any work can be done. Regardless of the device being tested, or the procedure being done, it must be given to the examiner first. If a computer is the object it will need to be physically delivered. Even if a forensic image of the physical computer is stored on a hard drive as a file, it must still be given to the examiner.

The general principles above will dictate what paperwork is needed and how the evidence will be handled. We just need to know that no matter what it is we are doing, or what it is we are examining, we must physically take possession of it before work can begin. The item to be examined can be transported to us via a third party or we may seize it onsite with a search warrant. Once possession has been established the next steps can begin. There is nothing stopping the examiner from making copies of the evidence onsite under Step 3 and then bringing it back to the lab for examination and beginning with Step 1 once they have returned.

3.2 Pre-processing

These are the steps taken before the full investigation or examination process gets underway. Generally it will consist of gathering information needed by the examiner to complete the following steps of the framework. Reading the case file to get a full understanding of what is going on would be the most obvious example. A detailed history of the accusations being made can provide vital clues that will let the examiner narrow their focus quicker.

Another common example would be researching the technology to be examined. If presented with a new laptop model for the first time an examiner would need to research how to take it apart before grabbing the screwdrivers. The same can be required if the examiner is faced with an exotic hardware RAID controller which they have never seen before. Some of these controllers will not work without proprietary drivers from the manufacturer being used.

This process would also need to be taken if some special software package needed to be examined. In many economic crime investigations a customer management program or order processing system will need to be examined. While most of these programs will have the same output when given the same input, how they accomplish this under the hood can be very different. Knowing how the tool works means we can detect any attempts to circumvent internal controls or regulatory requirements. The author has seen suspects who have paid to have software modified to hide the true amounts in their bookkeeping systems when viewed by the tax authorities.

3.3 Preservation/Imaging

The evidence being examined must be protected to maintain it in the condition in which it was at the time of seizure or receipt. While an examiner may not always be the person who made the image of the device under examination, they must implement effective controls over the digital evidence as soon as they have it in their possession. The most common task to perform here will be the imaging of computer hard drives and other digital evidence. Hardly a case will be seen without a digital storage device of some sort in it. Other devices such as USB, Firewire and other storage media will also be captured in this step.

Actions to ensure that no changes to the original media must be taken independent of which tools or methods are being used. This can include such things as hardware write blockers, software write blockers and/or forensically sound boot media. No method is ever entirely 100% safe so proper procedures must be followed to minimize the risk of a write being made to the media.

3.4 Research

This phase begins once the examination has started and is one of the preliminary steps that will be taken. Once the examiner has had the opportunity to look at the evidence that is available a plan of attack can be developed. To do this properly the examiner will need to know what it is they are dealing with. Getting detailed information on the data types being looked at will need to be accomplished.

Under this step will also be determining what the subject of the examination is. Knowing the facts of a case is not technically necessary for a successful examination but will greatly improve accuracy and reduce time to completion. Getting information as to who is involved and what they are suspected of doing allows a plan to be made for the next step. If there are witnesses statements as to how the crime supposedly transpired it can help speed along the process.

3.5 Analysis

This is listed as a step but in reality it is a linear process. It starts at one end (the left hand side) with a huge amount of data that needs to be examined. Working from the pile on the left towards the right side the data is examined, leads are developed and followed and questions are asked and answered. Data that is not relevant will be excluded and additional evidence that needs to be obtained can be added. [FS01] The process continues to the right until the only thing left is the relevant information.

The actual process will differ between examiners based on their training and experience level. A person from an IT administration background will do this much differently than a person from an intelligence background for example. While the results may be nearly the same for both of them, the person with the intelligence background will likely be much faster and have a better chance of finding links between diverse tidbits of information that they observed.

3.6 Presentation

No matter what work was performed the results must be given to the requestor in some physical form. In many jurisdictions this can be in electronic form. In Germany we commonly store the results on electronic media such as Blu-Ray disks but must always submit a printed version. This is due to the fact that German Criminal Procedure requires all reports to be in a printed format. If it cannot be placed in the case file it does not exist.

There are rarely exceptions made to this rule even when many pages need to be printed. The author once had to submit a report to a State Supreme Court that detailed transactions contained in a large SQL database. Even by shrinking the report down and fitting 10 transactions on a single A4 page in landscape mode, the report consisted of around 17,500 pages.

The important thing to remember is that you must make the results understandable and put them in a form requested by the person submitting the work. It must further meet the legal requirements of the jurisdiction. You might do the best work in the world and crack the biggest case ever, but if you cannot get others to understand the facts it was all for nothing.

3.7 Post-processing

When all the analysis and presentation work is completed it will be necessary to perform the post-processing steps. These will differ from lab to lab and typically entail archiving the evidence and work product from the case. Local policies will dictate what needs to be done which can range from writing the data to CD or DVD to storing it in an encrypted container on a secure SAN.

