Forensic Science International: Reports 1 (2019) 100003

Contents lists available at ScienceDirect

Forensic Science International: Reports

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

Short Communication

Raiders of the lost artefacts: Championing the need for digital forensics research

Graeme Horsman

School of Science, Engineering & Design, Teesside University, Middlesbrough, United Kingdom

ARTICLE INFO

Keywords:
Digital forensics
Digital artefact
Forensics
Research
Forensic science
Investigation

ABSTRACT

In digital forensics, the concept of a 'digital artefact' exists; coined here as '*a digital object containing data which may describe the past, present or future use or function of a piece of software, application or device for which it is attributable to*'. In almost all digital investigations, a practitioner will query any digital artefacts resident on any device subject to examination in order to establish the presence of potentially evidential information. Whilst on face value this task appears straightforward, in reality, the pace of change within technology can lead to a practitioner encountering many unknown or previously unseen artefacts with undocumented functionalities. This creates state of 'catch-up' in regards to investigatory techniques and knowledge as practitioners must seek to ascertain the relevance of such data through additional research and testing. Yet, the demands placed upon the role of the practitioner may prevent engagement in the testing and evaluation of new digital artefacts, leaving them reliant on the timely publication and dissemination of forensic research (whether academic, industry or vendor produced) as a support mechanism. Whilst digital artefact research has a clear applied value, the difficulty of measuring its impact means that it may not always be considered of worth by academic communities and their publication platforms. As a result, this work champions the need for 'digital artefact' research, calling for increased engagement in this form of research to support the forensic community.

1. Introduction

Almost all user interaction with digital operating systems, devices, and any software installed upon them results in the creation and/or modification of files containing both configuration settings and logs depicting usage. These files can be referred to as digital 'artefacts', and often form an important source of potentially evidential content in need of interpretation and extraction by those engaged with investigative casework in the field of digital forensics (DF). In almost all DF examinations, regardless of the device type subject to scrutiny, digital artefact information discloses part (or in some cases, all) of a device owner's behaviour whilst using their system; essential information needed for supporting the *post mortem* investigation of a criminal act where a digital device has been involved [1]. As a result, the reliance placed upon the ability to extract and interpret digital artefact data is great, where it remains paramount that the knowledge to obtain any evidential information present is available, accessible and that any subsequently undertaken processes yield accurate, reliable information.

The value of digital artefact research for the field of DF is clear; all published content has the potential to support past, current and future casework [2]. Where the function of a digital artefact has not yet been documented, industry practitioners are left with no choice but to undertake such work themselves in order to ascertain its value to a case in-hand. This is reiterated by Boucher and Le-Khac [3, p. 70]

> 'A computer forensic analyst first needs to have a proper understanding of the application artefacts. If existing documentation exists, the computer forensic analyst can use that as a starting point and ensure it applies to the version of application on the device they are analyzing. In absence of such documentation, the computer forensic analyst will have to invest time researching the application – where artefacts are stored, and sync features.' [3, p. 70]

Whilst digital artefact analysis and interpretation is a fundamental part of a DF practitioners role, they are often not best placed to generate, test and disseminate new (or thoroughly validate existing) digital artefact knowledge. Current DF field structures, obligations and budgetary limitations are challenging. Industry practitioners face large caseloads driven specifically in criminal spheres by tight Crown Prosecution Service in the United Kingdom (or equivalent jurisdictional structures) deadlines, leaving only minimal time for activities beyond the confines of any casework they are currently assigned to. Instead practitioners are often reliant on those with research responsibilities built into their working

E-mail address: g.horsman@tees.ac.uk (G. Horsman).

http://doi.org/10.1016/j.fsir.2019.100003
Received 12 April 2019Accepted 29 May 2019
Available online 10 June 2019

roles (most likely those involved in an academic or knowledge development capacity) to provide valid interpretations of digital artefacts which can then be deployed within a practical investigative scenario.

