future internet

MDPI

Article

Challenges of Network Forensic Investigation in Fog and Edge Computing

Daniel Spiekermann [1] and Jörg Keller [2,*]

[1] Faculty of Computer Science, Dortmund University of Applied Sciences and Arts, 44227 Dortmund, Germany; daniel.spiekermann@fh-dortmund.de
[2] Faculty of Mathematics and Computer Science, FernUniversität in Hagen, 58084 Hagen, Germany
* Correspondence: joerg.keller@fernuni-hagen.de

Abstract: While network forensics has matured over the decades and even made progress in the last 10 years when deployed in virtual networks, network forensics in fog and edge computing is still not progressed to that level despite the now widespread use of these paradigms. By using an approach similar to software testing, i.e., a mixture of systematic and experience, we analyze obstacles specific to forensics in fog and edge computing such as spatial dispersion and possibly incomplete recordings, and derive how far these obstacles can be overcome by adapting processes and techniques from other branches of network forensics, and how new solutions could look otherwise. In addition, we present a discussion of open problems of network forensics in fog and edge environments and discusses the challenges for an investigator.

Keywords: network forensics; fog computing; edge computing; cloud computing; internet of things; forensic investigation

Citation: Spiekermann, D.; Keller, J. Challenges of Network Forensic Investigation in Fog and Edge Computing. *Future Internet* **2023**, *15*, 342. https://doi.org/10.3390/fi15100342

Academic Editor: Alessandro Pozzebon

Received: 31 July 2023
Revised: 10 October 2023
Accepted: 11 October 2023
Published: 18 October 2023

1. Introduction

Over the years, the design of IT infrastructures has undergone a significant evolution, driven by advancements in technology, changing requirements, and the growth of connected devices. Starting with a mostly centralized design, in which mainframes and large servers were used to process and store data, the connected client devices had limited capabilities and relied on the central infrastructure for computing tasks. This approach had limitations in terms of latency, scalability, and network dependency, so the next step was the use of distributed computing, which expanded both the capabilities of networks and the computing power of the clients. Interconnected devices and distributed computation over multiple machines inside a local area network (LAN) were typically used to increase the overall performance. The most critical problem was the inflexible design, which hampered necessary changes like adding new machines for horizontal scaling or updating internals of the underlying network.

With the advent of cloud computing, the focus shifted to centralized data centers that provided scalable and on-demand computing resources over the internet. This allowed organizations the management of their computational needs and storing of large amounts of data in remote servers. Cloud computing offered flexibility, cost efficiency, and accessibility, but it also introduced new challenges related to latency, bandwidth constraints, and privacy concerns. With an increasing frequency of networking activities being involved in criminal activities, the number and importance of network forensic investigations started to grow as well [1]. Forensics of physical networks, i.e., tapping and recording at a router, had to extend to cloud infrastructures where network devices are not necessarily physical but often realized as part of the cloud software [2].

As the number of connected devices and the volume of data generated at the network edge increase, the limitations of these centralized cloud environments become more apparent. Edge computing emerged as a paradigm that aims to bring computation closer to

the data source, reducing latency and bandwidth requirements while improving response times and real-time processing capabilities.

Simultaneously, the rapid evolution of Internet of Things (IoT) devices continues, and the deployment of improved computing environments has gained significant attention due to its ability to provide low-latency and real-time processing capabilities. Edge and fog environments are characterized by a large number of interconnected devices, possibly distributed over a large area, with varying levels of computational power and storage capacity [3,4]. Thus, the distributed and heterogeneous nature of edge and fog environments introduces new challenges for conducting network forensic investigations, which extend to those environments as a consequence of their spread and relevance. Such investigations, which mainly serve to record traces of network packets for further analysis, become necessary as a consequence of the spread of edge and fog environments, be it for troubleshooting or for involvement in criminal activities [5]. Especially for the latter, completeness of recorded traces is important in a lawsuit, yet the spatial dispersion makes it challenging to obtain complete traces [1].

We investigate these challenges, i. e., we analyze the obstacles that are specific to forensic investigations in fog and edge computing environments, for example, the spatial dispersion of devices. We then strive to determine ways to overcome these obstacles by adapting processes and techniques from other branches of network forensics or creating new solutions. We also provide a discussion of open problems for forensics in fog and edge environments, and the challenges they still pose for forensic investigators.

We summarize our contributions as follows.

- We see the first contribution in identifying the above challenges, i.e., making the scientific world aware of the differences between network forensics in edge, fog and cloud forensics in contrast to network forensics in "classic" types of networks, especially as these differences so far have only been considered for one field (edge, fog, cloud) in isolation or not at all. Yet, as the importance of edge, fog and cloud computing is undisputed and growing, there is a need to act.
- As the second contribution, we strive to analyzefor which of these challenges existing solutions from other fields might be adapted, and for which of these challenges we are not aware of solutions.
- The third contribution is our approach of analyzing along dimensions as in software testing, which allows provision of a certain systematic analysis right away in contrast to a "brute force" approach of an extensive literature analysis for which some other approach for extracting the challenges (possibly ad hoc) would still have to be found and applied.

The remainder of this article is structured as follows. In Section 2, we summarize background information about edge and fog computing, as well as about network forensics, while in Section 3, we discuss related work. In Section 4, we discuss challenges and possible solutions. Finally, in Section 5, we offer some conclusions and an outlook to future work.

2. Background

2.1. Networking in Edge and Fog Computing

The shift to an edge-centric paradigm has various consequences to the network design of these infrastructures. The main idea of an edge-centric computing environment results in a computation on the edge of a network; in combination with fog computing, this change provides the possibility to take

> *the control of computing applications, data, and services away from some central nodes (the "core") to the other logical extreme (the "edge") of the Internet* [6].

