Information Systems Frontiers
https://doi.org/10.1007/s10796-022-10360-8

# The Case for Validating ADDIE Model as a Digital Forensic Model for Peer-to-Peer Network Investigation

Ahmad Sanda Musa[1] · Irfan-Ullah Awan[1] · Fatima Zahrah[2]

Accepted: 14 November 2022

**Abstract**
Rapid technological advancement can substantially impact the processes of digital forensic investigation and present a myriad of challenges to the investigator. With these challenges, it is necessary to have a standard digital forensic framework as the foundation of any digital investigation. State-of-the-art digital forensic models assume that it is safe to move from one investigation stage to the next. It guides the investigators with the required steps and procedures. This brings a great stride to validate a non-specific framework to be used in most digital investigation procedures. This paper considers a new technique for detecting active peers that participate in a peer-to-peer (P2P) network. As part of our study, we crawled the µTorrent P2P client over ten days in different instances while logging all participating peers. We then employed digital forensic techniques to analyse the popular users and generate evidence within them with high accuracy. We evaluated our approach against the standard Analysis, Design, Development, Implementation, and Evaluation (ADDIE) model for the digital investigation to achieve the credible digital evidence presented in this paper. Finally, we presented a validation case for the ADDIE model using the United States Daubert Test and the United Kingdom's Forensic Science Regulator Guidance – 218 (FSR-G-218) and Forensic Science Regulator Guidance – 201 (FSR-G-201) to formulate it as a standard digital forensic model.

**Keywords** Validation · ADDIE Model · Digital Forensics · Peer-to-Peer Network · Investigation

## 1 Introduction

The three most valuable assets of the internet are information shared in form of packets, bandwidth, and computing resources. However, due to the traditional client-server model, all these assets are largely under-utilized. This is because the information is not only hard to find but also impossible to index and catalogue. A recent study found that the world produced an estimated data of about 44 Zettabytes (44 × 10^21 bytes) in 2020, whereas the International Data Corporation (IDC) predicts that worlds data generation could grow to about 175 Zettabytes by 2025 (Stroud, 2020). Google search takes centre stage in the realm of internet searches with an estimated yearly search of 1.2 trillion (1.2 × 10^12) (Boskov, 2020). It has also been observed by Google that there are millions of internet users every day, which further evidences the significance of information and data. Owing to the transient nature of data on the internet and how much is added daily, finding valuable and unstructured information in real-time is increasingly complex.

Bandwidth, an important metric in Internet infrastructure, is quantified as the sum of data transferred in time, generally measured in bits per second (Reinsel et al., 2018). Since the world now relies on the internet to conduct day-to-day operations, internet speed is an important consideration that cannot be overemphasized. Too many people and devices trying to access resources on a network simultaneously could cause network congestion which has consequence of slow or no response at all. This issue is prevalent on hot links popular sites like eBay, Amazon, Facebook, and more recently, online video conferencing forums like Zoom and Microsoft Teams. The hot-links get hotter for bandwidth, and cold-links stay cold while heavily loaded nodes get overloaded for computing resources with idle nodes

✉ Ahmad Sanda Musa
ahmadsanda@ymail.com

[1] Department of Computer Science, University of Bradford, Bradford, UK

[2] Department of Computer Science, University of Oxford, Oxford, UK

Published online: 02 December 2022

remaining idle. However, it is important to understand that there are two different kinds of bandwidth speed: upload and download speed.

Upload speed is the rate at which data is conveyed to its destination, while download speed is the rate at which information is received (Reinsel et al., 2018). Regardless of the kind of bandwidth being utilized, bandwidth has been established as the primary catalyst for determining internet traffic. While Moore's law challenges the computing paradigm to produce better computing resources, the law states that processor speed or the overall processing power will double about every 18 months (Wardynski, 2019). The power of computers has been multiplying every year or and a half since the 1970s. Computing devices (cell phone, server, Personal Digital Assistants, Personal Computers) are more powerful than their predecessors of half-a-century ago(Norman, 2017). The law helped the storage capacity of these devices improve and increased dramatically year in year out. Although humans continue to struggle to advance knowledge, computations are still conducted mainly in the data centres (Tukur et al., 2020).

Peer-to-Peer (P2P) network combines the three most valuable assets of the internet; information, bandwidth, and computing resources by its architectural design (Musa, 2020a, 2020b; Wardynski, 2019). Peer-to-Peer network promotes the dynamic discovery of information, better utilization of bandwidth, processors, storage space, and other resources while ensuring each user contributes resources to the network (Peersman et al., 2016). These networks are part of highly distributed systems containing diverse peers to form a network. The peers are used to exchange content containing audio, video, data, and various files without using a single server as in client-server architecture. While peer-to-peer networking describes networks in which peer machines share tasks or responsibilities among themselves (Vishnumurthy & Francis, 2007). Peer-to-Peer networks are usually used to share files or content between two or more devices directly on the internet. A P2P application permits you to download files from other peers' hard drives and enables others to download from your computer's hard drive. The concept of P2P networking and applications has been discussed extensively in (Bodriagov & Buchegger, 2013; Imada & Ueda, 2016; Jo & Han, 2018; Musa et al., 2019; Vishnumurthy & Francis, 2007).

Peer-to-Peer has attracted a great deal of interest due to its ease of use and the ability of peers to join and leave the network without affecting the functionality of the system. This ability made it an avenue for the management and exchange of anonymous data about organizations, people, and governments, thereby making them prime targets of many cyber-attacks and malware distribution. As a result, security and privacy have remained a significant concern in the P2P network domain, characterized by equal sharing of information, bandwidth, and computing resources among peers (Washbourne, 2015). Therefore, there is need for adequate measures should be put in place to address the impact of distributing malicious contents on the networks.

Non-implementation of security mechanisms in the design of P2P networks has spawn an explosive distribution of malicious content on the networks rendering them more prone to attacks and making any credible digital investigation on the networks mostly futile (Alhazmi et al., 2017a). This security flaw has contributed to making P2P networks the best avenue for trading large amounts of data, which is necessary for modern computing needs. The annual SysAdmin, Audit, Network, and Security (SANS) Institute report of 2020 identified Analysis, Design, Development, Implementation, and Evaluation (ADDIE), as the proactive next-generation digital forensic investigation model. The ADDIE model of digital investigation outlines steps that ensure evidence chain of custody and forensic integrity is maintained. This paper presents a first of its kind investigation technique for P2P networks that incorporates the active monitoring of peers and simultaneous forensic analysis to produce credible digital evidence while ensuring integrity, high accuracy and accountability for malicious peers participating in the network. We studied the digital evidence while adhering to the ADDIE model of digital forensics standard to maintain evidence chain of custody, forensic integrity and accuracy verification to recover an irrefutable digital path of the most popular peers using their communication protocols, IP addresses and Secure Hashing Algorithm (SHA).

### 1.1 Motivation and Contribution

This work is motivated by the continuous mutation of security threats associated with the use of P2P networks, which results from its widespread and seemingly endless applications. Nevertheless, the main contribution is validating a novel forensic model for P2P – how our novel model can be used as an investigative guide to validate digital forensic procedures in P2P. The motive behind our focus in validating a new model for P2P is to guide investigators with necessary steps and procedures during investigation.

Our main contributions in this work are:

- We reviewed the history and recent trends of digital forensic models, ADDIE model and P2P network investigation.
- We established the susceptibility of oversight on a typical P2P network by presenting an active monitoring system that shows how P2P networks are not entirely anonymous after all and that successful monitoring can

be achieved without tempering with the usability and functionality of the P2P network.

- We proposed and presented a novel method of investigation in the ADDIE model to address the need for evidence chain of custody, forensic integrity, and accuracy verification.
- We proposed and presented a validation case for our novel method using multiple approved legislative guidance for methods validation and peer review approval to ensure the integrity of the investigation method.
- The proposed solution was evaluated using a real P2P network dataset, and it revealed to achieve remarkable evidence detection with an irrefutable digital path of participating peers using their communication protocols, IP, and SHA addresses.

The rest of the article is organized as follows: Sect. 2 reviews related works as the digital forensics' models, the history of the ADDIE model and P2P network investigation. In Sect. 3, the method validation processes are proposed, defined, and explained. We justified why validating novel methods is necessary in Sect. 4. In Sect. 5 the validation methodology and the ADDIE model is proposed by showcasing the usability of the model to digital investigations. Then in Sect. 6, we evaluated the validation of the model using real P2P network dataset and investigation techniques. Section 7 concludes the article along with future scope.

## 2 Related Works

In this section, we present a comprehensive review of digital forensic models, the ADDIE model and P2P network investigation. The findings show that the research community do not give much attention to investigating P2P networks using standard digital forensic models. Also, we found no literature that has tested their validation case with real dataset and investigation.

### 2.1 Digital Forensic Models

The increased automation and reliance on digital technology have led to the spontaneous increase in digital crimes. These crimes need a structured process to address them. Digital technology innovations such as social media networks, cloud computing systems, mobile technologies, internet of things (IoT) systems, encryption techniques, anti-forensic tools, utilization of private and portable browsers, malware infection, etc., steer digital investigators to various modern, complex and cumbersome challenges. Therefore, a structured, advanced, and scientific digital forensic process model is required to address these challenges.

Over the years, much research has been carried out in this field. Pollitt (1995) was one of the authors to have designed the first digital forensic model to the best of our knowledge. He compared and mapped the model with the view of admissibility of documentary evidence in a court of law. Before presenting any evidence in court, Pollitt (2007) identified the following steps: Acquisition --> Identification --> Evaluation --> Admission as Evidence. The author stated that digital evidence must be scientifically accurate and legally acceptable and that the process adhered to science and law.

In 2001, the first Digital Forensic Research Workshop (DFRWS) assembly produced a consensus document that defined the state of digital forensics (Palmer, 2001). Among their resolutions was that digital forensics was a framework with some fairly agreed-upon steps. The framework comprises of seven steps: Identification - Presentation - Collection - Examination - Analysis - Presentation - Decision. In 2002, the second DFRWS assembly developed a new enhanced digital forensic framework by improving their earlier model (Reith, M. Carr, C. and Gunsch, 2002). The improved framework standardizes the digital forensic investigation process, according to the assembly. The model consists of nine steps: Identification - Preparation - Approach Strategy - Preservation - Collection - Examination - Analysis - Presentation - Returning Evidence.

