future internet

MDPI

Article

Towards a Comprehensive Metaverse Forensic Framework Based on Technology Task Fit Model

Amna AlMutawa [1,†,‡], Richard Adeyemi Ikuesan [2,*,‡] and Huwida Said [1,‡]

[1] College of Technological Innovation, Zayed University, Abu Dhabi P.O. Box 144534, United Arab Emirates; m80008588@zu.ac.ae (A.A.); huwida.said@zu.ac.ae (H.S.)
[2] College of Interdisciplinary Studies, Zayed University, Abu Dhabi P.O. Box 144534, United Arab Emirates
* Correspondence: richard.ikuesan@zu.ac.ae
† Current address: Digital Evidence Department, Dubai Police, Dubai P.O. Box 1492, United Arab Emirates.
‡ These authors contributed equally to this work.

Abstract: This article introduces a robust metaverse forensic framework designed to facilitate the investigation of cybercrime within the dynamic and complex digital metaverse. In response to the growing potential for nefarious activities in this technological landscape, the framework is meticulously developed and aligned with international standardization, ensuring a comprehensive, reliable, and flexible approach to forensic investigations. Comprising seven distinct phases, including a crucial incident pre-response phase, the framework offers a detailed step-by-step guide that can be readily applied to any virtualized platform. Unlike previous studies that have primarily adapted the existing digital forensic methodologies, this proposed framework fills a critical research gap by providing a proactive and granular investigative process. The approach goes beyond mere adaptation, ensuring a comprehensive strategy that addresses the unique challenges posed by the metaverse environment. The seven phases cover a spectrum of forensic investigation, offering a thorough interpretation with careful consideration of real-life metaverse forensic scenarios. To validate its effectiveness, the proposed framework undergoes a rigorous evaluation against the appropriate ISO/IEC standards. Additionally, metaverse expert reviews, based on the task–technology fit theory, contribute valuable insights. The overall assessment confirms the framework's adherence to forensic standards, making it a reliable guide for investigators navigating the complexities of cybercrime in the metaverse. This comprehensive metaverse forensic framework provides investigators with a detailed and adaptable tool to address a wide range of cybercrime incidents within the evolving virtualized landscape. Furthermore, its stepwise guidance ensures a thorough and reliable investigation process, offering significant contributions to proactive security measures in the face of emerging challenges in the metaverse.

Keywords: metaverse; digital forensic framework; forensic readiness

Citation: AlMutawa, A.; Ikuesan, R.A.; Said, H. Towards a Comprehensive Metaverse Forensic Framework Based on Technology Task Fit Model. *Future Internet* **2024**, *16*, 437. https://doi.org/10.3390/fi16120437

Academic Editors: Peiying Zhang, Haotong Cao and Keping Yu

Received: 16 May 2024
Revised: 20 September 2024
Accepted: 25 September 2024
Published: 22 November 2024

1. Introduction

The metaverse is an emerging technology that represents the future iteration of the Internet, where the boundary between the virtual and real worlds becomes increasingly indistinct. It allows users to carry out real-world tasks virtually. With its foundation in the field of human-computer interaction, it has extended into a complex network of virtual environments, with a focus on business, education, and healthcare. In the context of education, the metaverse provides a virtual learning environment where students may engage in innovative educational scenarios and cooperative learning. Additionally, it benefits businesses by opening new channels for interaction, communication, and trade. This innovative concept introduces unique features like avatars, persistence, and continuous connectivity within virtual spaces without the need for physical, real-world movement. With applications spanning a wide range of fields, including social interactions and education, the metaverse has the potential to transform digital interactions completely. It is

made possible by 3D virtual worlds and augmented reality. The metaverse is generating excitement despite being in its early phases of development because of its vast potential. It promises to completely transform the way we connect with technology and with one another, whether it is for social interactions, work, education, or gaming. Its uses will probably grow more varied and complex as it develops, and the metaverse will play a significant role in our digital future.

As with any new technology, there are also unknown risks and challenges. In the metaverse, numerous cybercrimes pose significant concerns, including virtual property theft, where cybercriminals steal virtual assets acquired through gaming or purchases, often through hacking, phishing, or deceptive apps. Identity theft is another widespread issue, with cybercriminals using stolen login credentials or personal data to impersonate users or create fraudulent accounts [1]. Furthermore, the virtual world presents an ideal environment for cybercrime perpetuation. For example, phishing, cyberbullying, and online harassment have been reported in the literature [1,2]. These crime types necessitate the need for security capacity such as event blocking and reporting, as well as user education. Other common forms of crime within the metaverse include financial fraud, cyberextortion, and impersonation. Financial fraud encompasses a range of fraudulent online activities, such as phishing scams and credit card fraud, to obtain money or sensitive financial information. Cyberextortion crimes, which frequently employ strategies like ransomware assaults or distributed denial-of-service (DDoS) attacks, entail utilizing digital methods to extort money or assets from people or organizations. These cybercrimes highlight the need for robust cybersecurity measures in the metaverse [2].

Individuals and organizations must work together to reduce the danger of cybercrime in the metaverse. To begin, users must be educated about cybercrime threats, emphasizing the significance of strong passwords, multi-factor authentication, and caution while downloading virtual products and services. To protect users and their data, organizations must establish robust security measures such as strong authentication systems, data encryption, and thorough surveillance for suspicious activity. Furthermore, combating metaverse cybercrime requires a collective strategy. To combat this growing threat, law enforcement experts and business stakeholders should work together. Sharing intelligence, creating new investigation tools and procedures adapted to the metaverse, and prosecuting cybercriminals are all critical steps in establishing a secure virtual environment.

Different data sources and formats present unique obstacles for digital forensics in the metaverse when compared to traditional digital forensics (as summarized in Table 1). The decentralized nature of metaverse data, which are spread over a network of servers and devices, makes it more difficult to gather and preserve evidence than in traditional systems. Furthermore, the metaverse produces new kinds of data, such as chat logs, motion capture data, and 3D models, which calls for the creation of specific analytic tools and methods. Another significant difference is jurisdictional concerns. Crimes that happen in the metaverse could cross geographical boundaries, creating difficult moral and legal dilemmas over which jurisdiction has the right to conduct investigations. Furthermore, privacy considerations are paramount in the metaverse, where users may disclose sensitive personal information. Balancing the need for digital forensics investigations with user privacy protection is a crucial aspect that investigators must navigate. Forensic investigators face significant obstacles due to the volatility of data within the metaverse. The data constantly change as users interact with the virtual world, making the collection and preservation of evidence a dynamic process. Furthermore, the continuous evolution of the metaverse adds complexity by evolving data formats and protocols, creating difficulties in establishing dependable tools and techniques for analysis. As the metaverse expands, it is more important than ever to develop new innovative techniques for digital forensics. By tackling the difficulties brought on by decentralized data, changing formats, complex jurisdictional, and the constantly changing nature of user interactions in this new digital environment, these strategies seek to maintain the safety and security of the virtual world.

Table 1. Difference between digital forensics in the metaverse vs. the real world.

Feature	Metaverse	Real World
Data sources	Distributed, Diverse	Localized, Centralized
Data formats	3D Models, Motion Capture, Chat Logs	Files, Documents, Images
Jurisdiction	Complex, International	Clear, National
Privacy considerations	High	Moderate
Data volatility	High, Associated with real-time updates and interactions	Low, Available when stored

The current approaches to forensic investigation in the metaverse involve a comprehensive framework consisting of distinct phases. Data collection is a common phase. It involves the identification of possible sources of evidence and the gathering of information from users, services, and metaverse platform domains. Case-specific forensic data are extracted during the subsequent inspection and retrieval phase, overcoming any challenges posed by encryption, encoding, or compression. The analysis phase is similar to traditional forensic procedures in that it involves examining artifacts to make case-specific judgments that may be adjusted according to the specifics of the meta-crime. Further information is obtained through correlation studies, and conclusions are provided in the reporting phase, considering the difficulty of transforming 3D data into a 2D format that is acceptable to courts [3]. As shown in Table 1, the metaverse offers complexity in jurisdictional claims, as well as high volatility of digital instances. These inherent characteristics present a rather complicated investigation process that the traditional forensic framework cannot address.

A novel forensic framework is, therefore, needed to guide investigators in investigating cybercrime in the metaverse. This framework should provide investigators with a structured and systematic approach for collecting and analyzing evidence in the metaverse. The framework should also be flexible enough to adapt to the evolving nature of cybercrime in the metaverse. A forensic framework for investigating cybercrime in the metaverse will help to improve the ability of law enforcement to investigate and prosecute cybercrime in the metaverse. It will also help to protect victims of cybercrime and deter cybercrime in the metaverse. There are currently not many forensic frameworks available to investigate cybercrimes in the metaverse. This is a problem because it can make it difficult for law enforcement and investigators to gather evidence and track down attackers. This paper proposes a new forensic framework for investigating cybercrime in the metaverse. The forensic framework is designed to be flexible and adaptable to different scenarios of attacks on a variety of metaverse platforms and devices.

1.1. Problem Background

The fast rise and adoption of metaverse platforms has created a new digital ecosystem with its own set of problems and risks. As this virtual world grows more interconnected in our daily lives and business activities, the requirement for an efficient structure for managing and responding to metaverse incidents becomes crucial. Incidents in the metaverse cover a wide range of concerns, including digital crimes, data breaches, virtual asset theft, and security breaches. These crimes might have profound effects, impacting not just individual users but also businesses and organizations working in the metaverse.

