Available online at www.sciencedirect.com

ScienceDirect

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

Computer Law & Security Review

Legal and technical questions of file system reverse engineering

Radina Stoykova[a,b,*], *Rune Nordvik*[a,c], *Munnazzar Ahmed*, *Katrin Franke*[a], *Stefan Axelsson*[a,d], *Fergus Toolan*[c]

[a] *Norwegian University of Science and Technology, Gjøvik Norway*
[b] *University of Groningen Faculty of law, The Netherlands*
[c] *Norwegian Police University College, Oslo, Norway*
[d] *Stockholm University, Sweden*

ARTICLE INFO

Keywords:
Digital Forensics
Reverse Engineering
Criminal procedure
Intellectual Property
Government Vulnerability Disclosure

ABSTRACT

Reverse engineering of file systems is indispensable for tool testing, accurate evidence acquisition, and correct interpretation of data structures by law enforcement in criminal investigations. This position paper examines emerging techno-legal challenges from the practice of reverse engineering for law enforcement purposes. We demonstrate that this new context creates uncertainties about the legality of tools and methods used for evidence acquisition and the compliance of law enforcement with obligations to protect intellectual property and confidential information. Further identified are gaps between legal provisions and practice related to disclosure and peer-review of sensitive digital forensic methodology, trade secrets in investigations, and governmental vulnerability disclosure. It is demonstrated that reverse engineering of file systems is insufficiently addressed by legislators, which results in a lack of file system interpretation and validation information for law enforcement and their dependence on tools. Outlined are recommendations for further developments of digital forensic regulation.

1. Introduction

In the context of criminal investigation digital forensics is defined as "the use of scientifically derived and proven methods towards 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" [23]. Ergo, sufficient understanding of those digital sources and their underlying functionalities are crucial to capture, organize, and further interpret in order to derive inferences of user activities and digital evidence. File systems (FS) are one of the richest sources of user's activity, potentially keeping track of every file created, modified, copied or deleted during the entire life span of the device. Many file systems are proprietary, patented or a combination of open and closed source. Every update or improvement by the FS ven-

* Corresponding author.
E-mail addresses: adi.stoykova@gmail.com (R. Stoykova), rune.nordvik@phs.no (R. Nordvik), munnazzar@gmail.com (M. Ahmed), katrin.franke@ntnu.no (K. Franke), stefan.axelsson@ntnu.no (S. Axelsson), Fergus.Thomas.Toolan@phs.no (F. Toolan).

https://doi.org/10.1016/j.clsr.2022.105725

dor could result in inaccuracy of the digital forensic (DF) tools and an inability to interpret the FS structures by both tools and examiners. Therefore, reverse engineering (RE) is necessary for law enforcement agencies (LEA) to understand new FS systems and / or changes in existing data structures and also to determine tool limitations. While most of the efforts in reverse engineering are focused on code research, this paper examines the importance of reverse data engineering for data structures and organization analysis within file systems. This is an indispensable part of the forensic examination of file systems for evidence acquisition [43].

Reverse engineering of closed source file systems is necessary because the vendor documentation is either missing, treated as a trade secret, or is not sufficient for law enforcement needs.

1.1. *Research questions*

- Why LEAs need to perform Reverse Engineering and what are the current and future challenges of reverse engineering?
- How will reverse engineering of file systems impact the protection of intellectual property, personal data or security of vendors and third parties?
- How LEAs handle copyrighted material and security flaws in the underlying data structures?

These research questions are important as currently there is little information on how law enforcement handle copyrighted material. What are, if any, their obligations to report security flaws? How are methods and tools for investigation used and where in the current legal framework law enforcement are facing challenges? Can investigation methods be disclosed in trial without causing damage to different stake holders unrelated to the investigation?

1.2. *Definition and RE methods*

The use of reverse engineering techniques is permissible in order to determine the ideas and principles that underlie the functional elements of the software. This is usually done by examining its external inputs and outputs or testing the program/tool for errors and security flaws. Reverse engineering is defined as a "process of analyzing a subject system to identify the system's components and their interrelationships" [16, p. 15].The purpose of it is not replication of a program, but examination of its code, performance, or activity traces. [22]

This definition, however, requires a more detailed description of how reverse engineering is actually performed in respect to file systems. The file system is not software, but rather a set of logical structures, which are stored on virtual or physical storage and are largely independent of the operating system. The file system driver handles the storage and retrieval of files and directories. The file system is similar to a database management system rather than particular database content. Therefore, the provisions for reverse engineering of programs do not apply and, as a logical schema, and not as an instance of a database, file systems are not copyright protected *per se*. However, they can be protected as software-related inventions and are subject to trade secret, patents and licensing [51]. On the other hand, they are very valuable for both criminals and law enforcement, because file systems contain records with timestamps of files created or modified on a computer during its life span [14], thus they are a silent witness of most digital activities. Many vendors' efforts are dedicated to ensuring robust security of this data. As already observed, when digital investigators are dealing with new, unknown data structures in the file system, they need to reverse engineer or bypass security settings in order to gain access to the file system and to understand its structures. A known technique in mobile forensics is the use of chip off, but it is obsolete due to encryption [35], and therefore other techniques need to be exploited. This may expose copyrighted data or security flaws in systems.

In a digital forensic context, reverse engineering includes three main methods of analysis black-box testing, static-code analysis, and runtime analysis [1]. Commonly used are disassemblers, debuggers, file formats, system architectures, decompilers and low level code [1, p. 267] [4]

Black-box testing is based on sending known data or actions to a system (or part thereof), having the system perform its (perhaps undocumented) function, and then assessing the outcome by viewing the results [1, p. 267]. When performing file system reverse engineering we attempt to understand undocumented metadata structures. For example, creating a file is the input action (the known data), the file system driver uses hardware/software (the black box) to create the file, and the relevant outputs are the metadata structures and the file content as it is saved in the file system. File system metadata is any information that describes the files and directories in the file system [11]. Examples of metadata are file size, owner, timestamps, the file content on-disk location, etc.

Static-code analysis is used to scrutinize the executable code (machine code) or the source code[4] in order to understand the logic of the program function (what the function is meant to do) [1, p. 268]. We continue with the previous example; we are trying to identify and understand the logic of the program used by the driver to create the file. We use a special tool (disassembler) to convert object code into a more understandable language—assembly language—and we attempt to identify the driver's logic and functionality.

Runtime analysis is the examination of executable code (machine code) by observing the instructions as the program executes, normally using special software called debuggers, or tools that register which files have been accessed, or monitor network activity [4]. The debugger also converts the object code into more understandable assembly language.

There are several issues with RE techniques when used for forensic tasks in investigation. Black-box testing is a RE method which does not infringe intellectual property rights (IPRs), but requires experiments to be scientifically validated. The other methods may reveal IPR protected information since they are studying the source and object code of the FS driver functionality (looking inside the black box). Although existing decompilers can convert object code to source code

[4] The source code is not available in closed source file system, and it is arguable if assessing original source code can be considered reverse engineering

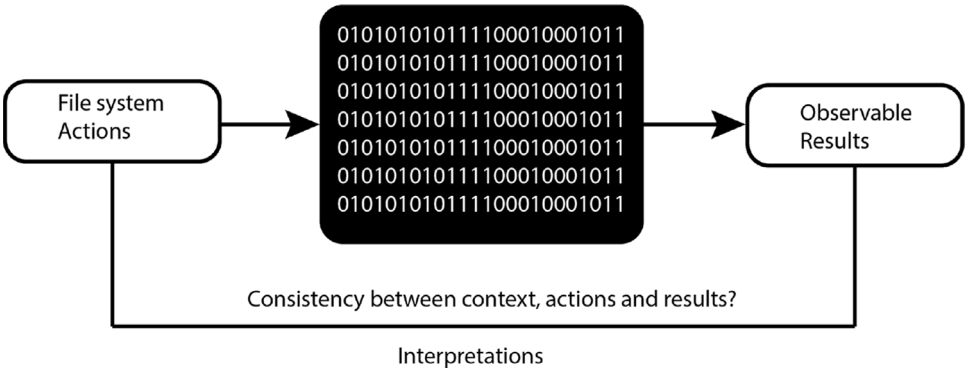

Fig. 1 – Black box testing.