In 2006, a group of scientists published a guide to integrating forensics into incident response as part of the special publication of the National Institute of Standards and Technology (NIST) (Karen et al., 2006). They defined the forensic process into the following basic phases: Collection - Examination - Analysis - Reporting. The group argued that their forensic model could be applied to any investigation, regardless of the situation.

The generic computer forensic investigative model (GCFIM) evolved from reviewing fifteen previous digital forensic models (Yusoff et al., 2011). The GCFIM consists of five steps as pre-process, acquisition, analysis, presentation, and post-process. The model was intended to serve as the basic and high-level digital forensic model and the basis for developing a new investigation methodology.

Agarwal et al., (2011) proposed the Systematic Digital Forensic Investigation Model (SRDFIM) by comparing and expanding previous digital forensic models. It consists of eleven phases: preparation, securing the scene, survey & recognition, documenting the scene, communication shielding, evidence collection, preservation, examination, analysis, presentation, and result and review. The model helps in reconstructing events by realizing specific properties of individuality, repeatability, reliability, performance, testability, scalability, quality, and standards in analysis concerning computer frauds and cybercrimes.

Montasari, (2016) assessed and evaluated eleven digital forensic models using the five Daubert Standard Criteria. The standard is approved in the United States (US) as the criteria for accepting scientific evidence. The authors reveal no formal, comprehensive model that incorporates the entire digital process that can be used in all fields of investigation despite using the Daubert Standard.

During the last decade, different digital forensic models continue to be developed by (Ali et al., 2017; Du et al., 2017; Hitchcock et al., 2016; Kaur et al., 2018; (Reith et al., 2002), Thakar et al., 2021; Zia et al., 2017) targeting distinct areas of digital forensics such as mobile forensics, digital forensics as a service, digital field triage, network forensics, the next generation digital forensic investigation model (NGDFIM), and IoT forensics respectively. Several researchers have adopted International Standard Organization (ISO) standards into their digital forensic framework to enhance and standardize their framework. Kao & Wu (2015) proposed a digital triage forensics framework of windows malware forensic toolkit based on ISO/IEC 27,037 to improve the speed and quality of investigations. The guidelines provide basic scenarios encountered throughout the digital evidence handling process and specify directions for standardization efforts. Kigwana et al., (2017) propose a digital forensic investigation framework based on ISO/IEC 27043:2015 to develop a standard eGovernment forensic investigation procedure. Similarly, Karie et al., (2019) explain that blockchain is a key factor that should be added to ISO/IEC 27043:2015 to establish a standardized digital forensic report generation process. While Mothi et al., (2020) proposed a novel mathematical principle to validate digital forensic models by countering anti-forensics techniques before being used in a real-time investigation.

After reviewing various digital forensic models to date, we found that most of the reviewed works and other similar research have proposed either digital forensic frameworks or made a case for framework validation. The few studies that discussed validation based on legislative procedure do not appear to have validated any standard digital forensic model. Howecer, none of the work reviewed considered investigating the digital threats of P2P networks. This means that all the related literature has left a wide gap in providing solutions to the security threats of the P2P network, especially tackling its anonymity. This paper addresses these gaps by proposing a novel method and its validation case based on P2P network investigation.

## 2.2 ADDIE Model

ADDIE model is part of the Instructional System Design (ISD) family. It was created in 1975 for the US Army by the Centre for Educational Technology at Florida State University (Branson et al., 1975). Being a leader in training and learning, the military significantly influenced corporate and educational activities by adapting the ADDIE model. DeSimone et al. 2002 (Desimone et al., 2002) consider ADDIE to be a *process model* if applied correctly and a guide for gaining direct intuitive insight into a problem. In 2017, (Stroud, 2020) of SANS institute used the ADDIE model for the Digital Forensics Framework for Instruction Design (DFFID) in their whitepaper as a comprehensive digital framework designed to guide the development of future digital forensics. In the ADDIE model, each phase has an outcome that feeds into the next steps as follows:

### 2.2.1 Analysis

The digital problem is investigated in the analysis phase, the investigator's goals and objectives are established, and the crime scene and existing investigative techniques and skills are identified. Below are some of the questions that are addressed during the analysis phase:

- What is the aim of the investigation?
- What type of difficulties exists?
- What are the acquisition techniques options?
- What tools are going to be used for the analysis?
- What is the timeline of the investigation?

### 2.2.2 Design

The design phase deals with the case objectives, assessment of tools, and the purpose of the investigation, documentation, and case planning. This phase of the forensic process should be systematic and specific. Systematic here means a logical, orderly method of identifying, developing, and evaluating a set of planned procedures targeted for achieving the investigation's goals. While specific means each component of the design phase needs to be executed meticulously to avoid evidence tempering.

The following steps are used for the design phase:

- Application of case strategies according to the intended recovery outcomes.
- Documentation of the case project, visual and technical design strategy.
- Duplication of the source file.

### 2.2.3 Development

The development phase is where the investigators create and execute the processes generated in the design and analysis phase. If using multiple tools and methods, the investigator works to develop and integrate the techniques. Then making sure there is a duplicate copy of the source file before the final review and integration of the final method.

### 2.2.4 Implementation

During the implementation phase, the forensic processes of the investigation and the case plan are developed. The individual experiences and skills of the investigator are added to the case procedure along with the expected outcomes, method of delivery, and investigation procedures. Preparation of the investigation includes training with all the tools (software or processes) to ensure that the application is viable and functional.

### 2.2.5 Evaluation

The evaluation phase of the digital forensic process can be divided into formative and summative divisions. Formative evaluation is present throughout all the stages of the ADDIE model. At the same time, the summative evaluation incorporates the entire case plan, investigative techniques used, evidence validation, timeline, and provides an interface for evidence presentation.

## 2.3 P2P Network Investigation

There are many published works (Alhazmi et al., 2017b; Fahimian et al., 2010; Imada & Ueda, 2016; Jo & Han, 2018; Liberatore et al., 2010; Mao et al., 2020; Musa et al., 2018, 2019; Scanlon et al., 2015a) on P2P network investigation. However, to the best of our knowledge and research, none of the works has addressed P2P security comprehensively, particularly the ubiquitous vulnerabilities of the P2P network as well as the threats posed to the diverse peers, and the need to identify those peers engendering the vulnerabilities. The security designs of (Venčkauskas et al., 2016, Jusas, et al., 2015) and (Venčkauskas et al., 2016), for example, have not been equipped to address issues such as live network monitoring, digital forensics, and evidence validation of P2P systems, which our proposed technique has addressed in Sects. 5 and 6.

Many of the related works also neglected the live monitoring and capture of P2P traffic in their investigations and analysis. While the few that did fail to extract the digital evidence according to the established digital forensic standards that ensure evidence integrity. For example, the authors of (Scanlon & Kechadi, 2014) only indicated the need for bespoke digital tools to combat cyber threats by outlining the investigative process through collaboration between stakeholders without actually performing an experiment or analysing their methodology. The author of (Venčkauskas et al., 2016, Jusas, et al., 2015) conducted a P2P investigation of evidence left in a windows 8 registry after installing, participating in a P2P session, and uninstalling the BitTorrent client.

Similar to recovering evidence from a local running computer, the authors of (Venčkauskas et al., 2016) designed a tool that searches for artefacts related to the use of BitTorrent client from a local computer. The same goes for the BitTorrent sync described by (Scanlon et al., 2014), which demonstrated remote evidence recovery from the BitTorrent sync shared folder. Identically, the authors of (Scanlon et al., 2015b) investigated the data remnants of the newer version of BitTorrent sync applications (version 2.x) using mobile and computer devices to extract evidence from installation, uninstallation, log-in, log-off, and file synchronization. However, all the works only proposed investigative methodologies from a local machine based on installation and uninstallation of BitTorrent clients or remote recovery on a computer device. Another investigation and analysis of BitTorrent sync were conducted by (Y. Y. Teing et al., 2017) to assist in the control of data flow across the platform. Also, the work was centred on replicated files by the BitTorrent sync remote peers, which introduce the risk of sabotage or malware infusion into the network by participating peers to throw off digital investigators.

On the other hand, (Wararkar et al., 2016) discusses the security problems of P2P using a central authority that will be responsible for securing other peers in an intranet network based on the proposed methodology of peer security for; Anonymity, Availability, File Authentication, Access Control, and Fair Trading. The authors of (Washbourne, 2015) reviewed the history P2P network security by evaluating its vulnerabilities, attack models, and preceding protection mechanisms of which none addressed live monitoring of P2P networks and accurate evidence recovery mechanism. Another P2P security survey (Amad et al., 2012) employed resource discovery search mechanisms to locate peers while incurring low overhead and low delay. They provided security solutions based on a semi-decentralized P2P network that uses central authority and protection mechanisms for arising P2P threats.

The security of the P2P network requires a holistic approach because of its distributed nature and difficulty in monitoring; the reason that necessitated accelerated research into security mechanisms of P2P monitoring and analysis. This reason is backed by (Venčkauskas, Jusas, et al., 2015) and (Venčkauskas et al., 2016). Although our work confronts the digital investigation of P2P holistically, our key contributions are the maintenance, assessment and validation of forensic integrity of the captured evidence using the ADDIE model(Allen, 2017; Nadiyah & Faaizah,

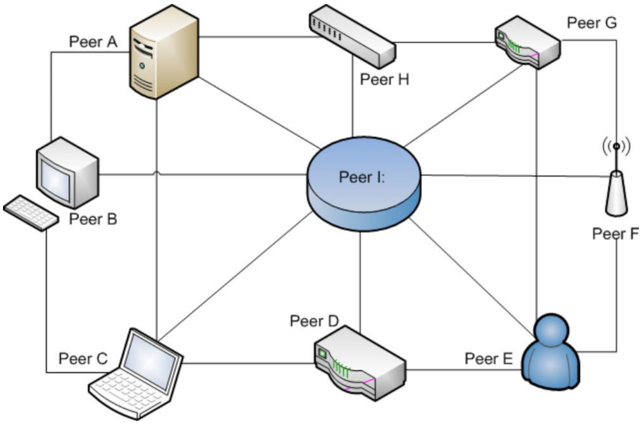


**Fig. 1** P2P Network Illustration

2015). The viability of credible forensic model is considered the weakest link that gets digital evidence invalidated in courts. Hence, we used the most recent and reviewed digital forensic model developed by an expert panel of digital forensics professionals for assessment and validation strategies (Stroud, 2020). ADDIE allowed us to authenticate the popularity of the captured hash values in the P2P network and extract credible digital evidence with high accuracy.