Creating a complete framework for metaverse incidents is critical and offers various advantages. These benefits include more effective incident response, more clarity in dealing with legal and compliance aspects, enhanced user protection, more remarkable economic growth, and the formation of best practices within the metaverse community. To summarize, developing such a framework is critical for addressing growing difficulties and ensuring the metaverse's secure and sustainable development. This paper aims to develop a comprehensive forensic framework for investigating cybercrime in the metaverse, addressing the unique challenges presented by virtual reality environments, and enhancing digital forensic investigators' capabilities as well as assisting them in effectively combating

cybercrime within virtual reality environments. This study, therefore, contributes to the literature in the following ways:

- Framework Development: Creation of an organized forensic framework customized to the metaverse, including criteria for digital evidence identification, preservation, and analysis;
- Survey Design and Distribution: Design and distribution of a survey to digital forensic investigators to gather their expert insight, opinion, and recommendations on the built metaverse forensic framework;
- Data Collection: Gathering of data, opinions, and expertise from digital forensic investigators on the proposed framework's practicability, relevance, and potential improvements;
- Analysis of Survey Results: Analysis of the survey results to gain an understanding of the challenges and requirements in metaverse cybercrime investigations.
- Framework Refinement: Refinement of the forensic framework based on the survey findings and analysis, ensuring that the metaverse forensic framework matches the requirements and expectations of digital forensic specialists.

1.2. Related Works and Theoretical Underpinning

This section provides insight into some related works and the theoretical justification for this study, which is further structured as follows:

- In Section 1.2.1, headed 'Cybercrime in Virtual world', this study looks at cybercrime in virtual environments. This section provides information about the nature of these digital crimes, how they work, the vulnerabilities they exploit, and the research-based solutions developed to address them;
- Section 1.2.2, titled 'Network Forensic Investigation Techniques', looks into several approaches used for researching network-based occurrences, emphasizing their importance in dealing with cyber threats;
- Section 1.2.3 of this manuscript concentrates on the 'Role of ISO Standards in Network Investigation', with a detailed comparison of ISO 27037 [4] and ISO 27043 [5]. This section emphasizes the unique properties of these standards as well as their importance in network investigations and forensic readiness;
- Section 1.2.4, 'Metaverse Framework Development', details the early efforts to create a framework for metaverse digital forensic investigations. It emphasizes the issues of this virtual world, highlighting the necessity for specific frameworks and approaches;
- Section 1.2.5, 'Comparison Between Framework Evaluation Approaches', investigates the existing approaches for assessing forensic investigative frameworks. This research investigates the advantages and disadvantages of several assessment methods, providing valuable insights for improving the effectiveness and efficiency of forensic investigations.

1.2.1. Cybercrime in the Virtual World

Unauthorized acquisition or theft of an individual's or organization's informational assets is referred to as virtual property theft. This includes illegally purchasing products from social media applications, online accounts, bitcoin, digital real estate, and intellectual property from people or businesses in the virtual world. This may happen in several ways. Still, those that are most common include using vulnerabilities in online applications, gaining access to user accounts without authorization, and tampering with in-app features to obtain unfair advantages. This crime takes advantage of vulnerabilities in the virtual platforms' security infrastructure, as well as users' trust in the safety of these settings. To address this risk, researchers have explored many mechanisms, such as blockchain technology. They are using multiple solutions to minimize it, such as hardening apps, using strong usernames/passwords and multifactor authentication (MFA), and providing transparent and secure ownership records for virtual assets [1].

In the metaverse, cyberbullying refers to the intentional and persistent use of online gaming consoles, social media, and virtual environments to harass, threaten, or harm others. This type of bullying takes advantage of people's vulnerability in online environments

where an in-person connection is absent, allowing offenders to engage in harmful behavior and remain anonymous. Cyberbullying is a broad term that includes a variety of behaviors [6], many of which take place online and involve hate speech, exclusion, impersonation, spreading false information, and direct harassment. It makes use of the long-lasting effects of digital information and the possibility of a large audience causing emotional distress and harm to victims. Various tactics, such as education and awareness campaigns, social media campaigns, in-game events, policies and procedures, parental participation, and digital health interventions, can be used to reduce cyberbullying [7].

Phishing is a prevalent cybercrime that entails the use of deceptive techniques to trick individuals into revealing critical information, such as login credentials. It can occur through various means, including email, instant messaging, and social media. Cybercriminals may disguise phishing attacks as messages from reliable sources, including administrators of virtual worlds or other users so that cybercriminals can obtain a user's virtual assets or even their actual financial information. There are several ways to carry out phishing attacks in the metaverse [8,9]. Cybercriminals may pose as genuine sources in emails or messages they send, requesting people to provide personal information or their login credentials. They could even make fake applications or web pages that seem like reliable platforms in an attempt to deceive users into giving vital data. Cybercriminals may also employ social engineering techniques to win over a user's trust before tricking them into disclosing their login passwords or other private information. Researchers and cybersecurity specialists advise using two-factor authentication, practicing safe surfing techniques when in virtual environments, and educating users to spot phishing efforts as ways to combat this [2].

Money laundering develops as a significant threat in the metaverse, adopting approaches such as the use of virtual currencies and anonymous payment channels for increased anonymity and lower detection rates. Criminals use these tactics to create many accounts and conduct financial transactions using stolen credit card information or prepaid gift cards, complicating the monitoring of fund origins. Virtual banks or in-world investment funds provide another avenue for criminals to deposit large sums and transfer funds to real-world banks; however, evolving terms of service in certain virtual worlds now require proof of government registration or financial institution charter, adding to the challenges of illicit banking services. Despite the anonymity provided by metaverse money laundering, there are drawbacks, such as possible financial constraints and the complexity of setting up accounts and transactions. Without proper protections, detection risks loom, emphasizing the need for regulatory measures that reflect reality. Collaboration between law enforcement and service providers is essential for the adoption of systems that detect suspicious activities suggestive of money laundering or terrorism funding. This issue is prevalent in massively online games (MOGs), which are online video games that accommodate many people and frequently feature persistent areas where interactions take place. Examples include Second Life, World of Warcraft, and Entropia Universe. Online financial service providers (OFSPs) within MOGs facilitate financial services, enabling players to trade virtual currencies or credits and offering functions like fund transfers and currency conversion [10]. A summary of these crimes, highlighting the weakness often exploited and potential research direction, is provided in Table 2. These crimes in the metaverse bother around the networks, the Internet, and physical devices. One area often associated with investigating such categories of crimes is network forensics. This is further presented in the next section.

Table 2. Summary of cybercrimes.

Crime Type	Description	Exploitation	Suggested Research Direction
Virtual Property Theft	Unauthorized acquisition of digital assets.	Security vulnerabilities, trust.	Blockchain technology, security.
Cyberbullying	Harassment in VR spaces	Anonymity, lack of moderation.	Content moderation, user education.
Phishing	Attempts to scam individuals into stealing their credentials and other information.	Human nature, Lack of security of controls.	Training and awareness of users, Implementation of rigorous controls (two-factor authentication)
Money laundering	Making illegally obtained money appear legitimate by disguising its true origin.	Anonymity and lack of regulation in the metaverse.	Metaverse service providers should implement detection systems for suspicious transactions.

1.2.2. Network Forensic Investigation Techniques

To investigate and evaluate network incidents and security breaches, network forensic techniques are employed [11,12]. These methods concentrate on detecting, collecting, and analyzing network data to recreate the sequence of security events. By detecting network weaknesses and communication channels, they aid in the tracking of internal and external network assaults. One strategy in network forensics is to record every packet and event that travels across the network. This enables the reconstruction of the recorded data to identify the source of the attack [1]. Other methods include packet sniffing: Packet sniffers, such as Ethereal, may collect and analyze data sent between computers on a network. These tools enable forensic investigators to gain insight into the hidden information in the various headers of the TCP/IP protocol stack, assisting them in gathering important information from packets. Furthermore, IP traceback techniques help forensic investigators determine the natural origins of attacking IP packets. These approaches enable victims to discover the network pathways taken by attack traffic without the need for assistance from Internet service providers (ISPs). Techniques such as packet marking can be used to reliably establish the origin of an Internet packet [2].

1.2.3. The Role of ISO Standards in Network Investigation

Network incidents, ranging from data breaches to cyber attacks, pose a significant threat to organizations and individuals. To effectively respond to these threats, the research systematically highlights the essential role of investigative techniques [13]. Such practices can detect malicious activity, attribute attacks, and close security vulnerabilities. However, these investigations are not without difficulties. One of the main problems is the lack of standardization and consistency [14]. Each analysis is unique, making it difficult to establish consistent procedures and protocols. This variability can complicate the reliability of forensic findings and the admissibility of evidence in court proceedings. Moreover, the authors in [15] strongly emphasize the importance of creating standards for the metaverse to make its technology better. Led by the Khronos Group, the Metaverse Standards Forum, which includes big companies like Google and Meta, is working on making rules for important technical things like 3D objects, how users interact, and the standards for augmented and virtual reality. Because metaverse technology is quite complex, it is important to coordinate and work together, and having standards is key to making sure everything works well and smoothly for users on different platforms. Prioritizing open standards is crucial to preventing fragmentation. Furthermore, to meet these challenges, international standards have been developed to guide investigators. The International Organization for Standardization (ISO) has introduced ISO/IEC 27037, a standard specifically designed to facilitate the collection and preservation of digital evidence [16] ISO standards provide a structured framework that increases the credibility of forensic findings [17]. They help ensure that investigations comply with established best practices and methods.

