Requirements for a public digital forensics cloud

Martin Morgenstern[1] and Wilfried Honekamp[2]

Abstract: The acquisition of digital evidence in criminal proceedings has become considerably more important in recent years. At the same time, the amount of data has also increased. The need to use cloud or big data solutions for digital forensics to be able to efficiently process the permanently increasing amount of data and number of cases has been recognised for years. By using public cloud providers, such as Amazon AWS and Microsoft Azure, to secure and analyse digital evidence, resources could be used in a scalable and flexible way. Forensic service providers have had to keep a large number of data carriers for forensic backups because they have to be available immediately in case of an emergency and cannot be procured only when needed.

Keywords: Digital Forensics, cloud, big data, digital evidence

1 Introduction

Due to the rapid increase in data quantity, source and diversity, an efficient evaluation of digital evidence with traditional technologies and methods is often no longer possible [TB16]. Leimbach and Bachlechner state that there is no exact limit to when a quantity of data becomes big data. They say that big data means a quantity of data that is so large that traditional technologies and methods for data processing and analysis can no longer be used efficiently. In addition to the amount of data, processing speed and heterogeneity are also decisive for the classification of data as big data [TL14, OD23]. Although the use of big data can make the analysis of unstructured mass data much more efficient, large amounts of data must first be backed up and then transferred to the big data environment. From the authors' point of view, current methods, such as the transport of data carriers, are not a practicable solution. An alternative to transporting data carriers can be the use of cloud services. Cloud computing is not to be confused with a simple classic client-server application. The National Institute of Standards and Technology has defined five characteristics of cloud services. These are self-service, access via a network, sharing of resources, rapid scalability and measurability of IT resources [TL14]. In practice, big data and cloud technologies can be combined. Long-term planning, storage and provisioning of data media would not be necessary when using public cloud providers, as the necessary resources can be scaled up in a few seconds. However, the use of public cloud providers

[1] Hochschule Stralsund, IACS, Zur Schwedenschanze 15, Stralsund, 18435, martin.morgenstern@hochschule-stralsund.de

[2] German Police University (DHPol), Institute for Police Technology (PTI), Zum Roten Berge 18-24 Münster, 48165, wilfried.honekamp@dhpol.de, https://orcid.org/0000-0003-2931-7047

for securing and analysing digital evidence seems to have been virtually ruled out in professional circles thus far due to legally unresolved issues or other reservations [TB16] [Ri22]. One conceivable solution could be the development of cloud-in-cloud software, including corresponding upload clients. The solution to be developed would have to implement all the requirements that still have to be collected to preserve the forensic usability of digital traces. For an efficient analysis of digital evidence, it is necessary to be able to react to changed requirements at short notice. This is currently a great challenge for the police for reasons of public procurement law [Ho23]. By using a public cloud infrastructure, the current need for short-term adaptability of analysis environments can be realised in a short time.