In our work, we approached P2P network security using three quality metrics; live monitoring, crawling as well as capturing of P2P artefacts and evidence validation. Each of the metrics are at a risk of failing the forensic integrity challenge which is the standard for a sound digital evidence (Oltsik et al., 2017). Therefore, the ADDIE model of the SANS is being employed to ensure the integrity of the investigation process (Oltsik et al., 2017). We present a typical P2P network illustration in Fig. 1.

## 3 Validation Case of a Digital Forensic Model

Digital forensic science is a broad scientific discipline that applies to matters of the law (Mothi et al., 2020). When an alleged crime is committed, scientific principles and practices are used to obtain evidence that the investigating officers and courts can prove reliable. Based on the definition of digital forensic science, numerous models, methods, and validation principles have been proposed over the years that suit different investigative methodologies and legislative policies (ENFSI, 2015). Some of the essential aspects of forensic science are the validation of digital forensic methods or procedures and tool testing. The National Institute of Standards and Technology (NIST, 2017) manages the tools testing aspect of digital forensic research. NIST tests various digital forensic tools and then publishes them on their website. In the United Kingdom (UK), there is Forensic Science Regulators – Guidance (FSR-G-218, 2020) for method validation and Daubert Standard (Meyers & Rogers, 2006) in the US to validate digital forensic methods and procedures.

The digital forensics discipline comprises of various types of digital devices that can be used either to enable the crime or as a target of the crime. The digital devices may have volatile memory, non-volatile memory, or even both. The methodologies and processes for recovering digital evidence are chosen based on the type of memory (Zia et al., 2017). Digital forensics is broadly classified into five main branches depending on the type of digital devices, media, or networks. The branches are Computer Forensics, Network Forensics, Mobile Device Forensics, Memory Forensics, and Email Forensics (Karie et al., 2019).

### 3.1 Network Forensics

Network forensics is the branch of digital forensics that focuses on monitoring, collecting, and analyzing computer network traffic to aid in the recovery of data, legal evidence, or detecting intrusion detection (Kaur et al., 2018). Network traffic is usually intercepted at the packet level, and data collection is collected at the network stack layer. The collected data as evidence can either be stored for later analysis or filtered in real-time. In contrast to other types of digital forensics, which use stored or static data with the risk of lost network traffic transmission, network forensics mainly deals with volatile and dynamic data that is rarely logged, thus leading to more proactive investigations that requires validation.

### 3.2 Method Validation

FSR-G-218 (2020) defines a method as a logical sequence of procedures or operations designed to accomplish a specified task. A method includes the interaction of the investigator and may consist of multiple tools or none. For example, acquiring a forensic image of a hard drive (i.e. a copy of a hard disk drive) with a tested write blocker and hard drive imager (SWGDE, 2015). And then using hashing algorithms to verify the data are not several tools or methods but part of one method. Suppose the hash algorithm or write blocker was required in other methods. In that case, they could be validated separately and brought together in the broader method to confirm that it meets the method's requirement (FSR-G-218, 2020). All method in science or engineering can be documented. Creating a draft Standard Operating Procedure (SOP) is good practice before trying any validation study, as validation is completed on the final method.

In the US, the Daubert Standard is used as guidance for any method or procedure adopted by an investigator to provide objective guidelines for judges to ascertain the admissibility of scientific evidence in court. The Daubert standard applies to those digital forensic methods or procedures used to uncover evidence from digital devices. It must satisfy the following criteria as clarified by (Meyers & Rogers, 2006):

a. “Testing: Can and has the scientific procedure been independently tested? Peer Review: Has the scientific procedure been published and subject to peer review?“
b. “Error rate: Is there a known error rate, or potential to know the error rate, associated with the use of this scientific procedure?
c. Standards: Are there standards and protocols for the execution of the methodology?“
d. “Acceptance: Does the relevant scientific community generally accept the scientific procedure?“

In the UK, House of Commons Science Technology Committee (2019) that: “The absence of an agreed protocol for the validation of scientific techniques prior to their being admitted in court is entirely unsatisfactory and that Judges are not well placed to determine scientific validity without input from scientists.“ The committee went on to mention that: “Establishment of a regulator is one of the options to be considered, as it is how the courts can be supported in appropriately weighing scientific evidence.“ Hence, the UK inaugurated the Forensic Science Advisory Council as the Forensic Science Regulators (FSR-G-201, 2020; FSR-G-218, 2020), also known as The Regulators, to develop a validation and accreditation test for scientific methods, which should build on the Daubert Test (Meyers & Rogers, 2006). In 2016, The Regulator had produced its 1st edition guidance on method validation in digital forensics as FSR-G-218. It amalgamates essential information from International Standards Organisation (ISO/IEC 17,025:, 2017), FSR-G-201 validation guidance found in Forensic Science Regulator (FSR-G-201, 2020), Scientific Working Group on Digital Evidence (SWGDE, 2015), International Laboratory Accreditation Cooperation (ILAC, 2014) and Criminal Practice Directions as mentioned in Courts and Tribunals Judiciary (2014). The FSR-G-218 was then updated and reproduced in 2020 to reflect current changes in digital forensic science (FSR-G-218, 2020). The following key criteria were mentioned as necessary steps for method validation (FSR-G-218, 2020):

a. “The validity of the model/theory”.
b. “The validity of the application of the model/theory in the method.“
c. “Any assumptions incorporated within the model/theory.“
d. “The validity of the assumptions and any limits on the application of the assumptions.“
e. “Limits on the application of the model/theory.“
f. “The robustness of the model/theory based on the information supporting it.“

## 4 Justifying the Validation of ADDIE Model

In Sect. 7.4.9 of FSR-G-201 (2020) mentioned that all method development should include risk analysis and mitigation. This will enable the validation to ensure that the method does manage these risks. Section 7.4.10 recognizes the human element in the investigation procedure as methods are more than just the analytical test and may include any error-trapping, such as second checks and peer review.

Consequently, Sect. 6.1.3 of FSR-G-218 (2020) stated that the validation of a new or novel method would require comprehensive testing. While Sect. 6.1.2 reiterated the definition of the specific purpose from the start, focusing on beginning with the most common functionality and requests. This is to prevent the scope of the validation study from straying into attempting to cover everything the method is intended for, which is not realistic or practical. Since the validation of the ADDIE model for digital evidence acquisition is sufficiently novel, the FSR-G-218 recommended that it may be beneficial for a version of the validation to be submitted in a journal for publication.

Both the FSR-G-218 and FSR-G-201 guidance on validating novel digital investigation methods stressed the need for a validated study, evaluation, and peer review as discussed in Sect. 2. Apart from this, proposed methods adopted from another field of study tend to prove effectiveness in problem-solving, as seen with the SIR model adoption from the field of medicine into malware investigation. The ILAC (ILAC, 2014) justifies the scientific community’s need for validation in Sect. 3.10 as far the processes will be documented for reproducibility and repeatability to ensure that different persons can arrive at compatible results.

The Regulators provide guidelines for detailed activities in handling potential digital evidence. These processes are required in an investigation to preserve the integrity of the digital evidence – an acceptable technique of acquiring digital evidence that will contribute to its admissibility in legal actions and other mandated instances (ISO/IEC 17,025:, 2017). The Regulators also outline general guidelines for collecting non-digital evidence that may be useful in the potential digital evidence analysis stage. The Regulators also intend to advise decision-makers who need to decide the reliability of digital evidence presented. It is crucial to carry out an investigation using an acceptable model to

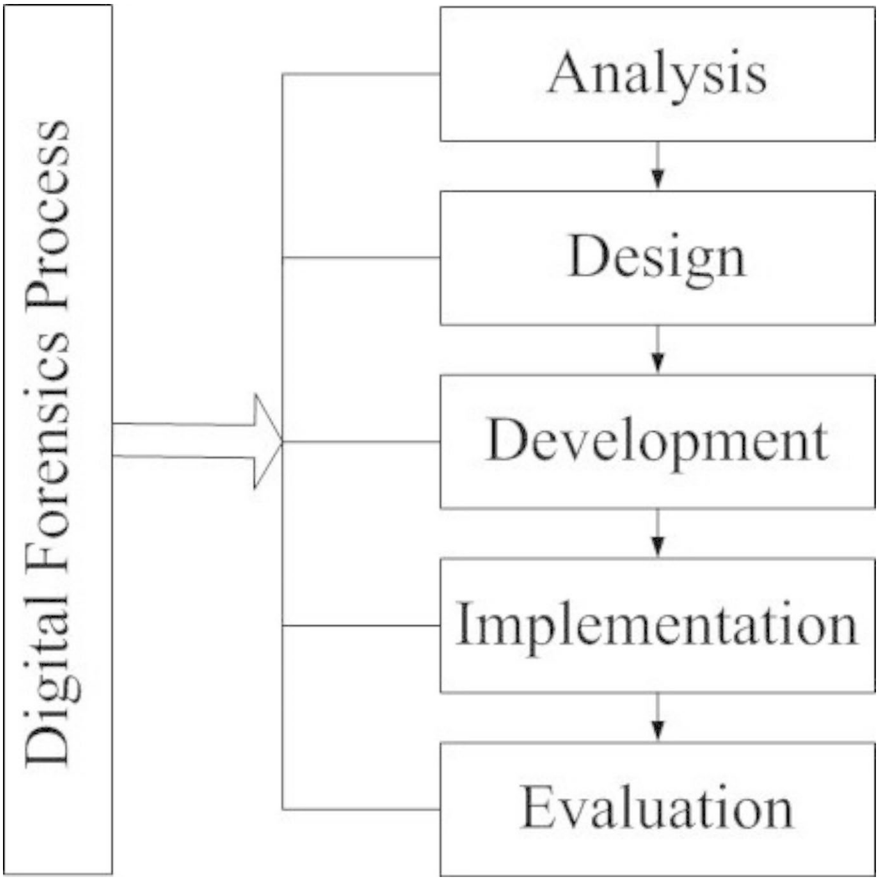


**Fig. 2** ADDIE Digital Forensics Model

ensure the authenticity and integrity of the likely digital evidence due to the fragility of digital evidence (ILAC, 2014).

