LOADFAST:
An Outcome-Driven Digital Forensics Methodology

By Alexander M. Rzasa

Digital forensics is a scientific field at the nexus between two perpetually evolving realms: information technology and the law. As such, digital forensic science can benefit greatly from clear methodologies that guide practitioners, researchers, theorists, students, and juries towards consistent, verifiable, and scientifically-sound outcomes. If the historically wide variety of digital forensics methodologies is any indication, such frameworks will continue to evolve at a pace commensurate with technological innovation. A review of key features present in multiple digital forensics methodologies highlights common, useful phases for any digital forensics process as a whole. Furthermore, analysis of these fundamental stages reveals that a digital forensics methodology with the greatest utility and longevity is both a broadly defined one, and one that begins with consideration of the ultimate goal rather than the first technical procedure. LOADFAST, an outcome-driven digital forensics methodology, embodies this principle through legal objective analysis, followed by evidence identification, collection, examination, analysis, and final application, in that order.

Literature Review

Forensic science, digital or otherwise, is the application of science to the law[1]. In contrast to other forensic sciences (for instance, those focusing on physical or psychiatric evidence), digital forensics applies scientific methods to the identification, collection, examination, and analysis of digitally stored information, or data[2]. As the sizes, scopes, and types of such data have expanded exponentially over time, so too have digital forensics methodologies grown and multiplied[3]. A thorough review of this evolutionary process in methodology development reveals a number of core elements common to all digital forensics approaches[4]. These core elements represent the key phases of all digital forensic investigations, regardless of the specific context of a given methodology or the detailed steps contained therein. As core elements, they also point the way towards a new, more outcome-driven digital forensics method focused on the principal driving force behind all forensic science: the law.

> *"As the sizes, scopes, and types of digital data have expanded exponentially over time, so too have digital forensics methodologies grown and multiplied."*

The Identification Phase

At the outset of any digital forensics procedure, data must be identified and located before further actions take place. Whether separated into initially broad "acquisition" and subsequently targeted "identification" steps, as in earlier methodologies[5], or consolidated as a more overarching "detection" step applicable to modern network forensic scenarios[6], the identification of data relevant to a desired investigatory outcome is the logical underpinning of any forensics method or process. Although some including NIST[7] subsume the identification of evidence into a collection phase, the majority of digital forensics methodologies treat identification as a distinct, earlier step[8]. Technical justification for this distinction may be found in both the changes to evidence that can be caused by collection methods[9], as well as the exponential growth in the average size of digital forensic evidence[10]. Both factors support the conclusion that proper identification of relevant sources of evidence, prior to decisions or actions regarding evidence collection, promotes efficacy and efficiency in digital forensic investigations.

The Collection Phase

Once potential sources of digital evidence have been identified, evidence collection can take place in a properly targeted manner. While some methodologies further subdivide the collection phase into more specific steps, such as "reconnaissance" and the physical transportation of hardware[11], the majority of digital forensics methods include a general collection phase[12,13]. Rapid technological developments, including the rise of cloud computing, underscore the advantage of the more broadly applicable collection frameworks for gathering forensic data. For example, in their Digital-Forensics-as-a-Service ("DFaaS") model, Du, Le-Khac, and Scanlon[14] noted several new sources of forensic data such as international cloud storage and Internet-of-Things ("IoT") devices that were not envisioned by earlier frameworks. With the possibility that neural implants or other unforeseen scientific advances may someday provide new sources of evidence, a broadly defined collection phase will continue to be the most widely useful in digital forensic methodologies. Therefore, more detailed collection procedures pertaining to specific scenarios and technologies are best housed in regularly updated manuals and procedural documents.

The Examination Phase

NIST provided the strongest rationale for a distinct examination phase (separate from and between both the collection and analysis phases) by highlighting the fact that, once data has been collected, additional steps must take place before analysis can occur[15]. Given the growing average case size of digital forensic evidence[16,17], filtering the wheat from electronic chaff has taken on even greater importance when searching for relevant pieces of information within a dataset. In addition to keyword and pattern-recognition tools, the examination phase may need to include the use of techniques to bypass data compression, encryption, or access control features[18,19]. Although some methodologies separate the preservation of data into a distinct step[20], a broadly inclusive examination phase reinforces the proposition that

accurate preservation of data should remain paramount across all stages of any digital forensics method. Also, as in the collection phase, a more general approach to data examination provides greater flexibility when investigators inevitably encounter new scenarios or technologies.