In crimes involving graphics of children being sexually exploited sometimes the courts will order the offending material to be removed and the computer be returned to the owner. This happens mostly when a third party is involved or there were only one or two pictures total. In this case the examiner will need to forensically sanitize the relevant devices and verify the process before the work is completed.

3.8 Return

Once an examination is completed the evidence must be returned to the person who submitted it. The evidence will need to be handled in accordance with local policy and relevant legal codes. Every jurisdiction will be different and even a single jurisdiction could have several conflicting rules based upon the crime being dealt with.

In Germany a computer containing images of children being exploited will typically be seized by the government as a tool used in a crime. The same can happen in a fraud case where a computer was used to propagate the fraud. In the event that there is no evidence that the person did what they are accused of, the device will be given back to them. This situation will also occur when a person is found not guilty at trial.

Either way after all the work is completed the items received in Step 1 will need to be given back.

4 Skill Levels

Beebe and Clark made the point that most frameworks today are single-tier. [BC01] They propose having sub-phases that fall under these top-level phases. This theory is more in line with how work in forensic computing is actually performed. When doing imaging of a system for example there are multiple methods of differing difficulty levels that can be used. Having the multiple sub-phases allows the user to escalate through them until they are able to complete their task.

This section is for the future expansion of the model to allow us to extend this concept and to be able to measure the performance of practitioners. No single person can know everything nor can they be good at everything that they do know. It is for this reason that we need to break tasks down into different skill levels to make the testing of forensic computing professionals possible. The tasks that will be captured in these levels will need to be concrete in nature. This means the steps will consist of such things as making an image of a floppy disk. What is expected will be defined and well as what results need to be observed. Only after these concrete tasks have been defined can any true measurement take place.

In making an image of a floppy disk we could have the following methods map to the appropriate skill level:

Skill Level 1 – Use an automated floppy imaging device.

Skill Level 2 – Use EnCase to image the floppy.

Skill Level 3 – Use Anadisk to dump the contents of the floppy.

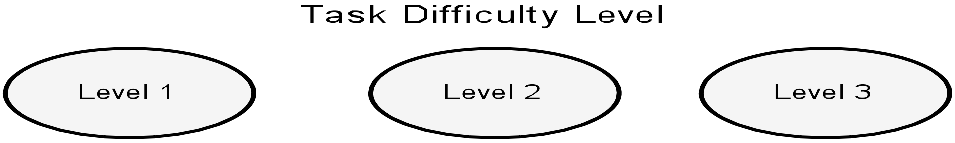

Figure 3: The three Skill Levels.

5 Test Case

In an effort to clarify how this framework functions we will use an example to demonstrate how the pieces work together. An investigation has been launched after a radio unit responded to a disturbance call at a multi-family house and discovered the body of a woman. The body was located in the bedroom of the top floor apartment. There was no evidence of forced entry and a laptop computer was found in a rucksack inside the closet. The apartment has a telephone and Internet service.

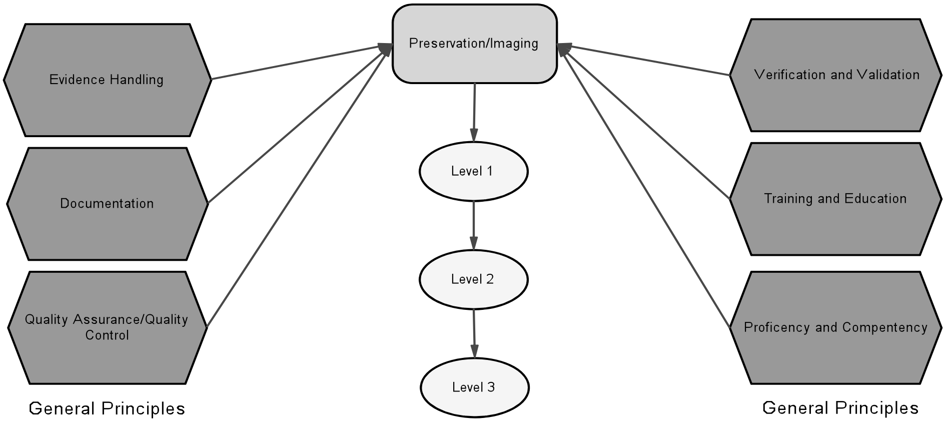

Figure 4: How it all fits together.

5.1 Forensic Process Step

The actual physical step we need to perform in this example is preservation/imaging. In this example the homicide detective took the laptop into evidence and transported it back to the station. At the station the detective personally brought the laptop to your office where you signed for it. Researching in the Internet you found out how to take the laptop apart and remove the hard drive for imaging. We will see below how the principles relate to the physical act of forensically copying the drive.

