Journal of International Technology and Information Management

Volume 28 | Issue 3 Article 4

2019

Use My Digital Forensics Tool...It's Shiny!

Kara Nance
Virginia Tech, knance@vt.edu

Vincent Nestler
California State University - San Bernardino, vnestler@csusb.edu

Matt Bishop

Recommended Citation

Nance, Kara; Nestler, Vincent; and Bishop, Matt (2019) "Use My Digital Forensics Tool...It's Shiny!," *Journal of International Technology and Information Management*: Vol. 28 : Iss. 3 , Article 4.
Available at: https://scholarworks.lib.csusb.edu/jitim/vol28/iss3/4

Use My Digital Forensics Tool… It's Shiny!

Kara Nance
Virginia Tech knance@vt.edu

Vincent Nestler
CSU San Bernardino vnestler@csusb.edu

Matt Bishop
UC Davis Bishop@ucdavis.edu

ABSTRACT

The tendency to use technologies without fully understanding the potential ramifications extends to all reaches of our lives. Digital forensics is not immune from this phenomenon. This paper discusses some past scenarios in which conclusions were drawn before all of the testing was complete. Digital forensics tools are then discussed including tool capabilities, tool analysis, and associated challenges. It identifies some potential issues and ramifications that may not be given appropriate consideration by digital forensic examiners or those who rely on these tools when weighing evidence. It concludes with some suggestions for future research directions that could answer some important questions about using digital forensics tools effectively.

Keywords: Digital Forensics, Cloud Forensics, Tool Validation, Digital Forensics Tools

INTRODUCTION

Throughout history, early adopters have flocked to new technologies and ideas and subsequently led throngs of new users to the same experiences. In the absence of a devil's advocate, the promises made by the technology creators are often taken at face-value. The creators will emphasize the features and capabilities that make the technology marketable and useful. However, they may not mention, or mention only in passing, the problems that the technology has—if indeed they know what these problems are. And as they rarely know all the characteristics of the environments in which the technology will be used, the creators may not be able to know all the problems that the technology will have during its lifetime. Thus, as important as questioning technology is, it is even more important to ask the right questions.

Cigarettes – Our Past

Until the 1950s, cigarettes were generally considered benign. Doctors said they helped soothe coughs and raw throats; movie stars and other celebrities made their use seem attractive and sexy. Cigarette manufacturers built advertising campaigns around these claims, and became very wealthy from the sales of tobacco products. But evidence that smoking could cause diseases and death mounted, and in 1964, the U.S. Surgeon-General published a report warning of dangers of smoking. Beginning in 1966, all cigarette packs sold in the United States were required to carry warnings about the hazards of cigarette smoking (from "may be hazardous to your health" to "causes lung cancer, heart disease, emphysema, and may complicate pregnancy").

According to documents released as a result of lawsuits and other legal processes, by the 1960s the tobacco industry had shown that cigarettes caused cancer in animals (Glantz et al., 1998). The industry's response was to take steps to minimize exposure to lawsuits, in part by concealing the evidence uncovered in their laboratories. The result of believing the claims that no evidence linked smoking to disease and death led to a lack of understanding of the problems, and the consequences were indeed disease and death.

Airline Scanners – Our Present

The U.S Transportation Security Agency (TSA) acquired scanning devices that use X-rays to produce an image of a person standing in the machine. The intent was to have devices that enabled TSA personnel to look for weapons in clothing without patting down the passenger. The devices were controversial for a number of reasons. The one that concerns us here is safety; there was considerable concern that the safety of the systems had not been properly tested. Four doctors at the University of California San Francisco, who are experts in cancer and medical imaging (and three of whom are members of the National Academy of Sciences), sent the Office of Science and Technology Policy a letter requesting a scientific study of this issue. The TSA's report, written by experts at the Johns Hopkins Advanced Physics Laboratory, states that the devices are safe if configured and used properly. Another part of the controversy concerned the storage of the images for later use.