The ISO standards in the area of network investigations serve as a model for consistency and reliability. In particular, ISO/IEC 27037 [4] provides investigators with a roadmap for the standardized conduct of forensic investigations. By adhering to these standards, investigators can ensure the credibility of their findings and the admissibility of evidence in court proceedings. These standards define best practices for collecting, protecting, and analyzing evidence. They highlight the importance of maintaining the integrity and authenticity of digital evidence, an essential aspect of any forensic investigation. ISO standards help bridge the gap between the ever-changing cyber threat landscape and the need for consistent investigative procedures. However, the adoption of ISO standards in network forensic investigations is not without complexities and challenges [18] Although these standards offer many benefits, researchers must overcome potential obstacles, including resource limitations and the need for specialized training. In [19–21], the authors suggested an IoT framework based on ISO/IEC 27043 [5], emphasizing the significance of the ISO/IEC 27043 standard for the readiness framework since it offers a standardized approach to digital forensic readiness (DFR) procedures. It provides rules and best practices for digital investigation planning, implementation, assessment, and concurrent operations. The ISO/IEC 27043 standard guarantees that relevant and meaningful forensic data are collected and maintained in a manner that can be used throughout an investigation. It also eliminates business interruptions, lowers investigative costs, and saves time by predefining, executing, and improving processes before an incident happens. The standard highlights the need to conduct readiness processes using standardized methods, which is a critical component for effective DFR. A comparative analysis of the contextual application of both standards is further presented in Table 3.

Table 3. Comparison between ISO/IEC 27043 and 27037.

Feature	ISO 27037	ISO 27043
Focus	Collection and preservation of digital evidence	Investigation of digital incidents: integrating the pre-incident component
Audience	Organizations that need to collect and preserve digital evidence for legal or investigative purposes	Organizations that need to investigate and respond to digital incidents
Scope	Provides guidelines for the identification, collection, acquisition, and preservation of digital evidence	Provides guidelines for the investigation of digital incidents, including planning, preparation, response, and recovery

1.2.4. Metaverse Framework

The fast-developing metaverse, which is gaining popularity among consumers and companies, also raises the possibility of criminal activity. In response, researchers developed a customized digital forensic investigation framework with four primary phases based on the National Institute of Standards and Technology (NIST) standard [22], which provides a widely used digital forensics framework. This framework is divided into four phases: data collection, evidence assessment and retrieval, analysis, and reporting. It is intended to be used as a guide for performing digital forensic investigations [3]. The framework is relevant to a variety of domains, including the metaverse, and assists investigators in successfully planning and executing their investigations. The data collection phase begins with the systematic gathering of relevant data from the metaverse and the actual world, which are carefully organized into the user domain, service domain, and metaverse platform domain. Following that is the examination and retrieval of evidence phase, in which investigators thoroughly examine and retrieve evidence, ensuring its proper preservation across all relevant domains. Following that, in the analysis phase, investigators look extensively into the gathered information, seeking insights and patterns to better understand the nature of the problem and identify the responsible parties. Finally, the reporting phase concludes with the production of a thorough investigation report, which combines data and evidence, facilitates contact with stakeholders, and lays out the basis for any legal proceedings.

These four phases are supplemented by three essential domains: the user domain, which focuses on user actions and interactions with technologies such as XR and sensors; the service domain, which includes various metaverse services such as e-commerce and cryptocurrency; and the metaverse platform domain, which is in charge of metaverse operation and management using technologies such as blockchain and AI [3]. This comprehensive approach solves the particular issues of digital forensic investigations in the complex metaverse environment, guaranteeing effective evidence collection and analysis while protecting data integrity and security. This rigorous investigational division across stages and domains solves the particular obstacles of digital forensic investigations inside the metaverse, enabling compelling evidence collecting and processing. However, the lack of forensic readiness and the inability to ensure the forensic soundness of the investigator's process presents a major limitation of the study.

Another framework was proposed by [23] to retrieve forensically significant data from IoT systems based on service interconnectivity. It proposes a service-interconnectivity-based forensic framework, identifies relevant forensic evidence, and introduces a proof-of-concept application for visualizing interconnectivity. The goal of the document is to improve knowledge and examination of linked IoT ecosystems through a thorough forensic approach. It also covers IoT services and talks about research on intelligent gadgets. The creation of a proof-of-concept tool for interconnection visualization, the suggestion of a phased IoT forensic framework, and a comparison with current frameworks are important aspects. To expand the scope of the investigation, find hidden evidence, establish a chain of events, find relevant information sources, enable thorough analysis, and enable a comprehensive response to cybercrimes, it is important to identify interconnectivity in IoT systems for forensic investigations.

Other studies, like [24], proposed creating a digital forensic investigation tool that is specific to the metaverse environment. A unique tool is required since the open-source and commercial digital forensic tools now in use do not include metaverse-analysis-specific capabilities or plugins. The goal of the suggested tool is to follow user activity while collecting and analyzing artifacts from many regions of the metaverse, such as client devices, platforms, clouds, and integrated analysis. Extensibility is given top priority in design so that new artifacts may be added for a variety of metaverse environments. The tool consists of a layer that processes standard file formats, an engine for parsing and analyzing data, and plugins that handle specific data for each artifact. The tool, which was developed using Python 3 and Flask, is verified on experimental datasets and displays the findings in a web page format that includes hash values for source artifact files, an integrated timeline, and basic metadata. The work's importance stems from its ability to meet the unique digital forensic requirements of the developing metaverse environment. With the growing popularity of the metaverse, the article helps lay the groundwork for metaverse digital forensics by providing investigators with useful tools and insights. Through scenario-based research, this study confirms the suggested procedure and illustrates how it may improve digital forensic investigations in the metaverse. To close the gap in the current tools' support for metaverse investigations and to increase the effectiveness and precision of digital forensic analysis in this new sector, the creation of this specific tool is very important.

1.2.5. Framework Evaluation Models

Framework evaluation models are used to analyze framework quality, effectiveness, and usefulness. There are various types available, each with their own set of benefits and drawbacks. When choosing a model, it is essential to consider both the specific purpose of the evaluation and the elements of the framework under discussion. Taken together, these points represent the internal and external validity of a measured instrument. This section examines the differences between selected evaluation models for theoretical frameworks depending on the purpose and context. While there are several such models, the technology adoption/acceptance model (TAM), theory of planned behavior (TPB), task–technology fit

(TTF), end-user computing satisfaction (EUCS), and unified theory of acceptance and use of technology (UTAUT) are commonly used in information systems literature [25–28].

The technology acceptance model (TAM) describes how users interact with technology and institutional institutions. It is based on two significant factors: perceived ease of use and perceived usefulness. Perceived usefulness measures how much an individual believes that adopting a given system will improve their work performance, whereas perceived ease of use measures how easy it is to use the system. These characteristics have a significant impact on an individual's attitude toward system usage, which influences their intentions and actual adoption. It proposes a direct relationship between perceived usefulness and behavioral intention, emphasizing the importance of an individual's attitude in shaping their decision to accept and use a system. In addition, it has been integrated with other models, including the task–technology Fit (TTF) model, to provide a more comprehensive explanation of variations in IT utilization [29].

End-user computing happiness (EUCS) is a model for measuring user happiness with technology, with a particular emphasis on the computing and usage aspects that make up an information system. EUCS includes an overall effective evaluation of the system by end users and employs a 12-item assessment to evaluate criteria such as content, correctness, format, simplicity of use, and timeliness [29]. It is a reliable predictor of user happiness, especially in integrated systems, and provides valuable insights into the identification of problematic issues in system implementation. It is crucial to highlight that EUCS may involve longitudinal studies to capture developing attitudes over time, and there may be issues with the precision and comparability of overall user satisfaction scores. According to the model, five aspects influence user satisfaction: perceived usefulness, perceived ease of use, information quality, system quality, and service quality. EUCS, as an adaptable tool, significantly contributes to understanding and improving user satisfaction across multiple technical contexts and may be used to evaluate many sorts of technology [29].

The unified theory of acceptance and use of technology (UTAUT) is a comprehensive model that combines and extends various technology acceptance theories, aiming to understand and predict technology adoption and usage. To gain insight into users' intentions and activities, it looks into variables such as performance expectations, convenience of use, social impact, and enabling conditions. UTAUT has several applications in information systems and technology, providing insights into the factors that influence technology adoption. Despite its widespread acceptance and use, several experts have raised concerns about its practicality and theoretical assumptions [30].

The theory of planned behavior (TPB) is a psychological theory designed to elucidate and foresee human conduct. It states that people's intentions—which are further influenced by their attitudes, subjective standards, and sense of behavioral control—determine their behaviors. Subjective norms are the perceived societal pressure to engage in a behavior; attitudes are an individual's positive or negative evaluation of an activity; and perceived behavioral control is an individual's belief in their ability to carry out the behavior. According to the theory of planned conduct (TPB), intentions are the primary factor that determines behavior; people are more likely to act when they have strong intentions to act [31].

TTF is a model that focuses on the compatibility of technology with the tasks of the user [29]. The model is based on the idea that individuals are more likely to accept and use technology if it is well-suited to the tasks at hand. When evaluating the fit between a technology and the user's tasks, TTF assesses three factors: task characteristics (complexity, frequency, importance), system characteristics (features, capabilities), and individual characteristics (user skills, experience, preferences). According to TTF, a good fit between the technology and the user's tasks will result in higher levels of user acceptability and utilization [29]. A concise summary of these common models showing their potential suitability for known context is further highlighted in Table 4.

Table 4. Summary of evaluation models.