Improved network techniques provide higher transmission rates in networks, and with the help of virtual networks, distributed devices can be interconnected like in an LAN. Therefore, edge and fog computing environments affect network design like content delivery networks, P2P and cloud architectures.

Networking in edge computing involves establishing communication and connectivity between edge devices, edge servers, and other components within the edge infrastructure. Figure 1 shows a sample interconnection between the involved devices. Endpoints (shown in the yellow area) are called edge devices. These devices, such as sensors, IoT devices, or smartphones, generate data or consume services at the network edge. They are typically resource-constrained and may have limited processing power, storage, and network capabilities. Intermediate nodes (shown in the blue area) are called edge servers and provide computational and storage resources closer to the edge devices. They act as local gateways, and aggregate, process and and analyze data from the edge devices. Edge servers can also host applications and services that offload processing tasks from the cloud and provide low-latency responses. Edge servers can be connected with each other, creating a hierarchy within edge servers with various interconnections and assigned jobs.

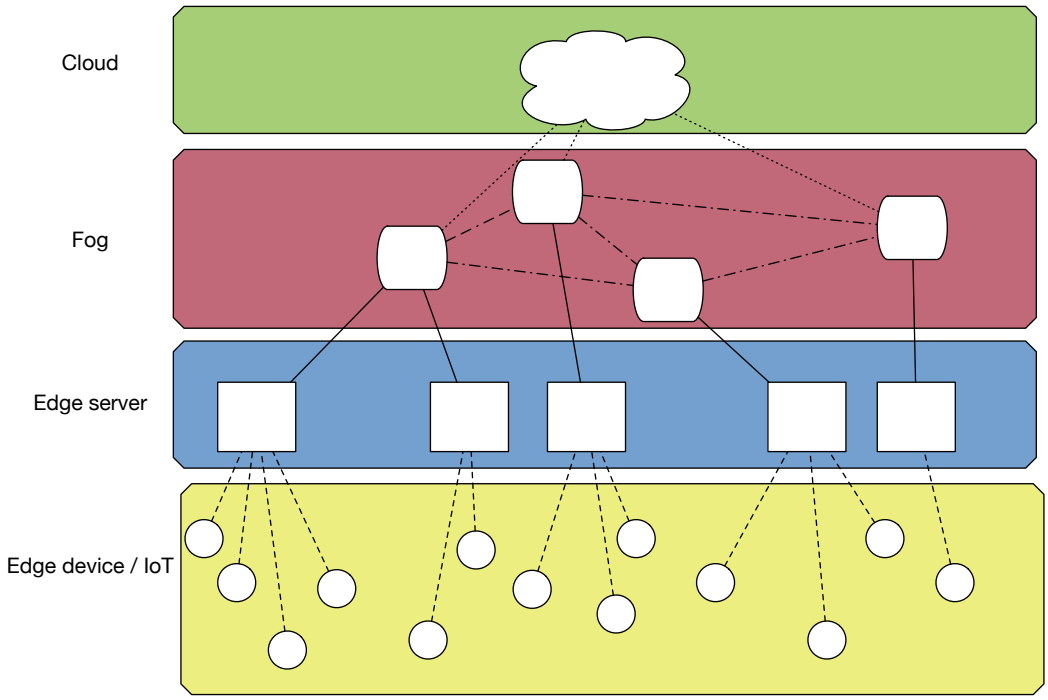

Figure 1. Edge and fog networking.

The edge network infrastructure (ENI) is responsible for connecting edge devices and edge servers. It may consist of wired and wireless connections, such as Ethernet, Wi-Fi, cellular networks, or specialized IoT protocols. The network infrastructure ensures reliable and efficient data transfer between edge devices and edge servers. For the communication between server and endpoints and for the communication inside the ENI, various protocols are used. These protocols can include TCP/IP, MQTT, Constrained Application Protocol (CoAP), Zigbee, Bluetooth, LoRaWAN, or custom protocols depending on the specific requirements of the edge environment [7]. When communicating with external destinations, the ENI provides a routing and traffic management platform. This can involve protocols like Border Gateway Protocol (BGP), routing tables, and Quality of Service (QoS) mechanisms to prioritize traffic and ensure efficient utilization of network resources.

A specific configuration is the opportunity to combine edge and cloud computing. The idea is to process time-critical tasks on the edge side, but to outsource resource-intensive, time-consuming or storage-intensive tasks to a server in the cloud environment.

On top of these servers, the fog network part starts. Fog computing softens the strict separation between edge and cloud computing by adding another area. Inside this area, computational power, storage, and networking are closer to the devices and sensors which generate the data. The summarization of the information of various sources reduces

the continuous communication with cloud servers from each device. Thus, latency and response times are reduced and real-time processing and low-latency communications are possible. In addition to this, more efficient bandwidth utilization is possible, which provides benefits for various fields like industrial automation [8], smart cities [9], autonomous vehicles [10], and healthcare applications [11].

Fog computing allows local processing and analysis of data, occurring near the source, which helps in making faster and more context-aware decisions. Networking in fog computing involves establishing and managing communication between various devices, sensors, fog nodes, and cloud resources. The use of local resources reduces the amount of data transferred to the cloud, but requires a continuous connection to the different devices on the edge side. Especially the fog nodes as intermediate points between devices and the cloud are critical for this connection. A fog node can be a single network device, like a router, a computational server or a resource-constrained device such as a set-top-box and access point [12]. Because of this diversity, the network capabilities of fog nodes differ. The correct location of these devices has a huge impact on the performance of the network [13]. The nodes are responsible for collecting data from devices, processing them locally, and forwarding relevant information to the cloud or other fog nodes for further analysis. Inadequate positioning of fog nodes results in high latency, low transfer rates because of long distances and time-consuming connections between the different devices and the nodes [14,15].