Unfortunately, the TSA's study is obscured in places. Specifically, there is little to no detail available on the software test procedures, the source code analysis procedures, and indeed on any penetration tests in which the goal of the testers is to subvert the software to (for example) fail to provide proper interlocking, to deliver a dangerously high dose of radiation, or to enable images to be stored or transmitted. Further, while the TSA claimed that images could not be stored, the same devices were used for courthouse security in Florida, and in that case images were stored. Thus, the question that should have been asked was whether the devices were safe and privacy-protecting *as configured and used in the airports*, and how that safety and privacy- preservation was assured in that environment (Mowery et al., 2014; Applied Physics Laboratory, 2009).

Cloud Technology – Our Future

The *race to the cloud* is another example of a new technology that is being widely adopted without appropriate consideration of the associated issues. While there are likely to be early adopters of most promising new technologies, cloud technologies have mandated adoption based on financial considerations with little or no associated identification of issues. As a part of The Accountable Government Initiative, Vivek Kundra, the U.S. Chief Information Officer, identified a "Cloud First" policy; requiring each U.S. agency to identify 3 "must move" systems within three months and move one to the cloud within 12 months (The White House, 2010). This very short window, coupled with the lack of understanding of the implications of using cloud technologies demonstrates a fundamental willingness to adopt now and evaluate later.

In the years since the ubiquitous use of multi-tenancy public cloud environments has become common there have been many cases in which the isolation between instances has been shown to be more fragile than initially thought. Cloud cartography and instance co-location efforts (Ristenpart, Tromer, et al., 2009) have demonstrated the ability to map a cloud environment and place adversarial instances in close proximity to targets. The hardware enhancements that have driven increased processing power for many years have also been shown to also have significant security implications. For example, timing attacks against shared resources such as caches; Spectre, Meltdown (Graz University of Technology, 2019) and the wide range of similar attacks that have resulted from an increased level of research into hardware vulnerabilities.

Software issues are no less prevalent in the cloud than elsewhere, but cloud environments suffer from very real supply chain issues. Images for almost any use case and software product are easy to find, but significant effort is then required to determine where the image came from, and how it was configured.

Even configuring security controls on resources has proven to be a challenge, with S3 buckets and open databases full of PII or commercial data frequently found exposed to the Internet with no access controls. While it is easy to place the blame for such incidents on the data owners and administrators, cloud providers' simple "click to deploy" interfaces make it quick and easy to create working instances, while the more nuanced security configuration is left as an option that can be easily overlooked or misconfigured (particularly when dealing with large or dynamic environments).

This tendency to use technologies without fully understanding the ramifications extends to all reaches of our lives. Digital forensics is not immune from this phenomenon. The motivations may be different as the objectives are more likely motivated by simplifying the process for the forensics examiner rather than lowering costs. The following sections discuss some digital forensic tools in this light and identify some potential issues and ramifications that may not be given appropriate consideration by digital forensic examiners or those who rely on these tools when weighing evidence.

DIGITAL FORENSICS TOOLS

While digital forensics used to be applied primarily to computer crime, the increasing predominance of electronic devices in all areas of our lives has contributed to a world where crimes that could not be informed by digital components are rare indeed. A mobile phone in the pocket of a burglar, the gps in the car used to escape from the crime scene, the red-light camera that snapped photo of the getaway all have the potential to provide valuable evidence to exonerate or help convict suspects.

Tools Analysis

The need to validate tools for the end user has been discussed in the academic and popular press for many years. NIST announced the Computer Forensics Tool Testing Program (CFTT), which is a very positive step in the validation of forensics tools. The effort involves major law enforcement players in the digital forensics realm and includes the capability for you to test your own tool using their methodology. The overall objective is to "provide forensics tool testing reports to the public." The reports are designed to provide test results with the information

needed to allow 1) developers to improve tools, 2) users to make informed choices, and 3) the legal community and others to understand the tools' capabilities (National Institute of Standards and Technology, 2019).
The site currently contains reports in the following digital forensics areas:

- Deleted File Recovery and Active File Listing (last update 7/14)
- Digital Data Acquisition (last update 7/14)
- Disk Imaging (last update 10/16)
- Forensics Media Preparation (Last update 12/11)
- Graphic File Carving (last update 7/14)
- Hardware Write Block (9/09)
- Mobile Device Acquisition (12/17)
- Software Write Block (1/08)
- Video File Carving (10/14)

The software industry tends to use a release-and-patch approach for software. This includes tools used in the digital forensics arena. As can be seen in the listing of forensics areas for which tool validation reports are published, the lag time in updating the tests is significant. This lack of currency greatly decreases the benefits of the reports to digital forensic examiners.