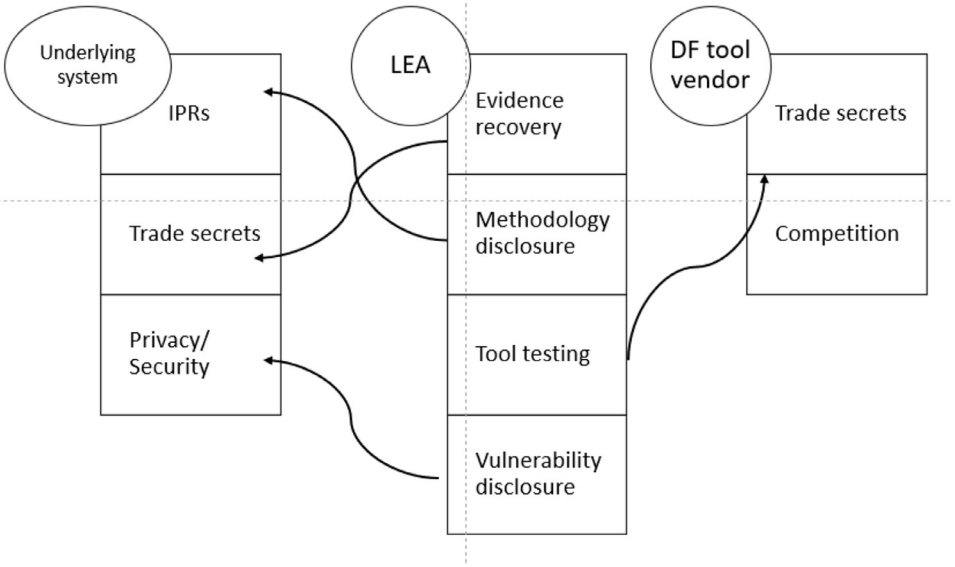

Fig. 2 – Overview of the impact of reverse engineering for law enforcement purposes.

they may not be accurate [28, p. 129] and do not interpret the intended purpose of structures for evidence purposes.

Most file systems used by Macintosh, Windows, etc. are proprietary and protected by copyright, patent or trade secret laws. Microsoft's exFAT file system is a patent-protected file system [72], while older file systems such as NTFS are copyrighted and mainly undocumented by Microsoft. When a file system is protected by patents, then the specifications need to be added to the patent application[5] [70] meaning that some metadata structures will be published by the vendor leading to a decreased need for reverse engineering. Unfortunately, even if parts of a file system are protected by patents, not all structures are documented. A file system may be updated after the patent application and therefore the specifications may not be correct or complete. These undocumented structures may be relevant to the criminal investigation and require reverse engineering. The documentation given by the FS vendor needs to be tested for its accuracy, which also requires reverse engineering.

1.3. *Organisation of this paper*

In Section 1 we have introduced the reader to reverse engineering of file systems, and the impact reverse engineering may have on revealing trade secrets, intellectual property rights, and security flaws. A brief description of the method used is given in Section 2. In Section 3 we provide the literature review of digital forensic studies in reverse engineering and legislative frameworks. Section 4 discusses the findings related to the research questions. In Section 5 we identify additional emerging challenges, while in Section 6 we describe the recommendations related to the research questions and further work.

2. Method and assumptions

This paper is a multidisciplinary literature review conducted by legal scholars, law-enforcement, and digital forensics spe-

[5] 35 U.S. Code §154, a-4: "A copy of the specification and drawing shall be annexed to the patent and be a part of such patent."

cialists, with the objective being to identify gaps between legal provisions and current digital forensic practices. The assumption is made that reverse engineering is a necessity in the described scenarios and many law enforcement agencies rely on the results of reverse engineering methods, which require legal evaluation. The interdisciplinary nature of the paper requires a level of abstraction of potential legal issues. Since both IPRs and criminal procedure are under national legislation, with limited international standardization, the paper doesn't examine concrete jurisdictions. Instead it aims at raising high-level, legal-technical problems.

3. Literature review

3.1. *Digital forensics research*

Sanger [64] describe that current Juris Doctor (JD) curricula do not contain education in forensic sciences, which they propose should be mandatory in legal education. The lawyers, judges, and prosecutors must have sufficient knowledge on scientific validity of digital forensic methodology and the reliability of the digital evidence. Otherwise, they will not be able to perform the legal evaluation of the evidence, or to decide which investigation methods or trade secrets could be disclosed publicly in trial and which need to be examined under non-disclosure agreements.

Twelve years ago Garfinkel [37] predicted that the lack of standards in the extraction of information from cell phones, video game consoles, telecommunications equipment, etc would become a major challenge. The techniques used to protect intellectual property make these systems more difficult to acquire and analyse. He describes that many law enforcement resources are used for reverse engineering without following a standard set of procedures. Le Khac et al. [49] describe vehicle forensics and address the challenge that obtaining proprietary information about the vehicle may be impossible due to intellectual property protection, and sharing information of discovered vulnerabilities can be used to compromise the safety of the vehicles. Further they describe tools, such as iVe [54], which are able to extract physical or logical data using the ODB II port (On-Board Diagnostic port) [75], but it is uncertain how this proprietary extraction is performed. They may use the infotainment system to gather the data, or they may analyse the QNX or VxWorks file systems. They also found that there was no forensic tool available to extract information from immobilizers or other electronic control units (ECUs), and they relied on using the third party diagnostic tool VCDS [62] to gather information from a 2012 VW Golf. Since it is necessary to turn on the car in order to use the VCDS tool to gather all information, important GPS location information is overwritten.

Currently, most cell phone reverse engineering is performed by DF researchers and/or commercial digital forensic tool providers. The DF practitioners in law enforcement depend on these digital forensic tools [36]. The detailed methodologies implemented are hidden as trade secrets within closed source tools. Adams [3] summarizes US case law to examine the legal issues which arise from digital forensic tool development. He argues that it is desirable for "forensic tools to be designed to avoid having them used in ways that exceed the scope of their authorization" considering their negative effects on privacy and security. Polanski [58] analysed whether reverse engineering is permissible under EU law. He posits that any computer program is protected as a literary work, and it is the high level source code and the object code that is protected. The graphical user interface and file formats can also be protected, but the functionality, ideas or principles of a program are not protected by copyright law. He also describes that observation of a legally acquired program in order to understand the ideas and principles utilized by the program is allowed, and that reverse engineering cannot be limited by a contract either.

