Designing Laboratory Forensics

Armel Lefebvre, Marco Spruit

Designing Laboratory Forensics

Armel Lefebvre[1][0000-0002-7428-1728] and Marco Spruit[1][0000-0002-9237-221X]

[1] Department of Information and Computing Sciences, Utrecht University, Princetonplein 5, 3584CC Utrecht, The Netherlands
{a.e.j.lefebvre,m.r.spruit}@uu.nl

Abstract. Recently, the topic of research data management (RDM) has emerged at the forefront of Open Science. Funders and publishers posit new expectations on data management planning and transparent reporting of research. At the same time, laboratories rely upon undocumented files to record data, process results and submit manuscripts which hinders repeatable and replicable management of experimental resources. In this study, we design a forensic process to reconstruct and evaluate data management practices in scientific laboratories. The process we design is named Laboratory Forensics (LF) as it combines digital forensic techniques and the systematic study of experimental data. We evaluate the effectiveness and usefulness of Laboratory Forensics with laboratory members and data managers. Our preliminary evaluation indicates that LF is a useful approach for assessing data management practices. However, LF needs further developments to be integrated into the information systems of scientific laboratories.

Keywords: Laboratory forensics, reproducibility, design science, open science

1 Introduction

Research data management (RDM) is a pillar of sound data preservation and dissemination practices as encouraged by Open Science [1]. However, RDM has not (yet) reached the maturity of data management in the industry in terms of research, governance, and technology [2]. These ad-hoc RDM practices result in digital resources being inconsistently preserved in laboratories, thereby increasing the complexity of finding and accessing research data by laboratory members and external parties (e.g., reader, reviewer, another laboratory). Therefore, the consistent documentation of research processes, preservation, and dissemination of the artifacts created is still a complex challenge [3].

It can be argued that finding experimental data on storage systems in a laboratory is similar to finding any evidence on any computer. As the original author of the files, a quick scan of the file hierarchy is enough to recover most of the files mostly needed for a given purpose. For instance, finding a file to send with an e-mail does not require an advanced process to locate, verify, and validate the files to send to a correspondent.

In contrast, when laboratory members are responsible for storing research data, it may be difficult for a third party to interpret the file hierarchy and identify relevant files [4]. In a scientific laboratory, it is not uncommon that files created by a laboratory

member need to be retrieved by others, for instance in the case a corresponding author has to respond to a request from another laboratory to access data [5]. At this point, the convenience of a simple file system becomes a significant limitation; the reason is that the understandability of the file structure largely depends on the efforts of the original authors to organize their folders and files.

Once experimental results have been published by a laboratory, the scientific community also benefits from available computational work. As noted by Peng [6], any attempt to reproduce published results require the availability of the original artifacts produced by the authors. In an era where computer technology has invaded scientific laboratories, few experimental works can avoid analytics software to study natural phenomena [7]. Still, the resulting publications often refer to a limited number of the original digital resources, if any [4]. Consequently, the reusability and replicability of published experiments remain challenging due to the lack of available original computational resources [8].

In this paper, we present the outcomes of a design science research (DSR) study focused on the design of a forensic approach which evaluates the functional repeatability and replicability of publications based on digital resources preserved on storage systems in a laboratory. The name of the approach is "Laboratory Forensics" as it combines digital forensic techniques on digital evidence. As further explained in Section 4, we aim at providing a set of artifacts that data managers and laboratory members can use to optimize the maximal availability of experimental evidence associated with scientific publications.

The main contribution of this work is a set of forensic techniques applicable to the extraction of experimental data from laboratories. Moreover, the outcomes of several forensic cases are evaluated with laboratory members and data managers in one university. By this, we show the feasibility and utility of laboratory forensics. The research question guiding this work is "How can digital forensics techniques be used to assess the reproducibility of scientific experiments?"

The paper is structured according to Hevner' s DSR model [9]. More information about DSR is given in Section 2. Briefly, the structure of the paper revolves around DSR rigor, relevance, and design cycles. In the literature review section (Section 3); we present digital forensics and experimental systems, both of interest for the rigor cycle [9]. Then, in the Design section, we describe the outcomes of the evaluation of the laboratory forensics approach on four cases (i.e., publications). Finally, we discuss future research and conclude in Section 7.

