C14 Modeling Digital Autopsies on Medical Autopsies

Martin S. Olivier, PhD, University of Pretoria, Computer Science, Pretoria 0002, SOUTH AFRICA*

After attending this presentation, attendees will be able to reflect on tests for "normality" during digital forensic examinations to exclude possible alternative explanations that may fit the facts in a case.

This presentation will impact the forensic science community by increasing reliability of findings in certain cases.

Forensic examination is at the core of digital forensics practice. Examination uses science to provide an answer to a question that is relevant for legal or related purposes. The question may entail association, event reconstruction, or some other insight from forensic evidence. Once an answer *x* is obtained, the question can be reformulated in the form: Is *x* true? The outcome of such an examination then is a (qualified) *yes* or *no* (or *unable to determine*). The need to qualify the *yes* or *no* relates to the level of certainty with which the question can be answered.

Digital forensics certainty (or error rate) remains problematic.[1,2] The premise of this presentation is that certainty is increased when alternative explanations have been eliminated. Digital forensic examination research often focuses on specific technologies that are subject to change — reducing certainty. This study suggests that more technology-neutral research needs to be done as a precondition for expressing confidence.

Unifying forensic science may be unrealistic, but metaphors from the medical sciences are common in digital forensics (e.g., the notion of a dead examination or the Autopsy Forensics Platform).[3] Conducting a thought experiment to explore a mapping between medical autopsies and digital forensic autopsies is therefore prudent.

The first striking similarity considered in this presentation is the crisis experienced in medicolegal death investigations in the 1800s due to the variety of (questionable) methods used. Rudolf Virchow is credited with establishing a method to conduct autopsies that met scientific standards and that subsequently became the standard protocol.[4] Arguments about the "scientificness" of digital forensics continue and are raised in the presentation.

One of the characteristics of the Virchow protocol is that the entire body is examined irrespective of the presumed cause of death. It avoids confirmation bias. The study demonstrates the general acceptance of this (unintuitive) imperative. The internal examination consists of a systematic removal of the organs; each organ is inspected to establish its consistency with expected ("normal") characteristics. Similar verification is a significant difference between autopsies in these disciplines. Another significant difference is the nature of findings. These differences and the validity of transferring imperatives from one discipline to the other are considered in the study.

Is it possible (and meaningful) to "remove organs" from digital artifacts and express an opinion on the normality of such "organs"? The digital equivalent of an organ is a system, subsystem, or an application (henceforth, system). The National Institute of Standards and Technology (NIST) National Software Reference Library already catalogs hashes of files occurring "normally" in many systems. This experiment requires more: it needs a version of a system consisting of a number of "known" files. A database with at least two sets per system is required — a set of file hashes for a minimal installation as well as a similar set for a full installation of a system. Details and relevant logic of which files should be included forms part of the presentation. In such a database, for any system *Si*, the set of hashes corresponding to a full install will be denoted by $\uparrow Si$ and $\downarrow Si$ will be used for the minimal case. Assume that *F* is the set of hashes of all found files. Then $FSi=\{f \in F | f \in \uparrow Si\}$ is a potential system (or "organ"); if $\downarrow Si \subseteq FSi$ then *FSi* may be considered "normal." It also means that every $f \in FSi$ has been accounted for. Shared files need special consideration. This presentation will argue that "normality" of files not included in the hash sets implies syntactic correctness. Additional criteria for some excluded categories apply.

The proposed approach verifies "normality" of system anatomy beyond the primary focus of the examination. This may be extended to physiological "normality" — where cause and effect, and, hence, valuable evidence may be revealed.

This presentation includes some observations about practical difficulties in identifying the "organs" from a small proof-of-concept experiment.

References:

1. E. Casey. *Digital Evidence and Computer Crime*. Academic Press, second edition, 2004
2. F. Cohen. *Digital Forensic Evidence Examination*. Fred Cohen & Associates, 3rd edition, 2012
3. B.D. Carrier. Risks of live digital forensic analysis. Communications of the *ACM*, 49(2):56–61, 2006
4. R. Virchow. Gesammelte abhandlungen zur wissenschaftlichen medicin von Rudolf Virchow. Grotesche Buchhandlung, 1862

Digital Autopsy, Normality in Digital Forensics, Science of Digital Forensics