# GROUP ASSIGNMENT

## TECHNOLOGY PARK MALAYSIA

## CT113-3-M-ADF

## ADVANCED DIGITAL FORENSICS

**HAND OUT DATE: 21 November 2024**

**HAND IN DATE: 17 January 2025**

**INSTRUCTIONS TO CANDIDATES:**

1. This is a group assignment with individual component consisting of 1 Section
2. Answer **ALL** questions
3. You will be given time as specified above to complete the assignment and submit it online through Moodle
4. Please contact the module lecturer before the start of the assessment should you need any clarification

## GROUP ASSIGNMENT

| | | |
|---|---|---|
| **NAME (TP NUMBER)** | : | Koo Wai Kit (TP081761)<br>Mostafa Aldabeeb (TP079442) |
| **INTAKE CODE** | : | APUMF2406CYS |
| **MODULE TITLE** | : | Advanced Digital Forensics (102024-MSB) |
| **MODULE LECTURER** | : | Dr. Mohamed Shabbir |
| **PROJECT TITLE** | : | ADF Group Assignment (Network Forensics) |
| **DATE ASSIGNED** | : | 21 November 2024 |
| **DATE COMPLETED** | : | 14 January 2024 |

# Contents

# 1. Abstract

The context of this report is to explore network forensics in cloud environment, more specifically in the case of a newly established company that moves all its services to the cloud. In this company, the IT manager is keen on keeping track of digital activities and daily transactions for security and compliance. The report explores the basics of network forensics and covers common investigation methods, tools, technologies, and frameworks. Next, it studies the mechanism in network forensics, that is, the classification and stages of the forensic investigation, and the key challenges including the data processing constraints, technical obstacles, legal issue, and the limited resources in the analysis of this field. To address these challenges, the report offers a set of strategic solutions. Implementing these recommendations will not only help the company to build a full network forensics approach to proactive monitoring, quick response to security incidents and legal standards compliance, but also align with the IT manager's objectives of securing cloud hosted services.

# 2. Introduction

As the world goes digital in record speed, and everyone is shifting towards the use of technology, network and cloud forensics come in handy. While organisations are moving their services to the cloud, the demand to analyse and investigate digital activities and transactions has increased dramatically. The term network forensics refers to the process of accurately capturing, analysing and using network data to understand events and look for signs of illegitimate actions (ECS Infotech, 2024). Likewise, cloud forensics is concerned with the acquisition and identification of artefacts from cloud platforms, which are characterised by factors such as data dynamics and shared tenancy (Brandefense, 2024). ECS Infotech (2024) mentions that sophisticated methods and procedures in these areas are crucial for generating proper, valid, and reliable results in forensics.

The purpose of this paper is to review the current developments in network forensics and the several approaches and processes involved in the field. This study attempts to find suitable methods to address the IT manager’s concerns and to help the company in its forensic capabilities through a critical analysis and synthesis of recent articles and research findings. In this report I will focus solely on network forensics, while my teammate will cover cloud forensics in a separate report.

## 3. Network Forensics: Technical Background

Network forensics is a subcategory of digital forensics that focuses on the security and investigation of network activities in modern information technology environments. With the rise of digitization, cybercriminals have been on the rise, hence, network forensics has become an essential discipline in investigating and making sense of these security incidents. Network forensics is the process of gathering and analysing evidence from network devices during or after a cybercrime to find out the original device that was used in the offence (Patil & Devane, 2022). The main purpose of any network forensic examination is to find evidence admissible in court against the attacker. In this section, some of the basic theoretical background and definitions of network forensics are provided, its key concepts and principles are briefly described.