## 5 Validating ADDIE Model

In this section, we propose a novel model for digital forensic science by validating the model using an investigative methodology. The use of digital forensic models is widespread, as the evidence gets checked through a series of processes that guarantees its credibility and accuracy (Antwi-boasiako & Venter, 2011). For this study, our main goal is the analysis of active digital evidence from P2P networks. Digital forensic investigation is fast becoming an imperative topic to enhance to the total security of P2P networks. A digital forensic analysis usually consists of these four critical processes: acquisition, identification, evaluation, and presentation (Homem et al., 2016). These processes were subject of several review and research as discussed in Sect. 2.1 and integrated to trace digital signatures from digital artefacts that can be presented for admissibility in a court of law. Consequently, researchers have reviewed the procedures into preservation, collection, examination, analysis, and presentation. Over the years, the digital forensic analysis model continued to be modified to reflect the current digital challenges by harmonizing and integrating existing iterative and multitier models to conduct digital investigations under legal terms and conditions (Oltsik et al., 2017). The SANS Institute (Stroud, 2020) recently revised the most dominant digital forensic methods in their annual report of 2020 to five critical steps: Analysis, Design, Development, Implementation, and Evaluation, as shown in Fig. 2.

### 5.1 Experimental Setup and Methodology

In order to collect information from the µTorrent network, such as the hash value and IP addresses, we employed the Kickass 2021 tracker https://Kickasstorrents.to/Usearch/Searchquery>, (n.d.) as explained in Sect. 6. Kickass 2021 tracker is executed over µTorrent client, which is a popular BitTorrent client (Bilgen & Wagner, 2017). We crawled the µTorrent network for 10 days, starting from March 5th, 2020. The network was crawled on four different occasions, with each crawl lasting 3 days, therefore obtaining 4 crawl datasets. The data was then loaded into Weka for processing. A set of scripts was used to obtain the popular peers and visualize the change in their popularity over different collection intervals. Table 1. presents the number of peers and the size of the packets recorded in each collection interval.

**Table 1** Total Number of Active Peers That Participated in the Network

| Day | Collection Period | No. of Available Peers | % of Packets Captured | Total Packets Captured (bytes) |
|---|---|---|---|---|
| Friday - Sunday | **March 5th – 7th** | **304** | **100%** | **92,378** |
| Monday - Wednesday | **March 8th – 10th** | **30** | **100%** | **36** |
| Thursday - Friday | **March 11th – 13th** | **287** | **100%** | **1646** |
| Saturday - Monday | **March 14th – 16th** | **2455** | **100%** | **33,087** |

The ADDIE model objectives of each phase are as follows:

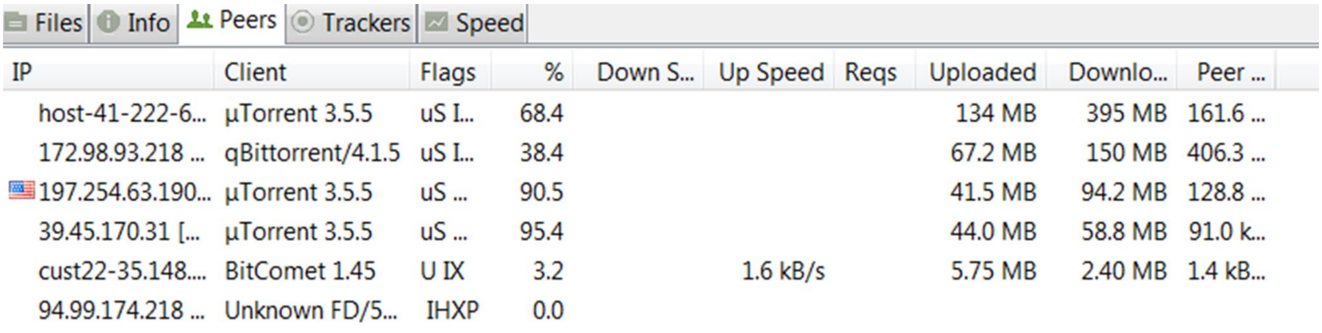
**Analysis** The Analysis phase of ADDIE is the initial stage and the most crucial model phase. It is where the investigation techniques are planned. This stage requires careful considerations because collecting incorrect data invalidates all the results in the ADDIE model. The investigation aims to collect digital evidence from the µTorrent network while Wireshark will facilitate the collection. Wireshark supports the detection of peers that participate in a network without jeopardizing the functionality or integrity of the network. The validity of the model and its applications are proved in this phase for method validation as described in Sect. 3.2.

**Design** In the Design phase, the focus is on the significance of the data to the digital investigation process. Wireshark was used to monitor and capture all the network traffic. Figure 3 shows active peers participating in the µTorrent network during the investigation. We ran the investigation for a total of ten days by participating in the download of a pirated movie that was still showing in the cinema at the time of the study. This was deemed necessary to test the usability of our model using real datasets. We operated under the assumption that Wireshark can capture all participating peers for validation as described in Sect. 3.2.

**Development** The significance of the data then guides the creation of the evidence file in the Development phase of the ADDIE model. The success of the model thus far can be seen visibly in Fig. 3 as participating peers are captured on the network.

**Implementation**: The Implementation phase puts all the four phases of the ADDIE model into practice, drawing upon the investigator's individual experience and delivery skills. Hence, we experimented as follows: In order to preserve a clean experimental environment, we ensured only µTorrent and Wireshark were running on the machine. We then started Wireshark first and enabled it to capture before simultaneously starting µTorrent. We then uploaded the tracker to start downloading. This ensured the clean capture of all the network traffic between the µTorrent and other clients holding the file. The capture ended when the file finished downloading. The evidence file content resulting from the first three phases of ADDIE is saved as the raw data of the investigation in this phase. In our case, this is when Wireshark completes its capture up to the database stage, as illustrated in Fig. 3. The data collected is then copied and transported to a database in .csv (comma separated values) format without losing the integrity of the data or altering its configuration.

**Evaluation** Finally, the effectiveness of the captured data and the investigator's expertise are assessed in the Evaluation phase of the design process followed by Sect. 6. Based on all the successfully executed phases, the robustness of the model has been proved for method validation as described in Sect. 3.2. Figure 4 illuminates the skeleton of our ADDIE model analysis and how the evidence detection



| IP | Client | Flags | % | Down S... | Up Speed | Reqs | Uploaded | Downlo... | Peer ... |
|---|---|---|---|---|---|---|---|---|---|
| host-41-222-6... | µTorrent 3.5.5 | uS I... | 68.4 | | | | 134 MB | 395 MB | 161.6 ... |
| 172.98.93.218 ... | qBittorrent/4.1.5 | uS I... | 38.4 | | | | 67.2 MB | 150 MB | 406.3 ... |
| 197.254.63.190... | µTorrent 3.5.5 | uS ... | 90.5 | | | | 41.5 MB | 94.2 MB | 128.8 ... |
| 39.45.170.31 [... | µTorrent 3.5.5 | uS ... | 95.4 | | | | 44.0 MB | 58.8 MB | 91.0 k... |
| cust22-35.148.... | BitComet 1.45 | U IX | 3.2 | | 1.6 kB/s | | 5.75 MB | 2.40 MB | 1.4 kB... |
| 94.99.174.218 ... | Unknown FD/5... | IHXP | 0.0 | | | | | | |

