Global Information Assurance Certification Paper

Tackling the Unique Digital Forensic Challenges for Law Enforcement in the Jurisdiction of the Ninth U.S. Circuit Court

GIAC (GCIA) Gold Certification

Author: John Garris, jgarr@sans.leemail.me
Advisor: Ovie Carroll
Accepted: November 17th, 2017

Abstract

The creation of a restrictive digital evidence search protocol by the U.S. Ninth Circuit Court of Appeals – the most stringent in the United States – triggered intense legal debate and caused significant turmoil regarding digital forensics procedures and practices in law enforcement operations. Understanding the Court's legal reasoning and the U.S. Department of Justice's counter-arguments regarding this protocol is critical in appreciating how the tension between privacy concerns and the challenges to law enforcement stand at the center of this unique Information Age issue. By focusing on the Court's core assumption that the seizure and search of electronically stored information are inherently overly intrusive, digital forensics practitioners have a worthy target to focus their efforts in the advancement of digital forensics processes, procedures, techniques, and tool-sets. This paper provides an overview of various proposals, developments, and possible approaches to help address the privacy concerns central to the Court's decision, while potentially improving the overall effectiveness and efficiency of digital forensic operations in law enforcement.

1. Introduction

The field of digital forensics continues to evolve at a rapid pace, adapting to explosive demands, including the increasing need for qualified digital forensics practitioners. These individuals must continuously adjust to regularly changing technologies while navigating complex and often varying legal requirements that sometimes impose significant limitations on the approaches and techniques they may legally apply (Bonelli, 2011).

The Western United States provides an example of a legal mandate with significant impact on digital forensics practitioners working in law enforcement. Over the course of the last several years, a sizable number of federal judges within the U.S. Ninth Circuit have been mandating uniquely restrictive search protocols for electronic devices and data seized under the authority of warrants they issue (Weinstein, 2014). Because these mandates are attached to search warrants, they are having a targeted and significant effect on law enforcement agencies operating within the Ninth Circuit's jurisdiction. Notably, the impact of this development on law enforcement operations is important due to the growing role and overall value of digital evidence in law enforcement operations in general. Also magnifying its effect is the outsized role the Ninth Circuit's jurisdiction plays in hosting many of the most consequential technology companies in the world (Goodison et al., 2015).

1.1. Challenges Can Also Represent Opportunity

The creation of the Ninth Circuit Court's digital evidence search protocol, the most stringent in the U.S., was the direct result of the Court's belief that the acquisition and search of electronically stored information by law enforcement is an inherently overly intrusive process (Blake, 2010). These new legal restrictions have triggered intense debate and caused a a great deal of disruption regarding digital forensics procedures and practices. The fact none of the other 12 circuits within the U.S. embraces the Ninth Circuit's position has only heightened confusion (Weinstein & Drake, 2014). Although the legal debate over this issue will no doubt continue, the potential opportunities this presents can be leveraged to justify investment in the development of new practices, procedures, and tool-sets that directly take on the Court's belief that the seizure and search of data are, by their very nature, overly intrusive. Not only would focused efforts to innovate demonstrate law enforcement's continuing good-faith in addressing the legitimate privacy concerns underlying the Court's ruling, but they could also help propel positive technical and procedural developments in furthering the discipline of digital forensics, to include improving the general efficiency of digital forensics operations. These future technical and procedural advancements could also present additional options for the judiciary in formulating new approaches for structuring the authorities granted in warrants.

John Garris, jgarr@sans.leemail.me

2. Privacy & Seizure of Data by Law Enforcement

To fully appreciate the larger legal issue that sets the stage for the current practice in the Ninth Circuit, it is important to understand these legal constraints are the outgrowth of protracted litigation flowing from the high-profile legal case, *United States v Comprehensive Drug Testing, Inc (U.S. v. CDT).* The core facts of this case center on a federal criminal investigation of alleged doping by a number of high-profile professional baseball players, and the federal government's search of drug testing data. Such data was seized from Comprehensive Drug Testing, Inc. (CDT), a third-party lab used by Bay Area Lab Cooperative (Balco) for the drug testing of Major League Baseball players (U.S. v. CDT, 2009). It is generally recognized that the law enforcement agency operating under the original warrant exceeded the scope of that warrant. However, the subsequent response by the Ninth Circuit was viewed by the U.S. Department of Justice (DoJ) as an extreme overreaction with potential for extreme damage to future law enforcement operations (Fritz & Roberts, 2013).

The original ruling of the Ninth Circuit was so alarming to the DoJ that the then Solicitor General for the U.S., Elena Kagan, was the keynote signatory of a petition requesting an en banc (expanded court) review of the matter (U.S. v. CDT, 2009). Although it is rather unusual for an appeals court ruling to be challenged in such a manner, such a prominent role of the Solicitor General in the petition leaves little room for doubt regarding the importance the federal executive branch placed on the future influence the ruling could have (Kalar, 2010). The jurisdiction of the Ninth Circuit includes nine western states and the territory of Guam, a very sizable swath of geography. However, the reach and effect of the Ninth Circuit's rulings on digital forensics are amplified by the inclusion of the notable world-leading technology companies located in the state of California alone (Ninth Circuit Jurisdictional Map).