### 3.1 Common investigation method

Packet marking is an early technique of network forensics which embeds evidence data into packet headers. But most of these methods were reactive, intended only to be used after an attack had happened (Patil & Devane, 2022). Today, network forensic analysts examine a variety of data files to determine attack vectors to investigate network related incidents. A common method is to collect traffic by capturing network packets and storing them into full packet capture (PCAP) files (Koroniotis et al., 2020). These PCAP files can be analysed, and it can tell you if an attack occurred, with the metadata such as timestamps and sources of the attack. Sikos (2020) highlights that the reconstruction of the entire network traffic for a specified time period can be enabled by these files. PCAP files are used by forensic investigators to detect and trace malicious online activities, data breaches, unauthorised access, intrusion attempts and malware infection. They can also reconstruct transmitted files like images, documents, and emails (Sikos, 2020).

In addition, Sikos (2020) and Koroniotis et al., (2020) mention that there are two primary methods used to analyse PCAP files, which are network flow analysis and deep packet inspection (DPI). DPI is a detailed examination of the payload in each of the packets within the network to analyse the captured traffic and to provide higher accuracy in detecting the attacks of specific types (Koroniotis et al., 2020).

The network packets are useful forms of network evidence. Along with data received from remote network services, they form real time network evidence. These packets have a very constrained though extremely important time frame within which evidential data can be generated or monitored. When combined with firewall logs and other network monitoring tools, network packets are one of the most valuable pieces of evidence and are often considered one of the most concrete types of evidence an investigator can obtain. Besides, the information that is obtained from network packets can be direct evidence, such as sender or receiver IP address or port number. The packet data could also give indirect evidence, for example, patterns of large amount of ICMP packets may indicate a denial of service (DoS) attack (Sikos, 2020).

However, DPI has several limitations, including the difficulty in analysing encrypted payloads, which are increasingly popular in modern networks, and the large storage capacity needed for the amount of data it produces. Furthermore, getting payload data via DPI can trigger privacy and ethical issues related to legal laws (Koroniotis et al., 2020).

In contrast, network flow analysis gives a summarised view of network traffic, extracting essential statistical features, such as connection speeds, the volume of data exchanged and timing information. The second approach can avoid the inherent privacy issues that DPI has by not looking at packet payloads (Sikos, 2020).

### 3.2 Tools and technologies

Packet analyzers, or packet sniffers, are essential software tools for network forensics. By intercepting and logging network traffic, they are able to decode and visualise the traffic. These tools can be used for many things, including separating network traffic, rebuilding transmitted files, identifying malicious online activities and breaches, identifying the sources of network attacks, and getting host based evidence. There are many packet analyzer software packages available, some with packet analysis as the sole purpose, while others have packet capture functions as part of a more general network toolkit. Some popular packet analyzers are Wireshark, Tcpdump, Ettercap, Capsa and more (Sikos, 2020).

Network capturing tools are built to capture network data in the form that is suitable for further analysis, such as PCAP files. In promiscuous mode, these tools generally work, and they capture all traffic within a local network. In addition, PCAP files can be processed by data flow extraction tools for summary and extraction of network flows, which presents a statistical overview of network activity. The use of hashing functions like SHA-256 is also important to make sure the collected data is kept intact by generating unique digests that we will be able to compare and make sure the data has not been tampered with (Koroniotis et al., 2020). An example of data flow extraction tool is Airbyte. It is an open-source data integration platform that extracts data from multiple sources to a destination using connectors, making it effective for data flow extraction (Airbyte, 2025).

Besides, network forensics is increasingly utilising deep learning techniques for detecting and tracking anomalous events in network traffic data (Koroniotis et al., 2020).

### 3.3 Frameworks

While investigations are now covering databases, computer networks, mobile devices, Internet of Things (IoT), and the cloud, existing network forensic models and frameworks are mostly focused on traditional computer systems, such as desktops and servers. This shift makes clear the need for new models, processes, and techniques adapted to the new investigations. Also, researchers have suggested the need for a unified integrated framework that integrates different subdomain frameworks in order to address challenges across different digital forensic domains and process models (Al-Dhaqm et al., 2021).

