2005 UCLA J.L. & Tech. 5

CONFLUENCE OF DIGITAL EVIDENCE AND THE LAW: ON THE FORENSIC SOUNDNESS OF LIVE-REMOTE DIGITAL EVIDENCE COLLECTION

ERIN E. KENNEALLY, M.F.S., J.D.[?]

> "What information consumes is rather obvious: it consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention and a need to allocate that attention efficiently among the overabundance of information sources that might consume it."[1]

I. Introduction

[¶1] This article advocates the formal recognition of an evolved digital evidence[2] acquisition process in light of the changing dynamics of computer searches and seizures. Other articles have argued for changes in legal procedural rules.[3] This article addresses the other side of the coin, namely, that the changing contexts of computer search and seizure and digital forensic investigation demand an evolution in forensic acquisition methodology, and that this evolved methodology can meet the standards for evidence admissibility and reliability. This methodology entails evidence recovery on live systems via a remote connection (hereinafter, "live-remote").

[¶2] While legal reform is a valuable component to evolving practice and is certainly nontrivial given the law's inertia, it is vital to address the technical procedure evolution because this is where the operational reality of digital evidence acquisition interfaces with legal standards and principles. When theory gives way to application, forensic practitioners encounter discord between principle and practice. More importantly, forensic practitioners must resolve these challenges amidst a

relative dearth of clear legal precedent to model the development and application of the methodology.

[¶3] Forensic practitioners[4] are first responders to the challenges that arise from the differential rate of change between the law and technology. This is to say, our system of law is designed to determine right and wrong in a rational and consistent manner and is consequently "hard coded" to resist rapid change. On the other hand, rapidly changing technologies constantly challenge determinations of what constitutes a wrong as well as whether the law has a role in defining efficient avoidance of the resulting harm.[5]

[¶4] Because technology changes at a much faster rate than the law and is arguably constrained only by the imaginations of its creators, a dichotomy arises between exploiting technology to enhance capabilities and staying within the bounds of legal, acceptable uses. What this means for forensic practitioners is that one hand giveth and the other taketh away: forensic practitioners' (both law enforcement and private sector forensic professionals) ability to leverage technology is bound by the legal standards and policies governing evidence reliability. In short, forensic techniques are defined not by technical feasibility but by legal standards for proving the truth of past events. Examples of constrained technology include the use of radar detectors to prove a driver violated speeding laws; polygraphs to prove the veracity of a suspect's alibi; latent fingerprinting using cyanoacrylate fuming to prove the presence of an individual at a crime scene; and thermal imaging technology to sense heat sources through walls for illegal drug detection.

[¶5] Forensics--whether involving the application of chemistry, molecular biology, or computer science--embodies those legal bounds in applying tools and technologies to prove the truth of a past event. The discipline of digital forensics has developed and/or applied technologies to enhance the identifying, correlative, and characterizing properties of electronic information. As with other forensic disciplines, technology is used to increase information symmetries so that

recreations of past events more accurately reflect the truth and justice is better served.

[¶6] The goals of digital forensics practitioners--identification, collection and preservation of digital information bearing evidentiary potential--can be achieved via existing tools and technologies yet the methodologies directing their use have not been formally vetted. Specifically, the ability to interact remotely (outside of physical proximity with the target computers) with live systems (digital crime scenes where the computer system is still running) is possible and is growing in practice. However, this methodology has yet to be systematically "sanctioned" as forensically sound.[6] This sanctioning is most effectively done by way of formal recognition by authoritative groups within the forensic community[7] or judge-made law interpretation, with the former bearing significant influence on the latter.

[¶7] While the lack of precedent is partially due to the novelty of the live-remote approach and dearth of courtroom opposition, lack of formal acceptance within the relevant community of practitioners can be ascribed to the inertia of a methodology traditionally based on physical interaction with static or “dead” systems. This traditional digital evidence acquisition reflects the nature of the physical crime scene where time and space served as boundaries. In this environment, evidence searches and seizures parallel that of traditional physical evidence--practitioners enter the location to be searched, seize computer hardware, and take the hardware offsite where it is digitally searched for potential evidence of crime.[8] Conversely, live-remote methodology does not necessitate taking systems offline or maintaining physical proximity with the target media.

[¶8] Failure to embrace and validate this evolved methodology will widen the gap between practice and principle, further straining the resources and ability of the law enforcement system to handle cases, strengthening credibility challenges lobbied at the forensic practitioner, and ultimately tarnishing the authenticity and admissibility of the resulting evidence

[¶9] The proliferation of digital evidence, the changing business and technology environments within which electronic traces are found, and the pressures on resources attendant to traditional forensic methodology are driving the call for acquisition methodology changes.[9] Although analysis of these drivers are beyond the scope of this article, this article contends that live-remote evidence acquisition techniques should be formally recognized as capable of rendering forensically-sound evidence. In reality, these techniques are already being applied and will likely become a de-facto standard. Yet, the interests of jurisprudence would be better served by proactively generating dialogue about the methodology among the relevant community.

[¶10] It is both logical and reasonable to presume that these forces of change will persist, so reluctance to endorse this live-remote methodology only delays the inevitable. This reluctance also fails to capitalize on the opportunity to inform the proper, consistent and uncontroverted application of forensic acquisition methodology in situations where it is warranted, such as in network environments or under constraints imposed by search warrant parameters. Failure to endorse the new techniques is reminiscent of "Security by Obscurity," a strategy which involves deliberately hiding information about the implementation or design of a technology to make it harder to break. Only in this case, the analogous criticism is that implementation of a methodology solution without overt acknowledgement does little to facilitate the systemic legal acceptance of that new methodology.

[¶11] An evolved methodology that implements live-remote evidence collection is needed to even the playing field for forensic practitioners. These practitioners are called upon to collect and interpret relevant data amidst increasingly high-volume, dynamic computer network contexts, while simultaneously adhering to legal pressures mandated by substantive and procedural standards and rules. Acceptance of live-remote techniques would enhance the capabilities of forensic practitioners while still fulfilling established evidentiary standards. This paper is intended to offer guidance on the yet-untested issue of the admissibility of live-

remote digital evidence acquisition, as well as to debunk the myth that dynamic, network evidence collection is unreliable.

[¶12] This recommendation, although untested in the courtroom, is nonetheless supported indirectly by case law and grounded in evidentiary standards. Part I recounts the application of legal standards governing the admission of physical evidence, including the comparable reliability challenges and subsequent controls used by forensic practitioners to effectively counteract opposition. Part II applies the same analytical analogy based on a rich history of physical evidence reliability challenges. These legal standards, challenges and controls are then applied to the live-remote methodology in Part III. Finally, Part IV explores inferences for evidentiary acceptance of the live-remote approach by comparatively analyzing case law regarding enhanced digital imaging and eye witness testimony.

II. Live-Remote Methodology and Traditional Physical Evidence - An Important Primer

[¶13] In the absence of case precedent[10] regarding the evidentiary admissibility or weight of digital evidence acquired remotely on a live system, the rich legal history of traditional, physical evidence serves to forecast potential challenges and rebuttals. Whether we're dealing with hairs and fibers, paper documents or digital evidence, the evidentiary standards are the same.