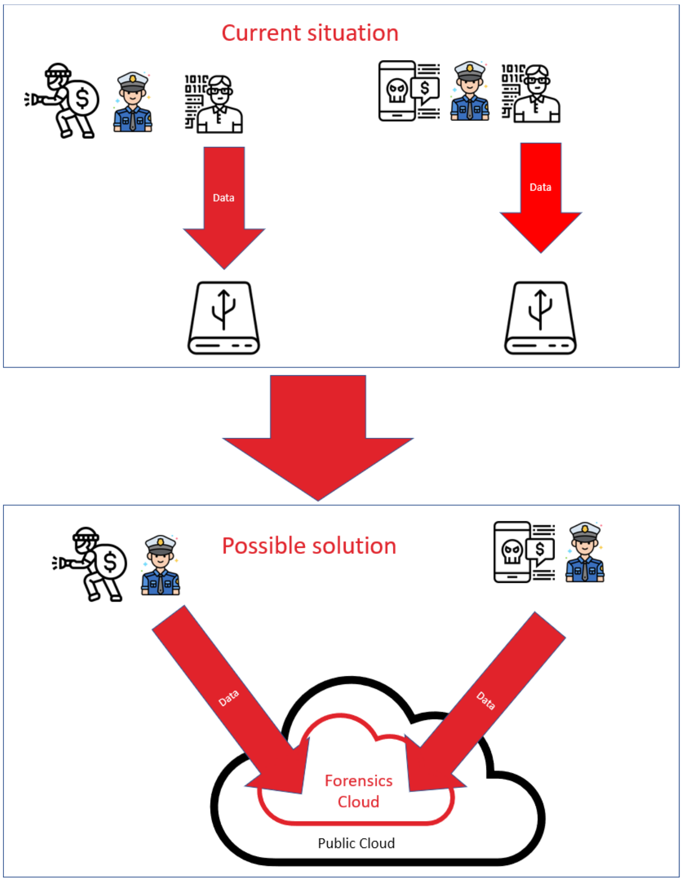

Fig. 1: Idea of a forensics cloud
(Icons made by RaftelDesign, Flat Icons, and Eucalyp from flaticons.com)

The need for digital forensics is also constantly increasing outside of law enforcement agencies. For example, in January 2023, the National Association of Statutory Health

Insurance Physicians invited tenders for incident response and digital forensics services with an estimated value of 500,000 euros for a period of 48 months. Digital forensics has developed into an important business area for private companies in recent years. Leading auditing firms as well as various specialised service providers in a wide range of company sizes offer computer forensic services [KB22].

Due to the increasing number of digital forensics experts, it is foreseeable that the number of private forensics service providers will increase in the coming years. However, especially for small forensics companies, the procurement of powerful hardware and software is a major hurdle. By providing cloud solutions for digital forensics that include not only analysis tools but almost the entire infrastructure needed, starting with the forensic backup of data, the entry hurdle into self-employment for digital forensic specialists can be significantly lowered [TB16].

There are many special fields in digital forensics, the number of which is constantly increasing. In addition to the quantity of data, the number of possible data sources is also increasing annually. This has led to smaller forensic service providers, in particular, often specialising in one area of digital forensics. These can be specialists for the analysis of certain types of data, e.g., multimedia forensics but also specialists for specific data sources such as motor vehicle forensics [MFH22] [Ha21] [Bö09].

To date, the securing of digital evidence has largely been done by forensic experts. However, this means that these experts must be available at all times. Spontaneous digital preservation of digital traces without digital forensic experts is therefore not possible at the present time. In this contribution, we analyse the requirements of a centrally available forensics cloud as the primary storage medium for digital evidence, to which all police officers entrusted with the case have access, and whether such a forensic cloud could lead to an increase in the efficiency of police work. The public digital forensics cloud to be established and introduced in Figure 1 offers a provider-independent possibility for collaboration between a large number of forensic experts. Since no requirements for such a cloud have been published yet, these are to be determined by expert knowledge acquisition.

2 Method

To capture the requirements for a forensics cloud, an expert survey was conducted using a structured questionnaire [Mo23]. The survey contained both open and closed questions. Closed questions were evaluated quantitatively, and open questions were evaluated with a qualitative content analysis according to Mayring [Ma22]. In some cases, additional information was provided for the closed questions, which was then also evaluated qualitatively.

In May 2023, four practitioners of digital forensics with several years of professional experience were interviewed as experts. Expert 1 is head of a digital forensics unit in a public security authority, has many years of experience in the field of IT forensics and is a publicly appointed expert in this field. Expert 2 has a professorship in IT forensics and works as a publicly appointed expert for digital forensics. Expert 3 works as an analyst and scientific coordinator for digital forensics in a state criminal investigation office. Expert 4 works as a course instructor for computers and cybercrime at a police training institution and has practical experience in securing digital traces.

A category system was developed analogous to [He14] for the analysis of the answers. It is essentially analogous to the questions asked.