In addition to the lack of currency, there is also a limit to the breadth of the tools that have been tested. The focus for the majority of the tools in the reports had been file systems forensics. File systems forensics represent an important subset of the critical digital forensic information that is needed for digital forensics analysts to understand. Missing from the categories are memory forensics, network forensics, cloud forensics, and the plethora of device forensics that are not encompassed in the mobile device family.

Perhaps the reporting mechanism, which is a very important step in advancing the state of validation of digital forensics tools, could be partially addressed by the formalization of a process for continuous evolution of the site contents if it is to be the definitive resource in this area. A plan for maintaining currency would include retesting of tools as new updates are released and method for evolution of the categories as the field of digital forensics continues to advance.

The following section provides some examples of specific digital forensics tools and some associated issues that might affect the appropriateness of their application to digital forensics cases.

Graphic File Carving Tools - Encase and FTK

The Encase 6.18.0.59 graphic file carving tool is one of the tools tested in 2014 with a report available on the CFTT site (Department of Homeland Security, 2014). The test was run with 40 graphic files. While there were only 40 files, 62 were carved, with 33 of the carved files being viewable (3 only partially). The rest of the files were either not-viewable gif files (4) or 25 false positives.

The FTK 4.1 graphic file carving tool was also tested in 2014 (Department of Homeland Security, 2014). The same 40 files were used and with this tool only 39 were carved. Of the files carved, 33 were viewable, 3 were partially viewable, and 3 were not viewable. The files not viewable were again gif files. There is no indication that they are the same 3 files in both tools.

What is it about the gif files that made them none viewable? Is it something that a criminal or state actor could investigate, discover and then include that attribute in their images? It would be beneficial to see the evolution of the tool and the associated tests in one chain to demonstrate the responsiveness of the organization in responding to issues identified in the validation testing process. Further, a subsequent validation of a more recent release may have concluded that this is no longer an issue.

NIST Tool Catalog

NIST hosts a list of tools that developers can self-register ("Computer Forensics Tools & Techniques Catalog - Home," 2019). Many tools are listed without having a report of the tool being tested. In fact, of the 243 tools listed on the site, only 56 of them state they have a report. Of those, only 34 have working links to actual reports. Of the 34 reports, many of those date back to 2012 and earlier. Most of the tools have gone through at least one revision since their report date.

Tools listed on the NIST Tools Catalog site have an implied validation. It is likely that people seeing a tool listed on the site will assume that the tool is appropriate for use in a digital forensics investigation. And perhaps it is, but without proper testing and validation, one cannot be sure and the time to find out should not be in the middle of a criminal investigation.

Another concern is how tools are registered with the site. A form is filled out by a tool developer and submitted. A person at NIST reviews the submission and then determines if it should be posted. The rubric through which this decision is made is not clear. Is it possible that a sophisticated hacker or state sponsored group could create a set of infected tools and have them posted to the site? This possibility motivates additional testing of the tools beyond operational validation.

As discussed above, there have been some steps taken towards improving the availability of information about tools and some vendors have allowed their tools to be tested through the CFTT process, there remain a plethora of tools that remain untested. Of primary concern is the prevalence of the use of tools in situations that affect legal outcomes and human lives without the tools being validated with scientific rigor.

CHALLENGES

In addition to specific issues related to validation of tools, there are additional challenges that digital forensics tools share with most other sectors in the software markets. Two of these issues that are particularly impactful are the uncontrolled proliferation of new tools and the lack of education in proper and appropriate use of the tools.

Tools Proliferation

As new technology emerges, so do the new tools. Long gone are the simple days where looking at hard drives alone was sufficient. The taxonomy of forensics tools has grown to include items such as GPS forensics, drone forensics and VoIP forensics. There are at present 32 different categories of tools. With new tools coming out and at such a pace, there is hardly time for the tools to mature and there is little time or manpower available to test all of the new tools. For many investigators low cost, easy access, and easy to use are often the major factors in tool selection. Yet these are not necessarily the measures that should be used in the determination of the tool to use.