3.2. *Comparison of legislative frameworks in relation to reverse engineering*

3.2.1. *EU vs US copyright law*

In the European Union, according to Art. 5 (3) of Directive 2009/24/EC (Software Directive) [31] "a person having a right to use a copy of a computer program shall be entitled, without the authorisation of the right-holder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlay any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do". In addition, European laws support interoperability between computer systems and software, and some proprietary software components could be reverse engineered in order to enable other or open-source services. This was common practice by the development of the NTFS driver for Linux [45, p. 16]. Also, interface specifications are considered not protected by copyright in Europe. Art. 6 of the Software Direcrive defines decompilation[6] as a legally-compliant practice "where reproduction of the code and translation of its form [...] are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs". However, the Directive does not address disassembling[7] as a separate issue.

In USA, software protection laws introduce some broad requirements on reverse engineering such as the need for authorisation (copy of the software must be legally obtained or the copyright owner must permit the reversing) and lawfulness (only according to the exemptions provided by law) [60]. In addition, the tools used must be legal and source code reproduction and further use of implementation details are prohibited.

The Digital Millenium Copyright act (DCMA) includes exception for lawfully authorised law enforcement, intelligence, and national security purposes, for making software interoperable, and for encryption and computer security research under certain conditions [60].

3.2.2. *Patent law*

A software patent does not protect source code, but rather the functionality embedded in it. Kumar and Kumar [48] de-

[6] The process of converting a binary program to readable high level source code.

[7] Similar to decompilation, but convert to an assembly code which is lower than the normal source code.

scribe that a governmental authority awards exclusive rights (patent) for a fixed number of years to the individual who first discloses the invention. The patent is an intellectual property right in exchange for full disclosure of the invention. Under the agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), signatory countries are obliged to make patents available for any technological invention. Important issues for software patents are where the boundary of what is patentable lies, and whether software patents discourage invention. They compare UK and US legislation and conclude that it is unclear what software categories are patentable. A patent emphasizing hardware rather than software is more likely to be patentable. When it comes to India and China software will need to be implemented in hardware or presented in material form in order to be considered patentable. The UK, India and China all require a technological application, while the US requires usefulness. The authors [48] describe that software is protected as works of literature, and patentable as a technical invention. Copyright protection does not protect ideas, while patents do. They are concerned that the monopoly effect of patents may block progress and new inventions. Moreover, technological inventions are often a combination of one or more patents and other non disclosed technologies, which may still require reverse engineering of the system.

3.2.3. *Trade secrets law*

European Directive 2016/943/EU [32] requires all countries to implement measures to protect trade secrets and to set obligations for law enforcement to protect confidential information during legal proceedings (Art. 9 in conjunction with Rec. 18).

By contrast, according to US Trade Secret Law, an individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that–(A) is made -(i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal." [71]

4. Discussion

4.1. *Technical challenges with reverse engineering in investigations*

Although the legal provisions for interoperability and testability of software generally allow for reverse engineering, laws in the US and Europe are broadly written and do not take existing methods into account, or sufficiently address new application of reverse engineering for digital forensics and evidence acquisition purposes. Further we argue that LEAs depend on system vendors and DF tool vendors. In order to overcome those dependencies LEAs must rely on reverse engineering. We argue, that current legislation does not reflect the full complexity of this new context, or the legality of different methods and tools used.

4.1.1. *Interpretation challenges*

Horsman argues that "tools for parsing of a file system may focus on displaying file and folder content to a user and inaccurately interpret file system metadata possibly due to insufficient testing" [44]. Reverse engineering of file systems is used to understand metadata structures, and can be used to:

- Discover malicious activity
- Understand and interpret the data structure
- Recover user data

Alternate Data Streams (ADS) in the NTFS file system are known to be exploited to hide malicious content. The technique of using tools that identify ADS have already been peer reviewed and published in the Digital Forensic community [10]. Even though not explicitly mentioned, since ADS was undocumented, the authors of tools supporting ADS had to initially perform reverse engineering or build on previous reverse engineering efforts.

Since file systems consist of metadata structures describing the file system and the files and directories it contains, previous research has tried to interpret these undocumented structures within closed source file systems by using reverse engineering [40,41].

4.1.2. *Peer review challenges*

There are no universally recognized standards for evaluating the reliability of digital evidence. However most countries have requirements for scientific validation of digital forensic findings. For example, the UK has complex reliability requirements, exclusionary rules, and follow ISO accreditation [27,66]. Others, such as Germany rely on formal accreditation and court-appointed experts [12]. In Norway, due to the early involvement of the court in the case, the judge has full discretion on the mandate and evaluation of the expert evidence where, for digital forensics, no formal requirements or quality controls are established [63]. The US Supreme Court formulated the Daubert standard[8] that requires the forensic theory or technique to be tested, peer-reviewed, generally accepted in the scientific community, and having known error rates. Some reverse engineering of file systems techniques and the techniques of using metadata structures to recover files are published and peer-reviewed digital forensic methodologies. [41,56,57] However, such RE techniques do not fully meet the Daubert standard for scientific validity in court since the RE methods are often not tested and no error rate is known.

In a similar vein, if LEA develop methodology to interpret file systems (in relation to a criminal case), that are unknown or unsupported by existing DF tools, it is a form of applied research and the methods used must be peer-reviewed in order to be validated and reused by others. Publishing of techniques in scientific journals is the preferred method to do

[8] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 1993. The Daubert criteria was further elaborated in General Electric Co. v. Joiner 522 U.S. 136 (1997), and Kumho Tire Co. v. Carmichaet 526 U.S. 137 (1999). Althought Daubert standard is jurisdiction-specific, it had a significant impact in the digital forensics domain and is considered a de facto standard.

so. However, public disclosure may create serious disadvantages. Firstly, criminals may misuse this information to break into systems, or to avoid prosecution by utilising anti-forensic techniques based on information found in these publications. LEA might need to protect their methods by keeping them confidential and reuse them in further investigations. If the LEA method describes weaknesses in the file system, vendors might update in order to prevent RE by others. Internal validation might lack impartiality or competence, while no validation can introduce inaccuracies in all investigations where the technique is subsequently used. Currently, there are no communication channels or independent bodies where applied research performed by LEA can be peer-reviewed for scientific validity and disseminated among LEAs without public disclosure.

4.1.3. *Method and tools challenges*

Understanding the inner workings of a closed source file system is a time consuming process for digital forensic research [67], and it is difficult to prove that the interpretation of the file system structures are complete and accurate. It should be stressed that the metadata structures identified from file system reverse engineering may not be exactly what exist on disk [14, p. 199]. In order to acquire digital evidence, LEAs must be able to test if the DF tool correctly interprets the file system, and in the case of errors and uncertainties to validate the results with reverse engineering techniques.

Numerous skills are required to perform reverse engineering of file systems including interpretation of hexadecimal and C structures, debugging, assembly, programming, knowledge of existing file system structure, performing reliable experiments, hypothesis testing, etc.

These limitations in the forensic tools and the lack of RE knowledge by the examiner could result in loss of evidence for the investigation. For instance, Microsoft's Resilient file system released with Windows 8 and Windows Server 2012 has a completely different storage engine than previous Microsoft file systems. It can manage vast amounts of data and has improved security and data integrity capabilities which reportedly limits the current forensic tools' ability to interpret it [56]. Apple implemented the new APFS file system in 2017, and at the time of release digital forensic tools had no support for APFS. The missing APFS support had a serious impact on criminal cases that included devices using the APFS file system, meaning many iOS and MacOS devices could not be investigated [41]. Current digital forensic tools do not support vehicle file systems such as QNX or VxWorks [49]. In the absence of protocols to track vendors' changes in system design, forensic examiners rely on reverse engineering or manual inspection of low-level processes in order to investigate the data, detect running malware, interpret underlying data structures for data recovery, or to create / improve forensic tools.