Furthermore, most of the network forensic frameworks focus on data collection phase and neglect other important phases of forensic investigation such as data preservation, examination/analysis and presentation (Al-Dhaqm et al., 2021). However, this focus is too narrow and can result in privacy violations and increased complexity in the frameworks (Koroniotis et al., 2020).

There have been developed several specific frameworks to deal with these issues. The Particle Deep Framework (PDF) developed by Koroniotis et al. (2020) applies optimisation and deep learning to identify and track attacks in the IoT networks as well as resolve privacy concerns in deep packet inspection based on network flow data. Additionally, some frameworks that use blockchain technology for evidence acquisition include Probe-IoT, FIF-IoT and Block4Forensic. A distributed public ledger is used in Probe-IoT and FIF-IoT to improve data integrity and reduce storage requirements, and in Block4Forensic, a fragmented ledger is used for the same purpose. Additionally, one framework has been developed for monitoring traffic from smart grid networks and control stations in order to acquire evidence during investigations (Koroniotis et al., 2020).

## 4. Network Forensics: Processes, Challenges and Solutions

When it comes to the use of cloud-hosted services as the primary infrastructure of the company, network forensics serves as a means to analyse and investigate digital activities. This section presents the key practises, issues, and approaches to network forensics to meet the IT manager's concerns and achieve effective network monitoring.

## 4.1 Processes

A standard digital forensic examination involves four steps of seizing the device, acquiring the data, analysing the information, and preparing a report (Sikos, 2021). In the field of network forensics, the focus is to look at security breaches that happen in the networks with the use of logs and packets that were captured in order to determine intrusions and other malicious activities. Techniques used by the network forensic professionals involve the use of tools for collection and documentation of evidence for analysis at a later time (Koroniotis et al., 2020). Waseem et al. (2021) also highlights that network forensics is a crucial part of securing network-based streaming data by monitoring, preventing, and diagnosing security incidents through network traffic surveillance and analysis for data breach and abuse scenarios.

### *4.1.1 Classification of Investigation*

Using network forensics can be classified according to the time of investigations and the technique of data processing, and it has its strengths and weaknesses. These categories are crucial for the IT manager concerned with monitoring digital activities in a cloud-hosted context to determine which approach to use.

One classification is based on the timing of the investigation. Online or live network forensics are the process of analyzing a running event as it progresses. This method proves most effective on large networks like cloud since it provides real-time response to security threats. On the other hand, offline network forensics involve the collection and storage of network information for processing after an occurrence of a network security breach. (Waseem et al., 2021).

The other classification is done based on the data processing mode. Proactive network forensics entails the use of automated tools for investigations at real time, thus helping to identify threats early and avoid situations where the attackers delete evidence. This is especially useful for the specific company involved as it guarantees steady scrutiny of the cloud hosted services. However, the reactive network forensics is done after the event in order to determine the source of problem. This approach is used to study the collected evidence for the purpose of recognising the threats and getting an understanding of the attack (Waseem et al., 2021). In relation to the IT manager's goals, integration of proactive forensics together with real-time monitoring tools would be beneficial in ensuring the security of cloud services with the use of reactive methods in gaining better understanding of any occurrences.

### *4.1.2 Stages of Investigation*

The process of network forensics consists of several critical stages:

a. **Identification**: The first stage is to identify possible sources of evidence. Some of the tools and techniques used by network forensic includes the tools for efficient gathering and preserving the evidence before analysis (Koroniotis et al., 2020).
b. **Collection**: The second stage is data collection after the evidence sources have been defined. This is usually achieved through the employment of tools used to sniff the network. Software like Wireshark, Tcpdump and Ettercap are used to analyze the data packets from the specific network in question (Koroniotis et al., 2020).
c. **Preservation**: It is important to maintain data collected integrity. This stage involves management of data and also usage of measures that will ensure that the data cannot be altered. One of the enforcement techniques is the use of hashes like SHA-256 as a way of getting unique identification for data. Such fingerprints act as a cheque mark to authenticate that the data has not been tampered with (Koroniotis et al., 2020).
d. **Examination**: The examination phase concentrates on analysing the gathered information in order to identify relevant information. To locate flow data, programmes such as Bro and Argus can be used to synopsize and crawl through packet capture files to find useful information (Koroniotis et al., 2020).
e. **Analysis**: The next step that follows when evidence has been identified and retrieved, is to assess the evidence for information that would be relevant to the cybercrime. This phase may include simple activities like analysing log files up to complex methods of the construction of the actions of the attacker. One of the most effective tools for this stage is a deep neural network (DNN) since DNN is capable of learning patterns of network traffic generally related with attacks. This is particularly done with the use of the particle swarm optimization (PSO) algorithm which selects the best hyperparameters for the DNN. After the training of the DNN, it can effectively distinguish normal traffic and malicious traffic (Koroniotis et al., 2020).
f. **Presentation**: The last step of the investigation process is the ability to present the results of the investigation in the best possible manner. This could include writing a report, giving a presentation or being part of a witness stand in legal proceedings.

There is always a concern for privacy at this stage and it is important to draught the report in a way that best presents the evidence gathered and the analysis done in reaching the conclusions (Koroniotis et al., 2020).

However, Koroniotis et al. (2020) highlights that it is important to note that those phases are not always sequential, as investigators might return to the previous phases if needed. For example, during examination, some possibilities for further evidence may be found, which need to be collected. Also, the steps that are required to be performed in each phase can be different based on the type of crime and the amount of resources the investigator has at his disposal.

In addition, there is a strong connection between network forensics and other subfields of digital forensics, including database, mobile, and IoT that are crucial to investigations. For instance, an attacker can compromise an organization's database by using a connected mobile device and later use an IoT device to conduct a DoS attack. In such cases, the investigators need to have knowledge in all three subdomains in order to collect and analyse the evidence (Al-Dhaqm et al., 2021).

When it comes to cloud services of the newly formed company, the introduction of a well-coordinated network forensic procedure will enable the IT manager to track various digital activities and transactions, so as to identify and respond to threats as soon as possible. Therefore, realising the connections between network forensics and other digital forensics subfields allows the company to strengthen its security in various devices and systems.

## 4.2 Challenges

### *4.2.1 Challenges from investigation timing and data processing mode*

For live network forensics, it is impossible to analyse a large number of real-time data produced by cloud services because it requires enormous computing and storage. Some issues related to the offline network forensics include the storage problem or even be overwhelmed with data that are frequently used, particularly in systems that have high turnover of data as it is in cloud-based systems. Additionally, proactive network forensics usually involves extensive computation and storage resources and space. Conversely, the success of reactive network forensics is directly proportional to the type and usefulness of information collected when the investigation is ongoing (Waseem et al., 2021).

### *4.2.2 Technical challenges*

There are a number of technical issues that affect network forensics, and these are likely to slow down investigations. One major challenge is the sheer volume and complexity of network data (Waseem et al., 2021). Processing big data can be computationally and time expensive, and the IoT network is made of a broad range of devices, operating systems, and communication standards (Al-Dhaqm et al., 2021). For investigative use, specialised tools have to be used to effectively process and analyse such large and disparate data sets for forensic analysis (Patil & Devane, 2022).

Another important factor to consider is data integrity. Maintaining the accuracy of network data is critical to investigation quality, while network data, especially in off-line cases where it is acquired post the event, is prone to alteration or deletion. Sometimes, there are no ways to cheque the reliability of data received from some sources, for instance, ISP logs (Patil & Devane, 2022). Moreover, Patil and Devane (2022) also discuss the problem of defining the real origin of attacks. Standard network protocols and tools generally go up to the edge router or ISP due to their design goal of routing and security rather than investigation. This limitation stems from the lack of detail of device level information in traditional network protocols.