Education about Tools

Many tools are released to the public and then used but without formal training. All tools have their quirks and use cases. Sometimes they are obvious but other times not. In the preceding examples with Encase and FTK testing, why would 3 gif files not show up when a graphic file carver is run? The answer to this question may have important bearing on a digital forensics case and could potentially change the classification of the crime when the number of images on a computer is a determining factor.

FUTURE CONSIDERATIONS

While the NIST plan provides a solid foundation to improve the state of digital forensics tools, there doesn't appear to be a structured approach for continuous process improvement from a presumably unbiased perspective. While the test reports do bring issues to light, the lack of a structured process diminishes the value of the collection as a current method for validating tools.

Clearly, there is a need for greater tool testing and reporting. To impart this need to future forensic investigators, tool testing should become part of the forensic curriculum. Available on the NIST the CFTT Federated Testing Forensic Tool Environment is a live Linux CD iso file that can be used for testing disk imaging tools, hardware write block tools and mobile device tools (NIST Tool Catalog). Introducing this a college forensic curriculum can teach students how to test tools, to learn about the functions and limitations of a tool, and most importantly, show them the importance of testing a tool before using it for investigations.

Forensic analysts need to become familiar with the reports that do exist and be aware of the limitations and anomalies that can arise from the use of a tool. Because a tool is listed on the NIST Catalog site does not mean a thorough examination of the tool was done or that a report on it exists. Sophisticated adversaries may do their own testing to find the limitations of a tool and exploit the weakness of the tool to prevent information from being discovered by the tool.

Defense attorneys may seize upon this issue of tools used that lack the proper testing and reporting. A good lawyer may call tools used to gather evidence into question. If the tool has significant problems when used in certain operating systems or settings, this may help them reach their goal of establishing reasonable doubt.

Finally, this reinforces the need for using multiple tools when analyzing evidence. While it may add time to an investigation, one tool can mitigate the issues of another. If one tool fails to find a particular gif file, perhaps another will.

REFERENCES

Applied Physics Laboratory. (2009). *Radiation Safety Engineering Assessment Report for the Rapiscan Secure 1000 in Single Pose Configuration*. Department of Homeland Security.

Computer Forensics Tools & Techniques Catalog - Home. (2019). Retrieved December 9, 2019, from Nist.gov website: https://toolcatalog.nist.gov/index.php

Department of Homeland Security. (2014a). *EnCase Forensic v6.18.0.59 Test Results for Graphic File Carving Tool*. Retrieved from https://www.dhs.gov/sites/default/files/publications/EnCase%20Forensic%20v6.18.0.59%20Test%20Report_IKS_0.pdf

Department of Homeland Security. (2014b). *FTK v4.1 Test Results for Graphic File Carving Tool*. Retrieved from https://www.dhs.gov/sites/default/files/publications/508_Test%20Report_NIST_FTK%20v4.1%20Test_%20August%202015_Final.pdf

Glantz, S., Slade, J., Bero, L., Hanauer, P., Barnes, D., & Koop, C. E. (1998). *The Cigarette Papers* (First). University of California Press.

Graz University of Technology. (2013). Meltdown and Spectre. Retrieved August 10, 2019, from Meltdownattack.com website: https://meltdownattack.com/

Mowery, K., Wypych, T., Singleton, C., Comfort, C., Rescorla, E., Diego, S., … Shacham, H. (2014). Security Analysis of a Full-Body Scanner Security Analysis of a Full-Body Scanner. *23rd USENIX Security Symposium*. Retrieved from https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-mowery.pdf

National Institute of Standards and Technology. (2017, May 8). Computer Forensics Tool Testing Program (CFTT). Retrieved August 9, 2019, from NIST website: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

NIST Tool Catalog. Retrieved April 15, 2019 from https://toolcatalog.nist.gov /index.php

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. *Proceedings of CCS ’09*. Retrieved from https://hovav.net/ucsd/dist/cloudsec.pdf

The White House. (2010). Presidential Memorandum--Accountable Government Initiative. Retrieved July 9, 2019, from The White House website: https://obamawhitehouse.archives.gov/realitycheck/the-press-office/2010/09/14/presidential-memorandum-accountable-government-initiative