2.2. Network Forensic Investigation

Network forensic investigation as a branch of digital investigations plays a crucial role in identifying and mitigating cybersecurity incidents, allowing organizations understanding and effective response to network breaches [16].

Network forensics refers to the process of collecting, analyzing, and interpreting network-related data. The source of data are network packet captures or system and event logs, e. g., extracted from network devices like firewalls and intrusion detection and prevention systems. The primary objective of network forensics is to identify the source, extent, and impact of a cyber incident, as well as to gather evidence for potential legal proceedings. By analyzing network data and communication details, a network forensic investigation can help determine how an attack was carried out, which vulnerabilities were exploited, and how to prevent similar incidents in the future.

Thus, attacks like malware injection, covert channels or denial of service can be analyzed and proper countermeasures become easier to implement. The systematic approach of capturing and analyzing network-related data helps investigators to understand the nature of an attack, strengthen their security defenses, and potentially prosecute perpetrators.

A common methodology for network forensic is abbreviated as OSCAR [1]. Figure 2 shows the five subsequent phases of this framework.

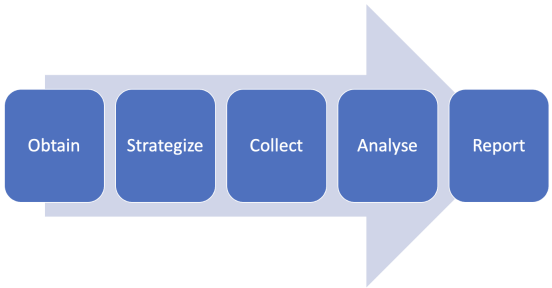

Figure 2. The OSCAR framework.

Especially collection of the evidence is a crucial part of the investigation process. In contrast to post mortem investigations in the field of computer or mobile device forensics, the *capturing* and *recording* of network traffic, which together comprise the collect phase, have to be performed in real time in the network [17]. Missed network packets are typically

inaccessible and therefore unusable for the subsequent analysis of the recorded network packets. Because of this, the deployed tools need access to the data transfer medium and require proper storage capacity. Neglecting these parameters results in incomplete packet captures hampering the phase of packet analysis. This stage entails the examination of the captured packets to reconstruct timelines, identify attack vectors or involved systems and uncover possible suspicious activities. The phase of reporting presents the findings and conclusions of the investigation.

3. Related Work

Fog and edge networks are used for different applications, thus resulting in various installations and techniques [18] like vehicular computing [19], mobility [20] or federated learning [21]. Edge and fog computing demand modern network infrastructures to interconnect the different devices and provide an ongoing connection between the network edge on the one side, the fog part as a middle-ware and the cloud on the other side. A discussion of techniques related to fog networks is presented in [5], discussing various network applications, ref. [22] with a special view on IoT, or [23], describing possible implementations in next-generation networks. Edge networks are discussed in [24] or [25], related to mobile edge networks. These networks differ from traditional and mostly static networks, e.g., [26] discusses application placement in such networks via machine learning. Whereas network forensic investigation in traditional networks is well-known [27,28], dynamic and virtual environments like cloud environments differ from these static environments and raise new challenges. In [2], the authors discuss various challenges like multitenancy, internal dynamic of the environment and jurisdiction issues. In [29], the new challenges of fog computing are described with a special view on information security and digital investigation in these environments. Ref. [30] describes the use of software-defined networks (SDN) and fog computing to manage the network traffic in IoT environments. In [31], SDN is used to improve the handling of streams of big data in Industrial IoT environments. A discussion of forensic investigation in fog environments is performed in [32], describing the problem of finding the relevant evidences in fog environments, or [33], discussing the trusted recording of evidence in a distributed ecosystem with multiple trust domains. The new environments provide new techniques for forensic investigation. Ref. [34] presents FoBI, a fog-based IoT forensic framework, which helps to collect relevant data from IoT devices.

In [35], forensics for fog computing are contrasted against cloud computing, but edge computing is not integrated. In contrast, ref. [36] considers forensics in edge networks with a focus on media transmission over 5G; similarly, ref. [37] considers them for smart homes. Both, however, do not consider the interference with fog and cloud computing. Edge forensics process over 5G is refined in [38] with the use of deep learning approaches, yet again seen without the other network parts. Ref. [39] concentrates on forensic evidence from devices in edge computing, while ref. [40] focuses on privacy-preserving forensics for offshore, i.e., low-bandwidth edge computing. Forensic challenges when connecting edge and cloud computing are discussed in [41], yet without looking at fog computing. None of these works consider all network parts together.

Intrusion detection systems for fog and cloud computing are surveyed in [42]. While the focus is not on forensics and packet capture, and edge is only treated in the form of edge devices, some of the problems coming from the distributed nature of edge, fog and cloud networks are similar for intrusion detection and forensic capture.

4. Challenges

The change in behavior in networking and the mixture of different technologies, processes and interconnections have a huge impact on the forensic investigation inside these environments. This section lists relevant challenges encountered during network forensic investigations in edge and fog environments. Each challenge is discussed and its impact on the investigation process is presented. To ensure a systematic process and to obtain a list of requirements that is as complete as possible, we take software testing as

an example and role model [43]. By this, we mean that we mentally apply the *concepts* of unit and integration tests onto the fog, edge and cloud structures in which forensic investigations are conducted. As we are not performing additional experiments for the present research alone, we mentally apply those concepts but do not actually perform a test on a real, distributed software system. By mentally applying the test concepts, we do not mean explicitly formulating a concrete hypothesis and formally testing mentally whether the hypothesis holds in the scenario, but arguing whether certain problems occur within a network component or during the collaboration of network components during capture and record of network packets. Extracting the challenges also involves concepts like bug hunting, i.e., looking at some scenarios in more detail or at a more detailed level.