Category	Name	Description
C 1	Qualification	This category records the relevant professional qualification of the participant.
C 1.1	Education	Contains the participant's vocational training.
C 1.2	Work experience	Contains the relevant professional experience of the participant.
C 2	Necessity as primary storage medium	The category analyses the need for a forensics cloud.
C 2.1	Lack of resources as a reason for not preserving evidence	It was asked whether there were any known cases in which digital evidence was not secured due to a lack of resources or skilled personnel.
C 2.2	Crime clearance rate	The experts were asked to assess whether more crimes could be solved if nontechnical personnel were enabled to secure digital traces in a spontaneous spontaneously, practicably and in a way that can be used in court.
C 3	Cooperation	
C 3.1	Development to date Specialisation	The experts were asked to indicate how, in their view, the role of specialisation has changed in recent years.
C 3.2	Importance of cooperation	The experts were asked about their experience of the role that cooperation between various governmental and nongovernmental experts already plays today.
C 3.3	Expectation of an increase in specialisation	It was asked whether an increase in specialisation is expected in the next few years.

C 4	Other	
C 4.1	Expected added value	The experts were asked to state whether, from their point of view, further added value that was not addressed in the previous questions can be expected from the planned forensics cloud.
C 4.2	Acceptance requirements	The experts were asked, what the important factors for the acceptance of a forensics cloud as the primary storage medium for criminally relevant data are.
C 4.3	Other comments	Finally, the participants were able to provide further comments on the topic.

Tab. 1: Categories for analysing

3 Results

This section presents the results of the evaluation of the interviews. The question of whether the participants were aware of cases in which digital traces were not secured due to a lack of resources was answered differently by all participants. One participant each answered this question with a yes or a no without further explanation. The other answers indicated that there were cases where traces were not saved. However, both experts wrote that the reasons for this were not a lack of technical equipment but mainly a lack of expertise on site. Expert 3 also stated that expertise available in other authorities may not always be shared due to official regulations. Another problem with new technologies is that the possibilities for data extraction have not yet been developed.

Another reason given for not securing evidence was poor preclearance, as well as simply not requesting IT forensics experts. Only one respondent believes that more crimes could be solved if nontechnical personnel were given the opportunity to secure data spontaneously, practically and in a court of law. All other respondents stated that at least some technical understanding is necessary to identify digital traces as such. Furthermore, one answer referred to the already existing nationwide information portal, where data can also be uploaded by citizens in case of special damage situations.

All participants confirmed that specialisation in IT forensics has increased in importance in recent years. In this context, two answers pointed out that despite specialisation, solid basic knowledge is necessary. In regard to specialisations in IT forensics, a distinction must be made between specialisations in data origin and data evaluation. The evaluation of data should be carried out independently of the data origin. Nevertheless, the type of possible data sources will continue to increase, which is why there will be an increase in specialisations here as well.

Due to specialisations but also for other reasons, cooperative work is already taking place between different IT forensics experts. In several federal states, state and nonstate investigators work together. This practice is not without controversy, as law enforcement is a sovereign task. An increase in specialisations is expected by all participants. Expert 1 added, "There will always be more specialisations, but they will require more and more cooperative collaboration for successful investigations. As things stand now, definitely also between governmental and nongovernmental forensic experts". The experts were asked what added value - not named in the previous questions - they expect from a vendor-independent forensics cloud as the primary storage medium for digital evidence. In one interview, this question was not answered. One expert stated that a corresponding solution is already being set up for law enforcement in Saxony.

Expert 1 sees a possible added value in only using the technology of large cloud providers to operate a private cloud for police investigative work with its own infrastructure. At present, there are still justified political reservations about the direct use of large cloud providers. These could also not be solved by using a cloud-in-variant solution.

Expert 3 sees cost savings as a possible advantage since any necessary licences could be used across authorities. Furthermore, the processing of the data can be more efficient due to the available computing power. The lack of transport of data carriers to analysts and investigators was also mentioned as an added value.