2 Design Science Research

Design science research (DSR) addresses organizational problems by designing useful IT artifacts such as software, methods, models, or design theories [10]. Hevner [9] describes a design process which consists of three cycles named the relevance, design, and, rigor cycles. The three-cycle DSR aims to ground artifact design in rigorous construction and evaluation methods. **Fig. 1** shows a typical three-cycle model adapted to the study presented in this paper.

In DSR, the rigor cycle draws upon a body of knowledge named "knowledge base." There, design scientists describe the theories, processes, and evidence used to justify and evaluate a designed artifact. We explain further the domain and methods which are included in the rigor cycle in the next section. Similarly, we elaborate on the relevance cycle in the domain relevance section, where we give more details about the context of data management in scientific laboratories and the evaluation criteria adopted in this study.

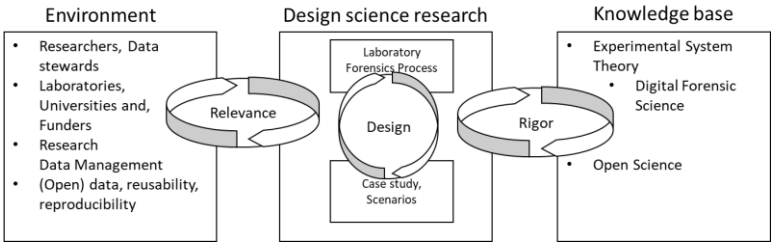

Fig. 1. The three cycles of a design science project, based on Hevner (2007)

3 Literature Review: The Rigor Cycle

In this section, we elaborate on two key aspects which drive our DSR study. First, we introduce digital forensics. Next, we briefly present a general view on the process and system of scientific experimentation.

3.1 Digital Forensics

Digital forensic science (DFS) has been defined as: "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations", p.16 [11]. In other words, DFS employs an ensemble of techniques to transform digital resources into evidence usable by third parties in a convincing way. DFS often relates to (cyber)criminal activities. Hence the outcomes of DFS investigations serve judiciary systems by reporting on digital evidence found on computers involved in criminal activities [12]. As we will explain in the design section, the constraints of reliability and rigorous reporting found in DF investigations form a strong basis of rigor to transfer DF techniques to scientific laboratories. The reason to investigate laboratories with DF techniques is twofold: one is reactive (i.e., something happened) and another proactive. The former refers to the investigation of the preserved evidence underlying scientific publications to reconstruct past experiments. The latter refers to digital forensics readiness, a field of DF which prepare information systems to deal with external threats [13]. In the context of Open Science, this translates to evaluating the readiness of data management to comply with the production, proper preservation, and, dissemination of high-quality scientific data [14].

Table 1. Forensic processes all converge towards a stable set of activities

Step	**Årnes**	**ENSFI**	**Casey**	**Candidate techniques** [11]
1	Identification	Identify	Preparation and Preservation	Audit Analysis, Case Management
2	Collection	Acquire	Extraction and Storage	Sampling, Data reduction
3	Examination	-	Examination and reporting	Filtering, Pattern matching
4	Analysis	Analysis	-	Statistical, Timeline
5	Presentation	Report	Sharing, correlating and distributing	Documentation, Impact statement

What can be seen from **Table 1** is that the DFS process described by Årnes [15] is more refined than the two others. The reason is that Årnes makes a distinction between the examination and analysis phases. This distinction is facilitating the decomposition of the forensic process into clearly defined steps. Also, this distinction refines the categorization of candidate techniques that are used at each stage of the process suggested by Palmer. Candidate techniques are methods from other disciplines that belong to an analysis step in digital forensics [11].

According to Årnes, a DF investigation starts with the identification of the data sources. The next step, i.e., collection, is the actual extraction of the evidence from existing storage systems. Collection requires an image of the disk of interest to the investigators as it would be impractical and even hazardous (e.g., unexpected modifications of files) to investigate the laboratory storage in use. Once the evidence is isolated from a computer device, the examination phase locates potential evidence. After the investigators have recovered potential evidence, the analysis phase takes place. The last step, presentation, is the translation of the findings into a format that can be understandable by the practitioners.