To complement and enhance the above approach, we use the literature and our multi-year experience in this field. Yet, we are aware that—as with any approach that is not completely formal and does not guarantee to prove properties as, e.g., in [44]—such a list of requirements remains a best-effort approach. Software testing, ranging from bug hunting to unit and integration tests, deals with differences between software specification and software implementation. Finding the cause for such differences is achieved in as systematic a manner as possible, yet it is helpful to know where to look first, i.e., for typical causes. For example, especially in embedded software, device characteristics and communication with other entities plays a role.

- **Device variety**
  The number of possible devices in fog and edge environments differs from small installations with only a few, mostly homogeneous devices to large-scale environments with a huge variety of different components.
  On the one hand, such devices are limited in their performance and software possibilities, for example, single-board computers like Raspberry Pi or Arduino, industrial gateways and Programmable Logic Controllers (PLCs) with a specific and robust network connection and industrial-grade specifications, smart cameras for real-time video and object identification, drones and autonomous vehicles, wearable devices like smartwatches or fitness trackers. Their job is to process and analyze the data on board. This enables real-time decision and autonomous operations in various applications without a continuous network connection to a central server.
  On the other hand, high-powered devices like edge servers and routers, which can be rack-mounted or in a smaller form factor, have higher computational resources. They provide increased processing power, storage capacity, and networking capabilities.
  The devices differ in their physical interfaces to connect to a network as well as in the deployed protocols and communication techniques. Some devices are always on and send data periodically; other devices are in stand-by for a longer period, but then send a bunch of data at a random timeslot.
  This variety of involved devices hampers an easy data acquisition process and demands a flexible and versatile capture process.
- **Cloud computing interaction**
  The evolution of fog and edge computing is blurring the lines between edge and cloud environments, creating a continuum that spans from the cloud to the edge devices. Organizations are adopting hybrid architectures that leverage the strengths of both edge and cloud computing. Critical and time-sensitive tasks are executed at the edge, while data that are not time critical are sent to the cloud for further analysis and storage, but the scheduling of this processing is again a complex problem [45]. A possible solution is the implementation of fog devices that create a separate layer between the edge and the cloud, processing various tasks at this position. This application placement depends on various aspects like purpose [46], energy consumption [47] or availability [48], but every installation impacts the position of a capture process as well as the analysis of the data.
- **Lack of centralized capture positions**
  The environments consist of a large number of distributed computing resources, which

we coined as spatial dispersion when introducing the field of investigation. This makes it challenging to have a centralized position to capture all relevant network traffic for the subsequent analysis of the data. This lack of centralized access makes it difficult to collect the entire relevant network traffic from all involved devices, especially as not all traffic is transported to the cloud.

- **Limited storage and processing capabilities**
  Edge and fog devices often have limited storage and processing capabilities compared to traditional servers. This limitation affects the amount of network traffic data that can be captured and stored for forensic analysis. It may be necessary to prioritize and filter data to reduce storage requirements, potentially leading to the loss of valuable forensic evidence (and/or incomplete capture). Edge servers typically provide higher storage capacities, but the access to these areas is typically limited to specific interfaces and APIs. As a result, the capture process has to be performed at a point inside the network that is suitable to collect all relevant traffics at once; the use of the devices for storing the captured data is not possible. This is a common problem in advanced network forensic investigation as discussed in [49].
- **Inherent dynamic**
  Fog nodes as well as edge end points might join or leave the network dynamically. This dynamic behavior results in similar challenges as discussed in [2] inside virtual networks. As a result, an installed capture process is threatened for missing network packets because of new or undetected, but relevant devices (so-called incomplete capture). Investigators need to adapt their techniques to handle the frequent changes in network topology and availability of fog nodes.
- **Data fragmentation and encryption**
  Nodes may perform data processing and aggregation, leading to data fragmentation and encryption. The problem of fragmented or encrypted data is a well-known problem in networks nowadays, which hampers the analysis of network traffic [50,51]. The encryption of network traffic is a common practice to prevent the plain text transmission [52]. If used, eavesdropping of the connection is still possible, but analyses like application identification or usage are hampered [53]. The analysis of these encrypted data is part of current research like [54,55]. The fragmentation of network traffic depends on the maximum transmission unit (MTU) of a network path. Routers inside a network set their own MTU if needed, which results in smaller network packets than initially sent [56]. The reconstruction of the fragmented network traffic has to be performed at the receiving side, so a packet capture process has to take care of collecting all fragments of the transmitted data. Otherwise, such an incomplete capture might led to the failure of a forensic analysis.
- **Trust and privacy concerns**
  Fog environments involve multiple stakeholders, including device owners, fog node operators, and cloud service providers. This distributed nature raises concerns about trust and privacy. Investigators may encounter difficulties in accessing and retrieving data from different entities due to legal, privacy, and permission-related issues.
- **Limited forensic tools and standards**
  Traditional network forensic tools and standards may not be fully applicable to fog environments. Fog nodes and edge devices often have resource constraints, making it challenging to deploy and execute complex forensic tools. Additionally, there may be a lack of standardized protocols and procedures specific to fog environments, hindering interoperability and consistency in forensic investigations.
- **Time synchronization and clock drift**
  Fog devices may have different clocks and varying levels of clock accuracy. Inaccurate time synchronization and clock drift can complicate the correlation of network events across fog nodes, affecting the accuracy and reliability of forensic investigations.
- **Jurisdiction**
  The distribution of edge and fog devices might result in installations all over the world.