2.1. On the Vanguard of Privacy Protection or Crippling Judicial Overreach?

The central aspect of the original Ninth Circuit ruling *in U.S. vs. CDT* that troubled the DoJ was the five-part search protocol it created. This original ruling mandated all future searches of electronically stored information (ESI) authorized by search warrants issued in the U.S. Ninth Circuit contain the search protocol (U.S. v. CDT, 2009). Fritz & Roberts' (2013) analysis of the subsequent en banc Ninth Circuit ruling on the matter found that, although the Court ultimately stepped back from mandating the five-part protocol requirements, the Court's final ruling still required judges in the Ninth Circuit to consider these procedural safeguards as "a useful tool for the future." As evidenced in the wording of many search warrants issued subsequent to the final *U.S. vs. CDT* decision, the original ruling may have lost the weight of a legal mandate, but it has nonetheless become the de facto standard for many

judges in the Ninth Circuit (Fritz & Roberts, 2013). As Blake (2010) noted in his analysis of Fourth Amendment considerations in the Digital Age, a fundamental assumption driving the Ninth Circuit's ruling in *U.S. v. CDT* was that "…over-seizing is an inherent part of the electronic search process." Hence, the Ninth Circuit Court came to believe prophylactic safeguards should be considered a needed precaution against the inherent risk seizures and searches of digital records pose to privacy rights (Blake, 2010).

2.2. The Nation's Top Cop Raises Dire Alarms

To appreciate the significant challenges several of these Ninth Circuit search warrant requirements impose on the digital forensics practitioner, it is helpful to briefly address the three requirements the federal government objected to most vociferously. These challenges are found in the DoJ's petition for an en banc review of the original *U.S. v. CDT* opinion (U.S. v. CDT, 2009). Those objections centered on the suspension of the "plain-view doctrine," the required use of additional personnel to act as "taint team" members, and the requirement to return or destroy data that cannot be readily demonstrated to be within the scope of the warrant within the allotted time frame.

Before examining DoJ's first objection, it is first helpful to layout the basic legal theory regarding the plain-view doctrine. This doctrine is a long-standing legal construct that permits a law enforcement officer to seize evidence of a crime, without first obtaining a search warrant, when that evidence is in plain sight of an officer who is lawfully present (Eyer, 1992). As argued by the federal government in their petition in response to the original *U.S. . CDT* ruling, a forswearing of the plain-view doctrine with regards to the search of electronic records would guarantee the loss of critical evidence not previously and explicitly known to the government before the petition for the warrant. However, Shuck (2012) found the original justification for the plain-view doctrine make its application in searches of electronically stored information (ESI) problematic for several reasons. Because the plain-view doctrine was developed by the judiciary to balance privacy rights with the potential loss of evidence in a dynamic physical environment, the post-seizure search of seized ESI in subsequent off-site reviews pose little danger of loss of evidence within the already-seized ESI (Shuck, 2012). Although the Ninth Circuits' rulings are often far outside the approaches taken by the other circuit courts, several other circuits have expressed reservations regarding a wholesale reliance on the plain-view doctrine in ESI searches (Bonelli, 2011).

As for the second requirement, the government flatly called the universal requirement for taint teams "unworkable" (U.S. v. CDT, 2009). In this arrangement, individuals searching seized ESI must be completely walled-off from the officers directly involved in conducting the investigation. The government noted the onerous challenges of this mandate, such as the burden of increased personnel requirements, compounded by the inherent difficulty of imparting to the separate taint team members the

needed knowledge level regarding the underlying investigation (U.S. v. CDT, 2009). Though she concedes that the scale of the potential resource burden this requirement could have on law enforcement is difficult to forecast, Shuck (2012) noted that taint teams have a long-standing role in ensuring certain seized information is not viewable by the investigative team. This protected data has typically involved attorney-client privileged information. Lastly, the government argued the requirement to return or destroy data not known to be responsive conflicted with Supreme Court's affirmed Federal Rules of Evidence. These rules provide that "… the officer who executes the return may retain a copy of the electronically stored information that is seized or copied" (U.S. v. CDT, 2009). It is important to note that the Federal Rules of Evidence (FRE) are promulgated by the U.S. Supreme Court and ratified by the U.S. Congress. As such, these rules govern the conduct of federal law enforcement and federal prosecutors. Although the FRE apply only to the federal judicial system, states typically mimic these rules, as a state may provide more protections but may not offer less than guaranteed by the U.S. Constitution (Cornell Legal Information Institute, 2017).

A key aspect of the requirement to return or destroy data that has been most concerning to law enforcement is the short timeline regularly imposed to review the ESI and document which files and records it knows to be in scope of the warrant – all other ESI must be destroyed or returned to the owner. Thus, the requirement to purge all seized ESI that cannot be determined to be within scope of the warrant must be accomplished within a fairly short time frame (Fritz & Roberts, 2013). This time constraint is particularly onerous for agencies struggling to obtain and retain qualified digital forensics practitioners. Exacerbating this time-centered requirement is the fact that these practitioners are juggling numerous other investigative and operational demands that are elevating the strains on a finite pool of increasingly important skill-sets. As argued by the Solicitor General in *U.S. v. CDT*, this requirement increases the risk that the government will regularly and forever lose vital evidence, both inculpatory as well as exculpatory. In any event, it is exceptionally uncommon for the investigating agency to have a full understanding of all aspects of the matter under investigation at the time search warrants are served. After all, the seizure and search of data is a key part of the evolving process of discovering the relevant facts relating to the underlying matter under investigation (Blake, 2010).

The evolution of the Ninth Circuit's position on this issue notwithstanding, Fritz & Roberts (2013) noted that search warrants issued by judges in the Ninth Circuit frequently include requirements following the key tenants of the original *U.S v. CDT* ruling. Thus, it would appear as though many judges within the Ninth Circuit have chosen to adopt much of the original search protocol, even though it is no longer strictly required. The practical effect the incorporation of these requirements in search warrant authorizations is having on digital forensics practitioners can be quite significant.

