Arriving at an Anti-forensics Consensus: Examining How to Define and Control the Anti-forensics Problem

By

Ryan Harris

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2006 USA

Lafayette, IN (Aug 14th - 16th)

available at www.sciencedirect.com

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem

Ryan Harris

CERIAS, Purdue University, West Lafayette, IN 47907, USA

Keywords:
Anti-forensics
Digital forensics
Digital evidence
Evidence manipulation
Guidelines

A B S T R A C T

There are no general frameworks with which we may analyze the anti-forensics situation. Solving anti-forensic issues requires that we create a consensus view of the problem itself. This paper attempts to arrive at a standardized method of addressing anti-forensics by defining the term, categorizing the anti-forensics techniques and outlining general guidelines to protect forensic integrity.

1. Introduction

Locard's principle states that when a crime is committed, there is a cross-transfer of evidence between the scene and the perpetrator (Saferstein, 1998). Forensic investigation endeavors to use science to uncover the transferred evidence and discern its meaning. The examination requires that the evidence be reliable and accurate to ensure a correct outcome. However, criminals may use anti-forensic methods to work against the process or interfere with the evidence itself.

Solving anti-forensic issues will require that we understand the actual problem itself. Several papers address facets of the problem. But there are no general frameworks in existence which allow us to analyze the anti-forensics situation as a whole. We do not even have a consensus on the proper definition of anti-forensics. Likewise, there are no general groupings of anti-forensic methods to aid our analysis. We need to create a standardized definition, categorize the techniques used, understand examples and determine mitigation strategies in order to address this problem completely.

2. Anti-forensics definition

Currently there is no unified definition for anti-forensics. This is not surprising however, since it is a relatively unexplored field. Several definitions are available and each has its own relative merits. Some of those definitions look only at specific segments of anti-forensics. Some have seen anti-forensics as simply breaking tools or avoiding detection (Foster and Liu, 2005) while others have only related anti-forensics to system intrusions (Shirani, 2002).

To arrive at a unified definition, it maybe beneficial to separately examine the base words which make up anti-forensics. According to Saferstein, forensics is "the application of science to those criminal and civil laws which are enforced by police agencies in a criminal justice system" (Saferstein, 1998). The dictionary defines anti as "opposed to" or "against"(Merriam-Webster's, 2003). So if we combine those two definitions we can preliminarily define anti-forensics as *methods used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system*. This definition provides a correct technical description of the problem, but it is too lengthy for standard use.

Considering that the forensic process relies on accurate evidence may help us craft a more concise definition. For example, Peron and Legary pinpoint anti-forensics as the attempt to "...limit the identification, collection, collation and validation of electronic data..." so that the crime investigation is hindered (Peron and Legary, 2005). This definition is not complete however, since it disregards the analysis of the

E-mail address: rmharris@cerias.purdue.edu

1742-2876/$ – see front matter © 2006 DFRWS. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2006.06.005

evidence. Evidence analysis is essential to the forensic process; therefore, we must include it if we list each phase in our definition. Another definition by Grugq identifies anti-forensics as ‘‘attempting to limit the quantity and quality of forensic evidence…’’ (Grugq, 2005). This definition is useful as well, but it only considers the evidence and completely ignores the forensic process.

If we combine Grugq’s ideas with those of Peron and Legary, we can arrive at a concise yet precise definition of anti-forensics. In this paper, we will consider anti-forensics to be *any attempts to compromise the availability or usefulness of evidence to the forensics process*. Compromising evidence availability includes any attempts to prevent evidence from existing, hiding existing evidence or otherwise manipulating evidence to ensure that it is no longer within reach of the investigator. Usefulness maybe compromised by obliterating the evidence itself or by destroying its integrity.

3. Types of anti-forensics

Just as there are varying definitions of anti-forensics, several groupings of anti-forensic methods have been proposed. Peron and Legary divide anti-forensic techniques into four categories by saying that an adversary can destroy, hide, manipulate or prevent the creation of evidence (Peron and Legary, 2005). Other categories are proposed by Rogers including data hiding, artifact wiping, trail obfuscation and attacks against the process and tools (Rogers, 2005).