As a result, different laws and jurisdictions are relevant for the access of the network packets. This is a common problem in modern, globally spread environments with distributed virtual network endpoints [2].

Table 1 summarizes the challenges and assigns them to Phases 3 and 4 of network forensic investigation, as the first two phases and the last phase of the OSCAR methodology (see Section 2.2) are rather non-technical. The collect phase is split into its parts, capture and record.

Table 1. Challenge Summary.

	Collect		Analyze
	Capture	**Record**	
Device variety	x	x	x
Cloud computing interaction	x	x	x
Lack of centralized capture position	x	x	x
Limited storage and processing capabilities	-	-	x
Inherent dynamic	x	-	x
Data fragmentation and encryption	-	x	-
Trust and privacy	x	-	x
Limited tools and standards	x	x	x
Time sync	-	x	-
Jurisdiction	x	-	x

Addressing these challenges requires the development of specialized forensic techniques and tools designed specifically for edge and fog environments. The packet capture and subsequent analysis of these data depends on the accessibility of the network traffic, typically performed near to the source of the data. Thus, integration of approaches like [39] into network forensic processes, even if those often focus on the edge network itself, are necessary. Yet, the distribution of the devices hampers these steps and therefore the entire network forensic investigation. In addition to this, the variety of edge devices and the inherent diversity of network connections and interfaces increase the complexity. Accessing the fog devices can improve this situation, because it reduces this variety and leads to reduced data size because of previous aggregation on the communication path, but may result in incomplete captures if the communication of the edge device happens alongside the fog device directly to different communication partners. Figure 3 shows the difference between the different capture positions and the accessibility of the network traffic of the data sources.

Whereas a capture process on Position 3 captures only the traffic of one edge device, Capture position 2 is able to collect the traffic of three edge devices and the edge server itself. Capture position 1 is able to collect the majority of the network traffic, but does not see network traffic between the edge device and the server if it is not forwarded into the cloud. Network forensics in fog and edge computing also necessitate collaboration between different stakeholders to establish guidelines, standards, and legal frameworks to facilitate effective network forensic investigations in fog environments.

Despite these paths to better solutions, a number of open problems and challenges remain.

The application-centric design of edge and fog infrastructures leads to various improvements and changes in the existing network designs. A possible improvement is the installation of edge servers, each aggregating data from a smaller subset of edge devices, based on various parameters like energy [57], response time [58] or overall profit [59]. Even artificial intelligence (AI) as a state-of-the-art technique is used in the field of edge and fog computing to find the best design or to improve the installations [60,61]. Thus, the design is becoming more dynamic and unpredictable, because the decision process is blurred. As a result, the proposed improvements of tools and techniques to a distributed design is faced with a new level of possible changes and reconfigurations based on AI [26,62].

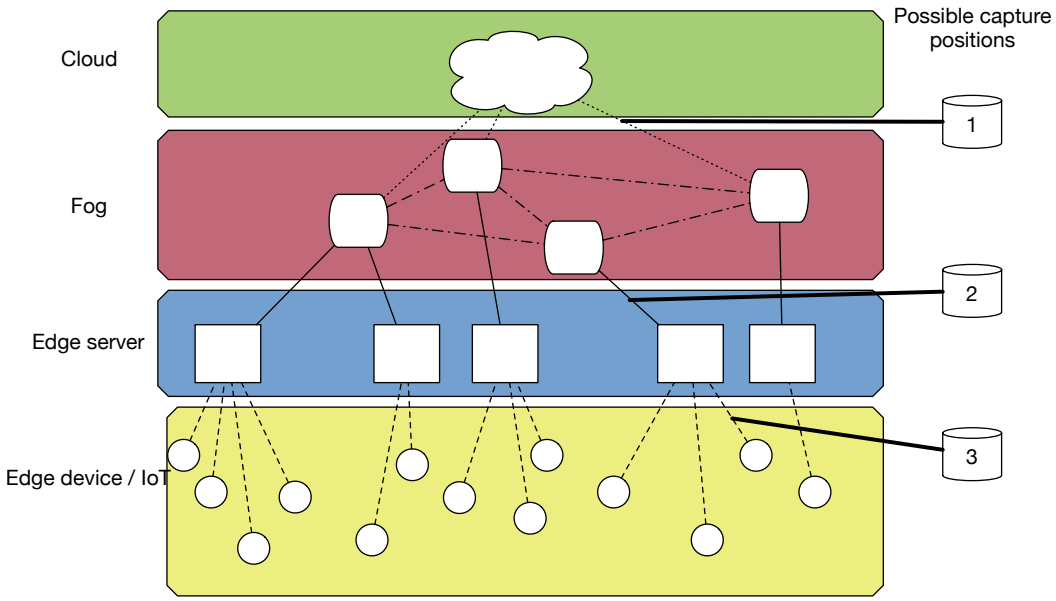

Figure 3. Capture positions and accessibility.

5. Conclusions

In this paper, we analyzed edge, fog and cloud network environments with a specific focus on network forensics. Fog and edge networks provide a relevant basis for the implementation of new applications and services. Devices on the edge side of the network collect and process data and control sensors based on these data. The correct transfer of data between the devices is a crucial task in these infrastructures. The possibility of dynamically adding and removing devices from these structures is a huge benefit, but results in new challenges for all kinds of forensic investigations. When devices are added in the network, the internal structure of the environment changes and includes the information of these new devices. A network forensic investigation focusing on the collection of the entire network traffic needs to recognize these changes to reconfigure the capture process. These techniques are known in virtual environments like clouds, but are hampered because of the variety of devices. The use of a fog network connecting fog devices to the edge devices impedes this process in a critical manner. Now, the traffic flow depends on the applications in use. Some of these do not need to send the data to the cloud; other applications might send their information via the fog devices to the cloud environment. As a result, running packet capture processes might miss relevant network packets. Processes storing the entire network communication on the devices are hampered by the low storage capacity on the devices themselves.