5.2 General Principles

Here we will look closer at the general principles we will follow when making our image of the hard rive removed from the laptop.

5.2.1 Evidence Handling

When the laptop was taken out of the evidence room the barcode on the evidence bag was scanned by the examiner as leaving that location. When the examiner gets to the imaging station the evidence management system was updated with the new location of the evidence by scanning the barcode again.

5.2.2 Documentation

Lab policy requires an imaging work form to be completed for the hard drive. This form is used to capture the model and serial number of the evidence among other relevant data. Where the image file is saved on the local computer file system will be noted and the status of the hash verification of the image will be written down. When done the form will be added to the case file.

5.2.3 Quality Assurance/Quality Control

QA/QC dictates that the hardware write blocker used for the imaging process will have initial and periodic testing. This testing will make sure that the device copies all data as expected and prevents all writes to the source media. QA/QC also covers verification conducted on the software tool used to make the image of the source drive.

5.2.4 Verification and Validation

These are the actual steps taken that are called for in QA/QC. A test set could consist of hashing the contents of a sample drive and then hooking it to a computer with the write blocker. Then the user can try to write files to the protected drive and then run another hash of the drive after rebooting the computer. If the values match the blocking device passes and can be used.

5.2.5 Training and Education

When a new tool is to be implemented the lab policy dictates that an examiner must be trained on it before they can use it. Examiners who have tested and validated the tool for the others can conduct internal training. When they have been trained to lab standards they will be able to conduct their own validation of the device.

5.2.6 Proficiency and Competency

This will capture the certifications the examiner has obtained. It will also be satisfied with the presentation of training records and internal testing results. The critical thing here is to show that the person doing the examination is skilled enough to do the work.

6 Framework Benefits

The major benefit of this new framework is that it can be used for investigating any crime where the processing of digital evidence is required. It is equally important that this framework is able to be used anywhere in the world regardless of the underlying legal system. By focusing more on results instead of telling the practitioner what they have to do we are giving them the flexibility to do their job better.

6 Framework Benefits

The major benefit of this new framework is that it can be used for investigating any crime where the processing of digital evidence is required. It is equally important that this framework is able to be used anywhere in the world regardless of the underlying legal system. By focusing more on results instead of telling the practitioner what they have to do we are giving them the flexibility to do their job better.

7 Future Work

Additional research is needed into what concrete tasks are needed for the actual forensic work steps detailed above. This will be the natural continuation in the process for making it possible to eventually measure the capabilities of a person working in forensic computing. Each of these tasks will need to be assigned an appropriate skill level based on polls conducted of professionals in the field. Additional papers will be released as the data is examined and results become available.

8 Conclusion

This new framework takes into consideration the work done by others in this field before us. Separating the principles out from the actual work steps gives us a layer of abstraction that makes the framework extremely flexible and robust. Even major changes in an existing legal system will allow the framework to continue to be utilized. This framework gives us a fresh way of working that is more closely aligned to the working environment in a traditional computer forensic laboratory. Finally it gives us the ability to use this framework anywhere in the world no matter the underlying legal code. Taken together we feel this framework is a starting point for improving the performance of forensic computing as well as the perception of its value by others.

Acknowledgments

I am very grateful to my Doctorate advisor, Professor Felix Freiling, of the University of Mannheim. He provided invaluable assistance by reviewing my writing and helping me to learn how to better put my ideas to paper.

Bibliography

[BCI01] Beebe, Nicole Lang, Clark, Jan Gayness, "A hierarchical, objectives-based framework for the digital investigation process", Digital Investigation, Volume 2, 2005

[CCE01] http://www.cce-bootcamp.com/

[CS01] Carrier, Brian, Spafford, Eugene H., "Getting Physical with the Digital Investigation Process", International Journal of Digital Evidence, Fall 2003, Volume 2, Issue 2

[FS01] Freiling, Felix, Schwittay, Bastian, "A Common Process Model for Incident Response and Computer Forensics", IMF 2007

[GUI01] http://www.guidancesoftware.com/training/course_listing.aspx

[ICM01] International Centre for Missing and Exploited Children, "Child Pornography: Model Legislation & Global Review", International Centre for Missing and Exploited Children, 2006

[PO01] Pollitt, Mark M., “An Ad Hoc Review of Digital Forensic Models”, Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07), 2007

[RCG01] Reith, Mark, Carr, Clint, Gunsch, Gregg, “An Examination of Digital Forensic Models”, International Journal of Digital Evidence, Fall 2002, Volume 1, Issue 3

[SH01] Sheldon, Andrew, “The future of forensic computing”, Digital Investigation, Volume 2, 2005