3.2 Laboratories and Experimental Artifacts

Scientific laboratories are standard organizational settings encountered in natural sciences such as Physics, Chemistry, and Biology [16, 17]. At their core, laboratories are organizations producing scientific knowledge by designing and operating experimental systems. Experimental systems are closed systems that enable the observation of natural phenomena with an ensemble of equipment, theory, and human intervention [18].

Moreover, experimental systems produce intermediate products from experimental events that are not part of the (communicated) output. These products are, for instance, exports from data analysis software, manuscript's drafts, quality controls, interactions between technicians and researchers (i.e., experimenters) and, computer scripts. The association for computing machinery (ACM) has highlighted the need for a better assessment of the quality and availability of digital artifacts underlying publications [19]. The ACM classifies artifacts in two categories: functional and reusable [19]. Functional

are artifacts that are consistent, documented, complete, and exercisable (i.e., runnable on a system).

4 Domain Relevance

4.1 Application Environment and Case Selection

In laboratories, scientists and technicians transform an object of study into data and data into scientific facts [20]. In science, facts are mainly communicated through scientific articles in journals which are presenting a curated version of experimental events [21]. Recently, journals developed new guidelines for more transparent reporting and enriched supplemental information [4]. Concurrently, public funding agencies encourage proper research data planning and management to foster high-quality data dissemination to mitigate the risks of poor RDM in laboratories. This trend presents several challenges for laboratories.

First, data management is not a priority, as it is often not rewarded by the academic system [22]. Second, as explained earlier, laboratories manipulate quite complex experimental processes to obtain results. As experimental processes rely on novel technology and people pushing forward the boundaries of a discipline, it is challenging to keep a record of the experimental evidence and activities produced during several years.

The case laboratory is a proteomics laboratory in the Netherlands that has produced over 400 publications in the last ten years. It makes this laboratory an ideal environment to design and evaluate our approach due to the complexity of the analyses done in the laboratory and a large number of authors (over 100) that worked or is currently working in the laboratory.

4.2 Evaluation Criteria

The criteria used to evaluate the outcomes of our LF approach are effectiveness and usefulness. First, we discussed the forensic results with two laboratory members, one experienced post-doc, acting as a data manager in the laboratory, and one a Ph.D. student who is the authors of one of the investigated publications. In addition, the outcomes of one forensic case were presented to 20 participants present at an RDM community event in February 2019. The participants were data managers, senior members of a data governance board, and members of RDM services at the University. Hence, both researchers and data managers could comment on the preliminary outcomes of the laboratory forensics approach presented in this paper.

The forensic cases are all publications originating from the investigated laboratory. The cases, i.e., publications, are selected primarily on the locality of the resources and their year of publication. For this study, we did not include any publication with multiple affiliations to limit the spreading of the files in separate laboratories. The publications are recent: CASE A and CASE C are from 2017, CASE B from 2018 and, CASE D from 2019. The reason is that the storage systems have been adapted recently, making

the retrieval of older files an extra challenge due to their relocation which influenced critical meta-data such as date of creation to a large extent.

5 Design Iterations

The LF process, see **Fig. 2**, is designed by integrating digital forensic activities shown in **Table 1** with evidence typically found in experimental science. The general idea is to merge meta-data collected from a file system in a laboratory (e.g., file names, date of creation, and date of modification) to software, methods and external sources found in the corresponding scientific article.