3. Pathways for Progress – Legal, Technical & Procedural

As noted earlier, the Court's CDT rulings triggered a great deal of debate and discussion centering on the challenges of protecting Fourth Amendment rights while not going too far as to undermine legitimate law enforcement capabilities. Although made without specific regard to the CDT rulings, several technical and procedural proposals are worth examining in that their future adoption could provide the added benefit of generally advancing the field of digital forensics while addressing fundamental privacy concerns relating to the seizure and search of ESI. Additionally, recent case law regarding search warrants, specifically "anticipatory warrants," could provide a pathway to the development of approaches in structuring search warrants that better balance privacy and compelling law enforcement objectives when the search and seizure involve ESI.

3.1. Reducing Reliance on the Plain View Doctrine

In his proposal which addresses what he saw as fundamental weaknesses in approaches to applying the plain-view doctrine to the search of ESI, Acharya (2013) advocated an abstracted, simplified approach to framing and bounding searches of ESI. Foundational to Acharya's (2013) approach is his adoption of Professor Orin Kerr's (2005) definition that a Fourth Amendment search of ESI only occurs as a practical matter when it is rendered for human observation, as opposed to simple automated processing or manipulation by information technology. This view generally accepts the Ninth Circuit Court's position that the initial seizure of ESI is necessarily expansive, invariably capturing data unrelated to the matter under investigation. Thus, Acharya (2013) argues that a practical approach to the post-seizure search of ESI is to bound it in terms of "semantic zones." Semantic zones represent nontechnical descriptions of the type of content an officer may lawfully search based directly on the parameters of the probable cause argued by the government to obtain the underlying search warrant. He further describes a semantic zone as data that comports to a particular semantic description of what is being sought, as opposed to technical terms specific to operating systems, file structures, or other technical constructs (Acharya, 2013). Thus, the use of semantic zones does not take a prescriptive approach as to the specifics regarding how to conduct a search of ESI, but more usefully restricts the search to particular classifications of information and data (Acharya, 2013).

Conceptually, Acharya's (2013) approach to limiting what is viewable by law enforcement post-seizure is attractive in its simplicity. However, his proposal presupposes the necessary technical capabilities and procedural guidelines are already available for application by law enforcement --

specifically, the ability to process seized data in an automated fashion to consistently and meaningfully classify it. Although that assumption outstrips current reality to varying degrees, digital forensics researchers and practitioners have advocated the development of advancements in digital forensics that could pave the way for putting Acharya's proposal into practice.

In her analysis of the unique challenges that the application of the plain-view doctrine presents in the area of computer searches, Bonelli (2011) found that the plain-view doctrine's application to ESI searches has had serious flaws. However, she also argued that its wholesale abandonment was impractical, as it would place too heavy a burden on law enforcement. Bonelli's (2011) assessment was informed by the fact the Fourth, Seventh and Tenth Circuits had already rejected the wholesale discarding of the plain-view doctrine in opinions subsequent to the Ninth Circuit's rulings in U.S. v. CDT. In fact, the opinions of the Tenth and Seventh Circuits adopted approaches that allow for the use of plain-view, but also placed constraints on law enforcement's ability to rely on plain-view in the search of seized ESI.

As a conceptual foundation to their approach to applying restrictions on the use of plain-view in computer searches, the Seventh and Tenth Circuits relied on the application of the idea of a "virtual file." This approach analogized the logical file systems used by computer systems as containers, much like suitcases are frequently divided via individualized zippered pockets (Bonelli, 2011). Thus, in assessing the reasonableness of an ESI seizure, the courts applied a two-part test: 1) Were the relevant files inside the scope of the warrant? If not, 2) Were the files discovered inadvertently? Bonelli (2011) argued that this "inadvertence" test represents the most practical approach to avoid the unreasonable limitations a complete abandonment of the plain-view doctrine would require while restraining law enforcement from turning a search into a wholesale search of all the contents of computer systems. However, the analogy the courts relied on in this approach, specifically comparing computer files (virtual files) to discretely separate containers in a suitcase, suffers from the same inherent limitations all analogies between ESI and the physical world share. Additionally, such a central reliance on trying to divine the intent of digital forensics practitioners can be rather problematic. This inherent difficulty is highlighted by the fact that research has shown an optimal structuring for digital forensics analysis involves teams of four (Carroll, 2017). Thus, trying to piece together the mindsets of multiple individuals conducting analysis on ESI after the fact would seem to strain the boundaries of practicality. Another significant limitation of this sole reliance on intent is that it does not adequately consider the many unknowable variables relating to the first-time search of massive volumes of data within the context of an investigation wherein law enforcement's understanding of the facts is typically evolving. After all, the development of relevant facts should be the central focus of an investigative effort.

3.2. “Anticipatory Warrants” - A Possible Pathway Forward

As noted earlier, a significant number of circuit court opinions have conceded that the plain-view doctrine is not particularly well-suited to the unique considerations relating to the seizure and search of ESI. Because a fundamental legal challenge centers on balancing privacy rights with the practical need for effective law enforcement, it would seem as though the development of a more flexible and calibrated approach to the apportionment of authorities to law enforcement in the execution of ESI search warrants is worth exploration. To that end, the concept of an "anticipatory search warrant," as affirmed in the 2006 Supreme Court decision *U.S. v. Grubbs,* could serve as a conceptual foundation for developing such a flexible and measured approach to search authorities. Not to completely do away with the plain-view doctrine in justifying the discovery of ESI during searches, but rather to reduce current reliance on it.

