Digital Evidence: The Moral Challenge

Tom Talleur, Managing Director, KPMG LLP's Forensic Practice

My colleagues, co-founders, and I, are fortunate to have this opportunity to characterize a framework for discourse on the topic of digital evidence in this initial edition of the International Journal of Digital Evidence (IJDE). In this respect, we have an opportunity to identify, prioritize, and focus upon some of the most important aspects of this issue, free of irrelevant influences.

Our deliberations begin at a most critical time indeed. The content of this journal may quickly and understandably focus on examinations of the best tools, techniques and related themes of interest to a wide range of readers. Because of this, I thought it might be helpful for all of us to reflect upon the humble origins of our craft and the conditions of the present, and thus embrace the moral challenge before us with a renewed sense of vision and conviction.

The impact of digital information technologies (DIT) upon our world certainly poses endless benefits for the citizens of our growing global village. Many global citizens have seen how technology may be used to advance the condition of man and to correct miscarriages of justice, as with the use of DNA analysis to reverse criminal convictions. But many have also observed, with increasing alarm, how DIT can provide a low cost, high performance, seemingly anonymous conduit empowering man to destroy property or injure the rights others at will, very quickly, and with devastating impact — a fact raising serious social, moral, and legal issues for debate. One need only read a United States newspaper article about the latest event of cyber related misbehavior, to infer the need for clarity in addressing the issues relating to digital evidence from the social, moral, and legal points of view, as well as technical perspectives.

Not surprisingly, the digital evidence recovery (DER) movement paralleled the rise in cyber related crimes. Save the earlier telephone hacker (Phreaker) threat, this movement started loosely in the United States in the early to mid-1980's featuring a handful of federal investigators, with a few state and local police officers and a smattering of prosecutors, striving to make sense out of and to bring order and insight to what then appeared to be a cascading problem: the use of computers by criminals and the need to recover digital evidence in connection with investigations. The level of individual technical skill on the part of these early

DER examiners notwithstanding, they were a small, close-knit, clever and resourceful group that began to congregate as the Federal Computer Investigations Committee. Their small size and self-critical nature, buttressed through the oversight of devoted prosecutors, ensured an effort to balance the rights of suspects with the need to make "good case law," while enforcing the law and addressing inadequacies in the law through legislative and other initiatives. To be sure, individual members of this group made mistakes as they attempted to address the pandemic dearth of knowledge, skills, abilities, and the lack of training in the field through advocacy and a "master craftsman to layman" approach in training. Often, the use of their findings in courts or other forums went unchallenged for a variety of reasons. All parties to the process knew that it would only be a matter of time before the judgment of all DER examiners would be questioned in every respect. The best efforts of these early DER pioneers notwithstanding, we now find ourselves as a global information society with moral challenges before us.

Most investigations and litigation in the United States today involve digital evidence. Law enforcement digital evidence examiners and some private sector service providers try to adhere to a general practice of functioning as *evidence specialists* to avoid the certain pitfalls associated with declaring themselves to be "technology experts." We do not yet have a generation of forensic investigators, examiners, and members of the legal profession who are equally adept at conducting sound, objective thorough investigations and positioning findings in the form of sound litigation in matters involving digital evidence.

In the private sector, DER has now become a "big business" of interest to litigators and professional service providers. Litigation in the form of "electronic discovery" is epidemic, as technologically challenged DER examiners and members of the legal profession struggle with technology issues, while setting case law precedent in the process. Victims and litigators regularly employ information technology or security specialists to deal with digital evidence matters not knowing or caring, in some instances, of the implications of their actions. Software development firms, sensing a profitable market, deploy "one-size-fits-all" digital forensic products for use by anyone able to afford the cost of the software along with one and two week commercial software certification courses – an approach that has had some appeal with members of the legal, audit, network security and other disciplinary communities seeking to "cross over" into the digital evidence field. These conditions raise a host a standards, independence, and

related issues implying the potential for mistakes in judgment, error, and even willful misbehavior on the part of examiners or others in the process, and raises frightening possibilities. DER examiners increasingly, and thankfully I might add, find their activities and judgments subject to searing scrutiny, with their practices and procedures coming into question on an increasing basis. Fortunately, both law enforcement and private sector practitioners have the beginning framework of standards posed by the International Organization of Computer Evidence (IOCE), the National Institute of Standards (NIST), and the United States Department of Justice[1]. So what might we do in this context? Obviously, it is neither likely nor desirable to suspend technology advancements or DER initiatives, but the stakes are high, given the potential and increasing impact digital evidence will have on the liberty and rights of individuals in the future.

With this in mind, I raise a theme that all might agree may form the basis of an underlying premise in the digital evidence field: that the use of digital evidence findings as a basis of making moral judgments about the actions and intentions of others is worthy of continuous reflection and debate as a conceptual underpinning to this discipline and the standards associated with it. This theme begs, of course, many of the central issues tugging at the conceptual framework of the digital evidence issue. These issues revolve around the need for a common understanding of the concept of evidence generally, standards in a variety of conceptual senses, and, a framework for making ethical judgments about the interpretations and uses of digital evidence in a broad sense.