With regard to the implementation of necessary encryption measures, all experts stated that current and the most secure procedures should be used. One participant pointed out that even with current encryption procedures in a cloud-in-cloud solution, it cannot be ruled out that the respective cloud operator gains access to sensitive data. At the latest, when the data are processed, they must be decrypted in the working memory. Research is currently being conducted into encryption methods that should enable processing without decryption, and the first test variants already exist. However, it will be several years before these could be used productively, which is still uncertain at present.

Almost all participants mentioned high security levels as an acceptance requirement for a forensics cloud. These were described in more detail in individual responses. Security must not be based on the self-commitment of individual cloud providers, which is currently the case with many public cloud providers. Security measures must not be outsourced but must be reflected in the technical solution used. Further acceptance requirements are simple usability and a fast internet connection of the cloud.

Two of the experts used the opportunity to make further comments on the topic. Expert 1 thinks that it would make sense to think about whether it might not also be more economical to build up one's own infrastructure. From a certain size upwards, this could be irrelevant in terms of costs, but this would have to be calculated. Furthermore, the normal police staff would have to be put in a position to recognise when experts might be necessary to secure data. A solution that is to be developed must also be politically feasible, particularly when data are secured by laypersons, as it can then be assumed that not all available data are secured.

Expert 3 states that direct data extraction to a cloud environment seems difficult because most tools need a direct connection to the device. Furthermore, some tools would require special hardware that could not be virtualised. The possibility that all police officers would be able to back up digital data themselves could only possibly lead to a relief of the forensic specialists. In return, however, the amount of secured data would increase, which would lead to a higher time requirement for its evaluation. Securing digital traces is not the everyday task of police officers. Therefore, a significantly higher error rate and increased probability of loss of evidence must be expected if all police members secure data themselves.

4 Discussion and Conclusions

A forensics cloud that can be used by all police staff has the potential to significantly improve the efficiency of securing and evaluating digital evidence. An increase in efficiency could be realised in particular through the elimination of transport routes, as well as a possible immediate backup of data. However, the results of the survey showed that when digital evidence is secured by nonforensic experts, it can be assumed that backups are not always carried out completely and professionally. In the worst case, there is even a fear of a break in the chain of custody. One of the main arguments against securing digital evidence by nonforensic experts is that they will overlook more digital traces than IT forensic experts do.

However, the problem listed is not entirely new. One result of the survey was that IT forensic experts were often not on site because the need for these experts was not recognised. The overlooking of digital traces in these cases is independent of whether the criminally relevant data are backed up in a cloud or on a local data carrier. A logical consequence of this experience should be to qualify all police officers to recognise digital traces as such. However, this qualification would require a basic understanding of digital traces [Ho23].

Another important aspect in connection with clouds is always the issue of security. Especially when processing data relevant to criminal law, a very high security standard must be guaranteed. Since direct storage and processing of data with a public cloud provider is considered too insecure by the authors, the basic idea to solve the problem is to develop a cloud-in-cloud solution. The approach should be that security measures can only be controlled by the owner of the forensics cloud. The security of the forensics cloud would need to be audited and certified by independent and trusted third parties. A residual risk of loss of confidentiality will never be completely excluded. At this point, a social discourse on what risks should be accepted would be appropriate.

The police infrastructure for the prosecution of criminal offences belongs to the critical infrastructure area. The status of Critical Infrastructure does not exclude that it is outsourced to external cloud providers. Following the general trend towards cloud computing, in recent years, operators of critical infrastructures have also begun to partially outsource their computer resources and use them as a service. These are, for example, banks or companies from the energy supply sector [We20a] [We20b] [Kü23]. The question therefore arises whether higher requirements apply to the storage of digital evidence than to other critical infrastructure. In contrast to banks and energy service providers, the police belong to the authorities and organisations with security tasks (BOS). [BB23] Particularly in the area of the police, a leak of confidential information can pose a direct threat to people's lives. Regardless of the expected risks, however, it has been shown that provider-independent forensic clouds can represent added value. It therefore seems sensible to explore the topic further. In particular, research should be conducted into how the identified risks could be minimised. Since even internal police systems can never guarantee 100% security, a follow-up study could compare the security of police systems with that of a possible forensics cloud.