The idea of an anticipatory search warrant, since it is purely a legal concept, is best described via the language of the Supreme Court's decision in *U.S. v. Grubbs*. The Court wrote, "an anticipatory warrant is a warrant based upon an affidavit showing probable cause that at some future time, but not presently, certain evidence of a crime will be located at a specific place" (U.S. v. Grubbs, 2006). To better understand the application and approach of this type of warrant, outlining the core facts in *U.S v. Grubbs* is instructive. Mr. Grubbs ordered child pornography from, unknown to Mr. Grubbs at the time, an undercover site operated by law enforcement agents from the U.S. Postal Service. After the order was placed, the agents wanted to search Mr. Grubbs' residence after delivery of the materials to prove he was in possession of them. However, they needed to obtain a search warrant before the delivery so that, once it was made, they could immediately start a search of his residence for the materials. In preparation, a warrant and affidavit were written in the usual manner, but in this case, they informed the judge what they knew and asked to have the authority to execute the warrant if a triggering event occurred. The triggering event in this instance, as spelled out in the warrant, was that the parcel in question had to be received by a person and taken into the identified residence (U.S. v. Grubbs, 2006). Thus, the idea of "triggering events" in the construction of search warrants could be leveraged to structure warrants such that they would only allow law enforcement the authority to preserve and search ESI when certain conditions are present with regards to definable characteristics of the questioned ESI.

Given the advancements continuously being made in digital forensics, a great deal is known about the many artifacts and other potentially valuable information available on personal use devices, though those artifacts and ESI are forever changing with the steady commercial advancements in consumer technologies. Some of the potentially valuable ESI that can be found on Microsoft Windows systems, as one instructive example, was outlined by Carroll (2017) in his description of the many challenges presented in digital investigative analysis. Examples of valuable information that can be located on modern MS Windows systems include the "System Resource Usage Monitor (SRUM)," the ESI found in the registry entry of instances of the "NTUSER.DAT" file, and the "LastVisitedPIDMRU," just to note a

few outlined by Carroll (2017). These data structures and associated ESI can individually and collectively provide invaluable information regarding the behavior of users of the system and can even provide insight as to the various geographic locations where a portable device has been used (Carroll, 2017). Thus, the many types of probative ESI available on computer systems, along with the application of the investigative steps that Carroll (2017) outlines, are part of the body of digital forensics knowledge that can be leveraged broadly into constructing various decision trees of triggering events based on the nature of the underlying investigation. By leveraging these numerous digital forensics artifacts, the digital forensics practitioner can more practically assess whether the devices and media at a search site contain ESI responsive to the search warrant and the underlying matter under investigation.

3.3. Accelerating Advancement Through Standardization

Garfinkel (2012) found that a persistent stumbling block to the advancement of digital forensics is the lack of standardization, particularly with regards to the collection and representation of important digital forensics information. To address this problem, he proposed the adoption of a "Digital Forensics Extensible Markup Language," or DFXML. This proposal is not borne out of a single obscure academic pursuit, but benefited from several earlier proposals by digital forensics practitioners and researchers to develop similar standards for the capture and consistent recording of metadata relating to the seized ESI. More specifically, Garfinkel (2012) describes the primary problem DFXML can help solve which relates to the limited number of data types the majority of the commercially available "monolithic systems" used by digital forensics practitioners can ingest and produce. This limitation restricts the ability of developers and researchers to create special purpose tools that can address relatively narrow but important problems by chaining discrete processes together based on the need and underlying investigative context (Garfinkel, 2012). Standardization in the approach to using uniformly and meaningfully defined metadata to describe ESI acquired and analyzed in support of a law enforcement investigations not only offers the realistic potential for improved technical capabilities, but it can also help address the assumption that these activities inherently involve overreach concerning Fourth Amendment protections. As one example, Garfinkel's (2012) DFXML proposal provides for the ability to expand upon the expressiveness of the language through a wide array of elements, to include incorporation of the Dublin Core Metadata Initiative annotations to describe "...individual files, or even byte runs within a file" (Garfinkel, 2012). This type of move towards standardization would open the door to greater efficiencies in the advancement of digital forensics.

When a standardized reporting schema for the characterization of individual files within a large volume of ESI seized during a warrant execution can be employed, Acharaya's (2013) proposal for limiting the scope of searches by way of "semantic zones" could move more rapidly from the theoretical to the practical. This approach is directly supportive of the digital forensics practitioner's need to have access

to increasingly precise and uniformly recognized conventions to zero-in on ESI of specific relevance to the underlying investigation (Garfinkel, 2010). An added benefit to the future adoption of relevant elements of the Dublin Core Metadata Initiative in a standardized language such as DFXML could be to help law enforcement agencies of different countries cooperate in the conduct of complex investigations of criminal activities with a global reach.

3.4. Re-Thinking the Traditional "Computer/Digital Forensics" Approach

Several scholars and researchers have noted the field of digital forensics has struggled to keep pace with rapid changes in technology and evolving legal demands. Both sets of challenges require a more rigorous self-assessment and innovation cycle to ensure the field continues to promote development at an acceptable pace. In Beebe's (2010) survey of senior computer forensics researchers and practitioners, she noted that many had worked very hard to win the trust of the judiciary with regards to the value and reliability of digital evidence. However, some respondents noted that digital forensics practitioners' early focus on the pursuit of credibility on par with more traditional forensic sciences could very well have skewed the community within law enforcement to become overly rigid with regards to practices in certain areas, particularly in ESI acquisition (Beebe, 2010). As Beebe (2010) noted in her research, this approach to ESI acquisition has proven successful in the near term, but has often proven rather inflexible in responding effectively to the rapid pace of change in the underlying technological landscape.