Although these categories differ, there are some overlaps between those proposed by Rogers and those of Peron and Legary. The data-hiding category from Rogers matches perfectly with Peron and Legary’s similarly named classification. Rogers’ artifact wiping category encapsulates ways of destroying evidence and ways of preventing its creation into single group (Rogers, 2005). However, he also provides two additional categories which cover areas that were not addressed by Peron and Legary. Trail obfuscation simply tries to add misdirection to the evidence (Rogers, 2005). His final category takes into account direct attacks against evidence gathering and analysis processes (Rogers, 2005).

Rogers’ categories are more complete than those proposed by Peron and Legary; however, there are some refinements which can still be made. Attacking the process and tools could also be considered a trail obfuscation technique. Additionally, the combination of source elimination and data destruction into a single category artificially creates overlap between those categories where one might not exist.

Dividing anti-forensics into four categories of evidence destruction, evidence source elimination, evidence hiding, and evidence counterfeiting takes into account elements from the categories of Rogers and of Peron and Legary (Table 1). Each of these proposed categories accounts for distinct actions that compromise the availability or usefulness of evidence to the forensic process. Evidence can be destroyed to prevent it from being found or to reduce its usefulness if it is found. Evidence can be hidden from casual view to reduce its availability to the investigator. Possible sources of evidence can be eliminated to ensure that evidence never gets created in the first place. Counterfeiting evidence can manipulate it to redirect blame, exploit weaknesses in the process or tools or otherwise corrupt the validity of the evidence so that it is no longer useful to the investigator.

3.1. *Destroying evidence*

Evidence destruction involves dismantling evidence or otherwise making it unusable to the investigative process. This method partially or completely obliterates the evidence; it is not simply making evidence inaccessible (such as evidence

Table 1 – Classification of common anti-forensic methods

Name	Destroying	Hiding	Eliminating source	Counterfeiting
MACE alterations	Erasing MACE information or overwriting with useless data			Overwriting with data which provides misleading information to investigators
Removing/wiping files	Overwriting contents with useless data	Deleting file (overwriting pointer to content)		
Data encapsulation		Hiding by placing files inside other files		
Account hijacking				Evidence is created to make it appear as if another person did the ‘‘bad act’’
Archive/image bombs				Evidence is created to attempt to compromise the analysis of an image
Disabling logs			Information about activities is never recorded	

hiding or evidence source manipulation). Physical world examples of destruction include wiping fingerprints off a gun or pouring bleach in blood to destroy DNA.

Since these actions work on existing evidence, the process of destruction may itself create evidence. For instance, the bottle that contained the bleach may now have fingerprints on it. In the electronic world, the same rules apply. Overwriting a file may partially or completely obliterate the file, but the software used to perform the wipe may create an additional evidence trail.

3.2. *Hiding evidence*

Hiding evidence is the act of removing evidence from view so that it is less likely to be incorporated into the forensic process. The evidence is not destroyed or manipulated however; it is just made less visible to the investigator. In the physical world, hiding evidence might involve throwing a gun down a storm drain or burying a body. Sometimes, it is not necessary to find the hidden evidence. In fact the presence of hiding tools on a system may itself become evidence (McCullagh, 2005).

While hiding evidence is not guaranteed to be successful, it can be highly effective because it depends on the inherent limitations of people. It can rely on the blind spots of the investigator by placing evidence at a location, the investigator would not normally examine. But it can also use the limitations in the physical or digital world. For example, an investigator cannot check every place in the world to find a piece of evidence. So, if a gun used in Miami ends up in New York City it effectively is hidden because of the physical search limitations of the investigator. In the digital world, hiding uses similar principles. Files can be placed in unusual places to exploit limitations of the digital forensics software, or can be renamed to take advantage of the inherent blind spots of the investigator.

3.3. *Eliminating evidence sources*

Evidence source elimination involves neutralizing evidentiary sources. There is no need to destroy evidence since it is never created. In the physical world, source elimination could be as simple as wearing rubber gloves to commit a crime. However, the actual process of source elimination could itself create evidence, as evidence destruction can. The rubber gloves used to hold the gun might become evidence, for example. Additionally, the very lack of evidence might become evidence. This sounds counterintuitive until we consider a gun completely devoid of fingerprints. A good investigator may think that the criminal wore gloves, so he might assume that the murder was carefully planned. These observations apply to the digital world as well.