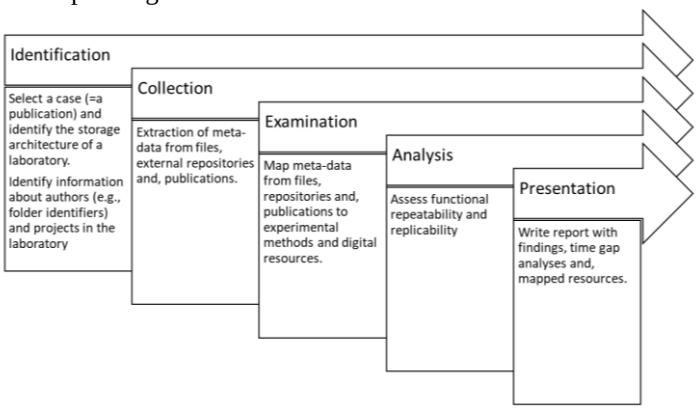

Fig. 2. An overview of the laboratory forensics process

To design our laboratory forensics approach, we first started with one publication, hereunder CASE A. The first design iteration was focused on adapting digital forensic techniques to the material available in on storage systems and their specific nature. The fact that (experimental) resources might be domain-specific made it necessary to redefine digital forensic activities which are increasing the likelihood of locating relevant material. **Fig. 2** shows the current iteration of the laboratory forensic process.

Table 2. The main activities of the laboratory forensics process

	Activity	Sub-activity	Example outcomes of CASE A
Identification	*Screen experimental report*	Identify laboratory employees	There are two authors in the author list and three laboratory members listed in the acknowledgment section.
		Collect information about the editorial process and deposited data	The paper was published in June 2017. It was received by the journal three months earlier, in March 2017. One repository is used to deposit raw data.
	Screen laboratory	Collect administrative data about current and former employees	One author is a principal investigator; two are postdocs. One member is a technician. One member with unknown status.

		Determine storage systems architecture	There are several shared volumes used by the laboratory members. The data is shared between raw, users, and projects volumes.
Collection	*Extract resources*	Extract experimental methods	There are two types of analyses reported in the paper, each with their own software and instrumentation. In CASE A, those are HDX-MS analysis and MS-MS analysis.
		Extract experimental resources	In the publication of CASE A, we extracted: Waters nano-Acquity UPLC system,[…], Swiss-Model, Phyre2 server, […] as a list of instruments and software.
		Extract external repositories and supplemental information	In CASE A, files have been deposited on PRIDE a digital repository, and an access number is present in the additional information.
	Make snapshots	Perform (targeted) snapshots of disk volumes	Select the user and project folders belonging to the laboratory members involved in the publication. Make a snapshot. For instance, in PowerShell (Windows) with the commands Get-ChildItem and Export-CSV.
Examination	*Process snapshots*	Consolidate snapshots	Merge user and project folders in one (tabular) data sets.
		Reduce noise	Duplicates and system files are deleted from the consolidated snapshot.
	Construct Annotated Experimental Resources Table (AERT)	Extract experimental methods	Determining what qualifies as an experimental method depends on the context of the analysis.
		Link experimental resources to methods	The software is extracted for each method mentioning the use of the software.
		Link laboratory instruments to methods	For a method, each instrument used can generate output with specific extensions (such as .RAW files in proteomics).
Analysis	*Map file paths*	Map files to AERT elements	File system meta-data might be inaccurate. Hence, cross-checking with elements in the AERT table is crucial not to include irrelevant files
	Filter file paths	Filter file paths referring to a publication	Not all files in a folder might belong to the analyzed publication; additional filtering is needed to exclude unnecessary files.
	Estimate functional repeatability and replicability	Estimate Method coverage	An estimation of the number of methods reported in the publication that are covered by evidence left on the storage.
		Estimate Software coverage	An indication of the number of software resources that are successfully identified from reading the file paths.
		Estimate Instrument coverage	An indication of the number of laboratory instruments that are identified by the investigator.
Presentation	*Report findings*	Report file mappings and their confidence	We included the folders of the first and last author in our analysis and reported the folders used during the analysis.
		Report functional repeatability	The extent to which preserved files are consistent, complete, and not fragmented.

		Report functional replicability	The extent to which disseminated files are consistent, complete, and not fragmented.
		Evaluate report with laboratory member(s)	We evaluated the report with one domain expert (laboratory member).

5.1 Laboratory Forensics in Action

A major challenge encountered during the investigation of CASE A was the low confidence that the files retrieved were related to the publication as much more (digital) material was generated by the instruments in the laboratory than necessary for the publication. This fact made the Annotated Experimental Resource Table (AERT) useful to guarantee that the files retrieved remain consistent with the resources reported in the investigated publication. The AERT is a spreadsheet containing all the methods described in the corresponding articles, the software and laboratory instruments used, and external resources such as an online database used by the experimenters. The AERT is helpful for systematic mapping of files and reported resources and excludes irrelevant material. We note that this mapping requires that LF investigators possess in-depth knowledge of storage systems and domain-specific knowledge (here in proteomics).