4.2. *Legal challenges with reverse engineering for law enforcement purposes*

Computer systems are a mixture of copyrights, patents, licenses, and freely accessible code. Reverse engineering of data structures is not regulated specifically for the purpose of digital evidence acquisition and analysis, but has implications with respect to intellectual property, trade secrets, system security, and data protection.

4.2.1. *Intellectual property challenges*

In the EU the source and object code of an original computer program are protected as literary work. [31, Art. 1] Software copyright is mostly restricted to direct reproduction of the source or object code. Art. 1 (2) of the Software directive must be interpreted that it does not provide protection in cases of non-literal infringements [55, ch 9 para 9.4]. Such infringements occur when the logic, structures or data formats of a software are reproduced. In this respect, the Court of Justice of the European union (CJEU) gave a landmark decision in the SAS case [17]. The court declared that logic, algorithms, programming languages and data formats are not protected by copyright. In a further judgement, the court also stated that under Art. 5 (1) of the Software Directive, the lawful purchaser of a program can decompile it in order to correct errors in its operations without the authorisation of the copyright holder [19]. Consequently, black-box testing does not impose a threat to intellectual property rights and trade secrets, because the forensic testing is performed without directly looking at source or object code. It is lawful and cannot be limited by a contractor licence agreement [58]. However, black-box RE might introduce inaccuracies and questions about the reliability of this method. For static-code and runtime analysis investigators must work with debuggers, decompilers, or disassemblers and use information from previous reverse engineering of the file system or similar open source work. Some of those RE methods may reveal IPR protected information since they study the source and object code of the FS driver functionality. Others may fall under the exemption of Art. 5 (3) the Software Directive as they aim to observe and study logical metadata structures and does not reproduce the source code.

Another possibility for law enforcement to lawfully perform reverse engineering is under the interoperability exemption. Art. 6 in conjunction with Rec. 15 of the Software Directive [31] permits the use of reverse engineering e.g. studying file systems in order to create interoperable DF tools or to validate the accuracy of existing ones. CJEU considered the refusal of Microsoft to provide sufficient interoperability information regarding its operating system a violation of competition and antitrust laws. The court held that Microsoft had a special responsibility to supply and authorize the use of interoperability information to others in order to achieve a high degree of interoperability that the circumstances required and not to hinder effective and undistorted competition in the Common Market [18]. Since then, Microsoft has published a substantial amount of information pertaining to protocols, APIs, etc. to enable the development of compatible software by third parties [53]. Moreover, the Software Directive limits contractual restrictions on reverse engineering to the extent decompiling is concerned [65]. The legal protection of interoperability is of relevance for developing and testing digital forensic tools by law enforcement because more information about closed source file system will become available to support development of alternative open source file system drivers. However, there is a difference between reverse engineering for interoperability and reverse engineering for investigative purposes since the former is focusing on creating a full implementa-

tion of the file system on an unsupported platform, while the latter is focusing on understanding the meaning of metadata structures mainly related to files. Arguably, information provided by vendors for interoperability is insufficient and does not meet the LEA's need for correct data interpretation. In the absence of legal provisions to compel software vendors to provide such information for law enforcement purposes, reverse engineering remains the only possible solution, although very burdensome and not always fully accurate.

In US perspective similar exceptions are found in copyright law. 17 U.S. Code §1201 (e) provides immunity for law enforcement authority who are lawfully authorized to circumvent technology means for copyright protection, including for the purpose of identifying and addressing security vulnerabilities and 17 U.S. Code §1201 (f) codifies an interoperability exemption [60]. However, a recent judgement in Oracle v. Google extended copyright protection to Java declaring code, which is considered an aberration of the global consensus for interoperability [34].

Even when reverse engineering for law enforcement is permissible under EU and US law, some questions remain unaddressed by the legislator e.g. law enforcement obligations in relation to disclosure of RE results to the defence, discovered sensitive or confidential data, or found security vulnerabilities in systems and their cross-jurisdictional effects. The legality of RE tools and methods or their impact on security of systems is largely unaddressed. In addition, some LEAs buy digital forensics tools from vendors who's responsibilities for reverse engineering are not clarified. As exemplified further, in most cases jurisdiction specific rules apply.

4.2.2. *Challenges with IPRs disclosure*

In most jurisdictions, a judge can issue a warrant for disclosure of copyright protected information for the purpose of criminal investigation. In the UK for example, the PACE production orders [42] allow the court to oblige an organisation to provide confidential content data (e.g. confidential files or e-mails) to law enforcement. The provision refers to information, which the organization has a duty to keep confidential, but it remains unclear if this includes security and copyrighted data, which the organisation has a right to keep confidential. Consequently, the right holder can limit the disclosure to the warrant's scope or challenge it in court. However, more commonly LEA can lawfully acquire the device (computer or mobile) proceed to a warrant and later on, during forensic analysis, establish the need of reverse engineering. The RE will be considered as digital evidence acquisition or analysis where no additional warrant will be necessary. In this case the right holder will not be able to protect their system, and it will be up to the LEA to follow general requirements for RE and to protect confidential information. Detailed documentation of the forensic methodology is not only important for its reliability validation but moreover for proving that the digital forensic examination was limited to the search warrant scope and did not violate privacy and data protection [3]. However, digital forensics methods are often poorly documented [43], while search warrants are broadly formulated and do not limit the scope of the digital investigation [69]. Problems with what is permissible after the device or electronic material is seized, and to what extent digital forensic techniques must be transparent are poorly addressed in the literature and in legislation. The aim of greater transparency in digital forensics must be combined with mitigation of the negative impact disclosure can have on trade secrets and system vendors' copyrights.

4.2.3. *Challenges with trade secrets disclosure*

Reverse engineering for investigation purposes might have further impact on trade secret protection. To exemplify the issues we discuss relevant legislation in Germany and the United States. Germany is an example of a European country that implemented the Trade secret Directive and regulates law enforcement activities in such context. According to current legislation, reverse engineering by LEA is considered unlawful, but a major legislative change was introduced recently. The published Draft Bill [38], in accordance with the Trade Secret Directive, states that reverse engineering is a permitted means for obtaining trade secrets when one of the following conditions is met: the product or object (i) has been made available to the public, or (ii) is lawfully in the possession of a party who is free from any legally valid duty of confidentiality. Thus, as long as the product or object has not been made publicly available, it remains possible to contractually prohibit reverse engineering to the extent permitted by law. This is contrary to the Software Directive as well as the German Copyright Act, which limit contractual restrictions on reverse engineering to the extent decompiling is concerned [65]. Reverse engineering (i.e. analysis and dismantling of products for the decoding of secrets) is now generally permissible according to the new regulation in Section 3 para. 1 no. 2 GeschGehG[9] - but still only within the restrictions of the laws against the unfair competition and the intellectual property laws [46]. A possible inadequacy of the system has emerged since, in criminal proceedings, the defence counsel has to be given access to files, but there is no explicit provision requiring them not to disclose the trade secrets contained therein [7]. The issues however, have been assessed by the German Supreme Court, which stated that the defence counsel can disclose to its client only the information that is indispensable for a proper defence [7].