It is somewhat ironic that the early need by law enforcement to develop tools and techniques for the extraction and interpretation of ESI was the primary impetus for the establishment of digital forensics. However, the same incentive, anchored by concerns for acceptance by the courts (of what was then) an entirely new form of evidence, appears to be a significant drag on law enforcement's willingness to adopt new practices. This pursuit of legitimacy in the eyes of the court steered most policies and practices to adhere to the central tenets that ESI acquisitions were to 1) avoid alterations; and 2) obtain all available data to ensure a full and accurate snapshot was taken of the systems in question (Beebe, 2010). However, Beebe's (2010) assessment of digital forensics practice found that the volume of data, the complexity of the underlying systems, coupled with the fact they are sometimes operationally critical and cannot be shutdown, makes the acquisition of all available ESI via an exact bit-for-bit image impractical in many instances. Thus, many organizational standards governing the acquisition of ESI fail to adequately take into account the many possible variables a practitioner will encounter as these organizations "...often present evidentiary principles as 'rules,' leaving little room for improvisation" (Beebe, 2010). This approach appears to have contributed to diminishing law enforcement's appetite for innovation in some areas of digital forensics.

A specific example where this drift towards rigidity in practice and procedure appears to have delayed progress is seen in the law enforcement community's slow adoption of the practice of acquiring data from random access memory (RAM) (Carroll, 2017). The wealth of valuable information found to be available in the RAM of most computer systems represents a challenge in that RAM cannot reliably, at least given present knowledge, be copied without altering some of the data held in the targeted, powered-on RAM. However, it has been demonstrated that the acquisition of ESI held in RAM can be accomplished reliably "... where evidence will likely be altered (albeit minimally and in a deterministic manner)..." (Beebe, 2010). Although the high volume of valuable information often present in RAM and its potential importance to an investigation has been known for several years, Carroll (2017) noted that the law enforcement community is still far from uniformly embracing the importance of trying to capture the ESI found in RAM as a standard practice. This reluctance appears to be anchored, in part at least, by concerns that traditional digital forensics procedures have placed great importance on techniques that do not alter the targeted ESI.

As noted earlier in Beebe's (2010) survey, besides the emphasis on avoiding alteration to ESI during acquisitions, the other major tenet that has served as the foundation for much of law enforcement's digital forensic practice is to attempt to obtain all available information to demonstrate completeness, thus avoiding allegations of bias. The basis for emphasizing the need to collect the most complete copy of data is of course quite sound, otherwise inculpatory ESI may be acquired at the exclusion of potentially exculpatory or vice versa. However, as the amount of data involved in search warrant operations has grown exponentially, the adherence to this tenet has had the unintended effect of triggering Fourth Amendment concerns, most glaringly via the Ninth Circuit's *U.S. v. CDT* rulings. The explosion in the volume of data, and the practical challenges of processing such a volume, has also had a very noticeable effect that brings into question the sanctity of completeness as a core tenet in ESI acquisitions.

In his assessment of current practice in "Digital Investigative Analysis," Carroll (2017) notes the current impracticality of the long-standing approach of claiming to conduct a complete analysis of the large volumes of data often seized during search warrant executions. The massive volumes of data found on individual devices have forced a new reality regarding how digital analysis is done. As Carroll (2017) points out "... there is no longer such a thing as a ‘full forensic analysis'". Although such a stark declaration is not common in the literature relating to digital forensics practice, the growing problem relating to the increasing volumes of ESI law enforcement agencies grapple with is a common theme in the literature. This fundamental fact adds weight to the argument against the Ninth Circuit's protocol step requiring seized data either be destroyed or returned within a specific period of time. The natural investigative and judicial process of iterative inquiries produce new questions triggered by the discovery of additional witnesses, information, etc. Once the ESI is no longer available, sources for potentially crucial answers will inevitably be irretrievably lost.

John Garris, jgarr@sans.leemail.me

In their assessment of digital forensic analysis in law enforcement – taken primarily from an international perspective – Hitchcock et al., (2016) noted their review of the literature was replete with examples of significant backlogs in the analysis of seized ESI experienced by most "Technical Crime Units." This backlog was not only having serious detrimental effects on the efficiency and effectiveness of investigative efforts, but it also represented a growing impediment to the requirement to provide defendants a reasonably speedy trial (Hitchcock et al., 2016). The results of their research led Hitchcock et al., (2016) to propose law enforcement agencies adopt a "Digital Forensics Triage Model" that is an adaptation of a triage model created earlier by Rogers et al. (2006). In the development of their triage model, Hitchcock et al., (2016) recognized the need for a more targeted and rapid process for the initial analysis of ESI. This approach improves the officer's ability to discover and extract time-sensitive information, such as the identity of at-risk victims, in a more efficient, yet defensible process than traditional approaches often used by law enforcement. Thus, these triage approaches all implicitly work from the same basic understanding that Carroll (2017) noted regarding the impracticality of actually conducting a "full forensic exam" of all the ESI typically obtained through the course of an investigation. These triage models, developed specifically for law enforcement needs, represent important advancements beyond the core traditional tenets of 1) alter nothing; and 2) be as comprehensive as possible in what is acquired. By promoting a context-driven approach that recognizes the value of conducting field-level triage reviews of systems during on-site search warrant executions, these models help promote the targeting of acquisitions at the very beginning of the search and seizure process. The added benefit of more uniform adoption of these models could also assuage Fourth Amendment concerns relating to potential overreach in what is initially seized and subsequently searched.

4. Findings and Discussion

The discipline and science of digital forensics offers unparalleled challenges to its practitioners. Fundamentally, these challenges stem from the unique properties, enormous volumes, and the increasing importance ESI plays in criminal and civil investigations. As if these challenges were not daunting enough, they are compounded by the fact the very creation of ESI is driven by advancements in a highly dynamic commercial information technology marketplace. These commercial advancements, in turn, frequently introduce new structures and formats of ESI, often along with important contextual changes regarding their creation and modification (Casey, 2000). However, digital forensics practitioners working in law enforcement have, on top of these core challenges, unique legal considerations and constraints with which to contend. As noted earlier, the protocol requirements often found in warrants issued within the Ninth Circuit are, currently at least, the more vexing for law enforcement to navigate. It is worth noting, once again, that the Ninth Circuit is something of an outlier in this area. This highlights how even the parameters of legal authorities are, in themselves, yet another shifting key variable with which the

practitioner must contend. Although very much interrelated, these challenges could be addressed from separate procedural, technical, and legal perspectives.