Model	Focus	Key Variables	Suitability
Technology Acceptance Model (TAM)	Perception of users on technology acceptance	Perceived usefulness, perceived ease of use, attitude, intention to use	Suitable for a wide range of contexts
End-User Computing Satisfaction (EUCS)	System quality, information quality, service quality	Perceived usefulness, perceived ease of use, information quality, system quality, service quality	Suitable for contexts where it is important to understand the factors that influence user satisfaction
Unified Theory of Acceptance and Use of Technology (UTAUT)	Perception of users on technology usage and acceptance	Performance expectancy, effort expectancy, social influence, facilitating conditions	Suitable for a wide range of contexts
Theory of Planned Behavior (TPB)	Explaining and predicting human behavior	Attitude, subjective norm, perceived behavioral control	Suitable for a wide range of contexts where human behavior is a key factor
Task–Technology Fit (TTF)	Fit between the technology and the user's tasks	Task characteristics, system characteristics, individual characteristics	Suitable for contexts where it is important to understand the fit between the technology and the user's tasks

1.3. Proposed Work

A high-level abstraction of the suggested framework, which is divided into seven related phases, is shown in Figure 1. The phases described in ISO/IEC 27043:2015 and the metaverse forensic framework, as explained by Seo et al. [3], have been strategically matched with these proposed phases. However, a detailed breakdown of the complete proposed framework is provided in Figure 2. While our suggested framework has some similarities to existing frameworks, each step provides a more in-depth method designed especially for digital investigations connected to incidents in the metaverse.The alignment to current standards guarantees a strong and uniform approach, while the distinct characteristics of every phase respond to the variety and complexity present in the metaverse environment.

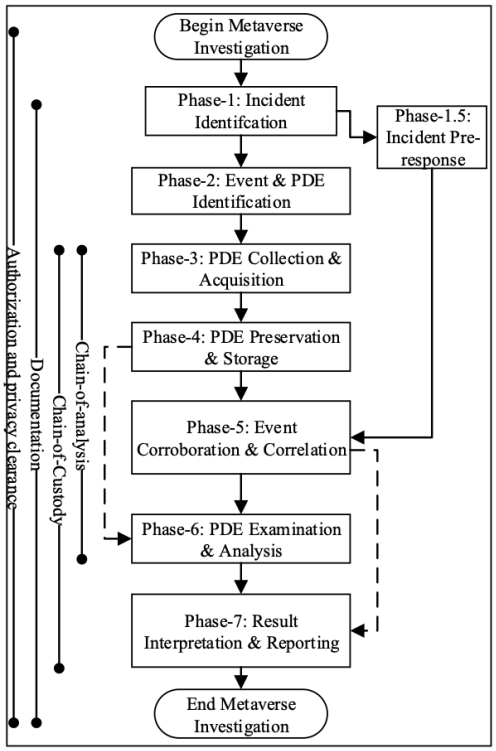

Figure 1. High Abstraction of Proposed Framework.

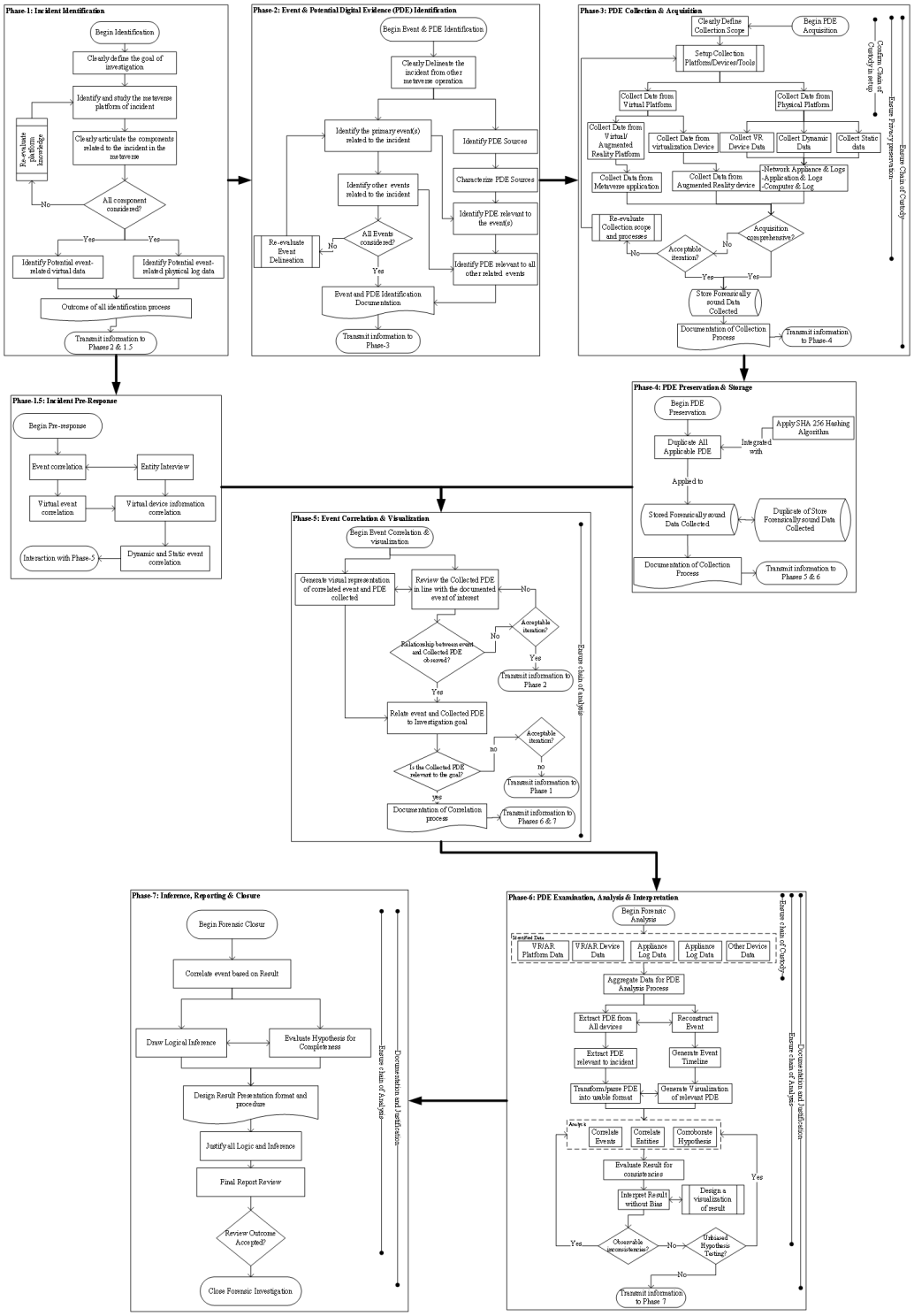

Figure 2. Proposed Metaverse Forensic Framework.

The first developed framework in [3] is meant to serve as a guide for digital forensic investigations in the metaverse. It is based on the NIST standard and has four phases: data collection, evidence assessment, analysis, and reporting. By combining three crucial domains—user, service, and metaverse platform—it methodically collects, investigates, and evaluates data to address issues in the metaverse environment. This all-inclusive strategy protects data security and integrity while guaranteeing efficient evidence gathering and analysis.

On the other hand, the proposed framework comprises seven phases and attempts to give a more comprehensive and in-depth procedure for digital investigations in the metaverse. It aligns with ISO/IEC 27043:2015 and the metaverse forensic framework mentioned in [3]. The readiness component is particularly covered by ISO/IEC 27043:2015 (as asserted in Table 3), whereas prior frameworks have placed less focus on this area. The proposed framework addresses the various and complicated characteristics of the metaverse environment while ensuring a strong and uniform approach by intentionally matching phases with defined criteria. This sophisticated approach is designed for events in the ever-changing metaverse and considers important factors like readiness that might improve the efficiency of digital investigations. The proposed framework, as detailed in Figure 2, comprises seven related main phases and a pre-response phase. An incident pre-response phase provides a mechanism for handling incidents in such a way that related events and information are documented before the main investigation. Information such as interviewing entities associated with the incident, identifying and documenting events associated with the incidents (both physical and virtual), and an initial correlation of events to ascertain the extent of the metaverse investigation are documented. The main phases of the proposed framework include:

1. **Incident identification**: This phase addresses the respective processes to follow when a security and or privacy violation is identified/reported within the metaverse for which investigation is requested.
2. **Event and potential digital evidence identification**: While the first phase addresses the process to follow to prepare for an investigation, this phase provides a guide on defining and identifying what constitutes potential digital artifacts (PDEs) within the metaverse. Within the metaverse platform, PDE preservation of volatile artifacts and non-volatile artifacts is a major focus of this phase. For example, artifacts related to users can be located in wearables (including head-mounted display units) and mobile devices. However, this would differ from common services associated with the platform. These would include the platform's logging system, the associated data center for the platform, and servers (database and logs).
3. **Collection and acquisition**: Upon identification of PDEs, this phase specifies how an investigator should acquire all identified PDEs in a forensically sound manner.
4. **Potential digital evidence preservation and storage**: This phase provides a forensically sound procedure for the preservation of all acquired and collected PDEs. This process also specifies the use of SHA-256 as the hashing algorithm, as opposed to the use of deprecated algorithms. The degree of volatility of PDE is given consideration in this phase.
5. **Event correlation and visualization**: Input to this phase includes both the incident pre-response phase and the PDE preservation phase. In this phase, an investigator is introduced to the procedure for aligning observed PDEs with the pre-response data collected (often by first responders or incident handlers).
6. **Potential digital evidence examination, analysis, and interpretation**: This phase provides a guided sequence on how an investigator can analyze PDEs extracted from a metaverse platform.
7. **Inference, reporting, and closure**: here, details on processes to make inferences and provide a forensic report on the conducted investigation are explained. An investigator would be required to ensure forensic soundness throughout this investigation process. Each phase in this proposed framework ensures documentation and verification of procedures.

