Digital Investigation 19 (2016) A1–A3

Contents lists available at ScienceDirect

Digital Investigation

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

Editorial

Differentiating the phases of digital investigations

Digital evidence can be useful in all phases of an investigation, such as generating investigative leads, handling crime scenes, and addressing probative questions. Although the phases are interdependent, they involve different knowledge, strategies and goals. Technical knowledge of digital evidence is useful, but not necessary, for developing leads in an investigation to find evidence sources, suspects, and victims (investigative activities). Processes such as extracting and observing data from digital devices are technical (technical processes), and do not involve interpretation or evaluation as these terms are defined in forensic science[1]. Studying digital evidence to address probative questions (evidence evaluation) requires higher levels of knowledge specialization, process formalization, testing implementation, research foundation, and quality oversight.

The lack of a formal differentiation between investigative activities, technical processes, and evidence interpretation is creating confusion and leading to some bad decisions.

Confusion about what aspects of digital forensic practice are investigative, technical, or evaluative has motivated courts in Europe and the U.S. to explore ways to restrict how members of law enforcement will process digital evidence, regardless of their role or qualifications. In some cases, courts have prohibited members of law enforcement from handling digital evidence at all, requiring an independent party to perform all processes.

To increase quality assurance, there is growing pressure on organizations performing digital forensic operations to be accredited, but it is unclear which activities require the rigorous quality controls of a laboratory environment.[2] For instance, questions are being raised as to whether digital investigators should be permitted to perform on-scene triage inspections of digital evidence. Due to the same confusion, some law enforcement entities maintain digital forensic units separately from their forensic laboratories. As a result, digital evidence is not treated in the same way as other forms of evidence.

These issues can be addressed more easily when a clear distinction is made between investigative activities, technical processes, and evidence evaluation. This distinction emerged from the OSAC DMSAC Science Task Group led by Mark Pollitt, and was influenced by work performed at University of Lausanne over the past decade by Pierre Margot, Olivier Ribaux, Christophe Champod and David-Olivier Jaquet-Chiffelle.

Technical processes

Making forensic copies of digital evidence, extracting all active and deleted files, observing data, and running presumptive tests such as automatically checking for potential child pornography all require technical knowledge and skill.

The person performing these technical processes must answer questions such as “Can the digital evidence be acquired in a forensically sound manner?,” “Can the data on the hard drive be decrypted?,” “Can active and deleted files be extracted from the digital evidence?,” “Do any files contain possible child pornography?,” and “Are there other potential sources of digital evidence in the cloud?”

Such technical processes have verifiable outcomes and can be safely performed without the stringent standards of a laboratory environment. Quality management systems and other measures typically found in forensic laboratories, such as peer review, are not necessary for such technical processes. Some level of repeatability, quality control and audit are required. Within such a framework, an administrative review of each technical process performed in a case may be sufficient to confirm that all tasks and supporting documents are complete.

Evidence evaluation

Forensic science studies evidence and its context to appraise accuracy, causation, linkages, spoliation, and

[1] Evaluation involves analysis of evidence to establish the relative likelihoods of different propositions, most typically a prosecution proposition relative to a defense proposition. Interpretation is more accurately used to describe the duty of a court to consider the evaluated forensic findings in the broader context of the case.

[2] A laboratory environment refers more to process than place, and could be just one qualified person using well established practices and tools. Certain laboratory-type processes may be performed outside the physical space of the actual laboratory.

http://dx.doi.org/10.1016/j.diin.2016.11.001
1742-2876/

meaning in order to addresses probative questions pertaining to evidence. The person evaluating digital evidence must address questions such as "Who downloaded certain files onto this computer?," "What camera was this digital photograph taken with?," "How did certain files come to be on this computer?," and "Was digital evidence on this computer intentionally destroyed?"

As noted in the first paragraph, addressing such questions involves interpretation and evaluation of digital evidence, which requires higher levels of knowledge specialization, process formalization, testing implementation, research foundation, and quality oversight. As summarized in the ILAC G19:08/2014 "Modules in a Forensic Science Process" under the section dealing with evaluation (described as interpretation) of the results of examinations and tests:

> *"Interpretation is when the conclusions drawn are based on more than just the result of the test at hand, for example conclusions drawn from observations at a scene of crime. Both in laboratory work and in scene of crime investigation there will be conclusions drawn based on observations and visual tests without objective examinations/tests necessarily being made. Interpretations shall be based on robust studies. In cases where this is not possible, the interpretation shall at least be supported by a documented body of evidence (records). When interpretations are made the limitations of the examination/testing used shall be fully considered. For example, definitive conclusions shall not be drawn from presumptive testing."*

The ACPO Good Practice Guide for Digital Evidence (version 5, March 2012) provides the following example to distinguish the evaluative process:

> *"the presence of indecent images of children on a computer would not in itself be sufficient evidence of possession, as the possessor must be aware of the existence of the images. A digital forensic practitioner may interpret the presence of other digital evidence (such as a list of recently opened files, recent search terms, the name and location of folders/files containing the material, or whether or not the computer is password protected) to establish the likelihood of the user being aware of the existence of these images."*

Significant differences

Investigative activities are exploratory in nature, formulating theories about who did what, when, when and how, and testing those theories against available information. Investigative activities are supported by technical processes and evidence evaluation.

Even if there is disagreement on the specifics of investigative activities, technical processes versus evidence evaluation, simply acknowledging that a distinction exists can guide decisions about which tasks in a digital investigation require the rigorous quality controls of a laboratory environment.