Whilst the academic environment could be considered a potential primary contributor of artefact research, arguably the typical methods of dissemination used by this industry (journals, conference platforms) have not always placed high value on this type of content. As with most academic research there remains a trade-off between the competing interests of the academic industry and that of the field which any work is aimed at. Publication venues may seek to prioritise those pieces of work which are likely to have a significant 'visible' and 'quantifiable' impact to their target discipline, attracting large citation counts and academic interest, with the work being a potential catalyst for future research outputs contributing to and developing a given topic. Whilst this approach is modelled upon improving both a discipline's baseline knowledge, and a publication venue's outward facing rankings, it does not always offer the greatest support to those fields who may seek benefit from standalone applied research, targeted exclusively at the industry practitioner, with a potentially narrow field of applicability.

Digital artefact research can be considered 'non-standard or non-traditional'; its impact is difficult to measure as current factors for evaluating research impact are academic focused. The DF field generally does not engage with academic platforms well and lacks the mechanisms to feedback into existing systems where a piece of research has offered notable applied value in any casework undertaken. Though digital artefact research may prove pivotal in solving one (or many) DF cases, the actual number will likely remain unknown due to lack of reporting (in some high-profile cases, media outlets may shed light on a subject). As a result, a quantification of any research's impact in DF is often unobtainable and this form of work is unlikely to attract large citation counts or trigger significant follow-on work. This is due to the fact that the target of such work is not additional academics who engage in the publication process, but those in industry who can take the knowledge provided and apply it to present and future case work they are involved in. In essence, anecdotally, DF artefact research impact is better measured in terms of 'cases contributed to' as opposed to citation counts. However, in reality such a measurement does not exist on a reliable large scale.

Any consensus that digital artefact research is not impactful is misleading. Such thinking is often based on values attributed to the published work (the journal impact factor where it is published etc.) which have been generated via arbitrary measures of worth designed for traditional academic works, which fail to capture the value of this applied form of research. Of further concern is the fact that these mechanisms which can be used to evaluate a publication can lead to digital artefact research being viewed unfavourably as a potential publishable piece of work. This view contravenes the fundamental purpose of undertaking research in the first instance; to support the development of knowledge within a given field in the most appropriate way. Arguably, research in the DF discipline can be seen to follow a small set of central core themes of work, which are surrounded by many singular topics which require digital artefact exploration and study. Digital artefact research is the product of an emerged, fast paced, technology driven field of forensic study where the targets of forensic analysis deviate massively, fluctuating over time, requiring the constant attention of those in a position to attribute meaning to such data [4]. This article champions the need for digital artefact research and published works as a means of supporting those involved in the legal and investigative processes of DF investigations, and issues a call to arms to encourage greater engagement and dissemination of such information.

2. The digital artefact

Whilst we must encourage digital artefact research, there is little wrote regarding the need for it, the challenges of undertaking the work or the form which it must take in order for its intended audience to obtain maximum benefit from it. In fact, even defining what a digital artefact is has caused the field of DF some trouble [5,6], an issue which aims to be addressed here, and therefore the following digital artefact definition is offered.

> *'A digital object containing data which may describe the past, present or future use or function of a piece of software, application or device for which it is attributable to'*

Following the suggested definition above, all digital files can be considered digital artefacts, but only a subset of artefacts within a given case will be forensically relevant to an investigation. Factors for determining applicability include suspected offence type and what can broadly be stated as associated artefact metadata; information which describes how the artefact has functioned on a system. Therefore almost all pieces of relevant digital evidence identified during an investigation will have originated from a digital artefact, highlighting the importance and need for this type of research. Even content found in unallocated portions of a device's storage media will have likely existed as a live digital artefact at some point prior to deletion and may have retained some or all of its structure and associated metadata. To demonstrate this point, Fig. 1 provides a simplistic overview of the origins of digital artefacts, which typically reside in one of two groups; 'primary' or 'secondary'. All primary digital artefacts originate from the founding operating system installed upon a device or any subsequently installed third party software/applications. In turn, the 'product' of any software (for example, documents produced from word processing software) also falls within this definition. Example primary artefact types include operating system configuration and installation files and installed software artefacts.

Secondary artefacts are those which are/were primary digital artefacts from an external system and have since been transferred onto the founding operating system via some form of interaction (automated or manual transfer via a form of removable media or interaction with a service etc.).