**Fig. 3** Active Peers on µTorrent Network

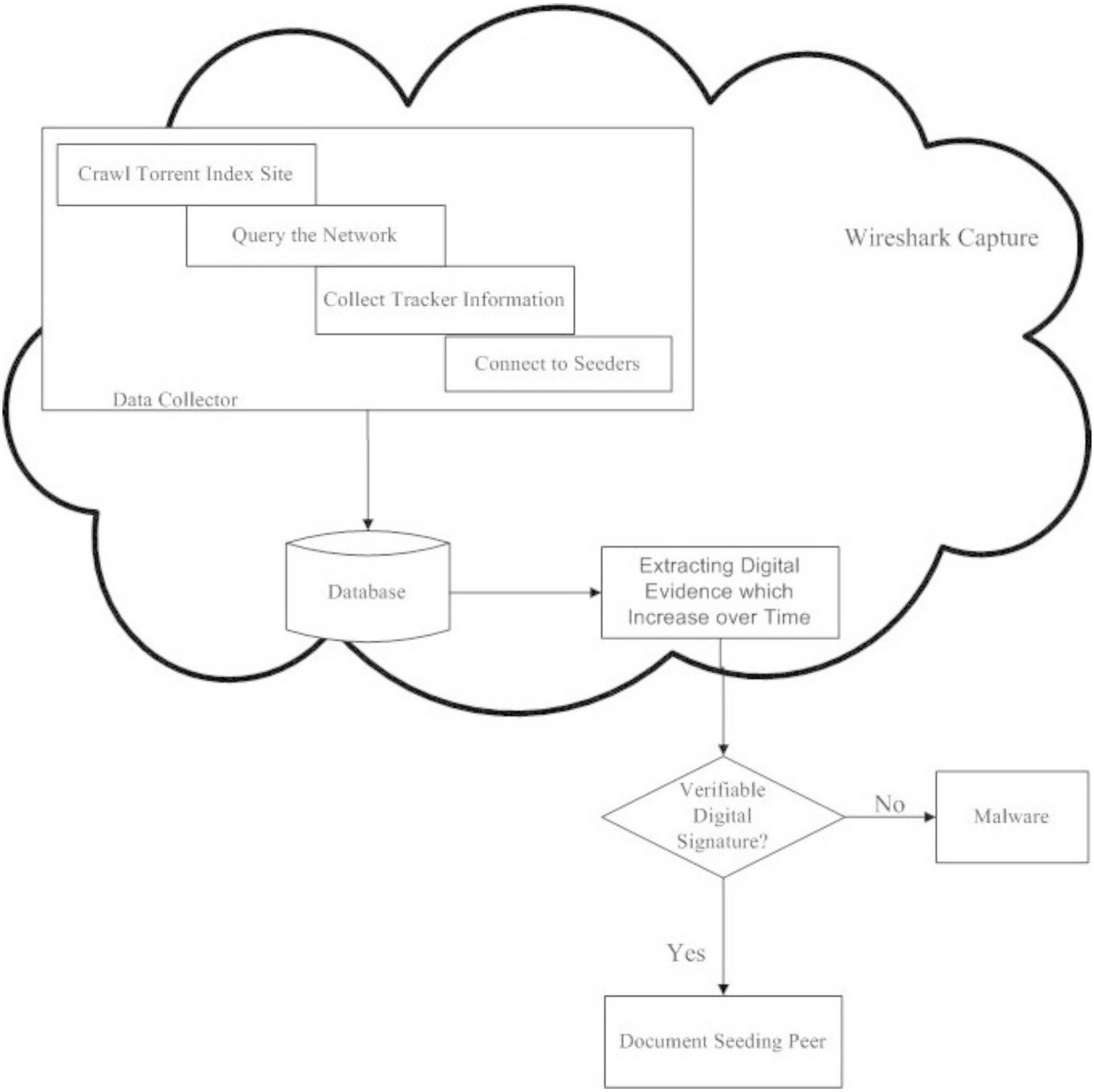


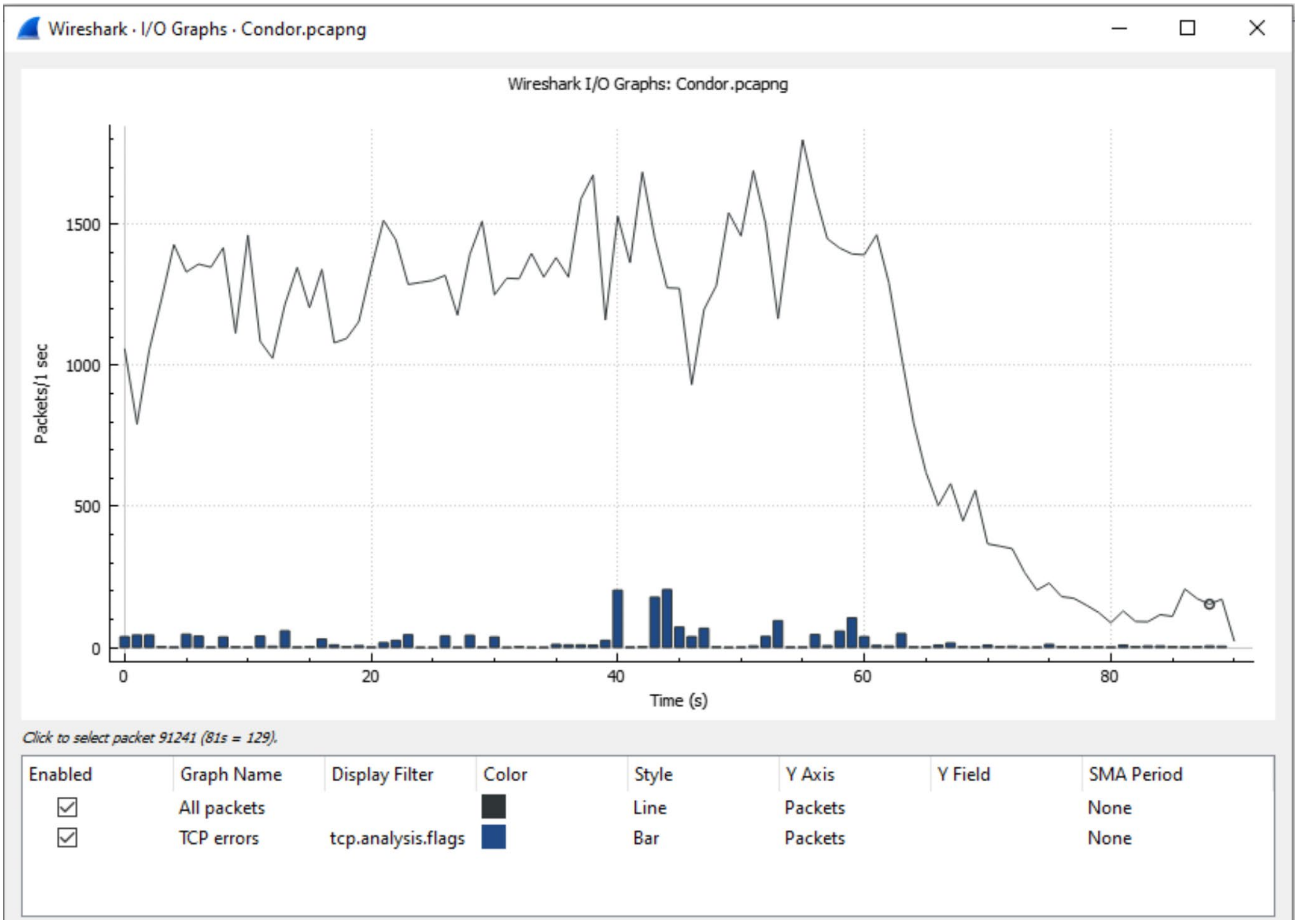
**Fig. 4** Evidence Collection Architecture

system maintained a simple architecture, as described in detail below.

Data Collector: The data collector stage is tasked with collecting tracker information from the crawled torrent index site and connecting to seeders. This is the normal process of acquiring a file in any torrent site, but here we are present in the network as passive agents to collect all the shared data and store it in a database (Fahimian et al., 2010). Wireshark supports the collection of data in this stage. The data collected could be usernames, peers' IP addresses, port numbers, crawl time, hash values, and other digital signatures of peers participating in the networks.

Active Analyser: The active analyser is simply tasked with listening on the P2P network and capturing hash values that increase over time.

Evidence Detector: The captured content hash values, which are found to be increasing over time in all seeding, are tagged and logged. If the hash values correspond with other distinct digital signatures, then we have a seeder. If


Wireshark · I/O Graphs · Condor.pcapng
Wireshark I/O Graphs: Condor.pcapng
Packets/1 sec
1500
1000
500
0
0
20
40
60
80
Time (s)

*Click to select packet 91241 (81s = 129).*

| Enabled | Graph Name | Display Filter | Color | Style | Y Axis | Y Field | SMA Period |
|---|---|---|---|---|---|---|---|
| ☑ | All packets | | ⬛ | Line | Packets | | None |
| ☑ | TCP errors | tcp.analysis.flags | 🟦 | Bar | Packets | | None |

**Fig. 5** TCP Error Rate of Session 4

the hash represents an empty file with variable unconfirmed data, then we have a suspect malware and therefore it is a bad file that does not get documented. (Y.-Y. Teing et al., 2016)

## 6 Evaluation

We will evaluate the validity of the ADDIE against the scientific acceptable standards of validating a new process model as follows:

### 6.1 Daubert Test Evaluation

The Daubert test was considered for application to the UK criminal law system in the Law Commission report of 2009 and 2011 *(The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales (LCCP190*>, 2009). They have also been applied successfully to support the admissibility of non-scientific testimony (e.g., Kumho Tire v. Carmichael 1999) (Heilbronner, 2018). We evaluated our experimental procedure in Sect. 5 for validation against the five-point Daubert test as follows:

**Testing: Has the scientific procedure been independently tested?**

ADDIE model is part of the Instructional System Design (ISD) family. It was created in 1975 for the US Army by the Centre for Educational Technology at Florida State University (Branson et al., 1975). Being a leader in training and learning, the military significantly influenced corporate and educational activities by adapting the ADDIE model. DeSimone et al. 2002 (Desimone et al., 2002) consider ADDIE to be a process model if applied correctly and a guide for gaining direct intuitive insight into a problem. In 2017, (Stroud, 2020) of SANS institute used the ADDIE model for the Digital Forensics Framework for Instruction Design (DFFID) in their whitepaper as a comprehensive digital framework designed to guide the development of future digital forensics. Moreover, Sect. 4.6, 4.7, and 4.8 has described a detailed independent use of the ADDIE model as a digital forensic model.

**Peer Review: Has the scientific procedure been published and subject to peer review?**

The methodology and results of Sects. 3, 4, and 5, have been submitted for peer review and publication to the Springer Special Issue in Cloud, IOT, and Data Science as follows:

**Musa, A.**, Awan, I., Zahrah F, The Case for Validating ADDIE Model as a Digital Forensic Model for Peer-to-Peer Network Investigation. Information System Frontier, (2022).

**Error rate: Is there a known error rate, or potential to know the error rate, associated with the use of this scientific procedure?**

The use of Wireshark provides TCP error rates over time as packets acknowledged (ACK) are transferred. Figure 5 shows when a packet is sent, and the ACK is received, and that most of the packets were ACK swiftly demonstrates the stability of the sequence that influences the TCP performance of our recovered evidence in Tables 1 and 2. The graph might illustrate instability, but this does not mean there is a problem because the communication time is presented in seconds and represents how the µTorrent application works. A typical example is when a node begins participating in the network but drops or fluctuates due to a network connection or another problem.

**Standards: Are there standards and protocols for the execution of the methodology?**

ADDIE model was created for the U.S. Army and was later recognized by DeSimone et al. 2002 (Desimone et al., 2002) to be a general process model and a guide for gaining direct intuitive insight into a problem. Therefore, the model is associated with the U.S. Federal rules as a standard digital forensic methodology. As evident in Sect. 2.2, the model standards continue to be refined with time.

**Acceptance: Does the relevant scientific community generally accept the scientific procedure?**

ADDIE has evolved many times over the years to become dynamic, iterative, and user-friendly. While the concept of ADDIE has been around since 1975, it has never been used for digital forensics or P2P network investigation. This is the first time ADDIE has been used as a digital forensic process for network forensics to the best of our knowledge. Therefore, due to its novelty, ADDIE is yet to be tested with the relevant scientific community.