The goal of the LF approach is to present to research a report on the state of the storage in terms of reproducibility. To evaluate the functional repeatability and replicability, the following classification indicating the degree to which the preserved evidence corresponds to the requirements of completeness and consistency of the artifacts as described by the Association for Computing Machinery (ACM) [19]. The classification shown in **Table 3**, i.e., low, medium, high repeatability/replicability is diverging from the ACM is two ways. First, functional artifacts are divided in terms of locality: repeatable is used for resources preserved in the laboratory, and replicable is used for resources disseminated in supplemental information and digital repositories. Second, in terms of degree (low, medium, high) to account for varying scenarios.

Table 3. Findings from the first iteration on one publication (CASE A)

	Outcomes	**CASE A**	**Comment**
Identification	Number of laboratory members	5	Each user folder of laboratory member has to be mapped and investigated.
	Number of external authors	2	Several authors from external research groups are listed. External authors do not have user folders. On the laboratory storage, authors are mentioned by name, identifier, or affiliations.
	Editorial process duration	From 29/03/2017 until 28/06/2017	Filter project folders that were updated (i.e., modified date) at the time of submission.
Collec-	Number of methods*	4	Four method subsections are referring to computational work or laboratory instruments manipulated with software.

	The number of software resources	10	There are ten software resources used (e.g., to preprocess and visualize data).
	Number of Instruments	5	Five laboratory instruments were used to generate raw data.
	Number of files (local/deposited)	3011 / 15	In total, the consolidated mappings contain 3011 files on the storage and 15 files in the external repository.
	Total file size	49.5 GB	The "weight" of digital evidence of the investigated publication is around 50 GB.
	Time delta **	1486 days	The first file included as experimental data was modified more than four years before the last file included.
Analysis	Corresponding software	5	Files corresponding to 5 software resources are located, which means five other software resources have no (explicit) traces left on the storage or online.
	Corresponding Instruments	4	One instrument could not be mapped to the digital evidence found.
Presentation	Functional Repeatability	MEDIUM	The evidence is complete and entirely consistent with the corresponding experimental report. However, files have not been aggregated in a project folder, which requires to investigate several folders across different folders to obtain the complete (computational) input.
	Functional Replicability	LOW	Only the necessary raw files of one method have been deposited. Direct replicability is therefore hindered by the absence of other artifacts which are necessary to replicate the results.
* Computational methods, ** based on file system meta-data, not the exact duration of experiments			

6 Evaluation of Laboratory Forensics Outcomes

We evaluated the usefulness of LF results with a member of the laboratory responsible for the storage infrastructure. We collected the impressions of our contact person after a short presentation of the forensic process and report of CASE A (see **Table 3**). The impressions formulated by the laboratory member indicate that our approach appears to be rigorous and convincing. The systematic classification of resources into instrument, methods, and software sheds new lights on the resources underlying a publication.

Next, the extent of the fragmentation of the files was not expected by our interviewee, which shows that the ability of an LF approach to gathering evidence beyond expected locations by users. Also, the communication of issues with a set of measurable indicators gives an overview of the strengths and weaknesses of data management for specific publications. A critical note was that the indicators and scoring method need further refinements and more transparency. For instance, the indicator of functional replicability should incorporate mandatory openness and non-mandatory openness. This distinction would help to distinguish scientific data dissemination imposed by publishers (mandatory) and self-motivated by researchers in the laboratory (non-mandatory).

Besides, we presented the outcomes of CASE A to the data management community meeting of our University in February 2019, attended by 20 participants. This presentation was meant to collect the impressions of people involved in data management services. There the main impressions of the participants are that although the approach is time-consuming, it seems worth to conduct such analyses to explain to researchers the importance of good data management practices. Even the fact that LF is challenging to accomplish is, by itself, a powerful example of problematic data management practices which data managers can use to engage with researchers about RDM practices. Further, to collect additional feedback about the effectiveness of the LF approach, we investigated three new cases to obtain better insights into alternative data management practices adopted by other laboratory members. The three additional cases are labeled case B, C, and D (see **Table 4**).