### *4.2.3 Legal challenges*

Legalities influence network forensics in a way that requires attention to a variety of matters that present legal complications. The first problem is the infringement of one's privacy. Network data, particularly, packet payloads are very sensitive to user privacy as most of the payloads may contain personal information. The access to such data can have unrestricted benefits which lead to ethical and legal concerns. Furthermore, methods such as DPI that may improve the identification of attacks also intensify privacy issues (Koroniotis et al., 2020).

Another important problem is the question of admissibility of evidence. To make network forensics obtained evidence admissible in a court of law, data integrity has to be achieved. Moreover, the methods of collection and analysis used must be legal to be admitted during the court trial in case needed (Patil & Devane, 2022).

### *4.2.4 Resource-related challenges*

The network forensics field faces important resource related challenges that inhibit the force and efficiency of the investigations. A major issue is the lack of cooperation from Internet Service Providers (ISPs). Information from ISPs is often the key to accurately identifying the true source of an attack. But these providers may be unwilling to give data for fear of hurting their competition or that their information is insecure (Patil & Devane, 2022).

Furthermore, investigations are complicated by the lack of standardisation in the various subdomains of network forensics. Lack of unified procedures and frameworks leads to proliferation of different and often scenario specific investigative models that do not seamlessly blend with each other (Al-Dhaqm et al., 2021).

Finally, there is a lack of tools and expertise to effectively analyse network data. Specialised tools are necessary for in depth investigations but the current market lacks advanced and comprehensive ones, especially for the newer domains such as IoT forensics. Additionally, there are not enough skilled forensic people who excel at using these tools and navigate the intricacies of the network environment (Waseem et al., 2021).

### 4.3 Solutions

#### *4.3.1 Tools proposed*

To address the challenge by the IT manager on how to monitor the digital activities and day-to-day transaction in the cloud-hosted environment, the following tools has been proposed:

a. **Wireshark (Packet Analyzer)**: Monitors and examines the communication that occurs in the network in an effort to detect improper behaviour (Sikos, 2020).
b. **Airbyte (Data Flow Extraction Tool)**: Enables quite smooth transition and consolidation of data from other sources for better and more controlled visibility (Airbyte, 2025).
c. **Particle Deep Framework (PDF)**: Ignores redundancy and dynamically employs deep learning techniques to monitor simulation and real network traffic for security and data theft risk (Koroniotis et al., 2020).

#### *4.3.2 Develop robust network forensics framework*

To improve the effectiveness of network forensics and overcome current limitations, particularly in the case of the company offering its cloud based services, it is essential to develop robust and standardised frameworks.

An alternative is to create integrated frameworks that integrate the concepts, processes and activities across different subdomains of network forensics. This allows the company to fill the gap between the lack of standardisation and to streamline investigations as well as improve collaboration between different forensic teams (Al-Dhaqm et al., 2021). This is important for the IT manager so they can monitor digital activities and transactions more efficiently to identify and respond to security incidents.

Furthermore, integration processes in different subdomains can also be harmonised to greatly improve the efficiency of data collection methods. With semantic logic integrated into these integrated approaches, the company can eliminate the redundancies and inconsistencies and make data collection procedures more efficient and applicable across different contexts (Al-Dhaqm et al., 2021). Eventually, this will give the IT manager a complete view of the network activity to prevent the company's cloud hosted services from security threats and maintain legality and ethical standards.

### *4.3.3 Enhance data acquisition and analysis process*

Data acquisition and analysis processes of the company should be improved. A major improvement is to represent network forensic data in a structured way that can help address data heterogeneity. The company can streamline the querying and aggregation of information from different sources by creating a unified data format, which makes automated analysis possible and saves the IT manager the time to monitor activities and spot anomalies in real time (Al-Dhaqm et al., 2021).

In addition, network data volume and complexity are growing and the need to manage them requires the use of new and advanced tools and techniques for understanding these data. Sophisticated solutions, such as deep learning models embodied by the Particle Deep Framework (PDF) can improve the accuracy and efficiency of attack detection (Koroniotis et al., 2020). This will allow the IT manager to respond more quickly to security incidents, which keep company cloud services secure.