This largely contrasts the benchmark framework presented in Seo et al. [3], which comprises only four phases: ***data collection, examination and evidence extraction, analysis, and reporting***. A framework should provide a procedural guide for ease of use, comparability, and repeatability. These characteristics are missing in the existing framework. Building on this baseline framework, the proposed framework provides an integral sequence and process for metaverse forensics.

2. Methods

The overall procedure followed to achieve the aim of this study is presented in this section. This includes the research design, the adapted measurement instruments, and respondents' selection criteria.

2.1. Research Design

A systematic research design is followed in the process of developing the proposed metaverse framework. The operational framework of this research design is visually represented in Figure 3 and encompasses three pivotal stages: framework development, respondent selection, and evaluation. These steps are explained in further detail below, as depicted in Figure 3.

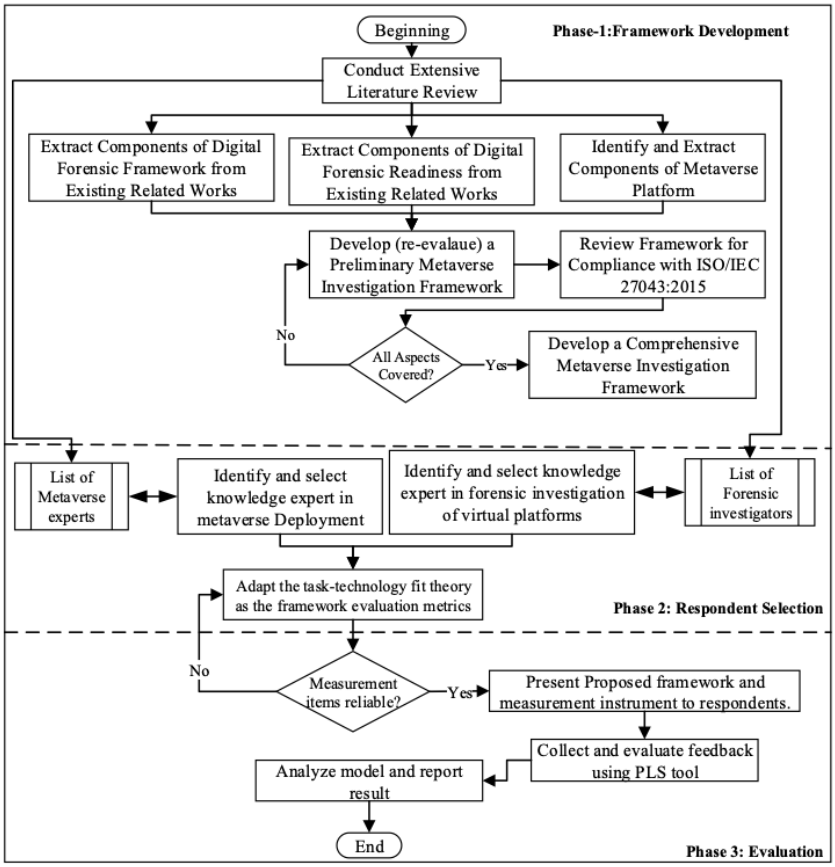

Figure 3. Operational Framework for Metaverse Forensic Framework Development.

- Phase 1: Framework Development
  Making Use of Existing Knowledge: The operational framework's initial phase depends on a wealth of current knowledge in the areas of metaverse frameworks, digital forensic readiness frameworks, and the ISO/IEC 27034:2015 standard. This phase, which deviates from traditional metaverse forensic frameworks, merges the essential components of digital forensic readiness with the complex architecture of metaverse platforms. An early investigation framework is methodically developed, beginning with implementing the ISO/IEC 27043 standard for preliminary benchmarking. A thorough framework is carefully constructed after validation of its compatibility with the existing investigative standard. It is critical to emphasize that this process is based on expert opinions and a well-planned series of investigation methods. The output of this phase is instrumental and serves as input to the subsequent Phase 3.
- Phase 2: Respondent Selection and Evaluation Metrics
  A careful selection of respondents is essential for assessing the entirely created frame-

work as highlighted in Figure 3. This involves finding potential metaverse experts, forensic researchers, and forensic practitioners, particularly those with experience in virtual forensics. A framework evaluation tool is thoroughly constructed after the careful selection of these qualified professionals. This instrument is based on the task–technology fit (TTF) hypothesis, which initially consisted of 16 components that give a conceptual framework for users to evaluate information systems or services within an organizational context.The structural composition of TTF, as used in this study, is presented in Figure 4.

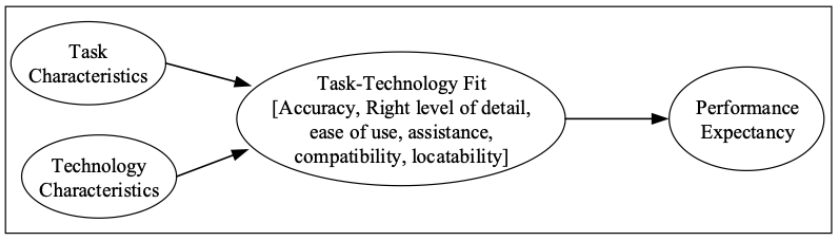

Figure 4. Theoretical Process of Model Evaluation for the Proposed Metaverse Forensics Framework.

This extensive study seeks to explore the efficacy of the proposed metaverse framework through the lens of task and technology characteristics, task–technology fit, and performance expectation variables. The following is the hypothesis of the study:

- Proposition 1: Respondents' evaluation of the fitness of the framework expressed by the TTF will be influenced by the task and technology characteristics of the metaverse platform. This proposition can be further defined as a null hypothesis of the form:

  H0: there is no statistically significant relationship between the metaverse investigation (task) characteristics (TAC) and the potential effectiveness of the proposed framework in conducting metaverse forensics

- Proposition 2: Respondents' evaluation of the TTF of the proposed framework will have significant explanatory power in predicting the performance expectancy of the proposed framework. This corresponds to the second null hypothesis, which posits the following:

  H1: there is no statistically significant relationship between the technology characteristics (TEC) of the proposed metaverse forensic framework and the actual expected effectiveness of the framework in aiding forensic practitioners in carrying out metaverse forensics.

  To elaborate on these constructs, Table 5 provides details of the measurement instruments, with a five-point Likert scale serving as the metric of evaluation. Expert reviews were used to evaluate the measurement instrument before distribution to respondents.

- Phase 3: Evaluation and Feedback

  In this critical step, the outputs from Phase 2 are combined with the results of the literature study from Phase 1. The measurement instrument and the developed metaverse investigation framework are sent to selected respondents based on preset selection criteria. The response from the selected respondents is evaluated in this phase. This evaluation considers the intrinsic relationship between the constructs with the potential of revealing causation. A partial least square structural equation modeling (PLS-SEM) approach is used to achieve this [32].

Table 5. Adapted TTF measurement Instrument.

Construct	Code	Description
Comprehensiveness (accuracy + right level of detail)	COM1	The framework contains an appropriate or adequate level of detail required to conduct a metaverse investigation.
	COM2	The framework, if followed, can generate the right and accurate detail needed to conduct a metaverse investigation.
	COM3	The respective phase of the framework provides an accurate step for investigating a metaverse platform.
Usability (ease of use + assistance)	USA1	structurally easy to follow and understand assistance)
	USA2	I can easily use this framework to conduct a metaverse investigation.
	USA3	This framework provides a relevant guide needed to conduct an effective metaverse investigation
Robustness (Compatibility + locatability)	ROB1	This framework makes it easy to know where to look for evidence in a metaverse during an investigation.
	ROB2	This framework can be applied to any metaverse platform without inconsistencies.
	ROB3	I can locate potential digital evidence within the metaverse platform using this framework.
Task Characteristics	TAC1	I sometimes deal with metaverse incidents
	TAC2	I sometimes deal with the investigation of metaverse cases
	TAC3	The metaverse is not a common investigation case within the digital forensic domain
	TAC4	Metaverse investigation involves virtual and physical platforms
	TAC5	The metaverse investigation process is not yet formalized like other digital forensic subdomains.
Technology characteristics	TEC1	A metaverse generally runs on a virtualized platform hosted on a physical device
	TEC2	The metaverse presents several opportunities for investigation
	TEC3	The metaverse presents opportunities for cybercriminals to conduct attacks
Performance expectancy	PEE1	Overall, this framework will aid me in conducting a digital investigation in the metaverse platform.
	PEE2	This framework will enhance my investigation process in the metaverse platform
	PEE3	This framework will simplify my investigation process in the metaverse platform.
	PEE4	This framework will quicken my investigation process within the metaverse platform.