But not only the capture and recording phases of forensic investigations are aggravated; even the analysis of the captured packets is complicated because of the decentralized nature of these infrastructures. The captured packets need to be merged and aggregated, which is a complex task because of aspects like different jurisdiction or different time syncs inside the network. These characteristics necessitate the development of novel forensic techniques tailored specifically for the new environments.

Our method to derive the challenges is based on a software-testing approach (see Section 4), and thus, like any software engineering approach that does not use strictly formal methods as in [44], it represents the best effort without guarantee of completeness. Yet, we consider the setting of forensics in fog, edge and cloud as too complex to apply formal approaches that prove presence or absence of certain properties such as completeness of capture. Our hope is that the first author's multi-year experience in network forensics, both academically and in actual law enforcement, reduces the chances for oversight. Still, our approach should be checked and possibly amended by other research. Moreover, other approaches may be possible, such as a literature search more extensive than ours, starting

from research questions about major vulnerabilities and attacks in edge and fog networks to the influence of topology and device types on attacks and their detection. The result would be to extract as many challenges and solution approaches as possible, yet with a similar quest to categorize the findings. Finally, we could offer only pointers on ways to solve some challenges. Other researchers who are made aware of the shortcomings we reported may provide further solutions to challenges. Thus, the present article might serve to spark further research in this important field.

Author Contributions: Conceptualization, D.S. and J.K.; methodology, D.S. and J.K.; analysis, D.S.; investigation, D.S. and J.K., writing—original draft preparation, D.S. and J.K.; writing—review and editing, D.S. and J.K.; visualization, D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Davidoff, S.; Ham, J. *Network Forensics: Tracking Hackers through Cyberspace*; Prentice Hall: Hoboken, NJ, USA, 2012.
2. Spiekermann, D.; Eggendorfer, T. Challenges of network forensic investigation in virtual networks. *J. Cyber Secur. Mobil.* **2016**, *5*, 15–46. [CrossRef]
3. Kimovski, D.; Mathá, R.; Hammer, J.; Mehran, N.; Hellwagner, H.; Prodan, R. Cloud, fog, or edge: Where to compute? *IEEE Internet Comput.* **2021**, *25*, 30–36. [CrossRef]
4. Kansal, P.; Kumar, M.; Verma, O.P. Classification of resource management approaches in fog/edge paradigm and future research prospects: A systematic review. *J. Supercomput.* **2022**, *78*, 13145–13204. [CrossRef]
5. Mukherjee, M.; Shu, L.; Wang, D. Survey of fog computing: Fundamental, network applications, and research challenges. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 1826–1857. [CrossRef]
6. Garcia Lopez, P.; Montresor, A.; Epema, D.; Datta, A.; Higashino, T.; Iamnitchi, A.; Barcellos, M.; Felber, P.; Riviere, E. Edge-Centric Computing: Vision and Challenges. *SIGCOMM Comput. Commun. Rev.* **2015**, *45*, 37–42. [CrossRef]
7. Hong, C.H.; Varghese, B. Resource management in fog/edge computing: A survey on architectures, infrastructure, and algorithms. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–37. [CrossRef]
8. Pop, P.; Raagaard, M.L.; Gutierrez, M.; Steiner, W. Enabling fog computing for industrial automation through time-sensitive networking (TSN). *IEEE Commun. Stand. Mag.* **2018**, *2*, 55–61. [CrossRef]
9. Giordano, A.; Spezzano, G.; Vinci, A. Smart agents and fog computing for smart city applications. In Proceedings of the Smart Cities: First International Conference, Smart-CT 2016, Málaga, Spain, 15–17 June 2016; Proceedings 1; Springer: Berlin/Heidelberg, Germany, 2016; pp. 137–146.
10. Wei, Z.; Li, B.; Zhang, R.; Cheng, X. Contract-Based Charging Protocol for Electric Vehicles with Vehicular Fog Computing: An Integrated Charging and Computing Perspective. *IEEE Internet Things J.* **2022**, *10*, 7667–7680. [CrossRef]
11. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N. Fog computing for Healthcare 4.0 environment: Opportunities and challenges. *Comput. Electr. Eng.* **2018**, *72*, 1–13. [CrossRef]
12. Yi, S.; Li, C.; Li, Q. A survey of fog computing: Concepts, applications and issues. In Proceedings of the 2015 Workshop on Mobile Big Data, Hangzhou, China, 21 June 2015; pp. 37–42.
13. C. da Silva, R.A.; S. da Fonseca, N.L. On the location of fog nodes in fog-cloud infrastructures. *Sensors* **2019**, *19*, 2445. [CrossRef]
14. La, Q.D.; Ngo, M.V.; Dinh, T.Q.; Quek, T.Q.; Shin, H. Enabling intelligence in fog computing to achieve energy and latency reduction. *Digit. Commun. Netw.* **2019**, *5*, 3–9. [CrossRef]
15. Lee, G.; Saad, W.; Bennis, M. An online optimization framework for distributed fog network formation with minimal latency. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 2244–2258. [CrossRef]
16. Garfinkel, S. Network forensics: Tapping the internet. *IEEE Internet Comput.* **2002**, *6*, 60–66.
17. Spiekermann, D.; Keller, J.; Eggendorfer, T. Improving Lawful Interception in Virtual Datacenters. In Proceedings of the Central European Cybersecurity Conference 2018, Ljubljana, Slovenia, 15–16 November 2018; pp. 1–6.
18. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 17 August 2012; pp. 13–16.
19. Huang, C.; Lu, R.; Choo, K.R. Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges. *IEEE Commun. Mag.* **2017**, *55*, 105–111. [CrossRef]
20. Cheng, N.; Xu, W.; Shi, W.; Zhou, Y.; Lu, N.; Zhou, H.; Shen, X. Air-ground integrated mobile edge networks: Architecture, challenges, and opportunities. *IEEE Commun. Mag.* **2018**, *56*, 26–32. [CrossRef]
21. Lim, W.Y.B.; Luong, N.C.; Hoang, D.T.; Jiao, Y.; Liang, Y.C.; Yang, Q.; Niyato, D.; Miao, C. Federated Learning in Mobile Edge Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2031–2063. [CrossRef]