A. Standards and Challenges--Authenticity, Originality

[¶14] The standards for the admissibility of evidence are relevance, authenticity, and reliability.[11] These preliminary determinations can occur under the auspices of Federal Rule of Evidence (F.R.E.) 901's requirement that the matter in question is what it is claimed to be, or via the more demanding showing of reliability for scientific, technical or specialized evidence under F.R.E. 702.[12] This judicial screening is meant to ensure that the evidence is reliable enough to go before a fact-finder, who decides what weight that evidence should carry. A basic

evidentiary tenet governing admissibility is that there are guarantees of trustworthiness attached to the evidence so that a jury is not unduly confused or prejudiced. Authentication standards are meant to ensure that the evidence is what it purports to be, and how rigorous a foundation is needed to make this finding depends on the existence of something that can be tested in order to prove a relationship between the evidence and an individual and control against the perpetration of fraud.[13]

[¶15] Another evidentiary lynchpin is that evidence is "original." Known as the Best Evidence Rule, the Federal Rules of Evidence maintain that:

> *An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."* [14]

Against this backdrop, challenges to authenticity and originality often come via claims that evidence has been contaminated or altered at some time between initial collection and eventual presentation in court. The initial actions of persons at the scene, for instance, serve as fodder for challenge. Given that those persons may have inadvertently deposited their own fingerprints, footprints, tool marks, hair, clothing fibers or biological materials at the scene opens a door to challenges that the evidence is not what it purports to be and that resulting analysis and event reconstruction is not reliable.

[¶16] Those challenges can gain significance as the size of the scene and the number of individuals increases. For instance, a murder scene in a public park may involve a host of potential contaminants, from paramedics and other first responders to members of the public. This could be further complicated if multiple scenes are implicated in the collection process, such as when a shooting spree occurs in

multiple rooms throughout a building. These situations are particularly ripe for cross contamination challenges. The risk of challenge is affected by the ability to secure the scene and limit the number of potential "alteration agents." A residential robbery may pose less of a contamination threat than a stabbing in an open-air market, for instance.

[¶17] Analysis and interpretation of physical evidence can also be challenged based on environmental conditions that may have altered evidence at the scene. For example, rain can dilute blood and bacteria can confuse forensic identification.

[¶18] Furthermore, evidence processing equipment, packaging materials, and processing techniques themselves may open multiple points of vulnerability where the source evidence can become exposed to change or alteration. An unsterilized preservation bag or use of chemical to enhance latent evidence may affect the authenticity and open the door to evidence integrity challenges, for example.

B. Countering the Challenges and Meeting the Standards

[¶19] Just as equivalent standards and challenges underlie physical evidence and digital evidence, so too can we extrapolate similar mechanisms to rebut authenticity challenges and assure evidence reliability.

[¶20] Chain-of-custody is one of the controls used by courts to satisfy admissibility standards. That is to say, the authenticity of physical evidence is shown by accounting for who, what, when, where and how a given piece of evidence was transferred from its initial discovery, through its collection, access, handling, storage and eventual presentation at trial. Chain-of-custody has been institutionalized as a procedure for the seizure of physical evidence by law enforcement, as well as for the handling of digital evidence by computer forensic examiners as a measure of evidence integrity.[15]

[¶21] As applied to the admission of physical evidence, the standard for chain-of-custody was defined in part by a seminal case in 1960 when the court set out the "substantially the same condition" test. The defense challenged the admission of marijuana evidence on the basis that it was unaccounted for between the time it was confiscated from the defendant and when it was introduced at trial. The Court of Appeals held:

> *Before a physical object connected with the commission of a crime may properly be admitted in evidence, there must be a showing that such object is in substantially the same condition as when the crime was committed. Factors to be considered in making this determination include the nature of the article, the circumstances surrounding the preservation and custody of it, and the likelihood of intermeddlers tampering with it. If upon consideration of such factors the trial judge is satisfied that in reasonable probability the article has not been changed in important respects, he may permit its introduction as evidence.*[16]

The test for determining proper chain-of-custody has sometimes been narrowed or broadened depending on the type of evidence at hand. For instance, chain-of-custody when applied to tape recordings has been held to an "indisputable fundamental trustworthiness" criteria.[17]

[¶22] In one case, the admissibility of police audio tapes of conversations between an undercover informant and the defendant regarding solicitation of murder was challenged because of a seven-minute gap in the recordings. The State of Texas rebutted the alteration claim by explaining that the gap was due to interference and loss of transmission rather than any alteration. Furthermore, it offered proof of chain-of-custody by showing the tapes were kept in secured steel cabinet, in the police department evidence room, and strict access control and documentation was maintained. In ruling that that proper chain-of-custody was established, the Court admitted the recordings based on the following tests:

> *The particular case in which a recording is offered is part of the circumstances to be considered in determining whether…chain-of-custody…has indisputable fundamental trustworthiness necessary for the recording's admission into evidence…. The burden is on the proponent to establish the necessary predicate [for admission of the tape recordings]. If alteration of a tape recording offered in evidence is accidental and is sufficiently explained so that its presence does not affect the reliability and trustworthiness, recordings can be admitted. When the defendant makes an attack on the chain-of-custody of a tape recording offered in evidence, [the] recording can be…omitted.*[18]

Whether the test is "substantially the same condition" or "trustworthiness" or some variation thereof, the defining thread is that courts rely on chain-of-custody as a control to gauge reliability and authenticity.

C. Chain-of-Custody and Digital Forensics

[¶23] To establish foundational support for the forensic soundness of live-remote digital evidence collection, it is useful to understand how chain-of-custody has been practically applied for physical evidence. Chain-of-custody is a process consisting of methodical checklists and procedures during the collection, preservation and analysis of evidence for the purpose of establishing authenticity and reliability of evidence. In other words, the evidence offeror tries to prove the chain-of-custody in order to rebut or minimize charges that evidence may be tainted or altered.

[¶24] Since chain-of-custody is functionally abstract, we can apply the court-proven principles, policies and procedures that control for the admission of physical evidence to digital evidence.

[¶25] As with chain-of-custody for physical evidence, the general chain-of-custody procedures followed by digital forensic practitioners to establish authenticity for

digital evidence include:

• Refraining from altering the original evidence both in collection, storage and analysis (e.g. analysis performed on evidence copies; cryptographically hashing original evidence)
• Documenting procedures used in the collection, storage and analysis

Specifically, the general forensic chain-of-custody procedures that control for:

1. What types of evidence have been collected;
2. Where the evidence was collected;
3. Who handled the evidence before it was collected by forensic practitioners, while it was stored, and after it was examined;
4. How the evidence was collected and stored; including what tools or methods were used to collect and/or store evidence;
5. When the evidence was collected.

• Documenting and explain any changes that may be made to evidence; establishing auditable procedures
• Maintaining the continuity of evidence
• Making a complete copy of data in question
• Utilizing a reliable copy process (e.g. independently verifiable; hashing for verification)
• Employing security measures (e.g. tamperproof storage, write protection)
• Properly labeling time, date, source (e.g. tracking numbers, tagging)
• Limiting and documenting the persons with access to data

[¶26] The principles underlying these forensic procedures for ensuring reliability of digital evidence include, but are not limited to:[19]

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.

2. Upon seizing digital evidence, actions taken should not change that evidence.

3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.

4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.

5. An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in his/her possession.

6. Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

[¶27] Having established the common principles between physical and digital evidence chain-of-custody controls, the focus now turns to establishing how the live-remote methodology can implement these "guarantees of trustworthiness" so that the collected data can be shown to “reflect the evidence accurately.” By doing so, conclusions drawn from evidence obtained via the live-remote methodology will be less open to challenge.