The Analysis Phase

Data analysis is the most critical step in any digital forensics methodology driven by real-world outcomes, because, at its core, digital forensics exists to provide actionable evidence for decision-makers. A growing number of methodologies indirectly support this proposition by including non-linear or feedback-loop analysis steps[21]. Others emphasize the importance of analysis by breaking this stage into individual steps that mirror the scientific method[22]. Many existing methodologies also recognize that analysis of data can occur during other phases, such as collection and examination[23], and some note that analysis is no longer limited to the laboratory setting[24]. At the other end of the spectrum, certain generalized methods reduce analysis to a component step within an overall "investigation" phase[25]. Whether detailed or specific, however, few digital forensics methods completely omit any analysis, review, or evaluation stage. Instead, the most prevalent distinctions between methodologies arise in areas outside the core forensic concepts of identification, collection, examination, and analysis.

Preparation, Preservation, Presentation, and other Procedural Considerations

As Yusoff, Ismail, and Hassan recognized, many differences within the ever-growing universe of digital forensics methodologies can be explained by subtle variances in procedural steps, such as those related to preparation, preservation, presentation, and other situation-specific considerations[26]. None of these considerations are without merit; however, some methods may prove too specific for general application due to the inclusion of particular, narrowly targeted stages. For example, due to the rapid development of new technologies including cloud computing, preexisting specificity regarding the nature of digital forensic evidence may narrow a methodology's long-term applicability[27,28]. Thus, more detailed approaches are by design tailored toward certain unique situations, rather than the longitudinal study and practice of digital forensics[29]. In contrast, broader-style methodologies distill the essence of digital forensics into generalized frameworks, not checklist procedures, but at times may not include sufficient detail to address all potential nuances[30,31].

Analysis

There is admittedly no 'one-size-fits-all' method for the study, development, practice, and application of digital forensics. At one end of the spectrum, highly specific methods such as the model presented by Perumal provide a logical and practical guide for investigations[32]. In contrast, other more global frameworks serve as general guidelines for creating and operating digital forensics organizations[33]. However, despite wide variations in their details and semantics, most digital forensics methodologies include some reference to the core principles of identification, collection, examination, and analysis. These principles can be unified and applied consistently by initially focusing on one key factor present in any digital forensics scenario: the intended outcome. Most methodologies are arranged in a logical, typically ordered pattern, and subdivided into discrete, sequential phases[34]. Although some digital forensics models are strictly linear[35,36] and some include feedback loops[37,38,39], all include a starting point and a targeted goal. This inherently sequential nature of digital forensics investigations means that certain phases are temporally dependent on others; for example, collection must take place prior to examination and analysis. As a result, most digital forensics methodologies begin with a general planning stage, initial collection, or some other foundational first step, and then progress to a conclusion. That conclusion is invariably aimed at uncovering truth through the analysis of evidence, because, whether or not a given examination results in court action, digital forensics is by definition rooted in the application of science to the law[40].

LOADFAST

Taking into account this fundamental legal aspect of all forensic science, the designers of any digital forensics method, procedure, or process should begin with the final step: the legal objective. By starting with the final goal, an outcome-based methodology can be designed and implemented more efficiently and effectively, omitting unnecessary steps or considerations. For example, different steps are typically required during criminal investigations of physically seized digital evidence compared to military operations examining possible network intrusions. Similarly, a different standard may apply to corporate defensive measures regarding data theft than would be employed in internal administrative personnel actions. In any individual digital forensics scenario, a different legal burden of proof will apply based upon the targeted outcome.

Therefore, digital forensics frameworks are best crafted when they employ LOADFAST: a Legal Objective Approach to Digital Forensic Analytical Science and Techniques. At its core, LOADFAST is a methodology that begins by examining the final stage of a digital forensics investigation, and then progresses through the steps necessary to reach a desired legal objective. Consequently, the first phase of LOADFAST is legal objective analysis, followed by evidence identification and collection as the second

phase. In the third phase, examination and analysis of collected evidence are merged, followed by a fourth, final application phase whereby the results of the evidence analysis are applied in seeking the targeted legal outcome.