2.2. Survey

An online survey was used to collect quantitative and qualitative data from a sample of digital forensic practitioners for the study. The questionnaire, which was mainly composed of quantitative measures, also included a limited number of connected open-ended questions. The participants were digital forensic investigators from the Dubai, Sharjah, and Abu Dhabi police departments. The questionnaire was held on the Questionpro survey website (https://www.questionpro.com accessed on 1 October 2023) from October 2023 till November 2023. The survey was formally sent to digital forensic professionals via an official letter developed inside Dubai Police and overseen by a high-ranking officer. An online questionnaire was used in the study to assess the efficiency of the created framework among digital forensics practitioners. The web-based survey had a total of 25 questions with an estimated response time of 10 min. The questionnaire was divided into two sections: the first collected demographic information while the second presented the created framework to participants. The second section used a 5-point Likert scale to assess the framework's perceived usability and efficacy. As shown in Table 5, this construct was examined using 21 statements that focused on distinct components of the framework, such as comprehensiveness, usability, robustness, task characteristics, technology characteristics, and performance expectancy. These were measured on a 5-point Likert scale (5 = strongly agree, 1 = strongly disagree). The last question was open-ended and aimed to obtain participants' thoughts and suggestions to improve the forensic framework.

2.3. Ethical Considerations and Ethical Approval

Pursuant to Zayed University policy, the survey and related documentation were submitted to the University Ethics Committee prior to the commencement of the survey. The Ethics Committee granted approval on 25 October 2023. The potential participants were also notified that participation was optional, that all replies were anonymized, and that all data were kept confidential in accordance with the University's study policies. Completing and submitting the survey indicated that the participants agreed to participate in the study.

3. Results and Analysis

The result of the quantitative evaluation of the proposed framework is presented in this section. It begins with a brief overview, and then a further description of the data and the analysis is given.

3.1. Overview

The Results chapter of the metaverse framework research study includes three key sections: descriptive analysis, which explores respondents' positive perspectives on clarity, usability, and effectiveness; measurement model, which ensures the validity and reliability of measurement instruments; and structural model, which provides a quantitative understanding of relationships between constructs. The chapter offers an in-depth overview of the metaverse framework by combining qualitative insights, measurement validity checks, and advanced quantitative analysis using SmartPLS version 4. The study's credibility is enhanced by the analysis and interpretation of raw data, which enrich the larger area of metaverse research by offering a comprehensive knowledge of user perceptions and the complex dynamics inside the framework.

3.2. Descriptive Analysis

To begin the analysis, this study presents descriptive statistics, which provide a synopsis of the respondents and the statistical composition of their responses. Detailed descriptive statistics are available as a Supplementary File upon request.

Demographic Information

The descriptive analysis of the 'respondents' characteristics was carried out to provide background information about the individuals who participated in the study; see Table 6. Giving demographic data on the respondent is typically implemented to obtain insight into topics that may be important for interpreting the study's findings rather than to address research questions or accomplish research objectives. Four demographic data points were considered and examined. This includes the gender, area of primary qualification, and year of experience in the field of forensics [33].

Table 6. Demographic Data of Respondents.

Demographic Items	No. of Respondents	Valid Percentage (%)
Gender:		
Male	12	33.33%
Female	24	66.67%
Other	0	0.00%
Area of primary qualification:		
Forensics expert	28	77.78%
Networking admin	0	0.00%
IT security	4	11.11%
Other	4	11.11%
Digital Investigation Experience:		
Less than 2 years	9	25.00%
2–5 years	11	30.56%
6–10 years	6	16.67%
more than 10 years	10	27.78%

The participant demographics in this study show a complex mix that provides insights into the variety of professions as shown in Table 6. First, 33.33% of the sample were made up of males, while 66.67% of the sample were female. The professional qualifications of the sample were highly diversified, with forensics skills accounting for 77.78% of qualifications, IT security qualifications accounting for 11.11%, and 'other' qualifications accounting for another 11.11%. When it came to professional experience, a clear trend could be seen: 25.00% of respondents had worked for less than 2 years, 30.56% for two to five years, 16.67% for 6 to 10 years, and 27.78% for more than 10 years. The study is enhanced by this complex demographic mosaic, which provides a more profound knowledge of viewpoints within the forensic and IT security community.

3.3. Measurement Model

As highlighted in Section 2, this study leverages structural equation modeling for the evaluation of the framework. A SEM typically uses a measurement model to evaluate the correlation and covariances among constructs and then uses a structure model to test for causation [34]. The measurement model is, therefore, the initial step in analyzing the PLS-SEM data. In measurement models, reliability analysis is taken into consideration. In carrying out the measurement model, all constructs and their corresponding measurement items were analyzed in line with the theoretical model defined in Figure 4. The final outcome of the measurement model is presented in Figure 5. It was observed that all the items in all constructs had a factor loading ≥0.5 except TAC5, with 0.292 loading. Consequently, when the item was removed, as the construct had sufficient items, an improved factor loading was observed for other items in the construct (TAC). The path coefficients among the constructs also show a significant relationship with TEC–>ROB and COM–>PEE reflecting an inverse relationship. The overall reliability metrics, further shown in Table 7, demonstrate the acceptability of the measurement model.

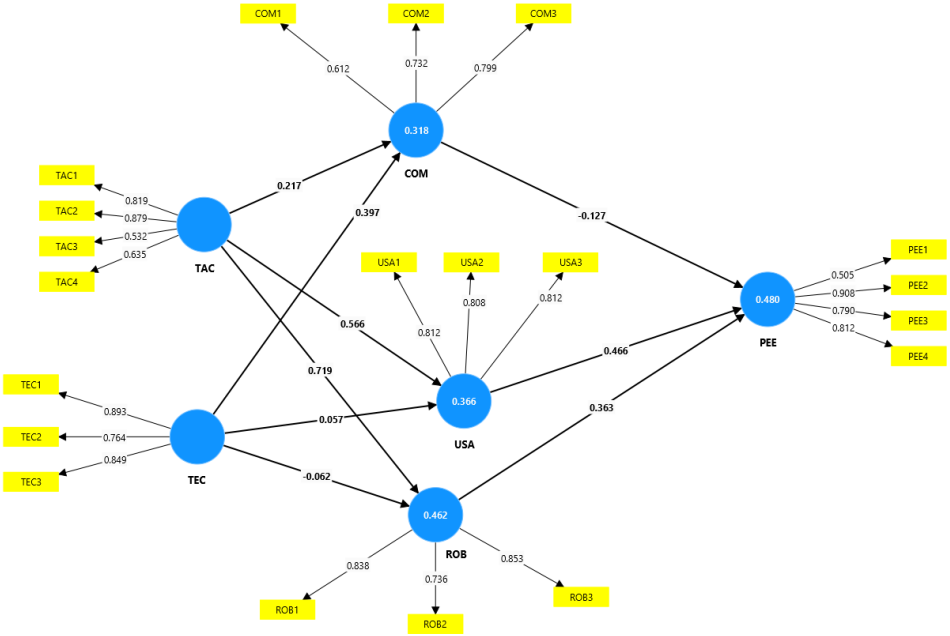

Figure 5. Measurement model.

Reliability Analysis

Split-half reliability, inter-rater reliability, test-retest reliability, and internal consistency are methods often used to evaluate construct dependability. Internal consistency was used in this study to assess dependability. The internal consistency of the instruments was investigated using composite reliability. According to [35,36], the thumb-rule for the composite reliability threshold value is ≥0.7. According to [37], values ranging

from 0.60 to 0.70 are considered acceptable, while values over 0.70 imply higher reliability. Table 7 shows the reliability metrics (Cronbach's alpha, composite reliability, and average variance extracted/explained) considered to evaluate the measurement model. The results (Table 7) demonstrate that all the constructs fall within an acceptable range, except for COM, which has a poor dependability value (low Cronbach's alpha, value of 0.55). To prove convergent validity, the average variance extracted (AVE) was also evaluated with a thumb rule of 0.5 value [38]. The computed AVE for all constructs (as shown in Table 7) was more than the 0.50 thumb rule, thus satisfying the requirement for accepting the measurement model. All measurement items generated factor loading higher than 0.5, as shown in Figure 5, further supporting the reliability of the measurement instruments. Additionally, convergent validity describes the degree to which each concept converges to explain the variance of its items, and average variance extracted (AVE) is the measure used to assess the convergent validity of constructs. Furthermore, discriminant validity is evaluated to explain the extent to which one construct is distinct from others in the structural model.

Table 7. Reliability Analysis.

Code	Cronbach's Alpha	Composite Reliability (CR)	Average Variance Extracted (AVE)
COM	**0.55**	0.760	0.516
PEE	0.774	0.847	0.591
ROB	0.736	0.851	0.657
TAC	0.704	0.815	0.533
TEC	0.788	0.875	0.701
USA	0.748	0.852	0.657

3.4. Structural Model

After ensuring the measurement model's requirements are met, the study investigates the inner relationships between independent and dependent variables. Standardized path coefficients, standard error, t-values, and *p*-values are among the critical metrics used to evaluate the relevance, direction, and strength of these associations. The study's direct correlations between variables may be understood and measured with the use of the structural model, shown in Figure 6.