Technical processes can be performed outside of a laboratory environment by professionals with basic training and limited oversight. Examples include:

- Decrypting data stored on storage media or mobile devices.
- Running an automated process to determine whether any files extracted from a computer match information in a database of known child pornography.
- Using a virus scanning tool to automatically determine whether any files extracted from a computer match information in a database of known malware
- Reviewing information extracted from a smartphone to see the cloud accounts that were configured on the device. Such rapid review enables prompt notification the cloud service providers to preserve any associated data on their systems.

These kinds of processes, sometimes referred to as triage, produce information that can provide a foundation for forensic analysis, but do not do not involve evaluation of digital evidence.

Evidence evaluation to address probative questions is most effectively performed by forensic personnel with specialized knowledge, skills, and abilities governed by robust quality management processes. Examples include:

- Authenticating a claim and associated digital evidence to establish its level of veracity.
- Analyzing the content and context of a file to evaluate whether or not it was tampered with.
- Studying user activities on a computer to evaluate whether or not they can be associated with a particular person.
- Comparing properties of a camera found at the suspect's home to evaluate whether or not it was used to take incriminating files found on the Internet.
- Reconstructing activities on a computer to evaluate the sequence of events and interactions between entities.

Evaluating digital evidence can be complex, and requires a careful approach to reduce potential cognitive bias. There is also some uncertainty in any result or conclusion, which can be expressed as a likelihood (e.g., confidence scale), or relative likelihood (e.g., likelihood ratios).

Distinguishing between technical processes and evidence evaluation helps avoid problems associated with unqualified individuals attempting to evaluate digital evidence without the necessary expertise and oversight. These problems include missed evidence, incorrect conclusions, and inability to address questions about the likelihoods of their conclusions.

Privacy

Even supposing that an individual is guilty of the crime being investigated, this does not negate their privacy rights in relation to activities that are unrelated to the crime. Both technical processes and evidence evaluation must remain within scope of the legal authorization that specifies what kinds of information may be sought. For instance, if there is no legal authorization to search for child pornography, it would be outside of legal scope to specifically search for files containing known child pornography.

In April, I participated in the National Cyber Crime Conference (NCCC) where a panel of judges expressed their concerns that digital searches could enable digital investigators to view everything on a computing device. This perception is fueling a debate in the U.S. about whether digital searches violate the Fourth Amendment prohibition against general searches. Reacting to these concerns, courts are considering measures to strictly limit digital searches by requiring search warrants to constrain how digital searches are performed by imposing search protocols that are limited to particular file formats, areas of devices, timeframes, or search methods. Imposing such constraints, even with good intentions, would substantially increase the risk of relevant digital evidence being overlooked or misunderstood. Even worse, such search protocols could be purposefully abused to prevent the evidence of criminal activity from being collected or analyzed.

An effective strategy already employed by other forensic disciplines, is to have personnel performing technical processes concentrate on finding, preserving, and documenting potential sources of digital evidence, recognizing potentially important elements that warrant further attention, and making digital evidence available for evidence evaluation. Problems can arise when individuals who are only trained to perform technical processes go beyond their expertise and attempt to evaluate evidence without adequate rigor to adequately address probative questions. When probative questions need to be addressed, these are posed formally for further evaluation by qualified personnel using well established practices and tools governed by the rigorous quality controls of a laboratory environment.

Accreditation

Whether at a crime scene or forensic laboratory, some level of quality control is needed to ensure that anyone handling digital evidence is properly trained and supervised, and that results are reliable. To address this need, many countries are requiring or encouraging organizations that perform digital investigations to be accredited. The U.S. Department of Justice announced a new policy requiring all Forensic Science Service Providers (FSSPs) to be accredited within five years. The EC Council has recommended, but not yet mandated, accreditation. The UK Forensic Science Regulator is focusing on accreditation of digital forensic service providers in the coming year.

Law enforcement organizations are concerned that this trend will prevent them from obtaining relevant information in a timely manner, causing cybertrails to grow cold and allowing criminals to escape. Prohibiting triage activities from being performed outside of a laboratory environment would delay relevant information being available for investigative purposes such as preserving cloud sources or apprehending suspects before they flee. Categorizing such activities as technical processes makes it more clear that the information has not undergone rigorous quality assessment and its veracity has not been evaluated. Clearly distinguishing technical processes from evidence evaluation also helps decide what needs to be accredited and according to which standards, e.g., ISO 17025 or ISO 17020.

Conclusion

Making a clear distinction between investigative activities, technical processes, and evidence evaluation helps clarify many hotly debated issues relating to digital investigations. This distinction can help reduce the risk of privacy violations by clarifying that individuals who are only trained to perform technical processes should not go beyond their expertise and attempt to evaluate digital evidence. This distinction can help international efforts to improve digital investigations and forensic science by clarifying which activities require the rigorous quality controls of a laboratory environment, and which do not. At an organizational level, evaluation of digital evidence can be integrated with existing forensic laboratories, while technical processes can be kept separate to serve both investigative and forensic needs. Standards and guidelines that are being developed by ASTM and SWGDE could be organized to cover technical processes and evidence evaluation distinctly. ENFSI has started down this road with their guideline for evaluative reporting in forensic science. Even when a single person is responsible for generating investigative leads, handling crime scenes, and addressing probative questions, conscious separation of each phase helps ensure that appropriate processes and oversight mechanisms are employed.

Eoghan Casey
École des Sciences Criminelles, Université de Lausanne, Batochime, CH - 1015, Lausanne, Switzerland
E-mail address: eoghan.casey@unil.ch