Phases of the LOADFAST Digital Forensics Methodology:

1. Legal Objective Analysis
2. Evidence Identification and Collection
3. Evidence Examination and Analysis
4. Application / Legal Result

At each stage of the LOADFAST approach, documentation, authentication, and integrity are core principles essential for the sound application of digital forensic science to the law. Although this outcome-based approach recognizes the unique nature of each individual scenario, at its core LOADFAST seeks to ensure the forensic soundness of digital evidence. Therefore, documentation is critically necessary during each phase in order to provide forensically-sound evidence with a record of its origination and subsequent processing. For example, real-time documentation of the chain of custody for all digital evidence will help forestall arguments by other parties that the evidence was changed, replaced, contaminated, misidentified, or otherwise improperly handled. LOADFAST recognizes that effective documentation supports the authentication and integrity of digital evidence when combined with four key considerations: an absence of changes to evidence made by investigators; an industry-standard level of competency for examiners; an independently verifiable audit trail; and effective managerial oversight[41]. Ultimately, it is the consistent application of documentation, authentication, and integrity to the digital forensic evidence identified, collected, examined, and analyzed under LOADFAST that leads to successful, targeted legal results.

Conclusion

LOADFAST is not intended as a procedure, checklist, guide, or other step-by-step method for digital forensics. Instead, LOADFAST is an overarching digital forensics methodology created to assist practitioners, researchers, theorists, students, and juries who are striving for consistent, verifiable, and scientifically-sound outcomes. By beginning with – and focusing on – the unique legal objective of any given digital forensics scenario, this methodology emphasizes an outcome-based approach when determining subsequent necessary steps. Through such reverse-planning, core principles governing the proper steps for handling digital evidence can be applied in a flexible, efficient, yet consistent manner, even in the face of legal or technological change. As new digital forensics methods continue to grow within the dynamic information technology landscape, their successful implementation of such goal-oriented design will ensure not only their longevity, but immediate utility – enabling them to LOADFAST.

Alex Rzasa is a public-sector attorney and Certified Information Systems Security Professional whose foremost interest is law enforcement cybersecurity. During prior private-sector practice, he zealously defended the interests of Maryland non-profit organizations and businesses, both by litigating and by helping clients create forward-thinking risk management strategies. Alex has applied his technical and legal knowledge both during operational IT contract work as well as at the Maryland General Assembly, where he drafted bipartisan legislation, forged policy research into analysis, and staffed technology, business, and economic workgroups. Alex earned a B.S. in Biological Sciences from the University of Maryland, College Park, and conducted neuroscience research as a Howard Hughes Medical Institute Research Fellow. Alex holds a J.D. with Honors from the University of Maryland School of Law, and served as an associate editor of the Maryland Law Review. The statements, views, and opinions expressed in his article are solely his own and do not convey or imply the endorsement of any other individual or organization.