22. Salman, O.; Elhajj, I.; Chehab, A.; Kayssi, A. IoT survey: An SDN and fog computing perspective. *Comput. Netw.* **2018**, *143*, 221–246. [CrossRef]
23. Qaisar, S.; Riaz, N. Fog networking: An enabler for next generation internet of things. In Proceedings of the Computational Science and Its Applications—ICCSA 2016: 16th International Conference, Beijing, China, 4–7 July 2016; Proceedings, Part II 16; Springer: Berlin/Heidelberg, Germany, 2016; pp. 353–365.
24. Liu, L.; Chen, C.; Pei, Q.; Maharjan, S.; Zhang, Y. Vehicular edge computing and networking: A survey. *Mob. Netw. Appl.* **2021**, *26*, 1145–1168. [CrossRef]
25. Wang, S.; Zhang, X.; Zhang, Y.; Wang, L.; Yang, J.; Wang, W. A survey on mobile edge networks: Convergence of computing, caching and communications. *IEEE Access* **2017**, *5*, 6757–6779. [CrossRef]
26. Song, F.; Zhu, M.; Zhou, Y.; You, I.; Zhang, H. Smart Collaborative Tracking for Ubiquitous Power IoT in Edge-Cloud Interplay Domain. *IEEE Internet Things J.* **2020**, *7*, 6046–6055. [CrossRef]
27. Khan, S.; Gani, A.; Wahab, A.W.A.; Shiraz, M.; Ahmad, I. Network forensics: Review, taxonomy, and open challenges. *J. Netw. Comput. Appl.* **2016**, *66*, 214–235. [CrossRef]
28. Qureshi, S.; Tunio, S.; Akhtar, F.; Wajahat, A.; Nazir, A.; Ullah, F. Network Forensics: A Comprehensive Review of Tools and Techniques. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*. [CrossRef]
29. Wang, Y.; Uehara, T.; Sasaki, R. Fog Computing: Issues and Challenges in Security and Forensics. In Proceedings of the 39th Annual Computer Software and Applications Conference, COMPSAC Workshops 2015, Taichung, Taiwan, 1–5 July 2015; Ahamed, S.I., Chang, C.K., Chu, W.C., Crnkovic, I., Hsiung, P., Huang, G., Yang, J., Eds.; IEEE Computer Society: Washington, DC, USA, 2015; pp. 53–59. [CrossRef]
30. Tomovic, S.; Yoshigoe, K.; Maljevic, I.; Radusinovic, I. Software-defined fog network architecture for IoT. *Wirel. Pers. Commun.* **2017**, *92*, 181–196. [CrossRef]
31. Kaur, K.; Garg, S.; Aujla, G.S.; Kumar, N.; Rodrigues, J.J.; Guizani, M. Edge computing in the industrial internet of things environment: Software-defined-networks-based edge-cloud interplay. *IEEE Commun. Mag.* **2018**, *56*, 44–51. [CrossRef]
32. Sandvik, J.; Franke, K.; Abie, H.; Årnes, A. Evidence in the fog—Triage in fog computing systems. *Forensic Sci. Int. Digit. Investig.* **2023**, *44*, 301506. [CrossRef]
33. Roman, R.; Lopez, J.; Mambo, M. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.* **2018**, *78*, 680–698. [CrossRef]
34. Al-Masri, E.; Bai, Y.; Li, J. A Fog-Based Digital Forensics Investigation Framework for IoT Systems. In Proceedings of the 2018 IEEE International Conference on Smart Cloud, SmartCloud 2018, New York, NY, USA, 21–23 September 2018; pp. 196–201. [CrossRef]
35. Sedaghat, S. New approach in the applications and forensics of the networks of the internet of things based on the fog infrastructure using SDN. *Int. J. Inf. Comput. Secur.* **2021**, *15*, 272–298. [CrossRef]
36. Math, S.; Tam, P.; Kim, S. Intelligent Media Forensics and Traffic Handling Scheme in 5G Edge Networks. *Secur. Commun. Netw.* **2021**, *2021*, 5589352:1–5589352:11. [CrossRef]
37. Oriwoh, E.; Sant, P. The Forensics Edge Management System: A Concept and Design. In Proceedings of the 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, UIC/ATC 2013, Vietri sul Mare, Sorrento Peninsula, Italy, 18–21 December 2013; IEEE Computer Society: Washington, DC, USA, 2013; pp. 544–550. [CrossRef]
38. Ding, F.; Zhu, G.; Alazab, M.; Li, X.; Yu, K. Deep-Learning-Empowered Digital Forensics for Edge Consumer Electronics in 5G HetNets. *IEEE Consum. Electron. Mag.* **2022**, *11*, 42–50. [CrossRef]
39. Shalaginov, A.; Iqbal, A.; Olegård, J. IoT Digital Forensics Readiness in the Edge: A Roadmap for Acquiring Digital Evidences from Intelligent Smart Applications. In Proceedings of the Edge Computing—EDGE 2020—4th International Conference, Held as Part of the Services Conference Federation, SCF 2020, Honolulu, HI, USA, 18–20 September 2020; Proceedings; Lecture Notes in Computer Science; Katangur, A., Lin, S., Wei, J., Yang, S., Zhang, L., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; Volume 12407, pp. 1–17. [CrossRef]
40. Ovesen, A.B.; Nordmo, T.S.; Johansen, H.D.; Riegler, M.A.; Halvorsen, P.; Johansen, D. File System Support for Privacy-Preserving Analysis and Forensics in Low-Bandwidth Edge Environments. *Information* **2021**, *12*, 430. [CrossRef]
41. Esposito, C.; Castiglione, A.; Pop, F.; Choo, K.R. Challenges of Connecting Edge and Cloud Computing: A Security and Forensic Perspective. *IEEE Cloud Comput.* **2017**, *4*, 13–17. [CrossRef]
42. Chang, V.; Golightly, L.; Modesti, P.; Xu, Q.A.; Doan, L.M.T.; Hall, K.; Boddu, S.; Kobusińska, A. A Survey on Intrusion Detection Systems for Fog and Cloud Computing. *Future Internet* **2022**, *14*, 89. [CrossRef]
43. Young, M.; Pezze, M. *Software Testing and Analysis: Process, Principles and Techniques*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2005.
44. Lynch, N.A. *Distributed Algorithms*; Morgan Kaufmann: Burlington, MA, USA, 1996.
45. Pham, X.Q.; Huh, E.N. Towards task scheduling in a cloud-fog computing system. In Proceedings of the 2016 18th Asia-Pacific Network Operations and Management Symposium (APNOMS), Kanazawa, Japan, 5–7 October 2016; pp. 1–4.
46. Goudarzi, M.; Wu, H.; Palaniswami, M.; Buyya, R. An application placement technique for concurrent IoT applications in edge and fog computing environments. *IEEE Trans. Mob. Comput.* **2020**, *20*, 1298–1311. [CrossRef]