5. Recommendations

The highly complex problem set present in digital forensics supporting law enforcement requires a flexible, well-researched approach that can adapt to the many and varying nuances presented in the advancement of digital forensics within the context of law enforcement operations. A multi-faceted approach that advances the reliability and efficiency of the discipline, while supporting the development of more useful legal frameworks for the underlying authority to seize and search ESI, is needed.

5.1. Constructing a Search Authority Framework More Tailored to ESI

Drawing from the legal construct of "triggering events" as outlined in *U.S. v. Grubbs*, future search warrants involving ESI could be structured to help address privacy concerns while reducing reliance on the plain-view doctrine. This approach could allow for a calibrated, conditions-based increase in search authorities within the confines of a warrant, but only if law enforcement personnel executing the warrants develop key information that satisfies court approved triggers. From a practical perspective, these triggers would need to be viewed as discovery thresholds where the authority of the search would expand if specified categories of ESI were found to be present. These triggers would be informed by the growing body of knowledge regarding digital forensics, the contextual value of specific ESI artifacts, computer science in general, as well as framed and informed by the facts of the underlying investigation. This approach would be fact-dependent but provide repeatable and useful frameworks. The importance of context in the application of threshold triggers is highlighted via one of numerous examples. For instance, the presence of malicious software during the review of a system used by a suspected 26-year-old hacker would generally need to be viewed differently from the discovery of the same malware on the system of a retired school bus driver under investigation for check fraud.

Since most investigations requiring a search warrant center on individuals, search warrant threshold triggers focusing on the existence of ESI attributable to specific individuals would be inherently useful in most search warrant applications. Thus, previews of systems during search warrant executions could assess whether evidence of accounts, such as email, social media, financial, or system user accounts associated with these individuals are present in the ESI. If so, the preservation of the data on the system and subsequent search authorities would apply as part of the initial analysis. Of course, the larger context of the requested search would always need to be factored-in first when using this framework of threshold triggers. For example, searches of ESI created and held by third-parties, such as was the case in *U.S. v. CDT*, would require a different approach in the establishment of threshold triggers, as opposed to requests to search personal use devices found in residences. This distinction would recognize the privacy

protections afforded individuals' ESI held by third-parties that are not involved in the matter under investigation.

Other potentially useful threshold triggers relate to time periods, IP addresses, and the types and purpose of software applications found on questioned systems. It is hard to imagine many instances where a law enforcement officer will not have a meaningful context by way of a specific time period when providing the facts in an affidavit in support of a search warrant request. That time period is especially useful in bounding the scope of the warrant and often expected by judges who are issuing search warrants. Of course, because the manipulation of a computer's system time can be used to alter time-related metadata for ESI created and manipulated on that system, use of time periods as a trigger threshold would generally need to account for that fact. Thus, one reasonable approach to structuring the warrant with regards to specific time periods would be to authorize the creation of timelines using the time-related metadata on the files found in the questioned ESI. Any significant anomaly in the distribution of these data, based on research and authoritative sources of information, could be the basis for a threshold trigger in of itself. The determination of what constitutes an anomaly will require recurring research.

Rounding out two more of many possible examples of threshold triggers for search authorities, the existence of specific IP addresses or other relatively unique Internet networking identifiers in questioned ESI could be used to demonstrate the additional search and analysis of the ESI to be entirely within scope of the underlying search authority. Much like the automated creation of time lines based on ESI metadata, an inventory of software found on the system could also be a useful threshold trigger. For example, if a system were found to have, or have had, certain categories of special-purpose software that are used to hide or destroy data, then that could be a reasonable threshold trigger for more expansive searches through the employment of specialized techniques and tools. As is the case with search warrants in general, the unique facts of each case must be considered when structuring the search warrant – the proposed approach to incorporating threshold triggers would be no different in that regard.

Lastly, it is helpful that a foundation for the implementation of threshold triggers is already available, as seen in Rogers et al., (2006) "Computer Forensics Field Triage Process Model." This model already fundamentally conforms to the approach taken in the Federal Rules of Evidence, wherein the seizure and search of ESI are approached as a two-part process, one of acquisition in the field, and then subsequent in-office analysis of the ESI. Thus, the Rogers et al., (2006) model can be readily adapted to the concept of threshold triggers for search warrant authority, as it calls for the on-site assessment of specific types of data sets to identify time-sensitive and perishable ESI. That approach can easily be adapted to demonstrate whether, based on an initial review on-site, court determined threshold triggers regarding the scope of the search authority permit the acquisition of the data. The same basic approach can be employed, depending on the structuring of the warrant and its use of trigger thresholds, during the subsequent in-office analysis of the seized ESI.

John Garris, jgarr@sans.leemail.me

5.2. Implications for Future Research

The prominence of ESI in nearly every aspect of life has naturally raised its importance within the context of law enforcement operations. Its ubiquity and importance in day-to-day life has also led to legitimate privacy concerns regarding how law enforcement conducts seizures and searches of ESI. Additional research and innovation regarding digital forensics is needed, not only to address narrow problem sets introduced with the latest commercial technology advancement, but to more broadly improve the overall quality of discussion and understanding of the discipline as it is applied to support law enforcement. As the controversy surrounding the *U.S. vs. CDT* ruling and subsequent fallout show, advances in legal frameworks and the development of useful tools for the judiciary are needed as well. Thus, specific areas of research should focus on technical and procedural advancements informed by the need to work toward greater consistency in both the description of ESI and the work-flow models used by law enforcement in the seizure and search of ESI.