2.1. Levels of digital artefact

Whilst digital artefacts can be categorised as either 'primary' or 'secondary' in origin, there are also arguably four 'levels' of artefact within each category (shown in Fig. 2), each maintaining a different level of 'case-impact' and research challenge. Level one artefacts are digital operating system artefacts (DOSAs), created during an operating system install and any subsequent interaction; these arguably maintain the slowest rate of internal structural change [4]. Despite somewhat regular updates, core DOSAs may remain structural comparable for long periods

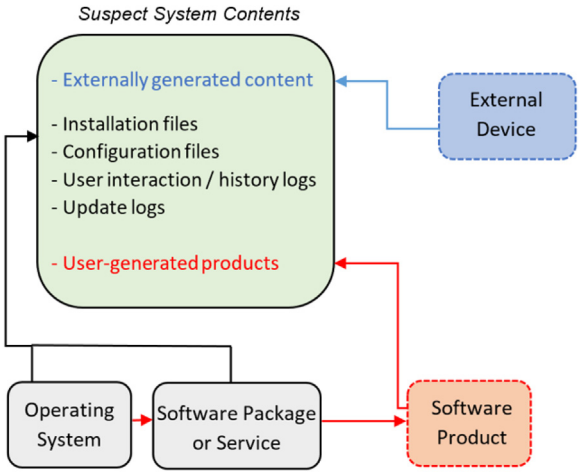

Fig. 1. Origins of digital artefacts.

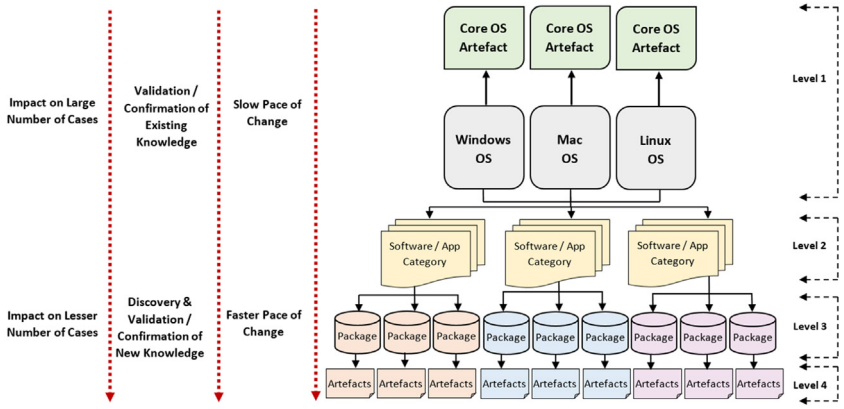

Fig. 2. A breakdown of the areas of DF artefact research.

of time, during the lifespan of the originating operating system or potentially across operating system major releases. If changes do occur to DOSAs, it may be that they are iterative as opposed to fundamental, meaning that research into DOSAs retains a longer lifespan of applicability to the DF practitioner. As a result, DOSA research is not just required to identify a specific DOSA and how it functions (which may already exist), but to also validate any existing knowledge in circulation and perceived understanding. Work documenting DOSAs is particularly pertinent as these artefacts often describe core user behaviour in a large number of cases (for example, Link Files, Prefetch etc.).

Level two focuses on categories of software and applications, for example, communication-based platforms, document processing platforms, cloud services etc. Here, change is somewhat quicker as new areas of technology and services are frequently introduced as the development of our digitally-focused society continues, bringing with them new data structures and protocols in need of investigation. Research at level two is often focuses on ascertaining functionality and the inner workings of a service and associated software. Where a target application is identified, level three and four artefact research will occur.

At level three is the development of new software and application packages within a defined category (for example, new communication software/applications). These create new data structures bespoke to a particular application type, leaving a digital footprint on an underlying operating system following any use. At level three, the pace of change increases as new software packages are produced on 'rapid release cycles' [4] within the competitive market of software development. Level 3 packages may cause a migration towards a specific data type requiring further and frequent research, seen now with the common implementation of SQLite in many application packages and the need to understand the forensic implications of this language.