In addition, organisations must implement a set of forensic readiness strategies that can help guide them towards collecting, preserving, network data in a forensically sound way. It involves setting policies on robust implementation of logging mechanisms, deployment of network monitoring tools as well as creating solid incident response procedure (Al-Dhaqm et al., 2021). Doing so allows the company to become proactive in preparing for possible security breaches and to keep evidence of those breaches in a documented and legalizable manner.

Finally, device fingerprinting techniques can be used to trace attacks to a specific device, bypassing limitations of traditional network tracing techniques (Patil & Devane, 2022). The company can develop secure protocols for the collection of device fingerprints in advance and thereby strengthen the overall cybersecurity posture, and improve the admissibility of evidence, in line with the IT manager's goals of providing secure cloud hosted services.

### *4.3.4 Address legal and privacy concerns*

In order to successfully resolve the legal and privacy challenges associated with network forensics, especially as the company provides its cloud based services, it is critical that robust strategies are implemented to address these problems.

A major solution is privacy preserving techniques like anonymization and differential privacy (Koroniotis et al., 2020). Using these techniques, the company can minimise privacy risk when accessing sensitive network data. This enables the IT manager to monitor the digital activities, while protecting user information and thereby ensuring compliance with privacy regulations and increase confidence from the stakeholders.

Furthermore, it is important to establish clear legal frameworks and guidelines for regulating data access, and evidence admissibility, and their collaboration with law enforcement agencies and ISPs. These frameworks will make it easier for the company to comply with privacy regulations and help with more effective investigations when security incidents do happen . The organization can develop a more structured legal environment to navigate the complexities of network forensics with more confidence, time to respond and mitigate potential threats, while maintaining compliance with legal obligations (Patil & Devane, 2022). Finally, this will enable the IT manager to achieve the company's security objectives in its cloud hosted services.

### *4.3.5 Foster collaboration and expertise*

Collaboration and building expertise among stakeholders are key to better utilising network forensics in the context of the company's cloud based services. Collaboration with ISPs is one important solution. This will encourage greater communication and cooperation between forensic investigators and internet service providers and can formulate clear protocols with respect to sharing data with what ISP's have concerns to data security. More timely access to critical evidence is critical in detecting and responding to potential security threats in real time, and this collaboration can result in more timely access to this critical evidence (Patil & Devane, 2022).

Furthermore, it is important to invest in training and education programs for network forensic investigators to respond to the gap in skills for this field. These programs should cover the usage of speculative software tools, the legal considerations of investigations as well as the latest technologies in the field of cloud and IoT forensics. This will enable the company to equip forensic teams with the skills and knowledge that they need to perform their duties, thereby enhancing the company investigative capabilities to conduct a prompt and effective response to any security incidents threatening the cloud hosted services of the company. Finally, this will act as an enabling condition for the IT manager's goals of keeping both security and compliance in his organisation's digital activities.

### *4.3.6 Automate forensic processes*

Machine learning and artificial intelligence can play a significant role in forensic automation speeding and accuracy of investigations . They can simplify some things such as data analysis, evidence identification, report generation, thereby minimizing the amount of human error as well as biases that will likely arise when things are manually done by humans (Al-Dhaqm et al., 2021). The company can accelerate its response to security incidents and have a more reliable analysis of digital activities in their cloud environment with automation of processes. This is in line with the IT manager's target to effectively monitor and secure the organisation's digital transactions, by offering a powerful solution for security and operational resilience.

## 5. Future Works

There is a vital need for a complete model or framework to fill the gap of standardisation in digital forensics. Such a framework would allow the field to be streamlined by integrating overlapping concepts, processes, tasks and activities. Forensic automation is another important area where it can reduce dependence on human operators and thereby minimise human error and bias. This can increase evidence reliability and expedite investigations (Al-Dhaqm et al., 2021).