3.4. *Counterfeiting evidence*

According to the dictionary, to counterfeit something is ‘‘to imitate or feign esp. with intent to deceive’’ (Merriam-Webster’s, 2003). Consequently, evidence counterfeiting is the act of creating a ‘‘faked’’ version of the evidence which is designed to appear to be something else. This includes creating evidence which functions as an attack against the process or tools such as discussed by Rogers. This category is unique because it involves the selective editing of existing evidence or creation of invalid evidence to corrupt the validity of the real evidence. The evidence can be in plain sight, have not been destroyed and yet still be invalid.

Other of the anti-forensic categories may need to be combined with this evidence counterfeiting for the intended result to be achieved. Consider a mob ‘‘hit’’ that is engineered to look like a suicide or a legitimate accident. In order to do this, rubber gloves would be needed (source elimination) to ensure that the hit man’s fingerprints are not present at the scene. However, actual fake evidence would also need to be created in order to convince the investigator that the scene was the result of a suicide. In the digital world, counterfeiting might include using another persons’ account or using a rooted box to launch attacks, thus casting apparent blame on someone other than the perpetrator.

4. Reducing the effectiveness of anti-forensic methods

In order for anti-forensic methods to work, they must rely on inherent problems with forensics. Anti-forensics often makes use of attacks on the investigators (Grugq, 2005) and may also take advantage of our dependency on specific tools or processes (Foster and Liu, 2005). Inherent physical and logical limitations of the investigative process and world in general can be exploited as well.

Since anti-forensics rely heavily on the forensics process being susceptible to these issues, resolving these concerns would theoretically solve the anti-forensics problem. Unfortunately, we cannot completely control these issues and we will never be able to completely prevent the corruption of evidence (Rogers, 2005). However, if we target the problems one by one, we might be able to minimize our susceptibility to anti-forensics.

4.1. *The human element*

Out of all the issues that anti-forensic methods exploit (Table 2), the most difficult problem to solve maybe the human element. Many aspects influence how effective an investigator will be when encountering anti-forensic measures. The alertness of the investigator, educational level, real world experience and willingness to think in new directions could all affect the detection of anti-forensics. Alertness is essential since anti-forensic measures could become more subtle (Rogers, 2005). The investigators educational level is important since that may determine whether the investigator has the understanding necessary to detect some of the more sophisticated attacks. However, real world experience is vital since the investigators intuition relies on experience. Lastly, if the investigator has a naturally inquisitive nature, he may be more willing to pursue unusual or difficult evidentiary challenges.

While not all of the human elements can be controlled, it is useful to manage the ones that we can. For example, we

Table 2 – Exploits of the methods

Name	Human element	Tool dependence	Physical/logical limitations
MACE alteration	Investigator may assume accuracy of dates and times	Tools may not function with invalid or missing dates and times	Invalid dates and times make collating information from multiple evidentiary sources difficult or impossible
Removing/wiping files	Investigator may fail to examine deleted files	Methods of restoring deleted files are specific to the tool – so effectiveness may vary	Time required to restore wiped file contents may outweigh the evidentiary value of the data it contained
Account hijacking	Investigator may fail to consider whether the owner of the account was actually the person at the keyboard	Tool may not be capable of extracting information that would aid investigator in determining who was in control of the account	Zombied computer accounts may produce so much indirection that it is almost impossible to actually find the origin of an attack. Lack of detailed information may keep investigator from determining actual account user
Archive/image bombs		Improperly designed software may crash	Useful information might be located in the bomb itself, but outside the logical limitations of the investigator's system
Disabling logs	Investigator may not notice missing log records	Software may not flag events that indicate logging was disabled	Missing data maybe impossible to reconstruct

cannot closely control an investigators' alertness, but we can help counteract some distracting influences. If investigators encounter a case that involves anti-forensics, we can reduce their caseload to ensure that they have adequate time to determine how to proceed. To increase educational level, investigators could be required to attend a set number of forensic classes each year. Real world experience can be enhanced by regularly ensuring that each investigator must perform at least some hands-on anti-forensics research each year.