Fortunately, as noted earlier, a lot of substantive work has already occurred in developing structures for improved uniformity and clarity in the characterization of ESI; see Garfinkel's (2012) proposal for DFXML and the complementary leveraging of the Dublin Core Metadata Initiative. It is difficult to see how a discipline such as digital forensics can advance at a more efficient pace without the adoption of a common language to describe the very subject under study. And when viewed from the perspective of the judiciary, it is no wonder there is confusion regarding important aspects of how digital forensics is conducted in law enforcement, and whether those practices are based on need, tradition, convenience, or some combination thereof.

In addition to advancing the discipline of digital forensics through the expansion and further development of how ESI is characterized, additional research is needed in the refinement of existing work-flow models that more directly address fundamental legal concerns. As noted earlier, the Ninth Circuit's belief that "…over-seizing is an inherent part of the electronic search process" (U.S. v. CDT, 2009), is not widely embraced by other courts. Nonetheless, that belief represents a conceptual pillar for many judges in the Ninth Circuit who regularly issue search warrants. Thus, one objective in the advancement of digital forensics work-flow models should be to challenge the Ninth Circuit's core assumption.

Rogers et al., (2006) produced a work-flow that could serve as a springboard in demonstrating good faith on the part of law enforcement regarding privacy concerns. In their model, Rogers et al., (2006) outlined practical steps for targeting the most relevant data through on-site triage of systems and media, thus increasing the speed at which critical data can be found, but also potentially limiting the volume of ESI seized at the point of search warrant execution. Additionally, Carroll et al., (2008) noted in their work that the analysis of ESI is, at its very core, an iterative process that often

repeatedly informs the investigative process, while also being informed by the findings of the larger investigative efforts. Thus, the well-intended requirement that law enforcement either destroy or return seized ESI within a relatively short time-period, as seen in the Ninth Circuit's search protocol, will likely be revealed as being fraught with pitfalls in the discovery of the facts relevant to the matter in question.

6. Conclusion

The pressing need to support law enforcement operations during the explosion of information technologies the past twenty-plus years was the early driving force behind the very creation of the discipline and study of digital forensics. The early recognition that this nascent discipline needed structure and repeatable processes so that its efforts would be accepted in court proceedings helped drive the embrace of scientific processes and related rigor – the term "forensics" was thus heavily emphasized as part of its very moniker. But as its credibility was enhanced with a rapid series of innovations, the attendant reliance on the rather rigid application of procedures, particularly relating to ESI acquisition, has started to paint some within the law enforcement digital forensics community into something of a conceptual corner. That is not to say digital forensics should reduce reliance on scientific principles, quite the opposite. Thus, the future focus of efforts to advance the discipline of digital forensics should be informed by the need to help law makers and the judiciary move beyond legal constructs better suited to a period of time that largely predates the ubiquity and increasing importance of ESI in everyday life.

John Garris, jgarr@sans.leemail.me

References

Acharya, A. (2013). Semantic Searches. *Duke Law Journal*, Vol. 63:393. Retrieved on July 24th, 2017 from: http://scholarship.law.duke.edu/cgi/viewcontent.cgi? article=3402&context=dlj

Beebe, Nicole. (2010) Digital Forensic Research: The Good, the Bad and the Unaddressed. Fifth IFIP WG 11.9 International Conference on Digital Forensics, Orlando, Florida, USA, January 26-28, 2009. Retrieved on July 12, 2017 from: https://link.springer.com/content/pdf/10.1007%2F978-3-642-04155-6_2.pdf

Blake, Scott D. (2010). Let's Be Reasonable: Fourth Amendment Principles in the Digital Age, 5 Seventh Circuit Rev. 491. Retrieved June 11th, from http://www.kentlaw.edu/7cr/ v5-2/blake.pdf

Bonelli, Alison (2011). Computer Searches in Plain View: An Analysis of the Ninth Circuit's Decision in United States v. Comprehensive Drug Testing, Inc. Retrieved May 22, 2017, from http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1087&context=jcl

Brief for the United States in Support of Rehearing En Banc by the Full Court at 1, United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (Ninth Cir. 2009) (Nos. 05-10067, 05-15006, 05-55354).

Carroll, Ovie (2017). Challenges in Modern Digital Investigative Analysis. *Forensic Science and Forensic Evidence I*. 65(1): 25-38. Retrieved June 3, 2017, from https://www.justice.gov/usao/page/file/931366/download

Carroll, O., Brannon, S., & Song, T. (2008). Computer Forensics: Digital Forensic Analysis Methodology. *Computer Forensics*. Vol 56, Number 1. Retrieved on July 12th, 2017 from: https://www.justice.gov/sites/default/files/usao/ legacy/2008/02/04/usab5601.pdf

Casey, E. (2000). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. San Diego, CA: Academic Press.