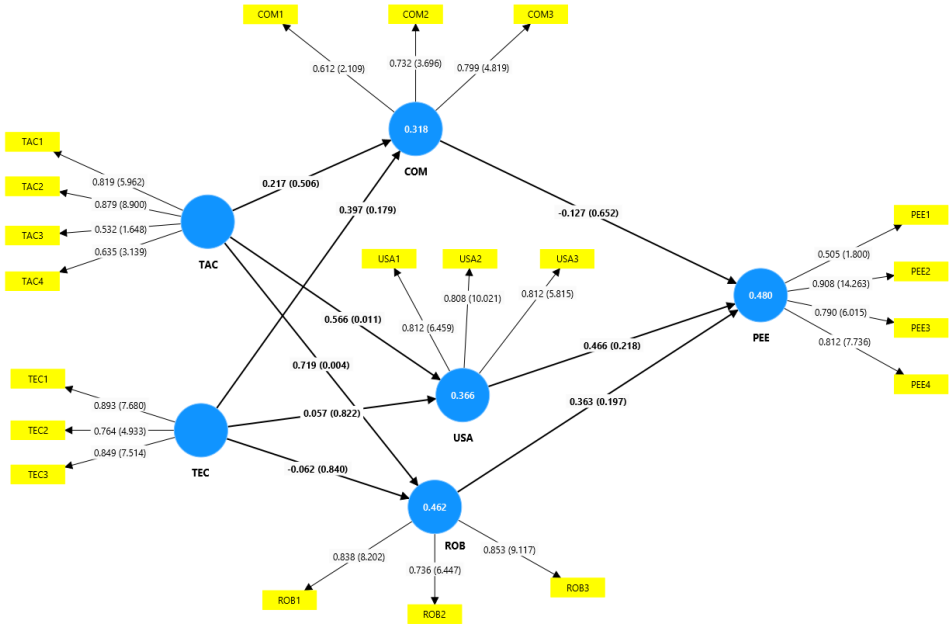

Figure 6. Structural model.

Hypothesis Testing

This section presents the results of the hypothesis testing. These hypotheses (null) are further recapitulated thus:

- H0: There is no statistically significant relationship between metaverse task characteristics and the perceived expectation of forensic examiners.
- H1: There is no statistically significant relationship between metaverse technology characteristics and the perceived expectation of forensic examiners in identifying, extracting, and preserving potential digital evidence.

The relationship between COM and PEE was not statistically significant (beta = −0.127, t = 0.451, $p > 0.05$), as shown in Table 8, which shows that the degree of comprehensiveness of the proposed framework is not capable of explaining the actual potential to use the proposed framework. Similarly, robustness (ROB) and performance expectation (PEE) did not exhibit a statistically significant relationship (beta = 0.363, t = 1.289, $p > 0.05$). Additionally, there was no evidence to support the relationship between task features and comprehensiveness (beta = 0.217, t = 0.664, $p > 0.05$). However, the results indicate that there is a positive and statistically significant relationship between task characteristics and robustness (beta = 0.719, t = 2.860, $p < 0.05$) as well as usability (beta = 0.566, t = 2.551, $p < 0.05$), respectively. Conversely, the p-value for each of the remaining direct relationships demonstrated a positive correlation, albeit statistically insignificant, with a p-value greater than 0.05. Attributively, this relatively poor significance can be linked to the limited number of responses. However, regarding the indirect effect, TAC and TEC to PEE, the result revealed a positive output, as shown in Table 9. Suffix to highlight that the defined null hypothesis of this study is hinged on this indirect relationship. Whilst the TAC showed a standardized beta coefficient of 0.498, the TEC had a much lower coefficient of 0.046 (negative relative relationship). Furthermore, the responses revealed that TAC has a statistically significant relationship with PEE (Beta coefficient = 0.498, $p < 0.05$) in contrast to TEC (Beta coefficient = −0.046, $p > 0.05$). In essence, the null hypothesis on the first hypothesis (H0) is rejected in favor of the alternate hypothesis. Conversely, the second null hypothesis (H1) is accepted. Therefore, the indirect relationship between task characteristics and performance expectancy shows that the respondents alluded that the proposed metaverse forensic framework can be used to conduct a digital forensic investigation in the metaverse platform. This further implies that the proposed framework addresses key factors and characteristics associated with the typical metaverse forensics processes.

Table 8. Direct relationship.

Relationships	Path-Coeff	Std Dev	*t*-Value	*p*-Value	Decision
COM->PEE	−0.127	0.281	0.451	0.652	Insignificant
ROB->PEE	0.363	0.282	1.289	0.197	Insignificant
TAC->COM	0.217	0.362	0.664	0.506	Insignificant
TAC->ROB	0.719	0.252	2.860	**0.004**	Significant
TAC->USA	0.566	0.222	2.551	**0.011**	Significant
TEC->COM	0.341	0.296	1.343	0.179	Insignificant
TEC->ROB	−0.142	0.309	0.202	0.840	Insignificant
TEC->USA	−0.016	0.253	0.225	0.822	Insignificant
USA->PEE	0.451	0.378	1.232	0.218	Insignificant

Table 9. Indirect Effect.

Relationship	Beta	*t* Statistics	*p* Values	Decision
TAC->PEE	0.498	2.372	**0.018**	Supported
TEC->PEE	−0.046	0.197	0.844	Not supported

4. Discussion

The rise of the metaverse signifies a fundamental change in how we communicate, work, and live digitally. There is much potential for creativity, cooperation, and business in this vast virtual world. However, these advantages also bring with them new, challenging problems, especially in the field of cybersecurity. Addressing the possible rise in cybercrimes in this digital ecosystem is essential as assets and activities progressively move to the metaverse. The complex structures of the metaverse may be beyond the capabilities of traditional forensic techniques, which were designed to examine events in the real world. Thus, the creation of specific frameworks that can guide forensic specialists in carrying out comprehensive and effective investigations in this virtual setting is crucial.

The four phases of the benchmarked framework [3]—data collection, evidence evaluation, analysis, and reporting—are based on the NIST standard. It focuses on three key domains: user, service, and metaverse platform. Thoroughly obtaining, examining, and assessing data ensure data security and integrity and make evidence collection and analysis more effective. Although this framework offers a strong basis for digital investigations in the metaverse, it might not be broad enough or deep enough to fully handle the complexity of this dynamic environment.

In response to this limitation, a new seven-phase framework that complies with ISO/IEC 27043:2015 and the metaverse forensic framework referenced in [3] has been offered as a solution to this issue. The goal of this new framework is to offer a more comprehensive process for digital investigations in the metaverse. Unlike the original framework, which might have placed less focus on readiness, the suggested structure takes readiness into account, making sure that investigators have the necessary resources to deal with the metaverse's constantly evolving features. The proposed framework provides a comprehensive method that is suited to the complexities of the metaverse environment by purposefully matching phases with specified criteria, hence improving the accuracy and efficiency of digital investigations.

The significance of the proposed framework is in its ability to provide a robust and consistent approach to digital investigations while addressing the diverse and complex nature of the metaverse environment. The proposed framework gives forensic investigators a useful tool to fight cybercrimes in this developing digital environment by complying with recognized standards like ISO/IEC 27043:2015 and the metaverse forensic framework mentioned in the previous research. The responses to the survey given by forensic professionals offer insightful information about how well the suggested framework works. The framework has the potential to greatly enhance the forensic investigation process in the metaverse, as seen by the overwhelmingly positive replies, with the majority of respondents indicating agreement or strong agreement with its accuracy, usability, and application. The significance and applicability of the proposed framework in tackling the particular difficulties faced by cyber investigators in the metaverse are highlighted by this solid support, highlighting its worth as a vital resource for forensic investigators working in this digital environment. The efficiency of the proposed framework is further supported by the analysis of the survey replies. The results of the investigation indicated a considerable indirect association between task characteristics and performance expectancy. This indicates that individuals who handle incidents involving the metaverse think this approach will aid, enhance, simplify, and quicken their investigation. On the other hand, performance expectancy is negatively and negligibly indirectly affected by technical characteristics. This shows that although people view the suggested framework favorably for helping with investigative activities, there can be concerns about the technology itself and how it would affect their expectations for performance. Despite this, the proposed framework provides a thorough and uniform approach that can improve digital investigations' effectiveness and efficacy while maintaining the environment's security and integrity. Although there are obstacles to its execution, proactive measures can be taken to maximize the framework's efficiency and guarantee its applicability in the metaverse's dynamic environment.

5. Conclusions

In conclusion, this study presents a new "Forensic Framework for Investigating Cybercrime in the Metaverse", expanding upon an earlier framework with more thorough phases and methodologies for investigation. This framework adds to the changing field of digital forensics by improving the current approach, especially regarding cybercrimes using the metaverse. The comparison with the earlier framework shows the improvements, highlighting the enhanced effectiveness and range of the suggested model.

Furthermore, by actively involving forensic professionals in the United Arab Emirates, the article expands its investigation beyond theoretical improvements. Their insightful opinions and valuable insights into the framework give the study a useful edge. A review of the responses indicates that these specialists are in complete agreement that the framework that was developed is highly beneficial and would help investigators of crimes connected to the metaverse tremendously. This real-world validation strengthens the suggested model's validity and suitability for use in actual forensic situations.

Even while the results are encouraging, there are several essential limits to be aware of. Further validation through extensive testing on real cases may be necessary to ensure the framework's effectiveness and flexibility in a variety of metaverse criminal scenarios. This can also include leveraging this proposed framework as a methodology for conducting a forensic investigation in the metaverse. Furthermore, to guarantee that the framework stays applicable and efficient, constant updates and modifications are required due to the dynamic nature of virtual environments and technology.

To verify the robustness and generalizability of the framework, the future research should concentrate on conducting experiments on a range of metaverse-related cases. The suggested framework will be improved and refined even more by ongoing cooperation with forensic specialists, incorporation of cutting-edge technology, and investigation of potential difficulties in various metaverse platforms. This research lays a strong foundation for future developments in the field of digital forensics and represents a significant step forward in tackling the difficulties presented by metaverse cybercrimes.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/fi16120437/s1.

Author Contributions: Conceptualization, R.A.I.; methodology, R.A.I.; software, R.A.I. and A.A.; validation, R.A.I., A.A. and H.S.; formal analysis, A.A. and R.A.I.; investigation, R.A.I. and A.A.; resources, H.S.; data curation, A.A.; writing—original draft preparation, A.A.; writing—review and editing, R.A.I. and H.S.; visualization, R.A.I. and A.A.; supervision, H.S. and R.A.I.; project administration, H.S.; funding acquisition, H.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declares no conflicts of interest.