4.2. *Dependence on tools*

The problem with depending on tools is that the tools are not immune to attack (Rogers, 2005). One method of mitigating this problem is to use a variety of tools. Another approach would be to encourage the vendors of the tools to improve the accuracy and efficacy of the tools as applied to anti-forensics.

In order to reduce the impact of anti-forensics on specific tools, it is necessary to use a wide variety of software. But it is difficult to encourage departments to use a diversity of tools since the tools are expensive and there is evidence that many police departments maybe underfunded (Council on Foreign Relations Independent Task Force, 2003). If cost considerations prevent a department from using a variety of tools, then they should use the most powerful combination of software that can be afforded.

Since we have seen that a variety of tools are not feasible for many departments, the best approach would be to make the software more effective. There are a variety of software packages; each with its own individual strengths. But there are some common ways in which all the packages can be improved. The effectiveness of the current forensic tools can be improved by ensuring that they comply with applicable specifications and conform to generally accepted norms, by utilizing what should be rather than what is and by learning from the anti-virus industry.

Building tools that act in accordance with specifications as well as generally accepted norms creates tools that will be flexible in a wide variety of situations. This makes the tools able to adjust to evidence that closely follows the specifications as well as evidence that follows norms but does not match specifications. For example, according to the original JPEG specification, only the first two bytes of the header are significant in identifying a JPEG image; the second two bytes are only used to identify the derivative. However, some tools look at the first four bytes of the header since there are only a few JPEG derivatives. AccessData's Forensic Toolkit, for instance, is unable to detect non-standard JPEG derivatives since it relies only on generally accepted norms. But, image-editing programs such as MS-PAINT are able to open the altered files correctly since they follow the specification. File Hound is able to detect these images since it follows the specifications rather than norms.

Another useful change would be to create tools that operate on what should be rather than just creating tools that look at what is. This involves making tools which not only check norms and specifications but also look for things that are out of place by using statistical analysis. People develop a sense of intuition by subconsciously gathering probabilistic (statistical) information from experience (Lieberman, 2003). We should create software that has a way of mimicking human intuition built in from the start.

For example, the Program Files directory is used to store binaries. The software should see if there is a high concentration of images in this directory, and if so, notify the examiner and flag them for more detailed investigation. Another example involves NTFS. To detect hidden data on a Master File Table based file system, the tool can look to see if non-standard NTFS flags are assigned to any files on the drive.

Human intuition may lead to flawed decisions (Lieberman, 2003). Similarly, software based tests which mimic intuition can result in flawed diagnosis. This means that investigators should exercise care when using information culled by the digital intuition. Despite the limitations, the software should help the investigator sift through the evidence by listing items which inherently seem out of place.

Perhaps it would be useful to take some ideas from the developers of anti-virus software. We could create software that employs updatable file-type detection routines. Rather than hard coding the software with file-type detection methods, we could create software which uses downloadable recognition routines. This way new file-types could be detected without needing a reinstall. Any undetected file-types could be electronically shipped back to the software manufacturer for identification and addition to the database.

4.3. Physical/logical limitations

Physical limitations include things such as hardware connectors and protocols as well as media storage formats. Storage space limitations and time and money factors are some examples of logical limitations. Unfortunately, physical and logical limitations will never go away. However, we should be taking steps to minimize their effects.

To combat some of the limitations, investigators could abide by the principle of the latest and greatest and the oldest and grayest. The first part of this principle is that investigators should have access to new hardware and software to enable them to deal with new threats. Therefore, investigators should not wait for a case which involves SATA drives to get and familiarize themselves with a SATA write blocker. As much as is feasible, they should have experience with the latest hardware and software available. The second part of the principle is that the actual software and hardware being investigated maybe ancient. It might be useful to keep a library of old hardware and software available so that the investigator does not encounter hardware or documents which cannot be accessed simply because of their age.

The impact of logical limitations maybe reduced by a variety of methods. These methods may include presenting information in multiple ways, using statistical analysis and massive indexing. Current forensics software may provide limited subsets of these methods, but they might not be used to their full effectiveness. Some forensics software presents multiple views of the information on the investigated system. Files maybe displayed in a tree view as well as a flat view of all files on the system. The investigator can sort all the files by type to allow him to look at all the graphics files in one view rather than trolling through every folder individually.