III. Applying Challenges and Controls to Live-Remote Methodology

A. Challenges in the Context of Tradition

[¶28] Before leaping from predictable challenges lobbied against physical evidence to the conjectured scrutiny of live-remote digital evidence collection, it is useful to understand how forensic practitioners have implemented reliability controls thus far.

[¶29] As discussed in Part II, forensic collection must be responsive to the particular environmental conditions that threaten to alter or otherwise affect the authenticity of the evidence. Forensic practitioners have responded to the volatile nature of computer network and disk evidence and the potentially destructive nature of acquisition and analysis by advocating that the digital crime scene be frozen – i.e., making a copy of all data on the original source media and performing subsequent filtering for evidence on a copy of that "dead" system. In other words, the standard operating procedure ("SOP") is to perform digital autopsies on copies of computer corpses.

[¶30] This traditional methodology implements the Best Evidence standard by taking the evidence-containing computer system offline and creating a bit-stream image of the entire original evidence disk. Known as "bit-stream imaging," this process involves copying all data from the original disk, sector-by-sector, to a target working disk or image file. If the target is a disk then any unused sectors on the target will be written with a known pattern for identification as non-evidence data. Thus, "originality" requirements have been fulfilled by anchoring on the media from which the potential evidence is acquired, the rationale being that in the event of evidence alteration due to practitioner action or hardware failure, another copy can be generated and analysis results will be reliable. Other ancillary techniques to ensure authenticity include write-blocking, error recovery and logging, and cryptographic hashing of the source before copying and the target evidence disk after the data has been written to it.[20]

[¶31] This methodology is premised on physical interaction with a static system, techniques which are different from dealing remotely with a live system. Judicial rulings that specifically address the acceptability of a particular forensic tool or technique are not plentiful, nor are they dispositive.[21] There are certainly cases where courts have ruled on forensic methodologies such as bit-stream imaging,[22] but rulings on point tend to be made in the context of challenges to search warrant execution rather than directly to the methodology itself. The consequence is that

the community is left to infer the acceptability of forensic methodologies, oftentimes from the courts' circular justification that the methodology comports with accepted SOPs,[23] thereby failing to offer precedent on point regarding the reliability of the technique itself. Regardless of whether the lack of precedent is due to deference to SOP compliance, stipulation, and/or lack of informed challenges, the traditional methodology has gained and maintained its authority in large part because of the de facto acceptance among forensic practitioners.

[¶32] There is not an equivalently robust precedent underpinning for digital forensics as there is with physical evidence methodologies, such as DNA fingerprinting. As a result, digital forensics practitioners are operating on a relatively clean slate in the case law proscribing or prescribing the reliability or admissibility of evidence obtained via a certain methodology. Because the de facto standards of forensic practitioners bear heavily on judge-made law the community will only be constrained by its own decisions and recommendations to test, accept and implement newer techniques.[24]

[¶33] Techniques for remote data access are not novel, nor are techniques for imaging or searching on live systems.[25] What is new are the forensic uses of these techniques for acquiring potential evidence so that it may be relied upon in court. The changing business and technology environments within which electronic artifacts are found, and the resource pressures attendant to traditional forensic methods will continue to combine and drive changes in digital forensic technology.

[¶34] In this changing environment, several questions remain. What are the risks and rewards of applying a live-remote methodology? What are the implications for forensic soundness, and how can live-remote methodology control for forensic integrity?

B. Rewards and Risks of the Live-Remote Methodology

[¶35] Although a comprehensive cost-benefit analysis of performing live-remote

forensics is beyond the scope of this paper,[26] the prominent advantages include: the ability to access data otherwise inaccessible via physical means (such as distributed network information), the ability to exclude non-relevant systems (resulting in reduced resources spent on back-end analyses),[27] minimized disruption to businesses by virtue of not having to take systems offline, fulfillment of Best Evidence requirements in light of the direct systems accessibility, the possibility of reading encrypted volumes or data (which proves valuable in obtaining passwords),[28] increased likelihood of accessibility to externally attached devices such as removable USB drives, the ability to search storage arrays, such as terabyte SANs that may be encountered in corporate enterprises or ISPs, and the ability to capture data from RAM memory, including running processes, active users, open ports, open connections and open files.[29] This lattermost capability has increased significance given the prevalence of malware that is increasingly being written to address space not captured on disk, such as exhibited by the SQL Slammer worm. Proving or rebutting Trojan Horse defenses may depend on the ability to ascertain whether malicious code was present.

[¶36] Another advantage from an operational perspective is that by designing tools that comprehensively implement live-remote methodologies, the error rate associated with piecemeal use of standalone utilities is arguably lowered.

[¶37] Shifting to the potential risks[30] involved with this methodology, the main critique focuses on integrity deficiencies. Specifically, the target operating system may be compromised so as to hide evidence or give false evidence, such as compromised executables, libraries or kernel level rootkits on the target system. Evidence may have been altered or destroyed by the software on the target system which performs the live-remote acquisition. Specifically, the servlet or agent may have altered the data by overwriting an existing file,[31] by modifying the registry if it is installed as a service, by overwriting previously deleted data,[32] by overwriting an unused portion of the disk;[33] or, by increasing the chances of system crash, the resulting corruption, system reboot and/or reconstruction may alter data.

[¶38] Other alteration risks may come from local system users or network communication activity, points of vulnerability opened by remote access logistics, or the outright inability to obtain evidence at all due to technical hurdles in gaining remote access.[34]

[¶39] Aside from risks to authenticity, acquiring files on live systems while users may be accessing them could invite original evidence challenges. In other words, a live image (or copy) can only be verified against itself from the point when acquisition occurred, whereas images of "dead" machines can be verified against the original media. The implication is that because integrity hashes of drives before and after acquisition will certainly differ due to changes during the copying of active media, the accuracy of the remote image may be in question.[35]

C. Implications for Forensic Integrity: Challenges Based on Rules of Evidence

[¶40] Opponents of a live-remote methodology contend that the implications for authenticity or reliability-accuracy, completeness, and verifiability--make this approach inappropriate.[36] In other words, an anticipated legal objection to the live-remote approach is that it fails to provide complete, verifiable, and/or accurate results, thus inviting authenticity or reliability challenges and threatening evidence admissibility or relative weight in a legal proceeding.[37]

[¶41] Recall that before evidence can be admitted, it must meet the foundation standard of authenticity.[38] Authentication requires that the offeror of the evidence show that the data collected and offered as evidence by this methodology is what it purports to be. The standard for admission is that there is a reasonable likelihood that the evidence is what it purports to be.[39]

[¶42] In addition to authenticity challenges, live-remote methodology opponents might challenge the reliability of the evidence. For evidence that is scientific,

technical or of a specialized nature, the Federal Rules of Evidence and case law provide standards used by trial courts to determine if such evidence gets admitted. This reliability standard is invoked if data collected using the technique is the basis for expert testimony. The resulting technical expert opinion is admissible if it is based on sufficient facts or data, is the result of reliable principles and methods, and the expert has applied the principles and methods reliably.[40] Reliability may turn on such factors as whether the technique or theory 1) can be and has been tested, 2) has been peer reviewed and published, 3) has a known or potential error rate, and 4) has been generally accepted by the relevant community.[41]