Under US Trade Secret Law law enforcement are exempt from the protection of trade secrets. The Parties have the right to disclose in confidence trade secrets to Federal, State, and local government officials, or to an attorney, for the sole purpose of reporting or investigating a suspected violation of law. Due to the peculiarities of competition law proceedings in the US when compared to the European model, the discovery process permits a party to demand disclosure of relevant information and potential evidence from the other party. This includes information on copyrighted material or trade secrets that are relevant for litigation. However, a party from whom discovery is sought may move the court to issue a protective order requiring no public disclosure or to reveal only in a limited manner a trade secret [7]. Nothing in this Agreement is intended to conflict with 18 U.S.C.§1833(b) or create liability for disclosures of trade secrets that are expressly allowed by 18 U.S.C.

[9] German Act on the Protection of Trade Secrets (Gesetz zum Schutz von Geschäftsgeheimnissen vom 18. April 2019 (BGBl. I S. 466)).

§1833(b). Wexler [74] argues against trade secret privileges in criminal cases, because if information on how evidence has been gathered is excluded from the case, this could jeopardize the accused's right to a fair trial. The ambiguous regulation in the US, as Wexler argues, leaves an open question whether trade secret privileges apply to criminal cases.

4.2.4. *FS vendors' copyrights*

When investigating a criminal case the aim is to find enough relevant information, which may have evidentiary value, to define hypotheses and then to try to falsify them in order to find the most likely hypothesis [33,59]. If such information is unavailable because of intellectual property rights protection, then this may impact the accuracy of the hypothesis testing, and decrease the reliability of identifying the most likely hypothesis. This may impact the right to a fair trial, because relevant evidence can not be accessed. This is also why law enforcement is facing challenges with intellectual property protection of file system vendors and digital forensic tool vendors. Some of the file systems and underlying functionalities are proprietary. The file system driver, the manager, is the software responsible for all the file system activity which it performs when users create, update, delete, move, or copy files. This driver can be a mixture of propriety and open-source code, and could be changed completely due to increased storage and processing capabilities of new computer systems when the vendor updates the driver. Law enforcement does not have access to the low-level changes of each file system version, since vendors' keep this information secret in order to preserve the integrity and security of their products, but more importantly protect customers' data and other confidential information. The vendors' objective is always to improve performance and customer experience [40, p.7], which can cause inaccuracy in digital forensic tools parsing the file system. Therefore, vendors may be reluctant to cooperate with LEA. Reverse engineering by LEA might lawfully reproduce IPR-protected information and trade secrets but the further use of such information depends on the jurisdiction specific rules.

4.2.5. *DF-tool vendors' copyrights*

DF-tool vendors also rely on reverse engineering of FS and protect their methods in order to have competitive products. Most of the digital forensic tools are closed source, and how the vendors have implemented the methods used is unknown to law enforcement. However, the use of closed-source forensic tools becomes increasingly problematic for law enforcement. Firstly, law enforcement can not blindly trust the accuracy of the tools, and best practice requires validation [44], which might affect copyrighted functions of the DF tool. Adams [3] is summarizing legal practice in the US and the legal issues related to the development of digital forensic tools. He states that reliability of DF tools can not be assumed due to many bugs, errors, and timestamp inaccuracies, while defence lawyers might request to review the source code of the forensic tool. Marshall and Paige further explain that it "should also be borne in mind that updates to hardware and software may have no apparent effect on system behaviour as far as a typical user is concerned, but may dramatically change the way in which internal processing is carried out and data is stored." This impacts both the ability to recover and interpret data and the behaviour of the tools used to perform these operations [52]. Current practices and legislation are not able to overcome system vendor and DF-tool vendor dependencies, which undermines the scientific validity of the performed digital forensics. Secondly, DF-tools are multi-purposed and are used in many different security, intelligence and investigation contexts. Commercial tool vendors do not necessarily account for the higher standards LEA need to meet in respect to reliability of methods for court proceedings. Marshall and Paige [52] conducted a questionnaire asking DF-tool vendors if they consider law enforcement (customer) requirements for their tools, and 12 of 14 vendors were confused about the meaning of law enforcement requirements. Moreover, new file systems or versions remain unsupported by DF tools for significant time periods [44], while investigations can not be dismissed until a tool to interpret the data is created. Therefore, the digital forensic examiner cannot rely solely on digital forensic tools. Carrier argues that "software developers must... release their source code if it is used to generate evidence. If a developer is unwilling to do so [...this] can be a factor when purchasing an analysis tool" [13]. As long as forensic tool vendors are implementing secret techniques in their tools, there will always be a need to perform reverse engineering of file system drivers and file system structures in order to identify new or updated structures that may have an impact on the investigation. In addition, the investigator could detect errors or forensic tools performing poorly on new data structures, which might require reverse engineering not only for the evidence file system, but also reverse engineering parts of the DF tool.

4.3. *Vulnerabilities disclosure*

During investigations LEA might discover security vulnerabilities. Currently, there is little information what are, if any, LEA's obligations to report security flaws. In the absence of a swift and secure communication process they might have little incentive to inform vendors, since this may impact law enforcement's ability to acquire data. The more difficult it is to acquire the data, the more resources law enforcement need to use on acquisition, which will make less time available for analysis. Moreover, device producers gradually increase security and privacy measures in their devices [6] and, in a worst case scenario, the police might not be able to gain access to pertinent data, which then threatens public safety.

Sharing methodologies or knowledge of newly discovered data structures with the court or the wider security and digital forensic communities might expose system's sensitive information to competitors and criminals. Therefore, security experts already discuss the danger of forensic data leakage and harden software against security flaws in file or operating systems. For example, the HFS journal writes a cache of changes to the file system allowing encryption key and file content recovery [76, p. 273], which could be of great value to forensic examiners, but is also considered providing insufficient security of the file systems unallocated space by the software developers. A report on government disclosure processes in Europe stated that only a limited number of countries have a transparent procedure for vulnerability disclosure [39, p.86]. Similar to the US Vulnerabilities Equities Process (VEP) the report

recommends adoption of procedures by all LEA, where they have: *(i)* an obligation to report vulnerabilities; *(ii)* may only temporarily restrict knowledge of a vulnerability; and *(iii)* an oversight body ensures compliance.

Currently, in the absence of a legal framework which regulates the relation of digital forensics and evidence with data protection and security laws, the process imposes a higher burden on the forensic examiner, to make decisions on disclosure of methodology, sensitive data or security vulnerabilities. Arguably, legal arguments with $3^{rd}{}^{rd}$ parties for security protection or investigation methods disclosure will reduce the efficiency and reliability of digital forensics.

4.4. *Circumvention of encryption/security and personal data leakage*

Often reverse engineering of file systems for digital forensics purposes includes circumvention of security measures or encryption [8], in order to make the data available. One of the biggest concerns about reverse engineering of file systems for evidence acquisition is that it can compromise system security, exposing vendor secrets and customer data, which is otherwise encrypted at the application layer. The dispute around governmental access to encrypted and protected data drew public attention with Apple's refusal to compromise its iPhone security in response to an FBI request to get access to the phone belonging to one of the San Bernardino shooters [50]. The iPhone's data was encrypted, but the software controlling the phone was not, which was a security flaw and the FBI requested this software to be substituted by Apple with one which allows rapid password guessing. It is interesting that the FBI withdrew the request because, according to anonymous sources, the Israeli company Cellebrite assisted the FBI in opening the phone [68]. Cellebrite is specialised in developing digital forensics tools and solutions. The US Court did not allow disclosure of the forensic examination and data recovery as "national security secrets and 'intelligence sources or methods' that are exempt from disclosure under the Freedom of Information Act" [21].