Additionally, modern protocols of the network are developed with reference to the regulation of the flow through the network, and not with reference to investigation (Patil &

Devane, 2022). Future work may include the creation of improved procedures that include components that are specifically designed to support forensic data collection and analysis.

Current data acquisition methods frequently yield data that cannot be represented in an ontology based manner, and thus the ability to represent structured data is essential. A critical step in moving towards forensic automation is developing strategies to represent data in a structured way to address data heterogeneity and lack of a unified format. Furthermore, the integration of artificial intelligence (AI) can greatly improve forensic investigations with AI packet analysis that would classify advanced network traffic and find patterns (Sikos, 2020).

A further layer of security against possible threats should be incorporated in the form of advanced intrusion and prevention detection systems on the network (Waseem et al., 2021). Finally, deep learning techniques can be applied to detect, and trace cyberattacks targeting IoT networks (Koroniotis et al., 2020).

## 6. Conclusion

In conclusion, this report has thoroughly investigated network forensics, the importance of which lies in improving the security and the integrity of a company’s digital operations in general, and for a start-up that relies entirely on the cloud for services. The IT manager's worries around monitoring digital activities and day to day transactions make it important to develop a network forensics framework to address these challenges.

This report proposes the processes described to classify investigations and stages of inquiry and provide a structured approach to performing network forensics. It is extremely important as it makes timely detection and response to possible security incidents possible in order to keep the organization’s cloud services secure and reliable. Additionally, the challenges presented: from technical issues like data volume and complexities to legal and privacy concerns, make the scope of network forensics a difficult and intricate one that the company needs to manage.

This report has proposed some solutions for the company to bolster the company’s forensic capabilities like improving acquisition of data and its analysis process, collaboration with the key stakeholders such as ISPs and automated forensic processes with advanced technologies. These strategies will not only speed up investigations but also give the IT manager the tools to monitor network activities and proactively.

Moreover, the future work discussed highlights the necessity to have standardised procedures and frameworks in the field of network forensics. This investment in research and development of these frameworks paves the way for ongoing forensic work, enabling the company to build a strong base for further forensic work that will make the cloud hosted environment more resilient and secure.

Finally, based on this report's recommendations, the company will greatly increase its capabilities to control digital activities, safeguard sensitive information, and adhere to legal and ethical norms. However, this proactive approach will not only build the company's cybersecurity posture, but it will also make the stakeholders feel comfortable that the organization continues to respect the integrity and security of the cloud based services it provides.

## 7. References

Airbyte. (2025, January 7). *10 best data extraction tools to follow in 2025*. https://airbyte.com/top-etl-tools-for-sources/top-data-extraction-tools

Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Abd Razak, S., Grispos, G., Choo, K. K. R., ... & Alsewari, A. A. (2021). Digital forensics subdomains: the state of the art and future directions. *IEEE Access, 9*, 152476-152502.

Brandefense. (2024, August 5). *The future of digital forensics: trends and technologies*. https://brandefense.io/blog/drps/the-future-of-digital-forensics-trends-and-technologies/

ECS Infotech. (2024, February 20). *Exploding the code of network forensics: an extensive investigation*. https://www.ecsinfotech.com/advanced-network-forensics-techniques/

Koroniotis, N., Moustafa, N., & Sitnikova, E. (2020). A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. *Future Generation Computer Systems, 110*, 91-106.

Patil, R. Y., & Devane, S. R. (2022). Network forensic investigation protocol to identify true origin of cyber crime. *Journal of King Saud University-Computer and Information Sciences, 34*(5), 2031-2044.

Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation, 32*, 200892.

Sikos, L. F. (2021). AI in digital forensics: Ontology engineering for cybercrime investigations. *Wiley Interdisciplinary Reviews: Forensic Science, 3*(3), e1394.

Waseem, Q., Alshamrani, S. S., Nisar, K., Wan Din, W. I. S., & Alghamdi, A. S. (2021). Future technology: Software-defined network (SDN) forensic. *Symmetry*, *13*(5), 767.

**Word count:** 4859