[¶43] As is the case with any "novel" technique, the live-remote methodology may be vulnerable to reliability attack because of its unfamiliarity amongst the relevant forensic community. Besides the obvious lack of general acceptance, testing and peer review associated with any new methodology, relative unfamiliarity may bear negative impact on the error rate in an operational setting. Also, live acquisition techniques may give rise to reliability challenges because unlike static collection and analysis, subsequent analysis is limited to the point-in-time collection (including any substantive data filtering that may have occurred during the live-remote acquisition). Should examination and analysis require revisiting, the entire drive context would not be available. Thus, live-remote methodology may invite challenge in cases where information that is seemingly non-relevant upon initial review and filtering may later become relevant in the context of subsequently-examined information.[42]

[¶44] To explain further, recall that the traditional methodology is based on an offline workflow that is static and relatively indiscriminate: collecting a bit-stream image file of the static disk, searching the image file, filtering for probative data, and extracting certain artifacts for presentation as evidence. Critics of the suggested live-remote methodology might criticize that dynamic and network-based acquisition of digital corpus renders incomplete, inaccurate, and/or unverifiable evidence. For instance, images of the live system cannot be verified against the source media because the entire digital scene is not "frozen" and will necessarily

change as a natural result of system operation. Therefore, subsequent analysis of data not acquired in the initial collection is not possible. This can affect the accuracy of conclusions drawn from the incomplete data. Judged from the viewpoint of the traditional methodology, in other words, the original disk can never be compared to the forensic copy to assure that an exact duplicate of the original evidence was searched and seized. The practical inference is that this process may be underinclusive and/or biased, resulting in the exclusion of exculpatory evidence and casting doubt on its authenticity.

[¶45] Furthermore, live-remote challengers might suggest that the point-in-time nature of the acquisition invites selective filtering of potential evidence.[43] Completeness is one factor in determining authenticity and reliability. A full and complete disk image, so the argument goes, provides a truly objective picture of the digital landscape. It allows practitioners, examiners, fact-finders, and even legal opponents to look at the data and reach the same conclusion. Proof of incomplete evidence acquisition opens the door to challenges that the collected evidence is prejudiced and inadmissible. Critics may advocate that static acquisition, on the other hand, forefends contentions that only inculpatory, biased data was gathered or that exculpatory evidence was not recorded.

[¶46] To the extent that front-end filtering is coupled with live-remote techniques, associated keyword search techniques may be vulnerable to the same incompleteness criticism. That is to say, while string searching is a predominant identification technique, it may not locate all information permitted within a search warrant. For example, searches for "gun", "drugs" and "Al Capone" can identify documents containing those terms that should be collected. However, keyword searches may not uncover the context of documents that may refer to the transactions that would qualify as evidence of the crime but do not contain the explicit keywords. Furthermore, filtering based on file extension alone, without analysis of the possibly unmatched underlying content, may cause mislabeled yet relevant data to be uncollected.[44]

[¶47] Finally, live-remote acquisition may violate the Best Evidence Rule if it is successfully argued that the selective collection does not render an accurate reflection of the data evidence.

[¶48] Recall, however, that the success of many of these challenges is predicated on the substance of what is acquired as a result of the live-remote technique rather than the soundness of the technique itself. It is analogous to challenging DNA evidence on the grounds of failure to collect a blood stain rather than scrutinizing the reliability of the PCR technique used to analyze the evidence that was collected. The search and filtering techniques which may be conjoined with live-remote acquisition, however, should be scrutinized independently and are beyond the scope of this paper. Many (if not most) search scenarios will be dictated by search warrant parameters, thus crippling challenges based on the substantive incompleteness of data collected via live-remote techniques.

D. Controlling for Forensic Integrity: Live-Remote Methodology Upholds Authenticity and Reliability Standards

[¶49] As discussed in the previous section, critics of live-remote techniques would argue that the authenticity of collected evidence is dubious.[45] Under the standard for authentication, which requires a reasonable likelihood that the evidence is what it purports to be--however, the offeror of evidence is not required to rule out all possibilities inconsistent with authenticity. This means that the live-remote techniques need not produce results that are 100% complete, accurate and verifiable in order to be admissible.

[¶50] Opponents of live-remote techniques might challenge authenticity by alleging that the digital data could have been altered after it was collected. This argument is based on the ease with which computer records may be modified without visible detection. This argument is no different than what is currently lobbied against the traditional "static, at-hand" approach. It is also a favorite weapon for challenges to physical evidence. However, under the "reasonable likelihood" test for

authentication, courts have generally not been receptive to such claims absent specific evidence of alteration. Furthermore, the live-remote methodology involves the use of cryptographic hashing techniques that are likewise a hallmark of traditional methodology and that have been held by courts as sufficient to prove the integrity of digital data.[46]

[¶51] Lastly, data authentication may not necessarily be precluded by the use of examination software that alters non-essential data but has no significant effect on the substantive data.[47] Therefore, live-remote techniques that may alter data on the evidence media do not necessarily invalidate the authenticity of the evidence or diminish the reliability of the methodology.

[¶52] Regarding authenticity challenges based on completeness, to be sure, it is impossible to verify that all possible evidence in a dynamic environment has been collected. This is due largely to the difficulty in defining the parameters of the digital crime scene. The live-remote method does not necessarily freeze time for the entire corpus of the digital crime scene, but does control selective portions. What is significant is that, for those selected portions of the scene, the same court-vetted, integrity-verifying hashing techniques used in traditional methods are employed to verify that what was originally captured is the same as what is being presented in court. Furthermore, courts have upheld evidence as being authentic in situations where the accuracy of the testing on the uncollected evidence was sufficient to infer lack of exculpatory value.[48]

[¶53] In response to challenges to Best Evidence requirements, copies and duplicates satisfy this standard if they are shown to "reflect the data accurately." Live-remote techniques can meet this requirement because they use the same court-accepted hashing techniques discussed earlier.[49] Therefore, selective collection challenges can be thwarted by reliance on hash verification, in the same manner as how challenges to the traditional methodology are countered.

[¶54] As far as reliability challenges are concerned, recall that the standard for evidence reliability (e.g. *Daubert*) is not invoked unless an expert is giving an opinion based on that method. In cases where evidence gathered via live-remote techniques is being presented as substantive, and not the basis for expert testimony, reliability proof is moot and any challenges would go to the weight of the evidence, as is the case with the evidence derived from the traditional methodology.

[¶55] In situations where the *Daubert* standard is invoked, the reliability challenges based on lack of testing, peer review, known and error rate, general acceptance are merely based on the immaturity of the live-remote methodology as opposed to any empirical dissonance among the relevant forensic community. Thus, as this methodology is tested and applied more frequently, the outcome of a *Daubert* scrutiny will become apparent and ripe for reliability determinations. Furthermore, it is helpful to note that even the traditional, "established" bit-stream methodology is subject to the very same challenges based on the non-exhaustive factors elicited in *Daubert*.

[¶56] Another criticism of the live-remote methodology is that it places digital forensics first responders in the position of making evidentiary relevance determinations at the inception of the forensics process in contrast to the traditional back-end filtering techniques. Some argue that this task is more appropriately handled during the examination phase in order to ensure objectivity and minimize errors that may have resulted from the pressures of the “real time” crime scene. It is critical to realize, however, that these early determinations are no different than choices made every day by practitioners responding to and processing physical crime scenes Investigators at physical crime scenes conduct the same front-end filtering, such as choosing which tools and techniques to use, and what raw evidence to collect and analyze. This is exhibited in their reasoned collection methodology which takes into account the context of the physical environment and the tools and techniques available.