Finally level four provides the greatest challenge in terms of developmental pace and focus here lies on the footprint left behind on a system by an application following specific types of usage. At this point, the type of data structures created by an application may be known (.sql etc.), but the challenge lies with establishing reliably those actions which cause data to be present on a device and what this means in a given scenario. When installed, a single application may generate hundreds of digital artefacts on an operating system, even before any user interaction has occurred. Once the application is in use, the amount of digital artefacts attributable to the software often grows as records of historical interactions and user configurations are stored. This alone requires a large amount of research to understand and reverse-engineer any artefact log data, however there is also the added challenge that the software itself may receive frequent updates. It remains a possibility that with every software update the internal structure and storage of associated artefacts changes, leaving previous interpretations of a digital artefact outdated and no longer wholly applicable. Even where change does not occur, this fact must be established and validated. The pace of change in technology provides a field-wide challenge, noted by Sommer [7, p. 118]

> 'The essential problem is that the speed of change is much faster than the rate at which an artefact with evidentiary potential can be identified and analysed, written up in a peer reviewed journal article, published and then made the subject of a reliable tool – which itself would then need to be validated.' [7, p. 118]

The speed of artefact developments across all four levels not only impacts the rate at which research can be produced, but also has an impact on the lifespan of applicability of such work, and this must be considered.

2.2. Artefact research lifespan

All research maintains a finite lifespan of applicability and as fundamental principles and practices develop, any designated piece of work may lose its continued importance within its subject discipline. While research may be field-defining and therefore a fundamental cornerstone from which future developments have been made, arguably there is a time when some research may no longer have a sustained impact on current developments. In the case of DF, artefact research tends to have a defined 'shelf-life', often considered to be the life of a particular application, software package or sustained use and presence of digital artefact, specifically if the research is applied in nature. Yet this view is arguably oversimplified, and in reality, DF artefact research goes through a series of stages of applicability (shown in Fig. 3).

First and perhaps most obvious, any digital artefact research remains relevant to the practitioner whilst the artefact which it targets remains in current use or circulation (its associated software is still marketed for operation). However, even after software ceases to be supported by its vendor, the software itself does not immediately stop being used; rather a gradual decrease in usage is more likely to be witnessed as migration to other platforms occur. As a result, even outdated software which remains in circulation may still be found in use on exhibits subject to DF investigation, expanding the length of applicability of any research. In addition, due to potential case backlogs [8,9], historical cases may contain outdated software usage due to the delay in an exhibit being examined. Finally, research maintains an 'informative/influential' phase once the artefact it has focused on is no longer apparent in DF investigations. Here, the work may still provide a baseline for informing those investigating the next generation of artefacts belonging to future software within the same type-category. Therefore in totality, the lifespan of applicability for digital artefact research can be years in length.

3. Overcoming the challenges

Whilst the case for encouraging the undertaking of digital artefact research has been made in the context of beneficiaries, it is also necessary to define those benefits gleaned from having researchers actively contributing to a body of this research type at a practical contribution

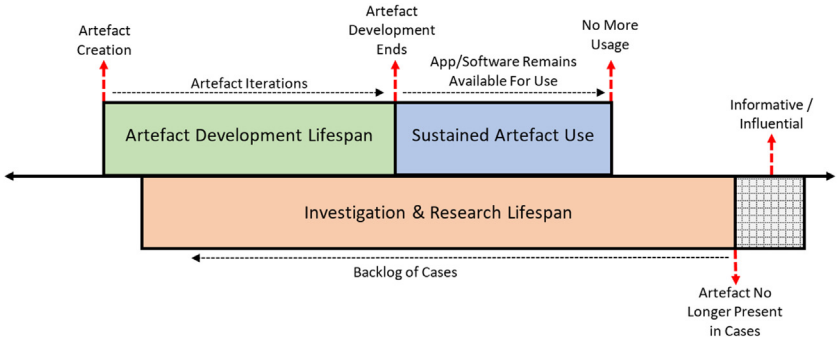

Fig. 3. The lifespan of artefact-based research.

level. Those engaging with artefact research are directly supporting practitioners in the following four problem areas:

The hunt for new artefacts: Through the active encouragement of those seeking and documenting digital artefacts, we increase the potential to discover new content which has not yet had its potential applicability to a DF investigation explored. Any work regarding artefacts which describe user behaviour is welcomed within the DF field as it directly supports the practitioner during their process of reconstruction system interactions. Where artefacts previously unknown to a practitioner and potentially the DF field are disclosed through new research, a practitioners' ability to carry out a comprehensive digital investigations is increased.
Validate 'the old': Whilst the discovery of '*the new*' maintains obvious benefits, artefact research must also consider contributions which validate existing artefact knowledge. All attempts to validate the functionality of digital artefacts through testing should be encouraged [10,11] as the field cannot simply rely on existing interpretations regarding artefact functionality because of such information being commonly accepted in previous times. Instead, hypotheses and knowledge must be regularly tested and existing knowledge re-validated in order to ensure it maintains its applicability and reliability. Validation in DF is a moving target, and work must match pace the technological change if the field is to uphold an acceptable level of forensic contribution to criminal investigations. Studies which scrutinise the work of others should be welcomed as a way of improving the reliability of any available knowledge sources, seen with the peer review mechanism promoted with the DFIR Review [12] scheme.
Functionality and interpretation (both new & old): An important aspect of research lies with determining the correct and complete functionality of an artefact. As noted above, this is a requirement of both new and known artefacts and includes ensuring findings have been correctly interpreted, that the impact of any findings have been thoroughly assessed along and the limitations of the research stated. This includes the testing of any competing hypotheses [13] and prevents any research from being incorrectly applied to an investigation.
Prevent practitioner misinterpretation: It is key to state that testing artefact functionality is important, yet not everyone is arguably good at it, or has the means to carry out this work [14]. Providing artefact research is carried out correctly, the product of such work can help to prevent the misinterpretation of an artefact's functionality and relevance [15]. Where the functionality and interpretation is established, those who have access to this content are able to contextualise the information and apply it to any cases where the research applies. This prevents those who may be relying on hearsay interpretations of data which are inaccurate or outdated, or content which documents incorrect findings through non-exhaustive testing.

For digital artefact research to tackle the aforementioned problem areas, it must contain designated information in order to meet the needs of the practitioner. In this respect, there are expectations placed upon the content of this form of work.

3.1. Expectation of research

For artefact research to be of value to the DF community, a number of core attributes must be present within the works, highlighted previously by Horsman [15,11], and summarised as follows:

Documented structure: A mapped internal structure of any digital artefact is compulsory. This allows practitioners to understand what content is in the artefact, how it is structured and if no current tool provides automated parsing for it, the potential for manual metadata extraction is supported. Further, those who may have the ability to produce an automated parsing approach for analysing the artefact are provided with a blue print of the artefact structure, aiding this process. A key goal of artefact research is to increase the conversion rate between knowledge discovery and tool production, making the application of such knowledge more viable in real-world investigative scenarios.
Metadata contents: Any internal artefact metadata of the artefact must be recorded including any data field structure and context. Any formatting or data conversion requirements should be stated and demonstrated, providing transparency in the testing and interpretation process.
Version control information: The version of the software/application associated with the artefact subject to the research must be noted. This provides a scope of applicability and reliability to the work and defines both the boundaries of usage and when future validation of any findings is required following any further software/application version iterations. In turn, the timing of the research should be recorded so that incremental developments to the work may be identifiable or if any subsequent work identifies any issues with the previous interpretations and findings.
Artefact scope: It is important that any work can address the research question of 'what can the artefact can tell the examiner?'. Whilst it is useful to establish what an artefact holds, research must also address why it holds such data and in what circumstances or set of actions causes this data occur. In that sense, meaning must be applied to the functionality of the artefact so that it is utilised in the correct evidential contexts. Once the scope of an artefact has been correctly defined, the chance of the artefact contents being misinterpreted is reduced.
Artefact constraints: In converse to an artefact's scope, constraints of applicability also need to be addressed, answering the question 'what does the artefact not mean'. In doing so, as above, the risk of practitioner misinterpretation is reduced.
Methodology and testing: Fully transparency is required with regards to any test methodology implemented as part of the research. This allows thorough peer scrutiny of the work and any issues to be highlighted and addressed, preventing the sharing of 'bad knowledge' [10].
Test Data: The disclosure of test data and test artefacts allows future validation of the work and for any weaknesses in the findings to be established. It also supports the identification of any artefact changes in future works.