## 6.2 Method Validation Evaluation

The first edition focus for accreditation in FSR-218 of the FSR was on the laboratory-developed methods, but the second and following editions incorporate the crime scene in its range (FSR-G-201, 2020). The requirement to describe the reliability of scientific evidence extends to any procedure when the operation impacts the results acquired, wherever it is used. The FSR guidance has accepted that assessing the completeness and relevance of objective evidence put together by others in developmental validation or collaborative studies should be somewhat straightforward if the requirements provided in the guidance for each of the stages of the validation process have been satisfied. Like the Daubert test, publications in respected scientific journals can be relied on in considering the scientific model concerning its limits and the validity of applicability (Ireland & Beaumont, 2015). However, the guidance expects that where a method applies any scientific model (or supports the interpretation or assessment of the results of a model), the specification should also address the following matters:

**"The validity of the model/theory" and "The validity of the application of the model/theory in the method"**

ADDIE has been a process model for years. As an adapted model, its applicability was reviewed to ensure that the model is fit for purpose for P2P network investigations. We tested the model in Sects. 2 and 3 to demonstrate that it is competent as a digital forensic model for P2P network investigation.

**"Any assumptions incorporated within the model/theory." and "The validity of the assumptions and any limits on the application of the assumptions." and "Limits on the application of the model/theory"**.

We made the following assumptions during our experiment:

1. We assumed that Wireshark could capture all the µTorrent network traffic during the experiment.
2. We relied on the validity of the evidence recovered from Wireshark, such as IP address, hash values, communication protocols, and etcetera.
3. We assumed that the applicability of ADDIE as a process model is capable of formulizing P2P network investigation.

The use of Wireshark is widespread as the de-facto standard for inspecting and analysing network packets. Summarily, it's a packet analysing tool that allows packet sniffing of the network and aids in viewing all the traffic that goes in and out of your network adapter. Therefore, we deem Wireshark valid to satisfy our assumptions 1 and 2. For assumption 3, ADDIE has only been tested on the µTorrent network, a decentralized P2P network and is yet to be tested on other P2P architecture, such as the centralized and hybrid design. However, the centralized design exhibits the same properties as the client/server network, and the hybrid network mixes the centralized and decentralized design. As such, the only limit to our assumptions is that the model is not yet widespread and tested on other P2P architectures. There are currently no limits declared on our model's application except the assumptions we made.

**"The robustness of the model/theory based on the information supporting it.“**

ADDIE model was created for the U.S. Army and was later recognized by DeSimone et al. 2002 (Desimone et al., 2002) to be a general process model and a guide for gaining direct intuitive insight into a problem. Consequently, the model is associated with the U.S. Federal rules as a standard digital forensic methodology. As evident in Sect. 2.2, the model standards continue to be refined with time to become dynamic, iterative, and user-friendly. While the concept of ADDIE has been around since 1975, it has never been used for digital forensics or P2P network investigation. This is the first time ADDIE has been used as a digital forensic process for network forensics to the best of our knowledge. Therefore, due to its novelty, ADDIE is yet to be tested with the relevant scientific community.

The evaluation of the ADDIE model is shown by using tools validated by (Stroud, 2020) to demonstrate the effectiveness of our model. The use of validated tools also supports our argument for method validation as the validity of the model has already been proved by a recognized international forensic unit. We used the SOP of the ADDIE model with the µTorrent P2P network to evaluate our proposed methodology from Sect. 2, due to its usability and it been the most popular BitTorrent client (Venčkauskas, Damaševičius, et al., 2015). µTorrent is a decentralized peer-to-peer file-sharing system that allows you to share or download torrent files with peers on the network. A torrent file is responsible for distributing metadata known as Torrents (Kotary & Nanda, 2020). The metadata instructs µTorrent to connect to remote peers for seeding. Seeders are the peers that actively share bits of files in the P2P network, while a peer is any computer running a µTorrent client (Khan et al., 2014). To share content, a peer first converts their file into a small torrent. The Torrent contains metadata about the file to be shared and the tracker, coordinating the file distribution. The peer identifies content using a Uniform Resource Locator (URL) known as the tracker designed to integrate persistently with other peers (Su et al., 2018). Its supremacy over plain Hypertext Transfer Protocol (HTTP) is that many secure simultaneous downloads of the same file are possible. The seeders upload chunks of packets to each other, making it feasible for the file source to support enormous seeders with only an economic increase in its load (Vlachos et al., 2004). A peer that wants to download the file must first get the metadata torrent file and connect to the specified tracker, which connects other peers to seed the bits of the file.

The acquisition of evidence from digital artefacts, such as the µTorrent client is used to investigate peers' malicious behaviours and patterns. There is sufficient evidence hidden in digital artefacts that needs careful analysis using suitable tools and techniques to visualize the evidence as done by (Hamidović & Hadžib, 2016). Often the content shared on P2P networks such as µTorrent are from peers that do not care about damaging the security and privacy laws of the land. Hence, several models of digital forensics have been proposed for diverse investigation forms for law enforcement, military, and business operations in digital investigation (Liu et al., 2018; Manesh et al., 2011; Shinder & Cross, 2008).

## 6.3 Validation Report

We have described the processes that make up a validation process of a digital forensic framework in Sect. 6.1 and 6.2. ADDIE model was validated against the Daubert test of US forensic standards and the FSR-G-201 and FSR-G-218 guidance of UK forensic standards. The model was evaluated based on the experiments conducted on µTorrent networks in Sect. 5.1. ADDIE model meets all the requirements of the Daubert test except for requirement 5 as it is yet to be tested with the relevant scientific community due to its novelty. The UK FSR-G-201 and FSR-G-218 guidance for method validation on new and adapted models/theory have also been satisfied except for the robustness of the model based on the information supporting it, which is also yet to be tested. Summarily, the UK and U.S forensic standards for validation are somewhat similar, with the former being more comprehensive and the latter being more accepted and tested. Therefore, the validation report has tested the usability of the method over the internationally approved standards appropriate to use the model.

## 6.4 Results

We validated our methodology by extracting the top popular file hash values in each of the collection periods of Table 2. We then selected the peers who were uniformly increasing in packets seeding for all the collection periods. We collated the top 3 peers with the highest percentage of packets shared throughout the µTorrent network session. Due to the frail nature of digital evidence acquisition, the data transferred from any forensic tool must be verifiable and identical to the original source file. That is how to ensure the integrity of the process by monitoring the files' hash value, IP addresses, and packets alongside the raw network traffic capture throughout the digital investigation process (Antwi-boasiako & Venter, 2011). We documented the top 3 peers with the highest percentage of packets shared throughout

**Table 2** Recovered Digital Evidence from All the Collection Periods

| Collection Period | IP | Protocol | SHA-256 Information Value |
|---|---|---|---|
| **March 5th – 7th** | 41.212.82.169 | TCP | 9285be3792998811b0a8c-d47a36711e3647fdbeda837e-ba5f7ac682e5aec96ad |
| | 115.187.49.130 | UDP | 9285be3792998811b0a8c-d47a36711e3647fdbeda837e-ba5f7ac682e5aec96ad |
| | 172.98.93.218 | UDP | 9285be3792998811b0a8c-d47a36711e3647fdbeda837e-ba5f7ac682e5aec96ad |
| **March 8th – 10th** | 207.180.192.206 | UDP | 7c24bf-cb537b125637d8c747bffa-b9a586787bb6ec41737828de-b6aa5d9d30f6 |
| | 54.146.221.202 | TCP | 7c24bf-cb537b125637d8c747bffa-b9a586787bb6ec41737828de-b6aa5d9d30f6 |
| | 114.38.138.7 | UDP | 7c24bf-cb537b125637d8c747bffa-b9a586787bb6ec41737828de-b6aa5d9d30f6 |
| **March 11th – 13th** | 216.241.154.212 | TCP | db946a96aff752b279ed6df-c6ee0857f059264513b4655ff 2bd76f1cd2740df6 |
| | 46.123.241.255 | TCP | db946a96aff752b279ed6df-c6ee0857f059264513b4655ff 2bd76f1cd2740df6 |
| | 184.90.233.60 | UDP | db946a96aff752b279ed6df-c6ee0857f059264513b4655ff 2bd76f1cd2740df6 |
| **March 14th – 16th** | 195.35.245.30 | UDP | 76448c2a84bbcd13e-fe10aa3a176c8d-d94bd3dd8d07abf9c-c5e474ce70134d10 |
| | 186.149.236.13 | UDP | 76448c2a84bbcd13e-fe10aa3a176c8d-d94bd3dd8d07abf9c-c5e474ce70134d10 |
| | 4.16.74.104 | TCP | 76448c2a84bbcd13e-fe10aa3a176c8d-d94bd3dd8d07abf9c-c5e474ce70134d10 |

the µTorrent network session. We then selected the peers that were uniformly increasing in packets seeding for all the collection periods. The peer's digital signatures were matched with the already verified hash values to check for integrity as illustrated in Table 2. By participating in the P2P network itself, the evidence collected does not need to be reverse engineered, i.e., all the evidence available can be matched with another regular client of that network using the hash values (Hamidović & Hadžib, 2016). This is because once any network traffic is collected, each packet is logged, timestamped, and traceable by its hash value. This technique simplifies real-time event reconstruction packet by packet, imitating the original traffic (Tukur et al., 2019).

Using the ADDIE model to complete our evaluation (Vijayakumar & Srinivasan, 2015), we implemented and evaluated that captured raw data presented in Table 2. The integrity of our evaluation was ensured through the implementation of regular hash checking on the collected data using SHA256 (Secure Hashing Algorithm producing a 256-bit long hash) (Norman, 2017). The hash value remained the same as the original value in each collection period throughout our evaluation. Wireshark collated a stream of hashed information stored on the external drive and was exported to a .csv format. During the transmission process, the integrity of each of the transferred chunks was maintained due to a SHA256 hash being computed as the chunk is being transmitted (Peterson & Davie, 2012). Also, once the transmission was completed, another SHA256 hash is taken on each chunk and was verified against the original. If, for any reason, hashes do not match at any point of the ADDIE process, the file's integrity has been compromised during the investigation. In such a case, the whole investigation has to be repeated from the Analysis stage of the ADDIE model using the original copy of the source file.

## 7 Conclusion

With the increase in network traffic mainly attributed to P2P technologies, there is a corresponding increase in the possibility of these technologies being the subject of a criminal investigation. Consequently, the number of investigations requiring digital forensic proficiency is rendering digital investigation slow and ultimately ineffective, with the pursuit of a perfect model for digital investigation as never-ending.