[¶57] Like those investigating a physical scene, digital forensics responders must choose what to collect based on the environment and their training and experience. Forensics practitioners at a homicide scene in a wooded area do not engage bulldozers to collect all the soil and surrounding brush, which might contain DNA or trace evidence of the murderer. Rather, they sift through areas likely to produce probative evidence. Digital forensics first responders' filtering and collection procedures are comparable and should not be distinguished merely because the crime scene is digital rather than physical.

E. Controlling for Forensic Integrity: Applying Chain-of-Custody to Live-Remote Methodology

[¶58] As discussed in Section I.B(3), chain-of-custody principles and procedures can be embedded in the live-remote methodology to provide "guarantees of trustworthiness." These principles and procedures can ensure that the collected data “reflects the evidence accurately.”

[¶59] Chain-of-custody is quite frequently used to rebut authenticity challenges based on general sources of contamination of physical evidence: number of individuals accessing the scene; security of the scene; environment threats such as weather; equipment and packaging; cross-contamination with other evidence; and, processing techniques used to enhance identification. We can extrapolate similar controls for "contamination" with the live-remote approach.

(a) Limiting Agents of Change- Environment, Equipment, Cross-Contamination:

[¶60] The purpose of limiting agents of change is to bolster the integrity of evidence collected by minimizing the effect of environmental variables on the artifacts. It is unreasonable to control for all possible changes to evidence (e.g., weather conditions affect physical evidence at crime scenes). However, forensic practitioners should understand what conditions may have had a relative affect on

the artifacts and be able to explain the evidentiary significance. In the electronic crime scene, this can be accomplished by implementing standard and secure identification procedures and by ensuring that live-remote techniques are transparent, consistent and designed to minimize alteration to the original media on the remote system or dependence on remote system libraries.[50] For example, the software implementing the methodology can run from system memory and calls to the system kernel can be controlled, thus limiting writes to the system disk.[51]

[¶61] If the software is installed on the target system, it can be pre-installed as a service in anticipation of an event. This technique would deem the software to be part of the original media, thus minimizing the post-event system changes which may invite evidence integrity challenges. Regardless, any changes to the registry and disk should be documented and those processes and changes can be tested, verified and reproduced by competent third parties in a controlled laboratory setting. Also, system metadata should not be changed, and executables and libraries on the remote system do not have to be relied on by the live-remote process, in keeping with sound forensic practices. This helps control for integrity of information collected regarding files, processes, network connections, etc. If changes are made, it is vital that forensic investigators understand the context of the changes and distinguish their "footprints" from those they encountered on the electronic scene.

[¶62] Documenting the forensic practitioner's "footprints" in the digital scene is paramount to rebutting alteration challenges. This includes documenting with specificity what is and is not captured, altered, or changed on the remote system.[52] In addition, forensic practitioners should be able to explain the relevance of the alterations and the consequence of actions performed. This control is critical to rebutting procedural challenges, which have been successful in hundreds of cases challenging DNA evidence. Sloppy or inadequate evidence handling procedures[53] rendered the DNA evidence inadmissible not because of doubts about the validity of the underlying science, but because of problems in the procedures used by lab analysts to form their conclusions.

(b) Securing the Scene:

[¶63] Every piece of live-remote software must have documented testing to verify that it does not introduce any vulnerabilities to the target system. This can be accomplished by using techniques such as remote connection authentication (in a technical, security sense) and encryption.[54] Furthermore, encrypting acquired evidence sent over the remote connection mitigates against provable challenges that the network traffic is being monitored by an interloper.[55] Also, the actual presence of the software performing the live-remote methodology can be concealed to further discredit claims that unauthorized persons contaminated the scene.[56]

[¶64] In general, alteration threats from the point of acquisition, through backend analysis and final presentation in court can be countered by implementing court-vetted cryptographic hashing techniques discussed earlier.[57] Finally, digitally signing the evidence transmitted will provide assurances that the integrity of the data has not been compromised.

F. Best Evidence Controls

[¶65] Opponents may claim that by not having the media corpse, efforts to prove integrity by way of hashing are dubious. However, practitioners using the live-remote methodology can show through sufficient testing and documentation that the same image/data acquisition results can be consistently captured and processed, as well as how the live-remote process affected the results of the live-remote acquisition.[58]

[¶66] Significantly, the credibility of Best Evidence challenges to live acquisition have been dealt a blow by recent case law which have held forensic disk images to be exact copies and admissible when the "original" is no longer available.

[¶67] In *Ohio v. Morris*,[59] the government's forensic analyst copied the hard drive of the Defendant's computer and returned it to the police department that seized it. However, prior to returning the computer, the analyst erased all the data on the drive. The evidence in question was actually presented at trial in the form of a copy of the hard drive. The Defendant argued that his due process rights were violated because he could not examine the original hard drive to determine whether it contained exculpatory evidence.

[¶68] The appellate court held that testimony about the imaging techniques of the software used to create a copy of the original drive was sufficient to show that the duplicate was admissible and the Defendant failed to specify what type of exculpatory evidence may have been lost during the copying process.[60]

IV. Live-Remote Reliability: Precedent by Analogy

A. Digital Image Enhancement and Best Evidence Challenges

[¶69] Given the relative dearth of precedent to guide the forensic application of live-remote techniques we can comparatively analyze digital imaging case law to gauge how courts may deal with the forthcoming challenges. Digital image enhancement is a process that relies on computer software designed to improve the image sharpness and contrast of a digital photograph by eliminating background patterns and colors.[61]

[¶70] Image enhancement has been adapted for use in fingerprint identification, where it is used to remove patterns from original latent fingerprints, including the background on a check, the dot pattern on newsprint, or the weave pattern on material that would otherwise interfere with identification. The process has also been used to improve the quality of latent prints lifted off blood stained fabrics and other difficult surfaces.

[¶71] The most compelling conceptual similarity is that both the enhanced image and the live-remote image are ripe for arguments that neither image is an "original" under Federal Rule 1001(3) or even a "duplicate" under Rule 1001(4). Under either rule the image must be shown to accurately reflect the original evidence. Both methods render evidence which, in a strict sense, differs from the original source. Digital image enhancement involves the computer altering the image by subtracting pixels and the live-remote methodology involves electronic acquisition while the system is changing. Also, if selective filtering techniques are used in the live-remote methodology, one could claim that the filtered image is not unlike the digital photograph whose background patterns and colors have been removed to better ascertain the underlying data of importance.

[¶72] Setting aside the obvious differences between evidence derived from the respective techniques, the similarities in the challenges to both techniques are worth analyzing. The framework within which courts have addressed *Daubert* reliability challenges to enhanced image techniques have been consistent with tradition. That is to say, courts are determining admissibility of evidence produced by this technique by requiring validation of the software used to create/enhance the disputed image. For foundational questions about expert testimony, courts are demanding that the testimony be the product of reliable principles and methods and that the witness applied the principles and methods reliably in the specific case. So, the establishment of proper protocol has not necessarily been an issue of weight, but rather, can go to admissibility.[62]

[¶73] In summary, the proponents of live-remote techniques should be prepared to address *Daubert* challenges by relying on the traditional, nonexclusive criteria that is well-established in case law: testability, peer review, error rates, and general acceptance.