Table 4. Summary of the outcomes of additional cases

Outcome	**CASE B**	**CASE C**	**CASE D**
Size	1.2 GB	2.6 GB	136.9 GB
Number of Preserved / Deposited files	689 / 0	137 / 123	939 / 179
Corresponding software	2 / 8	1 / 5	2 / 6
Corresponding instruments	3 / 4	3 / 4	1 / 2
Functional repeatability	MEDIUM	MEDIUM	MEDIUM
Functional replicability	LOW	HIGH	MEDIUM

The second evaluation was driven by the question of whether a forensic analysis of a storage system in a laboratory retrieves more relevant evidence than laboratory members when they are asked for searching underlying evidence publications. To achieve that, we asked two laboratory members to collect data underlying a publication used in one of the four investigated cases. More, we asked the laboratory members, hereafter participants, to elaborate on their search strategy and judge the extent, according to them, of the repeatability and replicability of the article they received.

The participants reported located files in a word document or during a live demonstration. Their outcomes are consistent with LF assessment, which showed that relevant files are all preserved but fragmented on the storage (hence medium repeatability). Also, the participants expressed their difficulties in locating legacy data or data created by another laboratory member in the past. In that case, we found that the presence of a reference list of files created by the forensic investigation is essential to evaluate whether the participants retrieved the complete list of files or evidence was still not located.

7 Discussion and Conclusion

Throughout this study, we answered the following question: “How can digital forensics techniques be used to assess the reproducibility of scientific experiments?” A design science approach has delivered preliminary artifacts and evidence that laboratory forensics (LF) is a useful approach for evaluating storage systems in laboratories. Despite

this, LF suffers from significant limitations in its current state. One limitation is that the LF process is yet to be further evaluated on a number of forensic cases in different environments to increase the rigor and reliability of LF investigations. These limitations are mainly due to the nature of reconstructing events from digital data [23] and the complicated extraction of experimental resources from publications. Moreover, access to storage systems in laboratories is needed, which might posit some additional challenges related to the privacy of the users. Despite the limitations of the current LF approach, LF has unique strengths compared to approaches for RDM such as post-publication curation of research data [3].

First, LF attempts to locate data despite reporting gaps and unavailable resources, unlike other studies relying on published material exclusively [24]. Collecting evidence from storage systems allows going beyond the written account of the events that occurred in a laboratory.

Second, an LF investigation actively seeks to reconstruct experiments to accurately report on which experimental resources are used, by whom and locate the underlying materials. This can serve as input for reproducibility studies, were retracing the full life cycle of scientific discoveries is a prerequisite for understanding all steps taken in an experiment to guarantee its reproducibility [25].

Last, the extraction of structured data about experimental methods, resources, and data together with evidence on storage systems might be of high value for designing ontologies representing a particular field of study [26] with a higher ability to manage the artifacts in use in laboratories and guarantee reproducible storage patterns.

To conclude, Laboratory Forensics demands further development, evaluation, automation, and tooling to become readily available for scientists and data managers. Hitherto, we have been able to show that in daily practices (digital) experimental resources are not preserved in a functionally repeatable and replicable way in the investigated laboratory. In short, laboratory forensics support the development of rigorous assessment of data management issues related to laboratory work. In upcoming research, we will further investigate the synergy of laboratory forensics with research data management practices.

References

1. European Commission: Access to and preservation of scientific information in Europe. (2015). https://doi.org/10.2777/975917.
2. Lefebvre, A., Schermerhorn, E., Spruit, M.: How Research Data Management Can Contribute to Efficient and Reliable Science. (2018).
3. Bechhofer, S., et al..: Why linked data is not enough for scientists. Futur. Gener. Comput. Syst. 29, 599–611 (2013). https://doi.org/10.1016/J.FUTURE.2011.08.004.
4. Federer, L.M., Belter, C.W., Joubert, D.J., Livinski, A., Lu, Y.-L., Snyders, L.N., Thompson, H.: Data sharing in PLOS ONE: An analysis of Data Availability Statements. PLoS One. 13, e0194768 (2018). https://doi.org/10.1371/journal.pone.0194768.
5. Collberg, C., Proebsting, T.A.: Repeatability in computer systems research. Commun.