File system encryption is a real challenge for law enforcement, especially since some devices have hardware encryption (for instance the Mac with the T2 chip has hardware encryption support [5]). Without the encryption key, as far as we know, it can not be decrypted within a reasonable time frame. This is of course good for privacy. However, law enforcement need access to data when investigating serious crime. It has also been suggested that vendors of devices should add back doors to their systems. This is not a good solution because back doors can be exploited by criminals and third parties [47] and compromise privacy [2]. Even governments need to keep secret information confidential, and strong encryption is one method [47] through which this is achieved. Some jurisdictions allow the police to compel the encryption key from suspects or their close circle [47]. Of course the disclosure of cryptographic keys also gives law enforcement access to more data than what is related to the crime under investigation, and may impact the right against self-incrimination and the right to silence. Additionally some EU countries have given LEAs hacking powers, allowing the police to hack into systems in order to gather information [47]. Authors emphasise the need for a legal framework to mitigate the risks of government hacking [26]. They recommend the adoption of guidelines for handling digital evidence, hacking only for "serious crimes", transparent reporting, and binding requirements for vendors of government hacking tools [24]. Without sufficient standards and documentation of how LEA examined the device after decryption, it will be difficult to prevent abuse of those broad powers and excessive intrusion in individuals' private sphere, including those not related to the investigation. In addition, file system encryption are measures taken by the vendors to protect personal data. The European data protection supervisor emphasises that the "decryption, reverse engineering or monitoring of communications protected by encryption should be prohibited [as well as...] facilitating 'backdoors' [30, p.36]. Interpol recently pointed out that tension between privacy and digital forensics might lead to "the limitation of utility of digital evidence by means of regulation and legislation" [61].

5. Emerging challenges

Due to the rapid growth of data and complexity, digital forensics requires more computational assistance and automation [15]. The introduction of automated, complex tools in investigations will sharpen the identified challenges with security, privacy, intellectual property, or methodology validation and disclosure. The lack of a regulatory framework to ensure accountability and reliability in big data analytics for investigations is already outlined as an emerging challenge for law enforcement [9]. Further, in mobile forensics most investigators rely on the digital forensic tools provided by commercial vendors. The current practice of "push-button forensics" and complex closed-source forensic tools [44] creates tool dependencies by LEA where they only report tool results, but can not sufficiently test the correctness of the tool interpretation in each case. DF tool vendors may implement automated analytic features to assist the investigator. How such functionalities are implemented is kept secret. In order to understand and validate the methods utilised by these digital forensic tools, the only option currently is to perform reverse engineering. Therefore, it is good practice to comply with the ABC model: "Assume nothing, Believe nothing, Challenge and Check everything" [33]. However, this is not necessarily done by practitioners because they do not have the time or knowledge. It's also legally unclear if they are allowed to perform reverse engineering and which methods they are allowed to use. Therefore, most investigators rely on the reverse engineering performed by commercial tool vendors, and use the tool that solves the investigative issues. It is also questionable if the commercial vendors are allowed to perform this reverse engineering. In the absence of robust formal procedure for validation, investigators can not avoid tool dependencies, which undermine the scientific soundness of the examination.

Further complications, are related to the trial proceedings. According to Art. 6 of the European Convention on Human Rights, the right to a fair trial requires public cross-examination of the digital evidence, opportunity for the defence to challenge digital forensic findings, to assess the

reliability and accuracy of the evidence and to oppose its use[10]. This means that if reverse engineering is part of the forensic examination, the methodology must be documented sufficiently in the investigation in order to enable cross-examination during trial proceedings. Moreover, law enforcement must use legal methods and tools to reverse engineer the file system. Court and/or defense review of scientific evidence is considered important to ensure an equality of arms, a fair trial and a safe verdict. This is far more important, where the forensic tool and method are novel or insufficiently validated [25]. The lawyers and the court need to verify the digital forensic examination and to keep sub-standard scientific techniques or methods out of the court [64]. The investigator could be reluctant to testify about investigation methods or security flaws in systems, and unfortunately we have seen in the USA the use of alternative explanations for how evidence was found, a practice known as "parallel construction" [20,73]. In this context, the need to preserve valuable investigation intelligence, know-how and methodology for further investigations prevents the trial parties scrutinizing the reliability of the forensic examination and the digital evidence itself. If the trial safeguards for admissibility and reliability of evidence are sufficient to scrutinize digital forensic techniques and tool results remains questionable [27]. One option may be the examination of the RE method under a non-disclosure agreement in closed door court proceedings for cases where vulnerabilities or trade secrets are disclosed. Another option is non-disclose of details of trade secrets or vulnerabilities. Both solutions will limit the right to information and accountability obligations for law enforcement. On the other hand the secrecy may protect third party copyrights, and mitigate the danger of criminals adapting their *modus operandi* according to disclosed law enforcement methods and disclosed vulnerabilities.

6. Conclusion, recommendations, and future work

Reverse engineering is an indispensable method for law enforcement in order to correctly interpret file systems, to acquire evidence and perform tool testing. When performing reverse engineering of closed-source file systems intellectual property and trade secrets might be exposed. Current legislation insufficiently addresses issues with sensitive methodology disclosure, security vulnerability disclosure, applied research by law enforcement, or tension between IPR protection and validation of forensic methodologies. Moreover, current practices and legislation are unable to overcome system- and DF-tool vendor dependencies, which undermine the scientific validity of the digital forensic process. File systems or applications are not built to comply with law enforcement needs and vendors of digital forensic tools do not necessarily consider the law enforcement obligations [52]. Below we list a few topics which are important to address:

- Legislators must reconsider the impact of digital forensic methods on intellectual property, data protection and security of commercial systems and to regulate the permissible techniques and tools which do not jeopardize existing or future security and allows cross-examination of the evidence for trial [3,61]. A regulation at European level can harmonize and set minimum standards for methods, validation, and disclosure which will support LEA's cooperation in all countries [39]. Further research is needed to establish the legal basis and scope of such legislation.
- We argue that file system vendors must sub-license and disclose the details regarding structures important for investigation. This requires information on how data is logically stored and how data structures should be interpreted for law enforcement purposes. Such measures will significantly reduce the resources needed for reverse engineering of file systems, which will remain reserved only for tool testing, validation and investigation. The approach could be further generalized to other storage solutions such as undocumented instances of databases used by applications.
- Digital forensic tool developers must have an obligation to provide LEA with information necessary for scientific validation of the tools and their interpretation of the file systems.
- New forensic methodologies including reverse engineering or other types of applied research during investigations must be documented according to formalized procedures in order for their scientific validity to be evaluated. This requires a level of transparency in digital forensics which is not reached currently due to closed-source tools and methods.
- Law Enforcement units need to test and peer-review their own techniques and methods [29]. It is not efficient that every lab perform their own testing of the same tools or tool versions. However, a detailed public dissemination of the techniques and methods may be exploited by criminals. It could be sufficient in more complex cases for another forensic examiner to reproduce the results and validate the tools.
- Law Enforcement need training in how to scientifically test tools and perform peer-review [29]. In a similar manner, lawyers and judges must be able to evaluate the scientific validity of the digital forensic methodology and the reliability of the digital evidence for legal argumentation in criminal proceedings [64].
- Governments must promote the vulnerability disclosure process [39] in order for security and privacy of individuals to be protected and cooperation with commercial vendors to be stimulated. Legislative decisions on the vulnerability of systems must not be left to the discretion of the investigators.
- There is a lack of secure communication channels between file system vendors, forensic tool developers, and law enforcement investigators. They must serve for exchange of confidential law enforcement information, testing of methodologies, and exchange of know-how without compromising security or privacy of customer data.