Bibliography

[BB23] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK): BOS, Behörden und Organisationen mit Sicherheitsaufgaben, https://www.bbk.bund.de/SharedDocs/Glossareintraege/DE/B/BOS.html, accessed: 30/06/2023.

[Bö09] Böhme, R.; Freiling, F.; Gloe, T.; Kirchner, M: Multimedia-Forensik als Teildisziplin der digitalen Forensik. Presentation at the GI Workshop „Multimedia-Forensik“, Lübeck, 2009.

[Kü23] Kümmerlein, K.: Ist die Cloud Teil der Energiewende? https://www.cloudcomputing-insider.de/ist-die-cloud-teil-der-energiewende-a-7462505e5f33964c04d7133f41100c12/, accessed: 30/06/2023.

[He14] Helfferich, C.: Leitfaden- und Experteninterviews. In N. Baur & J. Blasius (Hrsg.), Handbuch Methoden der empirischen Sozialforschung. Springer Fachmedien, Wiesbaden, pp. 559–574, 2014.

[Ho23] Honekamp, W.; Povalej, R., Rittelmeier, H., Fähndrich F.; Berner S.; Labudde, D.: Technologiegetriebene Polizeiausbildung im Umgang mit Digitalen Spuren. In: Handbuch Cyberkriminologie. Springer Fachmedien, Wiesbaden. pp. 1-30, 2022.

[KB22] Kassenärztliche Bundesvereinigung. Öffentliche Ausschreibung Berlin 2022 Rahmenvertrag digitale Forensik und Incident-Response. https://ausschreibungen-deutschland.de/1002019_Rahmenvertrag_digitale_Forensik_und_Incident-Response_2022_Berlin, accessed: 30/06/2023.

[LB14] Leimbach, T.; Bachlechner, D.: Big Data in der Cloud. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), Berlin, 2014.

[Ma22] Mayring, P.: Qualitative Inhaltsanalyse: Grundlagen und Techniken. Beltz, Weinheim, 2022.

[MFH22] Morgenstern, M.; Fähndrich. F; Honekamp, W.: Ontology in the Digital Forensics Domain: A Scoping Review. In: Demmler, D., Krupka, D. & Federrath, H. (Hrsg.), INFORMATIK 2022. Gesellschaft für Informatik, Bonn. pp. 71-80, 2022.

[Mo23] Morgenstern, M. Fragebogen zur Erfassung der Anforderungen an eine Forensik-Cloud. https://paperswithcode.com/paper/fragebogen-zur-erfassung-der-anforderungen-an, accessed: 11/07/2023.

[OD23] Oracle Deutschland. Was versteht man unter Big Data? https://www.oracle.com/de/big-data/what-is-big-data/accessed: 11/07/2023.

[Ri22] Rittelmeier, H.: Cloud-Konzepte für die digitale Forensik, Presentation, Interesting Times Forensics, Nüdlingen, 2022.

[TB16] Tabona, O., Blyth, A.; A forensic cloud environment to address the big data challenge in digital forensics. In 2016 SAI Computing Conference (SAI), London, pp. 579-584, 2016.

[We20a] Weidmann, T.: Solarisbank migriert als erste deutsche Bank vollständig in die Cloud, https://www.it-finanzmagazin.de/solarisbank-arbeitet-als-erste-deutsche-bank-ausschliesslich-in-der-cloud-115060/, accessed: 30/06/2023.

[We20b] Weidmann, T.: Deutsche Bank geht in die Google Cloud: Warum der Schritt überfällig ist, https://www.it-finanzmagazin.de/deutsche-bank-geht-in-die-google-cloud-warum-der-schritt-ueberfaellig-ist-115585/, accessed: 30/06/2023.