ACM. 59, 62–69 (2016). https://doi.org/10.1145/2812803.
6. Peng, R.D., Dominici, F., Zeger, S.L.: Reproducible epidemiologic research, (2006). https://doi.org/10.1093/aje/kwj093.
7. Stevens, H.: Life out of sequence: a data-driven history of bioinformatics. Univeristy of Chicago Press, Chicago, USA (2013). https://doi.org/10.1080/14636778.2015.1025127.
8. Ince, D.C., Hatton, L., Graham-Cumming, J.: The case for open computer programs. Nature. 482, 485–488 (2012). https://doi.org/10.1038/nature10836.
9. Hevner, A.R.: A Three Cycle View of Design Science Research. Scand. J. Inf. Syst. 19, 87–92 (2007). https://doi.org/http://aisel.aisnet.org/sjis/vol19/iss2/4.
10. Gregor, S., Hevner, A.R.: Positioning and Presenting Design Science for Maximum Impact. MIS Q. 37, 337–355 (2013). https://doi.org/10.2753/MIS0742-1222240302.
11. Palmer, G.: A Road Map for Digital Forensic Research. Proc. 2001 Digit. Forensics Res. Work. Conf. (2001). https://doi.org/10.1111/j.1365-2656.2005.01025.x.
12. Casey, E., Katz, G., Lewthwaite, J.: Honing digital forensic processes. Digit. Investig. 10, 138–147 (2013). https://doi.org/10.1016/j.diin.2013.07.002.
13. Rowlingson, R.: A Ten Step Process for Forensic Readiness. Int. J. Digit. Evid. . 2, (2004). https://doi.org/10.1162/NECO_a_00266.
14. Ayris, P., et al..: Towards a FAIR Internet of Data, Services and Things for Practicing Open Science. 3, 0 (2018). https://doi.org/10.2777/940154.
15. Årnes, A.: Digital Forensics. John Wiley & Sons (2017).
16. Franklin, A., Perovic, S.: Experiment in Physics. In: Zalta, E.N. (ed.) The Stanford Encyclopedia of Philosophy. Metaphysics Research Lab, Stanford University (2016).
17. Weber, M.: Experiment in Biology. In: Zalta, E.N. (ed.) The Stanford Encyclopedia of Philosophy. Metaphysics Research Lab, Stanford University (2018).
18. Radder, H.: Experimentation in the Natural Sciences. Presented at the (2012). https://doi.org/10.1007/978-94-007-4107-2_3.
19. ACM: Artifact Review and Badging, https://www.acm.org/publications/policies/artifact-review-badging.
20. Latour, B., Woolgar, S.: Laboratory life the construction of scientific facts. Princeton University Press, Princeton, NJ : (1986).
21. Borgman, C.L.: Data, disciplines, and scholarly publishing. In: Learned Publishing. pp. 29–38. John Wiley & Sons, Ltd (2008). https://doi.org/10.1087/095315108X254476.
22. Nosek, et al.: Promoting an open research culture, (2015). https://doi.org/10.1126/science.aab2374.
23. Mabey, M., Doupé, A., Zhao, Z., Ahn, G.-J.: Challenges, Opportunities and a Framework for Web Environment Forensics. Presented at the January 3 (2018). https://doi.org/10.1007/978-3-319-99277-8_2.
24. Federer, L.M., Belter, C.W., Joubert, D.J., Livinski, A., Lu, Y.-L., Snyders, L.N., Thompson, H.: Data sharing in PLOS ONE: An analysis of Data Availability Statements. PLoS One. 13, e0194768 (2018). https://doi.org/10.1371/journal.pone.0194768.
25. Huang, Y., Gottardo, R.: Comparability and reproducibility of biomedical data. Brief. Bioinform. 14, 391–401 (2013). https://doi.org/10.1093/bib/bbs078.
26. Hoehndorf, R., Dumontier, M., Gkoutos, G. V: Evaluation of research in biomedical ontologies. Brief. Bioinform. 14, 696–712 (2013). https://doi.org/10.1093/bib/bbs053.