47. Badri, H.; Bahreini, T.; Grosu, D.; Yang, K. Energy-aware application placement in mobile edge computing: A stochastic optimization approach. *IEEE Trans. Parallel Distrib. Syst.* **2019**, *31*, 909–922. [CrossRef]
48. Zhu, H.; Huang, C. Availability-aware mobile edge application placement in 5G networks. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6.
49. Spiekermann, D.; Eggendorfer, T.; Keller, J. A Study of Network Forensic Investigation in Docker Environments. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; ARES '19; Association for Computing Machinery: New York, NY, USA, 2019.
50. Corey, V.; Peterman, C.; Shearin, S.; Greenberg, M.S.; Van Bokkelen, J. Network forensics analysis. *IEEE Internet Comput.* **2002**, *6*, 60–66. [CrossRef]
51. Patil, R.Y.; Devane, S.R. Network forensic investigation protocol to identify true origin of cyber crime. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 2031–2044. [CrossRef]
52. Zhang, H.; Qin, B.; Tu, T.; Guo, Z.; Gao, F.; Wen, Q. An adaptive encryption-as-a-service architecture based on fog computing for real-time substation communications. *IEEE Trans. Ind. Inform.* **2019**, *16*, 658–668. [CrossRef]
53. Papadogiannaki, E.; Ioannidis, S. A survey on encrypted network traffic analysis applications, techniques, and countermeasures. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–35. [CrossRef]
54. Wang, P.; Wang, Z.; Ye, F.; Chen, X. Bytesgan: A semi-supervised generative adversarial network for encrypted traffic classification in SDN edge gateway. *Comput. Netw.* **2021**, *200*, 108535. [CrossRef]
55. Lawal, M.A.; Shaikh, R.A.; Hassan, S.R. An anomaly mitigation framework for iot using fog computing. *Electronics* **2020**, *9*, 1565. [CrossRef]
56. Tanenbaum, A.S.; Wetherall, D. *Computer Networks*, 6th ed.; Prentice Hall: Boston, MA, USA, 2021.
57. Li, Y.; Wang, S. An Energy-Aware Edge Server Placement Algorithm in Mobile Edge Computing. In Proceedings of the 2018 IEEE International Conference on Edge Computing (EDGE), San Francisco, CA, USA, 2–7 July 2018; pp. 66–73. [CrossRef]
58. Cao, K.; Li, L.; Cui, Y.; Wei, T.; Hu, S. Exploring placement of heterogeneous edge servers for response time minimization in mobile edge-cloud computing. *IEEE Trans. Ind. Inform.* **2020**, *17*, 494–503. [CrossRef]
59. Li, Y.; Zhou, A.; Ma, X.; Wang, S. Profit-aware edge server placement. *IEEE Internet Things J.* **2021**, *9*, 55–67. [CrossRef]
60. Mao, B.; Tang, F.; Kawamoto, Y.; Kato, N. AI models for green communications towards 6G. *IEEE Commun. Surv. Tutor.* **2021**, *24*, 210–247. [CrossRef]
61. Liu, D.; Kong, H.; Luo, X.; Liu, W.; Subramaniam, R. Bringing AI to edge: From deep learning's perspective. *Neurocomputing* **2022**, *485*, 297–320. [CrossRef]
62. Hua, H.; Li, Y.; Wang, T.; Dong, N.; Li, W.; Cao, J. Edge computing with artificial intelligence: A machine learning perspective. *ACM Comput. Surv.* **2023**, *55*, 1–35. [CrossRef]