This paper presented a proposed live monitoring methodology for P2P networks to provide accountability to the system. We have adopted a proven monitoring mechanism of live networks using Wireshark and made a case for its application as part of the processes of network forensics. We also made a case for applying the ADDIE model of digital forensics to passive digital evidence investigation, potentially revolutionizing network forensics through evidence validation. We also proposed a validation case to standardize the ADDIE model as a formal digital forensic model using the FSR-G-218 and FSR-G-201 legislative guidance.

There are many issues that need improvement, and we are actively working on them as part of our future works. One of them is searching the IP addresses of the most popular peers against DNS checkers and finding almost half of our recovered IP addresses masked under VPNs. Yet, we are confident that even if our digital evidence does not directly link a crime and its victim, it can be helpful in an investigation. Digital evidence can help reveal how a cybercrime was committed, support or disprove witness statements, provide investigative leads, and identify possible suspects.

## Declarations

**Conflict of interest** The authors can declare that there was no conflict of interest related to the content of this article.

## References

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118–131. https://www.researchgate.net/publication/228410430_Systematic_Digital_Forensic_Investigation_Model.

Alhazmi, A., Macia-Fernandez, G., Camacho, J., & Salah, S. (2017a). Torrent Forensics: Are your Files Being Shared in the BitTorrent Network? *CYBER 2017: The Second International Conference on Cyber-Technologies and Cyber-Systems Torrent*, *December*. https://www.researchgate.net/profile/Saeed-Salah/publication/322131860_Torrent_Forensics_Are_your_Files_Being_Shared_in_the_BitTorrent_Network/links/5a469a420f7e9ba868aa5068/Torrent-Forensics-Are-your-Files-Being-Shared-in-the-BitTorrent-Network.pdf

Alhazmi, A., Macia-Fernandez, G., Camacho, J., & Salah, S. (2017b). Torrent Forensics: Are your Files Being Shared in the BitTorrent Network? *CYBER 2017: The Second International Conference on Cyber-Technologies and Cyber-Systems Torrent*, *December*.

Ali, A., Abd Razak, S., Othman, S. H., Mohammed, A., & Saeed, F. (2017). A metamodel for mobile forensics investigation domain. *PLOS ONE*, *12*(4), e0176223. https://doi.org/10.1371/journal.pone.0176223.

Allen, M. (2017). Designing Online Asynchronous Information Literacy Instruction Using the ADDIE Model. In *Distributed Learning* (pp. 69–91). Elsevier. https://doi.org/10.1016/B978-0-08-100598-9.00004-0

Amad, M., Meddahi, A., & Aïssani, D. (2012). *Peer to Peer Networks Management Survey*. *9*(1), 139–148. http://arxiv.org/abs/1203.3351

Antwi-boasiako, A., & Venter, H. (2011). *Advances in Digital Forensics VII*. *361*, 23–38. https://doi.org/10.1007/978-3-642-24212-0

Bilgen, O., & Wagner, A. B. (2017). A new stable peer-to-peer protocol with non-persistent peers. *Proceedings - IEEE INFOCOM*, 1–21. https://doi.org/10.1109/INFOCOM.2017.8057141

Bodriagov, O., & Buchegger, S. (2013). Encryption for peer-to-peer social networks. In *Security and Privacy in Social Networks* (pp. 47–65). https://doi.org/10.1007/978-1-4614-4139-7_4

Boskov, N. (2020). *40 Jaw-Dropping Google Stats & Facts (2020 Edition)*. WebsiteBuilder. https://websitebuilder.org/blog/google-stats/

Branson, R. K., Rayner, G. T., Cox, L. J., Furman, J. P., King, F. J., & Hannum, W. H. (1975). Interservice Procedures for Instructional Systems Development. Executive Summary and Model. *TRADOC Pam 350 – 30, Ft. Monroe, VA: U.S. Army Training and Doctrine Command*, *1–5*, 1–185. https://apps.dtic.mil/sti/citations/ADA019486

Desimone, L., Werner, M., & Harris, M. (2002). Human Resource Development. *Academy of Management Journal*, *42*(3), 288–303.

Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. *European Conference on Information Warfare and Security, ECCWS*, 573–581. https://arxiv.org/ftp/arxiv/papers/1708/1708.01730.pdf

ENFSI (2015). *Best Practice Manual for the Forensic Recovery, Identification and Analysis of Explosives Traces*. *01*(November), 1–21. https://enfsi.eu/wp-content/uploads/2016/09/9._forensic_recovery_identification_and_analysis_of___explosives_traces_0.pdf

Fahimian, S., Movahed, A., & Kharrazi, M. (2010). Passive worm and malware detection in peer-to-peer networks. *Proceedings - IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, EUC 2010*, 561–565. https://doi.org/10.1109/EUC.2010.133

FSR-G-201 (2020). *Forensic Science Regulator Guidance: Expert Report Guidance*. *2*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/920449/201_-_FSR-G-201_Validation_Guidance_Issue_2.pdf

FSR-G-218 (2020). *Forensic Science Regulator Guidance: Expert Report Guidance*. *2*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/921392/218_Method_Validation_in_Digital_Forensics_Issue_2_New_Base_Final.pdf

Hamidović, H., & Hadžib, S. (2016). The Basic Steps of Digital evidence handling process. *International Journal of Information and Communication Technologies*, *4*(February), 113–122.

Heilbronner, R. L. (2018). Kumho Tire v. Carmichael. In *Encyclopedia of Clinical Neuropsychology* (pp. 1940–1940). Springer International Publishing. https://doi.org/10.1007/978-3-319-57111-9_999

Hitchcock, B., Le-Khac, N. A., & Scanlon, M. (2016). Tiered forensic methodology model for digital field triage by non-digital evidence specialists. *DFRWS 2016 EU - Proceedings of the 3rd Annual DFRWS Europe*, *16*, S75–S85. https://doi.org/10.1016/j.diin.2016.01.010

Homem, I., Kanter, T., & Rahmani, R. (2016). Improving distributed forensics and incident response in loosely controlled networked environments. *International Journal of Security and Its Applications*, *10*(1), 385–414. https://doi.org/10.14257/ijsia.2016.10.1.35.

House of Commons Science Technology Committee (2019). *Forensic Science on Trial*. https://publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf

ILAC (2014). Modules in a Forensic Science Process. *Ilac.Org*, 1–37. https://ilac.org/latest_ilac_news/ilac-g19082014-published/

Imada, N., & Ueda, K. (2016). Peer-to-Peer Network System and Application Design on Multiple Virtual Networks. *NBiS 2016–19th International Conference on Network-Based Information Systems*, 298–302. https://doi.org/10.1109/NBiS.2016.66

Ireland, J., & Beaumont, J. (2015). Admitting scientific expert evidence in the UK: reliability challenges and the need for revised criteria

– proposing an abridged daubert. *Journal of Forensic Practice*, *17*(1), 3–12. https://doi.org/10.1108/JFP-03-2014-0008.

ISO/IEC 17025 (2017). : *General requirements for the competence of testing and calibration laboratories*. https://www.iso.org/obp/ui/#iso:std:iso:679:ed-2:v1:en

Jo, S., & Han, J. (2018). Convergence P2P cloud computing. *Peer-to-Peer Networking and Applications*, *11*(6), 1153–1155. https://doi.org/10.1007/s12083-018-0661-1.

Kao, D. Y., & Wu, G. J. (2015). A Digital Triage Forensics framework of Window malware forensic toolkit: Based on ISO/IEC 27037:2012. *2015 International Carnahan Conference on Security Technology (ICCST)*, 217–222. https://doi.org/10.1109/CCST.2015.7389685

Karen, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. https://csrc.nist.gov/publications/detail/sp/800-39/final

Karie, N. M., Kebande, V. R., Venter, H. S., & Choo, K. K. R. (2019). On the importance of standardising the process of generating digital forensic reports. *Forensic Science International: Reports*, *1*, 100008. https://doi.org/10.1016/j.fsir.2019.100008.

Kaur, P., Bijalwan, A., Joshi, R. C., & Awasthi, A. (2018). Network Forensic Process Model and Framework: An Alternative Scenario. In *Intelligent Communication, Control and Devices* (pp. 493–502). https://doi.org/10.1007/978-981-10-5903-2_50

Khan, S., Shiraz, M., Wahid, A., Wahab, A., Gani, A., Han, Q., Bin, Z., & Rahman, A. (2014). A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing. *The Scientific World Journal*, *2014*.

Kickass (2021). (n.d.). https://kickasstorrents.to/usearch/searchquery/ Retrieved October 10, from

Kigwana, I., Kebande, V. R., & Venter, H. S. (2017). A proposed digital forensic investigation framework for an eGovernment structure for Uganda. *2017 IST-Africa Week Conference, IST-Africa 2017*. https://doi.org/10.23919/ISTAFRICA.2017.8102348

Kotary, D. K., & Nanda, S. J. (2020). Distributed clustering in peer to peer networks using multi-objective whale optimization. *Applied Soft Computing Journal*, *96*. https://doi.org/10.1016/j.asoc.2020.106625

Liberatore, M., Erdely, R., Kerle, T., Levine, B. N., & Shields, C. (2010). Forensic investigation of peer-to-peer file sharing networks. *DFRWS 2010 Annual Conference*, *7*. https://www.sciencedirect.com/science/article/pii/S1742287610000393

Liu, G., Yan, Z., & Pedrycz, W. (2018). Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey. *Journal of Network and Computer Applications*, *105*(October 2017), 105–122. https://doi.org/10.1016/j.jnca.2018.01.004

Manesh, T., Brijith, B., & Singh, M. P. (2011). An improved approach towards network forensic investigation of HTTP and FTP protocols. *Communications in Computer and Information Science*, *203 CCIS*, 385–392. https://doi.org/10.1007/978-3-642-24037-9_38

Mao, Y., Deb, S., Venkatakrishnan, S. B., Kannan, S., & Srinivasan, K. (2020). Perigee: Efficient Peer-to-Peer Network Design for Blockchains. *Proceedings of the Annual ACM Symposium on Principles of Distributed Computing*, 428–437. https://doi.org/10.1145/3382734.3405704

Meyers, M., & Rogers, M. (2006). Digital forensics: Meeting the challenges of scientific evidence. In *IFIP International Federation for Information Processing* (Vol. 194, pp. 43–50). https://doi.org/10.1007/0-387-31163-7_4

Montasari, R. (2016). Review and Assessment of the existing Digital forensic investigation process models. *International Journal of Computer Applications*, *147*(7), 41–49. https://doi.org/10.5120/ijca2016911194.