B. Controlling for Guarantees of Trustworthiness: Live-Remote Methodology and Eye Witness Evidence

[¶74] What does eyewitness testimony have to do with live-remote acquisition methodology? By understanding the principles and controls for eyewitness evidence admission, we can make a compelling case for the reliability of evidence derived from the live-remote methodology. Although the level of scrutiny applied to eyewitness testimony is far from monolithic or amenable to black-and-white formulas, there are universal "guarantees of trustworthiness" upon which fact finders rely to determine the admissibility and weight afforded to eye witness evidence.

[¶75] Generally, there are three factors upon which courts determine the credibility of eye testimony: the witness' perception, memory, and narration. Courts have implemented this principle by requiring the testimony of a witness who can speak to the identity and accuracy of the evidence-whether it is a tangible document or eyewitness testimony. The rationale is that having the personal presence of a witness who can be cross-examined about the actual event and its link to the evidence is a sufficient guarantee of authenticity.[63] In this way, oath, personal presence at trial and cross-examination are used as controls by which the witness and evidence can be tested for sources of unreliability: memory, perception, and narration bias.[64]

[¶76] For instance, if Jack was to testify that he saw the green Ducati hit the yellow Humvee at the intersection of Ash and Beech streets, he would be required to be present at court; swear to tell the truth; and answer questions such as how far he was from the intersection, what time of day it was, whether he wears glasses and had them on that day, what was he doing before witnessing the event, and whether he knows any of the litigants, for example. The questions would be designed to elicit whether variables such as time, distance and cognition contributed to Jack's memory, perception and narration of the accident, and ultimately, determine the reliability of Jack's testimony.

[¶77] So, controls are a way to determine whether an eye witness to a car accident, for example, is reliably conveying the truth of how, when, where, and who was

involved in the altercation. Likewise, variables that threaten to alter the evidence obtained via the live-remote methodology, such as file overwrites by the acquisition software, data manipulation by third parties on the network, or trojaned operating systems can be controlled by specific documentation of the data that is and is not captured and altered or changed on the remote system, limiting remote access to a small and provable number of people, and audit trails showing that the remote connection was authenticated and encrypted. These controls for digital evidence serve the same purpose as oath and cross-examination do for eye witness evidence and offer a reasoned basis upon which fact finders can determine if there are any environmental "biases" that affected the live-remote acquisition, and ultimately the picture of truth it paints.

[¶78] Recall also that those are the same variables for which chain-of-custody in physical and digital evidence methodologies control. The important take away is that the controls embedded in the live-remote methodology can be based on the same principled guarantees of trustworthiness that underlie age-old eye witness evidentiary jurisprudence.

V. CONCLUSION

[¶79] Digital forensics involves the application of tools and technologies to prove the truth of a past event. The discipline of digital forensics has developed methods to enhance the identification, correlation, and characterization of digital information. As with other forensic disciplines, technology is used to increase information symmetries so that recreations of past events more probably reflect the true event, and justice is served.

[¶80] An evolved methodology that implements live-remote evidence acquisition is needed to even the playing field for forensic practitioners who are called upon to collect and interpret relevant data in high-volume, dynamic computer network contexts, while simultaneously adhering to legal pressures mandated by substantive and procedural standards and rules. A call for acceptance of this

evolved methodology recognizes that technology should enhance the capabilities of forensic practitioners and can be done in fulfillment of established evidentiary standards. This paper has advocated that there is a sound forensic basis for the yet-untested issue of the admissibility of live-remote digital evidence acquisition. As such, it is offered to give credibility to this evolved methodology and debunk the myth that non-static, network evidence collection is unreliable.

[¶81] Given that techniques such as remote fingerprinting of physical devices already exist,[65] the task of determining the reliability of live-remote forensics techniques will certainly ripen into a requirement rather than an option. While the courts will ultimately opine its reliability, digital forensics practitioners should not wait for the adjudicative process to define appropriate methodologies. Rather, the techniques being applied in practice must be formalized into an applied methodology that has acceptance and endorsement from forensic practitioners and authoritative bodies within the relevant community. Failure to embrace and validate this evolved methodology will exacerbate the gap between practice and principle, further strain the resources and ability of the system to handle cases, strengthen credibility challenges lobbied at the forensic practitioner, and ultimately tarnish the authenticity and admissibility of the evidence produced.

[?] Erin Kenneally, M.F.S., J.D. is a licensed Attorney who holds Juris Doctorate and Master of Forensic Sciences degrees. Ms. Kenneally consults, researches, publishes, and speaks on prevailing and forthcoming issues at the crossroads of information technology and the law. This includes evidentiary, procedural, and policy implications related to digital forensics, information security and privacy technology. She has lectured and helped coordinate training conferences for officers of the court, law enforcement, and industry professionals concerned with digital evidence and information forensics. She is a Cyber Forensics Analyst at the San Diego Supercomputer Center, liaises and holds leadership positions with the Computer and Technology Computer High Tech Task Force (CATCH) and the Global Privacy

and Information Quality Working Group, and provides thought leadership to numerous private and government advisory committees engaged in information technology law issues.

[1] Nobel Laureate Economist Herbert A. Simon, *Designing Organizations for an Information Rich World, in* COMPUTERS, COMMUNICATIONS AND THE PUBLIC INTEREST 40, 40-41 (Martin Greenburger ed., 1971).

[2] "Digital Evidence" is defined as information stored or transmitted in binary form that may be relied upon in court. "Digital Forensics" is defined as the principles and processes used in the collection, preservation, examination, analysis and documentation of digital evidence. *See generally* Scientific Working Group on Digital Evidence (SWGDE) and International Organization on Digital Evidence (IOCE), *Digital Evidence: Standards and Principles*, 2 FORENSIC SCIENCE COMM. 2, (April 2000), *available at* http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm#Definitions.

For the purpose of this article, the terms "acquisition" and "collection" are used interchangeably to refer to the gathering and storage of information for examination in the context of legal proceedings.

[3] *E.g.,* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279 (2005); *see also* Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 74 MISS. L.J. 3, (forthcoming winter 2005), *available at* http://ssrn.com/abstract=665662.

[4] For the purpose of this article, "digital forensic practitioners" refers to the collective body of professionals who apply computer forensic methodologies. Insofar as the designation of forensic procedures (identification, collection, preservation, analysis and presentation) may differ between organizations, it is beyond the scope of this article to suggest roles and responsibilities between these individuals. Furthermore, the methodologies advocated are inclusive of both criminal prosecutions and civil discovery. The Supreme Court made clear in Lego v. Twomey, 404 U.S. 477 (1972), that the heightened burden of proof in criminal cases, that is, proof beyond a reasonable doubt, applies to the establishment of the facts underlying the conviction, and not to the admissibility of specific pieces of evidence offered to prove these facts. The standard of authentication of evidence is the same in civil and criminal cases. The Federal Rules of Evidence govern proceedings in the courts of the United States without regard to their civil or criminal nature. *See* FED. R. EVID. 101.

[5] Technology is defined as the directed application of abstract ideas; *see*, Daniel Berdichevsky and Eric Neuenschwander, *Toward An Ethics of Persuasive Technology*, 42 COMM. ASS'N COMPUTING MACHINERY 5, 51 (May 1999).