As mentioned in the section on tool dependence, statistical analysis of information is a method which might help investigators process more information in a shorter period of time. Statistics may help the investigator determine what appears out of place on a system. The final technique, massive indexing, is employed in current software such as AccessData's Forensic Toolkit as a method of locating information on a system. Unfortunately, the search algorithms are not sufficiently sophisticated and amount to little more than finding specific words in all the files. Perhaps forensics software could include the equivalent of a Google search engine to help investigators better wade through the information.

Some of our logical limitations occur because we do not adequately understand system specifications or capabilities. As a result, our forensics software may not be completely correct in processing digital evidence. To overcome these limitations we will need to encourage greater vendor cooperation. Investigators specifications must be closer to reality than those used by the investigated parties. Take NTFS for example. Brian Carrier's book, Forensic File System Analysis, needed to rely on NTFS documentation produced by a competitor to Microsoft rather than being able to get an exact answer directly from the vendor (Carrier, 2005). This hurts forensics because the perpetrators can research only the features of NTFS that will enable them perform their misdeeds. Yet, investigators will need to know the complete NTFS specifications to ensure that they have completely examined the evidence created by the perpetrator. Unfortunately, even though vendor participation is essential to overcoming some of the logical limitations of digital forensics, it is not forthcoming.

5. Conclusion

The number of scholarly papers on protecting against anti-forensic methods is greatly outnumbered by the number of websites about how to exploit the forensic process. Therefore, it would seem that perpetrators are working harder to subvert the system than academia is working to strengthen forensics.

Part of the reason for the lack of papers could be that we have not decided exactly what we are looking for. The current definitions all seem to concentrate on specific aspects of the problem, but never see the issue as a whole. We need to agree on a definition and ways of evaluating anti-forensic methods before we can determine how to respond. After all, if we cannot agree on how we should define the term and categorize the methods, how can we know an anti-forensics technique when we encounter it?

Another part of the problem maybe that we are pursuing the wrong path. Perhaps we are placing too much emphasis on forensic technology and ignoring the necessary training of people and development of processes. We cannot continue down the path that we are on simply because we have always traveled this way before. Maybe we need to take time to re-prioritize our look at forensics and create novel ways of fixing the root issues that anti-forensic methods exploit.

Acknowledgements

The author would like to thank Dr. Marc Rogers for his useful advice and comments about this paper.

REFERENCES

Carrier B. File system forensic analysis. Upper Saddle River, NJ: Addison-Wesley Professional; 2005.

Council on Foreign Relations Independent Task Force. Emergency responders: drastically underfunded, dangerously unprepared, http://www.cfr.org/content/publications/attachments/Responders_TF.pdf; 2003.

Foster JC, Liu V. Catch me if you can.... In: Blackhat briefings 2005, http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-foster-liu-update.pdf; 2005.

Grugq. The art of defiling: defeating forensic analysis. In: Blackhat briefings 2005, http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-grugq.pdf; 2005.

Lieberman MD. Intuition: a social cognitive neuroscience approach. Psychological Bulletin 2003;126(1):109–37, http://instruct1.cit.cornell.edu/courses/phi663/intcog.pdf.

McCullagh D. Minnesota court takes dim view of encryption. News.com. http://news.com.com/Minnesota+court+takes+dim+view+of+encryption/2100-1030_3-5718978.html; 2005.

Merriam-Webster's collegiate dictionary. 11th ed. Springfield, MA: Merriam-Webster; 2003.

Peron CSJ, Legary M. Digital anti-forensics: emerging trends in data transformation techniques, http://www.seccuris.com/documents/papers/Seccuris-Antiforensics.pdf.

Rogers M. Anti-forensics, http://www.cyberforensics.purdue.edu/docs/Lockheed.ppt; 2005.

Saferstein RE. Criminalistics: an introduction to forensic science. 6th ed. Upper Saddle River, NJ: Prentice Hall; 1998.

Shirani B. Anti-forensics. High Technology Crime Investigation Association, http://www.aversion.net/presentations/HTCIA-02/anti-forensics.ppt; 2002.

Ryan Harris is currently pursuing a MS in Information Security from Purdue University. He received his BS in Information Systems from Drexel University. His current interests center around technological and legal issues in digital forensics.