4. Moving forward

There is a need to carry out and disseminate digital artefact research in support of the DF industry, as those contributing to the existing body of digital artefact knowledge are helping to maintain and improve the standard of current and future DF investigations. A primary goal lies with encouraging those with the skills and ability to continue to engage and produce this type of work, where the value of this content must be appreciated not only by industry, but also within academic environments which are in a strong position to produce this content. With recognition comes the need for sustainability, and the creation of initiatives to keep producing outputs. Some inroads have been made with DFIR Review [12], Magnet's [16] Artefact Exchange and the Artefact Genome Project [6] but engagement will always remain an issue. One of the challenges is encouraging the sharing of information, preventing the hoarding of content, in line with what has been termed 'the silo mentality' [17].

Consideration must also be given to a suitable venue for distribution of the research, one which practitioners can use in confidence that available content is accurate, having been rigourously scrutinised. It is key to ensure that any research is accessible, making open access or similar initiatives beneficial for those in industry who typically do not maintain subscriptions to academic journals. Such platforms must address a trade-off between time-to-distribution and the need to thoroughly validate any contribution. Whilst a platform should ensure all submissions receive a complete review in order to minimise any chance of sharing erroneous knowledge, the review and distribution of content must be prompt, making the time from submission to publication and accessibility as small as possible.

Moving forward, we must make sure that digital artefact research is aligned with the needs of the DF field and the mechanisms needed to for those carrying out this work are available allowing work to be of maximum benefit. To some extent this requires great communication and collaboration between academia and industry to ensure that the needs of both are met in regards to producing this type of research.

Conflict of interest

None declared.

References

[1] M. Olivier, Digital forensic science: a manifesto, (South Afr. Comput. J. 28 (2) (2016) 46–49.
[2] K.M. Ovens, G. Morison, Forensic analysis of Kik messenger on iOS devices, (Digit. Invest. 17 (2016) 40–52.
[3] J. Boucher, N.A. Le-Khac, Forensic framework to identify local vs synced artefacts, (Digit. Invest. 24 (2018) S68–S75.
[4] A. Williams, J.P. Cassella, P.D. Maskell (Eds.), Forensic Science Education and Training: A Tool-kit for Lecturers and Practitioner Trainers, John Wiley & Sons, 2017.
[5] V.S. Harichandran, D. Walnycky, I. Baggili, F. Breitinger, CuFA: a more formal definition for digital forensic artifacts, (Digit. Invest. 18 (2016) S125–S137.
[6] University of New Haven, Artifact Genome Project, (2019) Available at: https://agp.newhaven.edu/about/start/ (accessed 06.04.19).
[7] P. Sommer, Accrediting digital forensics: what are the choices? (Digit. Invest. 25 (2018) 116–120.
[8] M. Scanlon, Battling the digital forensic backlog through data deduplication, Sixth International Conference on Innovative Computing Technology (INTECH), IEEE, August, 2016, pp. 10–14.
[9] D. Quick, K.K.R. Choo, Big Digital Forensic Data, Vol. 1: Data Reduction Framework and Selective Imaging, Springer, 2018.
[10] G. Horsman, Framework for Reliable Experimental Design (FRED): a research framework to ensure the dependable interpretation of digital data for digital forensics, (Comput. Secur. 73 (2018) 294–306.
[11] G. Horsman, Formalising investigative decision making in digital forensics: proposing the Digital Evidence Reporting and Decision Support (DERDS) framework, (Digit. Invest. 28 (2019) 146–151.
[12] DFIR Review, DFIR Review, (2019) Available at: https://www.dfrws.org/dfir-review (accessed 06.04.19).
[13] E. Casey, Clearly conveying digital forensic results, (Digit. Invest. 24 (2018) 1–3.
[14] G. Horsman, Tool testing and reliability issues in the field of digital forensics, (Digit. Invest. 28 (2019) 163–175.
[15] G. Horsman, "I couldn't find it your honour, it mustn't be there!" - tool errors, tool limitations and user error in digital forensics, (Sci. Justice 58 (6) (2018) 433–440.
[16] Magnet, Magnet Artifact Exchange, (2019) Available at: https://www.magnetforensics.com/artifact-exchange/ (accessed 06.04.19).
[17] M.K. Rogers, K. Seigfried, The future of computer forensics: a needs analysis survey, (Comput. Secur. 23 (1) (2004) 12–16.