[6] In other words, as of the date of this publication, there exists no case law precedent or standards document opining the reliability or admissibility of digital evidence acquired via live-remote methodology discussed herein. Attempts to introduce such evidence, or challenges to such attempts are effectively test cases which will furnish the basis against which subsequent evidence will be measured and upon which subsequent challenges will be patterned.

[7] For example, the Scientific Working Group on Digital Evidence (http://www.swgde.org), the International Association of Computer Investigative Specialists (http://www.iacis.org), the National Institute of Standards and Technology Computer Forensics Tool Testing Program (NIST-CFTT, http://www.cftt.nist.gov/project_overview.htm), and the Federal

Bureau of Investigation Computer Analysis Response Team (CART).

[8] Traditional methodology involves acquisition of dead/offline systems using standard connections to the target computer,such as directly attached IDE converter cables or client/server disk redirection software.

[9] *See* Erin E. Kenneally and Christopher Brown, *Risk Sensitive Digital Evidence Collection Methodology*, 2 DIGITAL INVESTIGATION 101 (2005), *available at* http://www.sciencedirect.com (type title of article in search field and conduct search; then follow hyperlink in the search results) (hereinafter RSEC).

[10] *See supra* note 7 and accompanying text.

[11] This includes that the evidence must not contain hearsay, unless it falls within an exception to the hearsay prohibition.

[12] FED. R. EVID. 901; FED. R. EVID. 702.

[13] Fred Galves, *Where the Not-So-Wild Things Are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance*, 13 HARV. J. L. & TECH. 161, 229-30 (2000).

[14] FED. R. EVID. 1001. Variations of this rule have been adopted by nearly every state in the United States. This “Best Evidence” standard has been interpreted to allow digital copies to meet the standard if assurances prove that it 'reflects the data accurately.'

[15] Erin E. Kenneally, *Gatekeeping Out of the Box: Open Source Software as a Mechanism to Assess the Reliability of Digital Evidence*, 6 VA. J.L. & TECH. 13(2001), http://www.vjolt.net/vol6/issue3/v6i3-a13-Kenneally.html.

[16] Gallego v. United States of America, 276 F.2d 914 (9th Cir.1960) (citing U.S. v. S.B. Pennick & Co., 136 F.2d 413, 415 (2d Cir. 1943)).

[17] Wayne v. State, 717 S.W.2d 140, 146 (Tex. App. 1986).

[18] *Id.* at 146-7.

[19] These principles were recommended by the G8 as developed by IOCE. *See* International Organization on Computer Evidence (IOCE) First Responders Guide Template (Dec. 14, 2000), *available at* http://ncfs.org/documents/ioce2000/reports/firstResponders.pdf; *see also* IOCE Principles and Definitions, *available at* http://ncfs.org/documents/ioce2002/reports/principlesDefinitions.pdf.

The live-remote collection methodology is based on the same core forensic principles that the traditional methodology seeks to uphold. The foremost international authority on digital forensics standards, the International Organization on Computer Evidence (IOCE), is a collaboration of government agencies whose purpose is to provide an international forum for law enforcement agencies to exchange information concerning computer investigation and computer forensic issues, including developing standards and principles for computer evidence.

The IOCE was formed in 1995. In December 1997, the G8 High Tech Crime Sub-Group

tasked IOCE to develop international standards for the exchange of digital evidence. By November 1999, the first product was ratified by IOCE. During 2000, the IOCE proposal was substantially accepted. *See* Mark M. Pollitt, *Report on Digital Evidence,* 13TH INTERPOL FORENSIC SCIENCE SYMPOSIUM, (Oct. 2001), *available at* http//www.interpol.int/Public/Forensic/IFSS/meeting13/Reviews/Digital.pdf.

[20] The NIST Disk Imaging Tool Specification 4.0.0 describes technical details of recommended processes used in bit-stream imaging for items such as write-blocking, error recovery and logging, *available at* http://www.cftt.nist.gov/disk_imaging.htm.

[21] In addition, obtaining judicial records of *Daubert* hearings and other in camera reviews of evidence challenges are very difficult to obtain, and are essentially predicated on a court-by-court search and manual retrieval of information.

[22] Quoting:

> Making a mirror image of the hard drive is central to the examination process and is a routine, technical step taken by well-trained CART agents. It is done to maintain the integrity and security of the original evidence. A mirror image is an exact duplicate of the entire hard drive, and includes all the scattered clusters of the active and deleted files and the slack and free space. Having such a mirror image of the hard drive also allows the examiner to reconstruct the steps of his examination at a later time.

U.S. v. Triumph Capital Group, Inc., 211 F. R. D. 31, 48 (D. Conn. 2002),

[23] Quoting:

> The methodology SA Rovelli used to search the hard drive was consistent with the methodology that a well-trained CART agent would use. The evidence establishes that SA Rovelli acted in good faith and conducted an extensive, careful and thorough examination of the entire hard drive and attempted to stay within, as far as practicable and possible under the circumstances, the methodology and limits set out in the warrant.

Triumph, 211 F. R. D. at 45.

[24] *See* RSEC *supra* note 11. While the courts will ultimately opine on the reliability of a methodology, digital forensics practitioners should not wait for the adjudicative process to define appropriate methodologies. First, most reported computer forensics cases come from trial courts and have little precedential value. Second, since few computer forensics cases get appealed, there is not much guidance to be gained from courts of appeals. Even when such cases are appealed, appellate review is a deferential standard, so most of the methodology determinations will remain at the trial court level. Finally, decisions that are reported generally involve cases at the far end of the spectrum, thus arguably offering dubious guidance to those methodologies generated from mainstream activities.

[25] Examples of techniques and utilities include netcat, telnet, virtual private network tools, and network drive mounting. For a list of tools and utilities, see, for example, NetAdminTools.com.

[26] *See* RSEC *supra* note 11.

[27] The basis for this claimed advantage, in comparison to collection on dead systems/networks, is that the live-remote methodology entails front-end filtering of non-

relevant artifacts whereas traditional techniques oftentimes involve imaging systems that "may" have evidence. By filtering on the backend (after collection), large amounts of irrelevant data are potentially collected up front, adding to resource burden.

[28] This applies to situation where the encrypted data is accessible in memory on the live system, and not as easily obtained when the system is taken down and imaged.

[29] *See generally* Eoghan Casey and Aaron Stanley, *Tool Review--Remote Forensic Preservation and Examination Tools*, 1 DIGITAL INVESTIGATION 241, 284-297 (2005); Philip Sealey, *Remote Forensics,* 1 DIGITAL INVESTIGATION 241, 261-265 (2005) *available at* http://www.sciencedirect.com.

[30] *Id.*

[31] *Id.* This is unlikely since the OS usually writes to free space.

[32] *Id.* If the program is loaded and run in memory it could still get saved on the disk as part of the swap file.

[33] *Id.* The BIOS or OS does not usually address this.

[34] *Id.* For instance, access control lists, port restrictions and/or firewalls may prevent network access; also, the target OS must be accessible using the remote access technique (e.g., the servlet must be compiled to work with the specific OS).

[35] *See* Casey, *supra* note 30.

[36] *See* California v. Trombetta, 467 U.S. 479, 485 (1984); *see also*, U. S. v. Valenzuela-Bernal, 458 U.S. 858, 867 (1982).