Of course, some may reject this lattermost idea altogether. After all, are not DER examiners simply "fact finders" who report their interpretations to others who then render judgments based upon their reports? Perhaps. But somehow this contention seems to conflict with the premise and long established practice that examiners must know "all of the relevant facts" in a given case prior to conducting an examination, so that their analysis is relevant. Are we now performing an ethical analysis in the process, since we a) have the facts b) render judgments about we will and

[1] Established in 1995, IOCE is a forum for accredited international law enforcement agencies to exchange information about computer crime investigations and related forensic issues. The Scientific Working Group on Digital Evidence is a US-based component of the IOCE. NIST has published "First Responder" guidelines for computer crimes and is in the process of researching standards in related areas. The DoJ Criminal Division has published several publications addressing computer crimes and evidence suggesting potential standards for evidence collection.

will not report as relevant and c) interpret what we report to others? Can we now assert we are just "independent fact finders" and that we do not make ethical judgments about others in the process of our examinations? Do we need to consider an overarching standard for ethical conduct on the part of all DER examiners?

Perhaps we might turn our attention for the moment to the concept of evidence, generally. In this respect, the issue of digital evidence relates more to the concept of evidence and knowing, in general, than it does to the digital technologies we often place at the focal point of discussions through our discussions of tools and techniques. This in turn begs the issue of the conditions to know.

The first generally accepted condition to the concept of knowing is, if one claims to know something, then that which he or she knows must be true. Stated differently, it is contradictory to assert that one knows something and that the object of his knowing is not true, unless, the person making the claim is willfully untruthful, has been mislead, is mistaken, is making a playful utterance, or the like. Second, if one claims to know something, he or she must believe it. Again, stated differently, it is contradictory to assert that one knows something, but that he or she does not believe in knowing the object of his knowledge, unless, the person making the claim is willfully untruthful, has been misled, is mistaken, is making a playful utterance, or the like. And finally, if one knows something, he or she should be able to give good evidence for it.

Those DER examiners who consider themselves to be "fact finders" only may be relieved to know that, with respect to the conditions to know as I have cited them above, we are concerned only with derivative knowledge (since we perform examinations based upon extant material following premises, fact patterns, through standards, policies, procedures, etc.) and not epistemic knowledge (for matters that are claimed to be "self-evident"). Also, it might be presumed that these conditions of derivative knowledge are implicit in the daily representations of DER examiners, litigators and expert witnesses as they represent their findings. It is possible, for example, that well intentioned but untrained, poorly trained, technology-challenged, lazy, or careless persons, or those of malign intent, acting as witnesses, victims, or examiners, could alter or misrepresent digital evidence leading, for example, to the wrongful conviction of an individual in a court of law. These individuals, save those of malign intent, could literally believe their actions as meeting the conditions of knowing even with the "good evidence

standard" as described above. As disconcerting as this possibility is, we at least know that the actions of those involved in many instances are subject to independent oversight or judgment.

It is clear that we no longer live in a world where a handful of federal investigators subject to strict oversight conduct digital evidence examinations. Second, it is clear that we do operate in a world where DER examiners make moral judgments about the actions and intent of others based upon their examinations. The question remains, what basis exists for these practitioners to claim they make these judgments in accordance with an overarching framework for an ethical analysis standard? Is there a need to set this standard now? My hope is that we will remain mindful of this issue and address it in our future deliberations along with the overarching issue areas of ethics, morality, and relevant law, following the precepts of critical thinking. My belief is that this issue will become increasingly important, especially when we find ourselves gravitating to granular dialogues about technologies, methodologies, and related tactical issues.

About the Author

Tom Talleur (ttalleur@cox.rr.com) is a Managing Director in KPMG LLP's Forensic Practice and the firm's U.S. practice leader for Forensic Technology Services. He has extensive executive, law enforcement, intelligence community, and public policy making experience regarding cyber crimes, advanced technology exploitations, and national infrastructure defense matters. He completed a 31-year career as a US federal criminal investigator in December 1999 and served as the Advanced Technology Programs Executive in charge of the Network & Advanced Technology Crimes Division at NASA just prior to joining KPMG. He is the recipient of awards from the White House and the Attorney General for his work in the computer crime field.

A graduate of the US Naval War College and the Federal Executive Institute, Mr. Talleur is a keynote speaker to a number of associations and training seminars around the world and serves as an analyst and consultant for television, radio and print media on topics related to computer crimes and the exploitation of technologies. He is a Seized Computer Evidence Recovery Specialist, Certified Fraud Examiner, and a UNIX and Network Security Specialist. He is an advisor to the President of the Information Systems Security Association (ISSA) (http://www.issa.org/board.html), President of the National Capitol Region ISSA Chapter (www.issa-dc.org) and a cyber crime commentator for E-Business Advisor magazine. He also serves on the editorial oversight board of the International Journal of Digital Evidence.