[10] See the requirements by European Court of Human rights in Allan v. the United Kingdom, judgement of 5 November 2002, para 47; Bykov v. Russia [GC], 4378/02, 10 March 2009; Dragojević v. Croatia, judgement of 15 April 2015, para 129.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

Legal and technical questions of file system reverse engineering (Mendeley Data)

REFERENCES

Aarnes A. Digital Forensics. John Wiley & Sons, Ltd.; 2017.

Abelson H, Anderson R, Bellovin SM, Benaloh J, Blaze M, Diffie W, Gilmore J, Green M, Landau S, Neumann PG, Rivest RL, Schiller JI, Schneier B, Specter MA, Weitzner DJ. Keys under doormats: Mandating insecurity by requiring government access to all data and communication. Journal of Cybersecurity 2015;1(1):6979.

Adams CW. Legal issues pertaining to the development of digital forensic tools. Third International Workshop on Systematic Approaches to Digital Forensic Engineering 2008:123-132. doi:10.1109/SADFE.2008.17.

Alrammal M, Naveed M, Sallam S, Tsaramirsis G. Malware analysis: Reverse engineering tools using santuko linux. Materials Today: Proceedings 2022;60:1367–78. doi:10.1016/j.matpr.2021.10.243.

Apple. About encrypted storage on your new mac. https://support.apple.com/en-us/HT208344 Visited 2020-06-30; 2018.

Apple. Privacy. https://www.apple.com/privacy/ Visited 2020-06-30; 2020.

Baker & McKenzie law firm for the European Commission. Study on trade secrets and confidential business information in the internal market. https://ec.europa.eu/growth/content/study-trade-secrets-and-confidential-business-information-internal-market-0_en Visited 2020-06-30; 2013.

Balogun A.M., Zhu S.Y.. Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology. https://arxiv.org/ftp/arxiv/papers/1312/1312.3183.pdf; 2013.

Broeders D, Schrijvers E, van der Sloot B, van Brakel R, de Hoog J, Ballin EH. Big data and security policies: Towards a framework for regulating the phases of analytics and use of big data. Computer Law & Security Review 2017;33(3):309–23. doi:10.1016/j.clsr.2017.03.002.

Broomfield M. Ntfs alternate data streams: focused hacking. Network Security 2006;2006(8):7–9. doi:10.1016/S1353-4858(06)70430-5.

Buchholz F, Spafford E. On the role of file system metadata in digital forensics. Digital Investigation 2004;1(4):298–309. doi:10.1016/j.diin.2004.10.002.

Burkhard B, Burkhard G. Admission and presentation of evidence in germany. Loyola of Los Angles International and Comparative Law Review 1994;16(3):609–27.

Carrier B.. Open source digital forensics tools: The legal argument. http://www.digital-evidence.org/papers/opensrc_legal.pdf Visited 2020-06-30; 2002.

Carrier B. File System Forensic Analysis. Addison-Wesley Professional; 2005.

Caviglione L, Wendzel S, Mazurczyk W. The future of digital forensics: Challenges and the road ahead. IEEE Security Privacy 2017;15(6):12–17.

Chikofsky E, Cross J. Reverse engineering and design recovery: a taxonomy. IEEE Software 1990;7(1):13–17. doi:10.1109/52.43044.

CJEU. Judgment of the Court (Grand Chamber), 2 may 2012 SAS Institute inc. v World Programming Ltd. ECLI:EU:C:2012:259; 2012a. Visited 2020-06-30.

CJEU. Judgment of the Court (Grand Chamber), 27 june 2012 Microsoft Corp. v European Commission. ECLI:EU:T:2012:323 Visited 2020-06-30; 2012b.

CJEU. Judgment of the Court, 6 october 2021 Top system sa inc. v Belgian state. ECLI:EU:C:2021:811 Visited 2022-06-06; 2021.

Criminal Legal News. Parallel construction: Building criminal cases using secret, unconstitutional surveillance. https://www.criminallegalnews.org/news/2018/may/14/parallel-construction-building-criminal-cases-using-secret-unconstitutional-surveillance/ Visited 2020-06-30; 2018.

D.D.C. D.C.C.. Associated press v. federal bureau of investigation, civil action no. 16-cv-1850. 2017.

Deursen Av, Burd E. Guest editorial: Software reverse engineering. J Syst Softw 2005;77(3):209211. doi:10.1016/j.jss.2004.03.031.

DFWRS. A road map for digital forensic research. https://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf Visited 2020-06-30; 2001.

Directorate General for Internal Policies. Department C: Citizen's rights and Constitutional Affairs. Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices. https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf Visited 2020-06-30; 2017.

Doyle S. Quality management in forensic science. 1st. London, United Kingdom; San Diego, CA, United States: Elsevier Academic Press; 2019.

Dr. Sven Herpig. A framework for government hacking in criminal investigations. https://www.stiftung-nv.de/en/publication/framework-government-hacking-criminal-investigations Visited 2020-06-30; 2018.

Edmond G. Is reliability sufficient? the law commission and expert evidence in international and interdisciplinary perspective (part 1). The International Journal of Evidence and Proof 2012;16:30–65.

Eilam E. Reversing - Secrets of reverse engineering. Wiley Publishing, Inc.; 2005.

ENFSI. Best practice manual for the forensic examination of digital technology. http://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf Visited 2020-06-30; 2015.

European Data Protection Supervisor. Opinion 06/2017 on the proposal for eprivacy regulation. https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf Visited 2020-06-30; 2017.

European Parliament and Council of the European Union. Directive 2009/24/ec of the european parliament and of the council of 23 april 2009 on the legal protection of computer programs. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0024&from=EN; 2009.

European Parliament and Council of the European Union. Directive (eu) 2016/943 of the european parliament and of the council of 8 june 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943 Visited 2020-06-30; 2016.

Fahsing IA. The Making of an Expert Detective, Thinking and Deciding in Criminal Investigations. University of Gothenburg, Department of Psychology: University of Gothenburg; 2016. https://gupea.ub.gu.se/bitstream/2077/47515/1/gupea_2077_47515_1.pdf.