[37] *See* RSEC *supra* note 11. Another legal underpinning likely to be raised by opponents of live-remote methodology is based on the constitutionally guaranteed access to evidence under the Due Process clause of the 5th and 14th Amendments. This fundamental standard of fairness has been interpreted to oblige the government to afford criminal defendants a meaningful opportunity to present a complete defense. It also imposes a duty on the government to preserve and disclose material exculpatory evidence for use by the defense. *See* United States v. Agurs, 427 U.S. 97(1976); Brady v. Maryland, 373 U.S. 83 (1963). Legal analysis of Due Process challenges is beyond the scope of this article since it implicates the substance of what may be acquired, whereas the purpose of this article is to advocate the forensic soundness of the technique. That is not to say that the latter does not have an effect on the former, but a more comprehensive discussion of Due Process issues is better served by referencing RSEC, *supra* note 11.

[38] Section II.A,Standards and Challenges .

[39] FED. R. EVID.. 901(a).

[40] *See* FED. R. EVID.702 (as amended); *See generally* Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993), (establishing guidelines for the Federal standard for expert testimony reliability) and, Kumho Tire Co., Ltd., v. Carmichael, 526 U.S. 137 (1999) (extending *Daubert* to technical areas other than those considered strictly scientific).

[41] *Daubert* involved challenges to the admission of scientific evidence, and aimed to bring clarity to the reliability requirements enunciated in the Federal Rules of Evidence. The criteria espoused in *Daubert* was the Court's attempt to provide guidelines for ensuring that technical evidence is grounded in knowledge derived from the methods and procedures of science. By tying the validity of the knowledge to the underlying scientific methodology, the Court defined reliability as something that can be validated by testing and supported by more than subjective beliefs or unsupported speculation. *See* Erin E. Kenneally, Gatekeeping Out of the Box: Open Source Software as a Mechanism to Assess the Reliability of Digital Evidence, *supra note* 16.

[42] *See* U.S. v. Triumph Capital Group, Inc., 211 F. R. D. 31, 63 (D. Conn. 2002) (approving agent's use of an additional keyword search where additional keyword was based on the result of previous forensic examination).

[43] *See supra* note 35 and accompanying text.

[44] Triumph, 211 F. R. D. 31 at 62-63.

[45] Challenges related to other evidentiary considerations--relevance and hearsay--are not addressed herein, primarily because the nature of those challenges are not a function of the forensic collection methodology so much as they are predicated on judicial determinations of the nature of the substantive digital evidence itself (e.g. computer-generated or computer-stored).

[46] *See* Ohio v. Morris, 2005 Ohio 599 (Ohio Ct. App. Wayne County Feb. 16, 2005).

[47] *See* NATIONAL INSTITUTE OF JUSTICE COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIOGATIONS (July 2002) *available at* http://www.cybercrime.gov/s&smanual2002.pdf.

[48] California v. Trombetta, 467 U.S. 479, 489 (1984). The Court noted that categorical evidence of the accuracy of the testing process--the Intoxilyzer's measurement of samples--could supply the missing predicate. Since that machine was highly accurate, was periodically and frequently checked for malfunction, and had rare false positives that were caused by known interferences that could be investigated and disproved in a particular case, the Court found that the evidence of test results was highly reliable and thereby concluded that the missing breath samples lacked significant exculpatory value.

[49] *See* State v. Cook, 149 Ohio App. 3d 422 (2002).

[50] Standard and secure identification procedures can include techniques grounded in Public Key Infrastructure (PKI) or peer reviewed challenge and reply based systems. In this context, "open" refers to the transparency of the technique such that third parties could replicate the technique in the same context and generate the same results. "Open" does not refer to lack of security or confidentiality of the remote acquisition path.

[51] *See* Casey , *supra* note 30 at 292.

[52] For example, how much and what data is changing on the remote system during acquisition such as changes in process memory, data on mounted network shares, metadata.

[53] HARLAN LEVY, AND THE BLOOD CRIED OUT, 45-46 (BasicBooks, 1996).

[54] Further examples include access control lists for specific host connections and audit trails evidencing the actions of the forensic practitioner. In addition, software code integrity checking would mitigate against challenges that vulnerabilities in the live-remote software compromised the integrity of the evidence.

[55] For example, authorization and encryption can be accomplished by implementing global unique identifiers, public, private and/or session key techniques.

[56] In other words, concealment techniques can help prevent unauthorized users from disabling the live-remote software or wholesale deleting of valuable evidence by hiding the fact that it is running forensics on the live system. Note that this is less effective if untrusted users have root level access to the target system.

[57] The technique of hashing involves calculating and storing a mathematically unique value for data. Hashing is part of traditional forensic imaging methodology to ensure evidence integrity; *see* Ohio v. Morris, 2005 Ohio 599 (validating the MD5 hashing process).

[58] *See* Casey *supra* note 30.

[59] S*ee* Ohio v. Morris, 2005 Ohio 599, (Ohio Ct. App. Wayne County, Feb. 16, 2005).

[60] FED. R. EVID. 1003 permits the admission of a duplicate unless "a genuine question is raised as to the authenticity of the original" or "in the circumstances it would be unfair to admit the duplicate in lieu of the original."

[61] *See* GREGORY P. JOSEPH, MODERN VISUAL EVIDENCE 8-22 (Law Journal Press 1999). It is a subtractive process in which certain elements are filtered, but none are added based on preconceived notions of what the final image should look like. *See* William Watling, *Using the FFT in Forensic Digital Image Enhancement*, 43 J. FORENSIC IDENT. Ident. 574, 583 (1993), " [i]mage enhancement makes what is there more usable." Digital images are composed of millions of tiny dots referred to as "pixels." Then, based on degradation models developed in research, the software manipulates the pixels to filter out graininess and improve brightness and contrast.

See Alan L. McRoberts, *Digital Image Processing as a Means of Enhancing Latent Fingerprints*, PROCEEDINGS OF THE INTERNATIONAL FORENSIC SYMPOSIUM ON LATENT PRINTS, 165, 165-66 (July 7-10, 1987), *available at* http://www.scafo.org/library/mcroberts1987.pdf.

[62] Edward Imwinkelried, *The Debate in the DNA Cases Over the Foundation for the Admission of Scientific Evidence: The Importance of Human Error as a Cause of Forensic Misanalysis*, 69 WASH. U. L. Q. 19 (1991). As amended, in 2000, Rule 702 now mandates that the proponent demonstrate both that "the testimony is the product of reliable principles and methods" and that "the witness has applied the principles and methods reliably to the facts of the case." Prior to that amendment, prosecutors sometimes argued that proof of proper test procedure was not a required element of the foundation for expert testimony.

[63] See Galves *supra* note 14 at 229.

[64] *Id.* at 230.

[65] Tadayoshi Kohno, Andre Broido and K. C. Claffy, *Remote Physical Device Fingerprinting*, 2005 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS SYMPOSIUM ON SECURITY AND PRIVACY 1, 211, *available at* http://www.caida.org/outreach/papers/2005/fingerprinting/KohnoBroidoClaffy05-devicefingerprinting.pdf. By exploiting small, microscopic deviations in device hardware such as clock skews, the techniques can be applied to obtain information about whether two devices on the Internet, possibly shifted in time or IP addresses, are actually the same physical device. These techniques do not require any modification to the fingerprinted devices.