Cornell Law School Legal Information Institute. Overview of Criminal Procedure. Retrieved on Aug 20, 2017 from https://www.law.cornell.edu

John Garris, jgarr@sans.leemail.me

/wex/criminal_procedure

Eyer, Robin (1992). "Comment, The Plain View Doctrine After Horton v. California: Fourth Amendment Concerns and the Problem of Pretext". *Dickinson Law Review*. 96 (3): 467, 482–83

Federal Rules of Criminal Procedure. TITLE VIII. Supplementary and Special Proceedings. Rule 41 - Search and Seizure. Retrieved on Aug 29, 2017 from: https://www.law.cornell.edu/rules/frcrmp/rule_41

Fritz, M., & Roberts, J. (2013). Defending Electronic Searches and Seizures. *New York Law Journal*. Retrieved June 2, 2017, from http://www.newyorklawjournal.com/id=1202626843402/Defending-Electronic- Searches-and-Seizures?mcode=0&curindex=0&curpage=ALL

Garfinkel, Simson. (2010). Digital Forensics Research: The Next 10 Years. The Digital Forensic Research Conference DFRWS 2010 (Aug 2nd – 4th). Retrieved on Aug 20, 2017 from: https://dfrws.org/sites/default/files/session-files/paper- digital_forensics_research_-_the_next_10_years.pdf

Garfinkel, Simson. (2012). Digital Forensics XML and the DFXML Toolset. Digital Investigation. Vol 8, 161-174. Retrieved on July 24, 2017 from https://simson.net/clips/academic/2012.DI.dfxml.pdf

Goodison, S., Davis, R., & Jackson, B. (2015). Digital Evidence and the U.S. Criminal Justice System. *Rand Corp, Research Reporting,* 1-32. Retrieved June 16, 2017, from http://www.rand.org/pubs/research_reports/RR890.html

Hitchcock, B, Le-Khac, N., & Scanlon, M. (2016). Tiered Forensic Methodology Model for Digital Field Triage by non-digital Evidence Specialists. Third Annual European Forensic Research Conference DFRWS Europe 2016. Retrieved on Aug 22, 2017 from http://ac.els-cdn.com/S1742287616300044/1-s2.0- S1742287616300044- main.pdf?_tid=2ad9e95e-956c-11e7-bd98-00000aacb35f&acdnat=1504967926_0255f18d1162176af7f275aa9b549abe

Map of the U.S. Ninth Circuit:. (n.d.). Retrieved June 24, 2017, from https://www.ca9.uscourts.gov/content/view.php?pk_id=0000000135

SWGDE Best Practices for Computer Forensics, Ver 3.1 (2014). Scientific Working Group on Digital Evidence. Retrieved on May 25, 2017, from

https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensics

Kerr, Orin. (2005). Search Warrants in an Era of Digital Evidence. Mississippi Law Journal. Vol 75, 85-144. Retrieved on July 20, 2017 from https://www.olemiss.edu/depts/ncjrl/pdf/02-KERR.pdf

Reamey, G. (2013). The Promise of Things to Come - Anticipatory Warrants in Texas. Baylor Law Review, 65(2), 473-509. Retrieved August 18, 2017, from http://www.baylor.edu/content/services/document.php/206146.pdf

Rogers M.K,. Goldman J., Mislan R, Wedge T., Debrota S. Computer Forensics Field Triage Process Model. *Journal of Digital Forensics, Security and Law* 2006;1(2). Retrieved on Aug 7, 2017 from http://ojs.jdfsl.org/index.php/jdfsl/article/view/222/174

Schuck, C. (2012). A Search for the Caselaw to Support the Computer Search "Guidance" in United States v. Comprehensive Drug Testing. Retrieved July 28, 2017 from https://law.lclark.edu/live/files/11320-lcb162art10schuckpdf

U.S. Supreme Court. U.S. v. Grubbs. 21 Mar. 2006. Retrieved on Aug 28, 2017 from: www.supremecourt.gov/opinions/05pdf/04-1414.pdf.

Weinstein, J., & Drake, W. (2014). Public Safety, Privacy, and Particularity: A New Approach to Search Warrants for Digital Evidence. *Bloomberg Electronic Commerce & Law Report,* 1-6. Retrieved June 9, 2017, from http://www.steptoe.com/assets/htmldocuments/Weinstein-Drake-digital-evidence- web.pdf ISSN 1098-5190

Last Updated: January 21st, 2019

Upcoming Training

SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC503: Intrusion Detection In-Depth	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS Northern VA Spring- Tysons 2019	Tysons, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS London February 2019	London, United Kingdom	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201902,	Feb 27, 2019 - Apr 04, 2019	vLive
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Madrid March 2019	Madrid, Spain	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KY	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, Kingdom Of Saudi Arabia	Apr 13, 2019 - Apr 18, 2019	Live Event
Community SANS New York SEC503	New York, NY	Apr 29, 2019 - May 04, 2019	Community SANS
SANS Security West 2019	San Diego, CA	May 09, 2019 - May 16, 2019	Live Event
SANS Northern VA Spring- Reston 2019	Reston, VA	May 19, 2019 - May 24, 2019	Live Event
SANS Amsterdam May 2019	Amsterdam, Netherlands	May 20, 2019 - May 25, 2019	Live Event
SANS San Antonio 2019	San Antonio, TX	May 28, 2019 - Jun 02, 2019	Live Event
San Antonio 2019 - SEC503: Intrusion Detection In-Depth	San Antonio, TX	May 28, 2019 - Jun 02, 2019	vLive
SANS London June 2019	London, United Kingdom	Jun 03, 2019 - Jun 08, 2019	Live Event
SANSFIRE 2019	Washington, DC	Jun 15, 2019 - Jun 22, 2019	Live Event
Security Operations Summit & Training 2019	New Orleans, LA	Jun 24, 2019 - Jul 01, 2019	Live Event
SANS Paris July 2019	Paris, France	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS Rocky Mountain 2019	Denver, CO	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS Columbia 2019	Columbia, MD	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS Boston Summer 2019	Boston, MA	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS Chicago 2019	Chicago, IL	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS Copenhagen August 2019	Copenhagen, Denmark	Aug 26, 2019 - Aug 31, 2019	Live Event
SANS Network Security 2019	Las Vegas, NV	Sep 09, 2019 - Sep 16, 2019	Live Event
SANS Oslo September 2019	Oslo, Norway	Sep 09, 2019 - Sep 14, 2019	Live Event
SANS London September 2019	London, United Kingdom	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS OnDemand	Online	Anytime	Self Paced