1. National Institute for Standards and Technology (NIST), Guide to Integrating Forensic Techniques into Incident Response (Special Publication 800-86) (Gaithersburg, MD: Department of Commerce, 2006), https://doi.org/10.6028/NIST.SP.800-86.
2. Ibid.
3. Irons, Alastair; Lallie, Harjinder S. 2014. "Digital Forensics to Intelligent Forensics." Future Internet 6, no. 3: 584-596. https://doi.org/10.3390/fi6030584.
4. Yunus Yusoff, Roslan Ismail, and Zainuddin Hassan, "Common Phases of Computer Forensics Investigation Models," International Journal of Computer Science & Information Technology (IJCSIT) 3, no. 3 (June 2011): 17-31. https://doi.org/10.5121/ijcsit.2011.3302.
5. Mark Pollitt, "Computer Forensics: An Approach to Evidence in Cyberspace," Proceedings from the National Information Systems Security Conference 2 (1995): 487-491, http://digitalevidencepro.com/Resources/Approach.pdf.
6. Emmanuel S. Pilli, R. C. Joshi, and Rajdeep Niyogi, "Network Forensic Frameworks: Survey and Research Challenges," The International Journal of Digital Forensics & Incident Response 7, no. 1-2 (October 2010): 14-27, https://doi.org/10.1016/j.diin.2010.02.003.
7. NIST.
8. Mark Reith, Clint Carr, and Gregg Gunsch, "An Examination of Digital Forensic Models," International Journal of Digital Evidence 1, no. 3 (Fall 2002), https://utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf.
9. Jason Sachowski, Implementing Digital Forensic Readiness: From Reactive to Proactive Process (Cambridge, MA: Syngress, 2016). Retrieved from http://library.books24x7.com.cobalt.champlain.edu/.
10. Irons and Lallie.
11. Sundresan Perumal, "Digital Forensic Model Based On Malaysian Investigation Process," IJCSNS International Journal of Computer Science and Network Security 9, no. 8 (August 2009): 38-44, http://paper.ijcsns.org/07_book/200908/20090805.pdf.
12. Xiaoyu Du, Nhien-An Le-Khac, and Mark Scanlon, "Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service," Proceedings from the European Conference on Information Warfare and Security, 2017, https://search-proquest-com.cobalt.champlain.edu/central/docview/1966799146/fulltext.
13. Yusoff, Ismail, and Hassan.
14. Du, Le-Khac, and Scanlon.
15. NIST.
16. Irons and Lallie.
17. Khuram Mushtaque, Kamran Ahsan, and Ahmer Umer, "Digital Forensic Investigation Models: An Evolution Study," Journal of Information Systems and Technology Management 12, no. 2 (August 2015): 233-244, https://doi.org/10.4301/S1807-17752015000200003.
18. NIST.
19. Sachowski.
20. Ben Hitchcock, Nhien-An Le-Khac, and Mark Scanlon, "Tiered Forensic Methodology Model for Digital Field Triage by Nondigital Evidence Specialists," Digital Investigation 16 (March 29, 2016): S75-S85, https://doi.org/10.1016/j.diin.2016.01.010.
21. Venansius Baryamureeba and Florence Tushabe, "The Enhanced Digital Investigation Process Model," Proceedings of The Digital Forensic Research Workshop, May 27, 2004, https://dfrws.org/sites/default/files/session-files/paper-the_enhanced_digital_investigation_process_model.pdf.
22. Séamus Ciardhuáin, "An Extended Model of Cybercrime Investigations," International Journal of Digital Evidence 3, no. 1 (Summer 2004): 1-22, https://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf.
23. Hitchcock, Le-Khac, and Scanlon.
24. Jooyoung Lee and Sungyong Un, "Digital Forensics as a Service: A Case Study of Forensic Indexed Search," Proceedings from the 2012 International Conference on ICT Convergence, October 2012, https://doi.org/10.1109/ICTC.2012.6387185.
25. Michael Kohn, J. Eloff, and M. Olivier, "Framework for a Digital Forensic Investigation," Proceedings of the ISSA 2006 from Insight to Foresight Conference, 2006, https://pdfs.semanticscholar.org/ca35/dd6c4370b85c00708db55ec7fc882ea3ca7a.pdf.
26. Yusoff, Ismail, and Hassan.
27. Ciardhuáin.
28. Perumal.
29. Marcus Rogers et al., "Computer Forensics Field Triage Process Model," Journal of Digital Forensics, Security and Law 1, no. 2 (2006): 19-38, http://ojs.jdfsl.org/index.php/jdfsl/article/download/222/174.
30. NIST.
31. Kohn, Eloff, and Olivier.
32. Perumal.
33. Kohn, Eloff, and Olivier
34. Yusoff, Ismail, and Hassan.
35. Pollitt.
36. Kohn, Eloff, and Olivier.
37. Baryamureeba and Tushabe.
38. Pilli, Joshi, and Niyogi.
39. Yusoff, Ismail, and Hassan.
40. NIST.
41. Halil Ibrahim Bulbil, H. Guclu Yavuzcan, and Mesut Ozel, "Digital Forensics: An Analytical Crime Scene Procedure Model (ACSPM)," Forensic Science International 233, no. 1-3 (December 10, 2013): 244-56, https://doi.org/10.1016/j.forsciint.2013.09.007.