Flore Brunetti. Oracle v. Google and the Brain Teaser of API Copyright Protection. https://blog.jipel.law.nyu.edu/2019/03/

oracle-v-google-and-the-brain-teaser-of-api-copyright-protection/ Visited 2020-06-30; 2019.
Fukami A, Nishimura K. Forensic analysis of water damaged mobile devices. Digital Investigation 2019;29:S71–9. doi:10.1016/j.diin.2019.04.009.
Garfinkel S.. Digital Forensics. https://www.americanscientist.org/article/digital-forensics Visited 2020-06-30; 2013.
Garfinkel SL. Digital forensics research: The next 10 years. Digital Investigation 2010;7:S64-S73. doi:10.1016/j.diin.2010.05.009. The Proceedings of the Tenth Annual DFRWS Conference.
German Federal Ministry of Justice and Consumer Protection. Act on protection of trade secret (gesetz zur umsetzung der richtlinie (eu) 2016/943 zum schutz von geschftsgeheimnissen vor rechtswidrigem erwerb sowie rechtswidriger nutzung und offenlegung). https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/GeschGehG.htmlin Visited 2020-06-30; 2020.
Gianluca Varisco L.A.. Ceps report - software vulnerability disclosure in europe technology, policies and legal challenges. https://www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf Visited 2020-06-30; 2017.
Hamm J.. Extended FAT File System. https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf Visited 2020-06-30; 2013.
Hansen KH, Toolan F. Decoding the apfs file system. Digital Investigation 2017;22:107–32. doi:10.1016/j.diin.2017.07.003.
H.M.S.O. Police and criminal evidence act 1984 (s. 66), codes of practice. london: H.m.s.o. http://www.legislation.gov.uk/ukpga/1984/60/schedule/1 Visited 2020-06-30; 1985.
Horsman G. Framework for reliable experimental design (fred): A research framework to ensure the dependable interpretation of digital data for digital forensics. Computers & Security 2018;73:294–306. doi:10.1016/j.cose.2017.11.009.
Horsman G. Tool testing and reliability issues in the field of digital forensics. Digital Investigation 2019;28:163–75. doi:10.1016/j.diin.2019.01.009.
Huebner E, Zanero S. Open Source Software for Digital Forensics. Springer; 2010.
Konstantin von Werder. Germany introduces new trade secrets act which imposes extensive preventive measures on companies. https://www.mayerbrown.com/en/perspectives-events/blogs/2019/04/germany-introduces-new-trade-secrets-act-which-imposes-extensive-preventive-measures-on-companies Visited 2020-06-30; 2019.
Koops BJ, Kosta E. Looking for some light through the lens of 'cryptowar history': Policy options for law enforcement authorities against 'going dark'. Computer Law & Security Review 2018;34(4):890–900. doi:10.1016/j.clsr.2018.06.003. http://www.sciencedirect.com/science/article/pii/S0267364918302413.
Kumar H, Kumar D. Protecting software programmes vis-Ã-vis patentability of software. Computer Law & Security Review 2011;27(5):529–36. doi:10.1016/j.clsr.2011.07.011.
Le-Khac NA, Jacobs D, Nijhoff J, Bertens K, Choo KKR. Smart vehicle forensics: Challenges and case study. Future Generation Computer Systems 2018. doi:10.1016/j.future.2018.05.081.
Lev Grossman. Inside apple ceo tim cook's fight with the fbi. https://time.com/4262480/tim-cook-apple-fbi-2/ Visited 2020-06-30; 2016.
magazine W.I.P.O.W.. Patent protection for software-implemented inventions. https://www.wipo.int/wipo_magazine/en/2017/01/article_0002.html; 2017.
Marshall AM, Paige R. Requirements in digital forensics method definition: Observations from a uk study. Digital Investigation 2018;27:23–9. doi:10.1016/j.diin.2018.09.004. http://www.sciencedirect.com/science/article/pii/S1742287618302718.
Microsoft. Interoperability principles program. https://docs.microsoft.com/en-us/openspecs/dev_center/ms-devcentlp/d84cac00-b312-44ee-9156-23bde6477c3d~:text=Microsoft%20will%20launch%20a%20Document,widely%20deployed%20document%20format%20implementations Visited 2020-06-30; 2008.
MSAB. iVe Vehicle Forensics. https://www.msab.com/products/ive-vehicle-forensics/ Visited 2020-06-30; 2020.
Murray A. Information technology law: the law and society. Fourth edition. Oxford, United Kingdom ; New York, NY: Oxford University Press; 2019.
Nordvik R, Georges H, Toolan F, Axelsson S. Reverse engineering of refs. Digital Investigation 2019;30:127–47. doi:10.1016/j.diin.2019.07.004.
Plum J, Dewald A. Forensic apfs file recovery. Proceedings of the 13th International Conference on Availability, Reliability and Security. New York, NY, USA: Association for Computing Machinery; 2018. p. 1–10.
Polański PP. Some reflections on the duality of regime for software protection in the european union. Computer Law & Security Review 2013;29(3):282–8. doi:10.1016/j.clsr.2013.03.012.
Popper K.R.. Science: Conjectures and refutations. http://www.nemenmanlab.org/~ilya/images/0/07/Popper-1953.pdf Visited 2020-06-30; 1953.
Pub. L. No. 105-304.S.. The digital millennium copyright act, section 1201 (a) (1) (a) and 1201 (2). Oct. 28, 1998.
Reedy P. Interpol review of digital evidence 2016 - 2019. Forensic Science International: Synergy 2020. doi:10.1016/j.fsisyn.2020.01.015. 19th Interpol International Forensic Science Managers Symposium.
Ross-Tech. Vcds windows-based diagnostic software for vw / audi / seat / skoda. https://www.ross-tech.com/vag-com/ Visited 2020-07-07; 2020.
Sakkyndig Norges Domstoler (THE Courts of Norway). Expert. https://www.domstol.no/sivil-sak/aktorene-i-retten/sakkyndige/ Visited 2020-06-30; 2011.
Sanger RM. Forensics: Educating the Lawyers. SSRN Scholarly Paper. Social Science Research Network; 2018. Rochester, NY; https://papers.ssrn.com/abstract=3303376.
Schonig Wolfgang, Partner, MORRISON & FOERSTER LLP. Update on implementation of the eu trade secrets directive into german law. https://www.mofo.com/resources/insights/180505-eu-directive.html Visited 2020-06-30; 2020.
Sommer P. Accrediting digital forensics: What are the choices? Digital Investigation 2018;25:116–20.
Tobin L, Shosha A, Gladyshev P. Reverse engineering a cctv system, a case study. Digital Investigation 2014;11(3):179–86. doi:10.1016/j.diin.2014.07.002. Special Issue: Embedded Forensics.
Tova Cohen. Israeli firm helping fbi to open encrypted iphone: report. https://www.reuters.com/article/us-apple-encryption-cellebrite/israeli-firm-helping-fbi-to-open-encrypted-iphone-report-idUSKCN0WP17J Visited 2020-06-30; 2016.
UK Law Commission. Consultation paper no 235: Search warrants. chapter 10. https://www.lawcom.gov.uk/project/search-warrants/ Visited 2020-06-30; 2018.
United States Code. Title 35, united states code. https://www.law.cornell.edu/uscode/text/35/154 Visited 2020-06-30; 1952.
U.S.C.. 18 u.s.c. §1833(b). n.d.
Vandermeer Y, Le-Khac N, Carthy J, Kechadi MT. Forensic analysis

of the exfat artefacts. CoRR 2018;abs/1804.08653. http://arxiv.org/abs/1804.08653.
Watch H.R.. Us: Secret evidence erodes fair trial rights government hides investigative methods from accused. https://www.hrw.org/news/2018/01/09/us-secret-evidence-erodes-fair-trial-rights Blogpost, visited 2020-06-30; 2018.
Wexler R. Life, liberty, and trade secrets. Stanford Law Review 2018;70:1343–429. https://www.stanfordlawreview.org/print/article/life-liberty-and-trade-secrets/.
Wikipedia. On-board diagnostics. https://en.wikipedia.org/wiki/On-board_diagnosticsOBD-II Visited 2020-07-07; 2020.
Zdziarski J. Hacking and Securing IOS Applications: Stealing Data, Hijacking Software, and How to Prevent It. OReilly Media, Inc.; 2012.