References

1. Teodorov, A.V. Cybercrimes in the Metaverse: Challenges and Solutions. In Proceedings of the International Conference on Cybersecurity and Cybercrime, New York, NY, USA, 30 November–1 December 2023 ; Volume 10, pp. 209–215. [CrossRef]
2. Qin, H.X. Identity, Crimes, and Law Enforcement in the Metaverse. *arXiv* **2022**, arXiv:2210.06134. [CrossRef]
3. Seo, S.; Seok, B.; Lee, C. Digital forensic investigation framework for the metaverse. *J. Supercomput.* **2023**, *79*, 9467–9485. [CrossRef]
4. ISO—International Organization for Standardization. *Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*; ISO—International Organization for Standardization: Geneva, Switzerland, 2011.
5. *ISO/IEC 27043:2015*; International Standard, Information Technology—Security Techniques—Incident Investigation Principles and Processes. International Organization for Standardization: Geneva, Switzerland, 2015; Volume 1, pp. 1–30.

6. Al-Romaihi, S.K.; Ikuesan, R.A. Cyberbullying Indicator as a Precursor to a Cyber Construct Development. In Proceedings of the International Conference on Cyber Warfare and Security, Academic Conferences International Limited, Albany, NY, USA, 17–18 March 2022; Volume 17, pp. 1–6.
7. Upadhyay, U.; Kumar, A.; Sharma, G.; Gupta, B.B.; Alhalabi, W.; Arya, V.; Chui, K.T. Cyberbullying in the metaverse: A prescriptive perception on global information systems for user protection. *J. Glob. Inf. Manag.* **2023**, *31*, 1–25. [CrossRef]
8. Al Ali, T.; Alfulaiti, S.; Abuzour, M.; Almaqahami, S.; Ikuesan, R. Digital Forensic in a Virtual World: A Case of Metaverse and VR. In Proceedings of the ECCWS 2023 22nd European Conference on Cyber Warfare and Security, Piraeus, Greece, 22–23 June 2023; Academic Conferences and Publishing Limited: Reading, UK, 2023.
9. Alkuwaiti, A.; Alremeithi, M.; Alobeidli, H.; Ikuesan, R. Towards the Development of Indicators of Fake Websites for Digital Investigation. In Proceedings of the European Conference on Cyber Warfare and Security, Athens, Greece, 22–23 June 2023; Volume 22, pp. 33–43.
10. Irwin, A.S.; Slay, J.; Choo, K.K.R.; Lui, L. Money laundering and terrorism financing in virtual environments: A feasibility study. *J. Money Laund. Control.* **2014**, *17*, 50–75. [CrossRef]
11. Adeyemi, I.R.; Abd Razak, S.; Azhan, N.A.N. A review of current research in network forensic analysis. *Int. J. Digit. Crime Forensics (IJDCF)* **2013**, *5*, 1–26. [CrossRef]
12. Mukkamala, S.; Sung, A.H. Identifying significant features for network forensic analysis using artificial intelligent techniques. *Int. J. Digit. Evid.* **2003**, *1*, 1–17.
13. Wang, Y.; Su, Z.; Zhang, N.; Xing, R.; Liu, D.; Luan, T.H.; Shen, X. A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Commun. Surv. Tutorials* **2022**, *25*, 319–352. [CrossRef]
14. Barbe, H.; Müller, J.L.; Siegel, B.; Fromberger, P. An Open Source Virtual Reality Training Framework for the Criminal Justice System. *Crim. Justice Behav.* **2023**, *50*, 294–303. [CrossRef]
15. Koziol, M. The Metaverse Needs Standards, Too. *IEEE Spectrum*, 31 August 2022. Available online: https://spectrum.ieee.org/metaverse-standards-forum (accessed on 15 May 2024).
16. Bulbul, H.I.; Yavuzcan, H.G.; Ozel, M. Digital forensics: An analytical crime scene procedure model (ACSPM). *Forensic Sci. Int.* **2013**, *233*, 244–256. [CrossRef]
17. Kebande, V.R.; Venter, H.S. Novel digital forensic readiness technique in the cloud environment. *Aust. J. Forensic Sci.* **2018**, *50*, 552–591. [CrossRef]
18. Pfeuffer, K.; Geiger, M.J.; Prange, S.; Mecke, L.; Buschek, D.; Alt, F. *Behavioural Biometrics in VR;* Association for Computing Machinery: New York, NY, USA, 2019. [CrossRef]
19. Kebande, V.R.; Mudau, P.P.; Ikuesan, R.A.; Venter, H.; Choo, K.K.R. Holistic digital forensic readiness framework for IoT-enabled organizations. *Forensic Sci. Int. Rep.* **2020**, *2*, 100117. [CrossRef]
20. Elyas, M.; Ahmad, A.; Maynard, S.B.; Lonie, A. Digital forensic readiness: Expert perspectives on a theoretical framework. *Comput. Secur.* **2015**, *52*, 70–89. [CrossRef]
21. Elshenraki, H.N. Forecasting Cyber Crime in the Metaverse Era: Future Criminal Methods-Readiness Requirements. In *Forecasting Cyber Crimes in the Age of the Metaverse*; IGI Global: Hershey, PA, USA, 2024; pp. 1–23.
22. James, R.L.; Barbara, G.; John, M.B.; Kelly, Sauerwein, K.; Reed, C.; Corrine, E.L. *NIST Internal Report 8354: 2022 Digital Investigation Techniques: A NIST Scientific Foundation Review*; NIST: Gaithersburg, MD, USA, 2022; Volume 1, pp. 1–3.
23. Kim, J.; Park, J.; Lee, S. An improved IoT forensic model to identify interconnectivity between things. *Forensic Sci. Int. Digit. Investig.* **2023**, *44*, 301499. [CrossRef]
24. Kim, D.; Oh, S.; Shon, T. Digital forensic approaches for metaverse ecosystems. *Forensic Sci. Int. Digit. Investig.* **2023**, *46*, 301608. [CrossRef]
25. Liang, T.P.; Kohli, R.; Huang, H.C.; Li, Z.L. What drives the adoption of the blockchain technology? A fit-viability perspective. *J. Manag. Inf. Syst.* **2021**, *38*, 314–337. [CrossRef]
26. Alyoussef, I.Y. Acceptance of e-learning in higher education: The role of task-technology fit with the information systems success model. *Heliyon* **2023**, *9*, e13751. [CrossRef]
27. Ajzen, I. The theory of planned behavior: Frequently asked questions. *Hum. Behav. Emerg. Technol.* **2020**, *2*, 314–324. [CrossRef]
28. Yuriev, A.; Dahmen, M.; Paillé, P.; Boiral, O.; Guillaumie, L. Pro-environmental behaviors through the lens of the theory of planned behavior: A scoping review. *Resour. Conserv. Recycl.* **2020**, *155*, 104660. [CrossRef]
29. Anggara, R.; Budiyanto, C.W.; Hatta, P. *Comparison between TAM, EUCS, TTF Analysis to Evaluate User Acceptance for Conference Management System*; American Institute of Physics Inc.: College Park, MD, USA, 2019; Volume 2194. [CrossRef]
30. Taherdoost, H. *A Review of Technology Acceptance and Adoption Models and Theories;* Elsevier: Amsterdam, The Netherlands, 2018; Volume 22, pp. 960–967. [CrossRef]
31. Cheng, E.W. Choosing between the theory of planned behavior (TPB) and the technology acceptance model (TAM). *Educ. Technol. Res. Dev.* **2019**, *67*, 21–37. [CrossRef]
32. Al-Dhaqm, A.; Abd Razak, S.; Siddique, K.; Ikuesan, R.A.; Kebande, V.R. Towards the development of an integrated incident response model for database forensic investigation field. *IEEE Access* **2020**, *8*, 145018–145032. [CrossRef]
33. Hammer, C.S. The importance of participant demographics. *Am. J. Speech Lang. Pathol.* **2011**, *20*, 261. [CrossRef] [PubMed]
34. Beauducel, A.; Herzberg, P. On the Performance of Maximum Likelihood Versus Means and Variance Adjusted Weighted Least Squares Estimation in CFA. *Struct. Equ.-Model. Multidiscip. J. Struct. Eq. Model.* **2006**, *13*, 186–203. [CrossRef]

35. Gefen, D.; Straub, D.; Boudreau, M.C. Structural equation modeling and regression: Guidelines for research practice. *Commun. Assoc. Inf. Syst.* **2000**, *4*, 7. [CrossRef]
36. Kumar, A.; Srivastava, A.; Misra, S.C. Assessment of the factors for the adoption of Internet of things (IoT) in the logistics: A PLS-SEM (partial least squares structural equation modeling) approach. *Int. J. Qual. Reliab. Manag.* **2024**, *41*, 1308–1336. [CrossRef]
37. Diamantopoulos, A.; Sarstedt, M.; Fuchs, C.; Wilczynski, P.; Kaiser, S. Guidelines for choosing between multi-item and single-item scales for construct measurement: A predictive validity perspective. *J. Acad. Mark. Sci.* **2012**, *40*, 434–449. [CrossRef]
38. Hair, J.F.; Risher, J.J.; Sarstedt, M.; Ringle, C.M. When to use and how to report the results of PLS-SEM. *Eur. Bus. Rev.* **2019**, *31*, 2–24. [CrossRef]