Mothi, D., Janicke, H., & Wagner, I. (2020). A novel principle to validate digital forensic models. *Forensic Science International: Digital Investigation*, *33*(2011). https://doi.org/10.1016/j.fsidi.2020.200904

Musa, A. (2020a). Analysis of UDP Traffic norms through packet sniffing on peer-to- peer networks. *JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION ISSN: 2277-0011. Journal Homepage: Www Atbuftejoste Com*, *8*(2), 286–292.

Musa, A. (2020b). Packet tracing and analysis of TCP Traffic on Transport Layer of peer to peer networks. *JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION ISSN: 2277-0011. Journal Homepage: Www Atbuftejoste Com*, *8*(2), 270–276.

Musa, A., Abubakar, A., Gimba, U. A., & Rasheed, R. A. (2019). An investigation into peer-to-peer network security using wireshark. *2019 15th International Conference on Electronics, Computer and Computation, ICECCO 2019*, *Icecco*. https://doi.org/10.1109/ICECCO48375.2019.9043236

Musa, A., Almohannadi, H., & Alhamar, J. (2018). Malware propagation modelling in peer-to-peer networks: A review. *Proceedings – 2018 IEEE 6th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2018*, 198–202. https://doi.org/10.1109/W-FiCloud.2018.00038

Nadiyah, R. S., & Faaizah, S. (2015). The development of Online Project Based Collaborative Learning using ADDIE Model. *Procedia - Social and Behavioral Sciences*, *195*, 1803–1812. https://doi.org/10.1016/j.sbspro.2015.06.392.

NIST (2017). *Computer Forensics Tool Testing Program (CFTT)*. https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

Norman, T. (2017). Information Technology Systems Infrastructure. In *Effective Physical Security: Fifth Edition* (pp. 311–341). Elsevier. https://doi.org/10.1016/B978-0-12-804462-9.00018-X

Oltsik, B. J., Senior, E. S. G., & Analyst, P. (2017). *Digital Transformation, Network Security, and Forcepoint*. *January*.

Palmer, G. (2001). A road map for digital forensic research. *Proceedings of the Digital Forensic Research Conference, DFRWS 2001 USA*, iii–42. https://slidelegend.com/a-road-map-for-digital-forensic-research-dfrws_5a0d193c1723dd47c60097b1.html

Peersman, C., Schulze, C., Rashid, A., Brennan, M., & Fischer, C. (2016). iCOP: live forensics to reveal previously unknown criminal media on P2P networks. *Digital Investigation*, *18*, 50–64. https://doi.org/10.1016/j.diin.2016.07.002.

Peterson, L. L., & Davie, B. S. (2012). Applications. In *Computer Networks* (pp. 697–800). Elsevier. https://doi.org/10.1016/b978-0-12-385059-1.00009-0

Pollitt, M. (1995). Computer forensics: An approach to evidence in cyberspace. *In Proceedings of the National Information Systems Security Conference*, 487–491.

Pollitt, M. M. (2007). An Ad Hoc Review of Digital Forensic Models. *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)*, 43–54. https://doi.org/10.1109/SADFE.2007.3

Reinsel, D., Gantz, J., & Rydning, J. (2018). The Digitization of the World - From Edge to Core.Framingham: International Data Corporation, *November*, US44413318. https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of Digital Forensic Models. *International Journal of Digital Evidence*, *1*(3), 1–12.

Scanlon, M., Farina, J., & Kechadi, M. T. (2015a). Network investigation methodology for BitTorrent Sync: a peer-to-peer based file synchronisation service. *Computers and Security*, *54*, 27–43. https://doi.org/10.1016/j.cose.2015.05.003.

Scanlon, M., Farina, J., & Kechadi, M. T. (2015b). Network investigation methodology for BitTorrent Sync: a peer-to-peer based file synchronisation service. *Computers and Security*, *54*, 27–43. https://doi.org/10.1016/j.cose.2015.05.003.

Scanlon, M., Farina, J., Khac, N. A., Le, & Kechadi, T. (2014). Leveraging decentralization to extend the Digital evidence Acquisition Window: Case Study on BitTorrent Sync. *Journal of Digital Forensics Security and Law*, *9*(December), 85–99. https://doi.org/10.1080/15313204.2014.941449.

Scanlon, M., & Kechadi, T. (2014). The Case for a Collaborative Universal Peer-to-Peer Botnet Investigation Framework. *Proceedings of the 9th International Conference on Cyber Warfare and Security*, 287–293. https://doi.org/10.1038/nature03184

Shinder, L., & Cross, M. (2008). Understanding the Technology. In *Scene of the Cybercrime* (pp. 121–200). Elsevier. https://doi.org/10.1016/b978-1-59749-276-8.00004-2

Stroud, L. (2020). *Information Security Reading Room Assisted Security Investigations Using ______________________ Th e In st itu te, A ho et ai ns ll Ri gh ts*. https://www.sans.org/reading-room/whitepapers/bestprac/forensication-education-digital-forensics-instructional-framework-37582

Su, S. C., Chen, Y. R., Tsai, S. C., & Lin, Y. B. (2018). Detecting P2P Botnet in Software Defined Networks. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/4723862

SWGDE (2015). *SWGDE Establishing Confidence in DF Results 020515.pdf.* https://www.irisinvestigations.com/wp-content/uploads/2016/12/ToolBox/02-STANDARDS & BEST PRACTICES/SWGDE Establishing Confidence in DF Results 020515.pdf

Teing, Y. Y., Dehghantanha, A., Raymond Choo, K. K., & Yang, L. T. (2016). Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study. *Computers and Electrical Engineering*, *0*(0), 1–14. https://doi.org/10.1016/j.compeleceng.2016.08.020.

Teing, Y. Y., Dehghantanha, A., Choo, K. K. R., & Yang, L. T. (2017). Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study. *Computers and Electrical Engineering*, *58*, 350–363. https://doi.org/10.1016/j.compeleceng.2016.08.020.

Thakar, A. A., Kumar, K., & Patel, B. (2021). Next Generation Digital Forensic Investigation Model (NGDFIM) - Enhanced, Time Reducing and Comprehensive Framework. *Journal of Physics: Conference Series*, *1767*(1). https://doi.org/10.1088/1742-6596/1767/1/012054

*The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales (LCCP190)* (2009). https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

Tukur, Y. M., Thakker, D., & Awan, I. U. (2019). Multi-layer approach to internet of things (IoT) security. *Proceedings – 2019 International Conference on Future Internet of Things and Cloud, FiCloud 2019*, 109–116. https://doi.org/10.1109/FiCloud.2019.00023

Tukur, Y. M., Thakker, D., & Awan, I. U. (2020). Edge-based blockchain enabled anomaly detection for insider attack prevention in internet of things. *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.4158.

Venčkauskas, A., Damaševičius, R., Jusas, N., Jusas, V., & Maciulevičius, S. (2015). *Investigation of Artefacts Left by BitTorrent Client in Windows 8 Registry*. *3*(2), 25–31. https://doi.org/10.12691/iscf-3-2-1

Venčkauskas, A., Jusas, V., Paulikas, K., & Toldinas, J. (2015). Investigation of artifacts left by bittorrent client on the local computer operating under windows 8.1. *Information Technology and Control*, *44*(4), 451–461. https://doi.org/10.5755/j01.itc.44.4.13082.

Venčkauskas, A., Jusas, V., Paulikas, K., & Toldinas, J. (2016). A methodology and tool for investigation of artifacts left by the BitTorrent client. *Symmetry*, *8*(6), https://doi.org/10.3390/sym8060040.

Vijayakumar, S., & Srinivasan, D. M. P. (2015). Efficacy of Addie Model in the Digital Classroom: an Evidence Based Study.LangLit An International Peer-Reviewed Open Access Journal, *2*(1).

Vishnumurthy, V., & Francis, P. (2007). A comparison of structured and unstructured P2P approaches to heterogeneous random peer selection. *2007 USENIX Annual Technical Conference on Proceedings of the USENIX Annual Technical Conference*, 24. http://portal.acm.org/citation.cfm?id=1364409

Vlachos, V., Androutsellis-Theotokis, S., & Spinellis, D. (2004). Security applications of peer-to-peer networks. *Computer Networks*, *45*(2), 195–205. https://doi.org/10.1016/j.comnet.2004.01.002.

Wararkar, P., Kapil, N., Rehani, V., Mehra, Y., & Bhatnagar, Y. (2016). Resolving problems based on peer to peer Network Security Issue's. *Physics Procedia*, *78*, 652–659. https://doi.org/10.1016/j.procs.2016.02.113.

Wardynski, D. (2019). *End Of Moore's Law - What's Next For The Future Of Computing*. Brainspire. https://www.brainspire.com/blog/end-of-moores-law-whats-next-for-the-future-of-computing

Washbourne, L. (2015). *A survey of P2P network security*. 1–12. http://arxiv.org/abs/1504.01358

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, *3*(3), 17–31. https://doi.org/10.5121/ijcsit.2011.3302.

Zia, T., Liu, P., & Han, W. (2017). Application-specific digital forensics investigative model in internet of things (IoT). *ACM International Conference Proceeding Series*, *Part F1305*. https://doi.org/10.1145/3098954.3104052

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Ahmad Sanda Musa** is a Lecturer of Computing and Cybersecurity at Canterbury Christ Church University. He received a BSc degree in Software Engineering from the American University of Nigeria, an MSc in Forensic Computing and a PhD Computer Science degree from the University of Bradford. His research focusses on digital forensics, computer security, network topology and security, and peer-to-peer networking.

**Irfan Awan** is a Professor of Computer Science at the University of Bradford. He received his PhD in Performance Modelling of Communication Networks from the University of Bradford, UK, in 1997. He joined the University of Bradford and became a Professor of Computer Science in 2009. His research focuses on Network Security, Cyber Security, and Performance Modeling of Cloud and Communication Networks.

**Fatimah Zahrah** is a Computer Science doctoral student at the University of Oxford. She received a first-class degree with honours in Computer Science from the University of Bradford. Her research interests are software development, databases, network modelling and cybersecurity.