Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 7 No. 5 (2023) 1097 - 1110 ISSN Media Electronic: 2580-0760

Comparative Study of Cloud Forensic Investigation Using ADAM And NIST 800-86 Methods in Private Cloud Computing

Reza Febriana[1], Ahmad Luthfi[2]
[1,2]Department of Informatics Master, Faculty of Industrial Technology, Universitas Islam Indonesia, Yogyakarta, Indonesia
[1]rezafebriana1@gmail.com, [2]ahmad.luthfi@uii.ac.id

Abstract

As information technology advances, the associated risks also increase, particularly in the field of private cloud computing services. These services are subject to potential risks of internal abuse, either due to system vulnerabilities or other factors. However, the investigation of these incidents in private cloud computing varies greatly due to the different frameworks and unique characteristics of each cloud service. The lack of a standardized approach to analyzing and assessing investigative processes in cloud computing services has been a persistent problem. This lack of consensus impacts the accuracy, efficiency, and process of data acquisition when dealing with digital evidence in each method, causing concern among researchers. To overcome this, a comparative study was carried out with a focus on the ADAM (The Advanced Data Acquisition Model) method and the NIST (National Institute of Standards and Technology) method. The goal is to identify the most effective investigative process for dealing with cyber attack incidents on both the server and client side of cloud computing services. By testing these methods in a network that is built on private cloud computing services, then for the results from this research include the weaknesses and strengths of the ADAM and NIST methods are found when applied to cloud computing case studies and these have not been identified in previous research, then produce recommendations for investigators when conducting investigations on case studies on cloud computing, and in this study managed to find a bug in the ownCloud application version 10.9.1. Then this study also aims to provide researchers with valuable references to carry out analysis and assessment in the investigative process, where standardization is still an unresolved issue.

Keywords: framework; ADAM; NIST; cloud; comparison

1. Introduction

In the process of technological development in the field of cloud computing that creates various features with diverse usage needs. This is proportional to the risk of potential loss arising from its development. The potential dangers of private cloud computing services include the risk of misuse by internal parties due to their private use. The potential for misuse of private cloud computing services can occur due to system weaknesses used or for other reasons [1] - [3].

However, based on research related to cloud computing, the guidelines and methods of acquisition digital evidence in the cloud computing are outdated and scarce. There are no explicit rules for acquisition digital evidence in cloud computing, according to a number of relevant research. As well as the investigation process in each case on private cloud computing services that are not the same due to differences in the types and characteristics of these cloud computing services [4] - [6].

Because it refers to these problems, in this research a standard assessment was made using parameters related to the level of effectiveness of the method for conducting case investigations on private cloud computing services . So in this research a comparison of private cloud computing investigative methods was conducted between ADAM (The Advanced Data Acquisition Model) and NIST 800-86 (National Institute of Standards and Technology) to determine which method is most effective. for personal cloud computing services [7], [8].

Based on previous research references discussing the ADAM method in conducting private cloud computing service investigations with the RSIA XYZ case study. This research leads to an investigation of system weaknesses that have the potential to cause internal abuse by company insiders [9].

Furthermore, based on research that discusses the NIST 800-86 method used for the investigation process of private cloud computing services, and the research

Accepted: 17-07-2023 | Received in revised: 28-09-2023 | Published: 01-10-2023

carried out is to create a simulation to analyze digital evidence using the NIST 800-86 method for digital evidence from 5 scenarios that have been prepared and related with potentially abused cloud computing services [10], [11].

The determination of these two methods as a comparison in this research refers to two discussions in previous research which have successfully used each of these methods for private cloud computing investigative and after examining them in previous research each has different characteristics so that it can be used as a comparison in this study [1], [9], [12].

Based on the purpose of this study by comparing the most effective method between the ADAM method and the NIST 800-86 method for use in the investigation process on private cloud computing services, further the results of this comparison can be used by investigators as a recomendation in terms of conducting in the investigation process on private cloud computing services [1], [13].

2. Research Methods

The proposed research method is a flow of steps which shown in Figure 1.

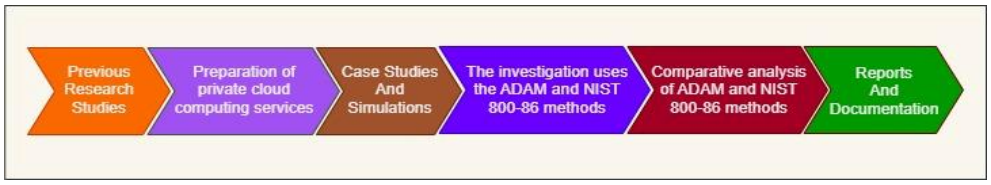

Figure 1. The steps of the research method

Previous research studies are a review of theoretical summaries and research conclusions obtained from previous research reference sources and are used as the basic foundation of this research process [9].

The preparation of private cloud computing services is carried out by creating a topology simulation in a computer laboratory according to the design topology in the case study at company x which is described in Figure 2 [9], [14].

As explained in Figure 2, there is a server as a service provider for private cloud computing from this case study using owncloud version 10.9.1 as the cloud computing service provider software and the IP address 192.168.1.8. Then there is 1 switch and 1 access point to connect the client to the server and among them there are 2 PC devices used as clients on the local network which are connected to the switch and 2 laptop devices as clients which access from the internet or from the local network via wireless media which are connected to the access point and there are 1 router that uses the NAT (Network Address Translation) feature to change IP private to IP public so that clients connected to the internet can connect to the private cloud computing service.

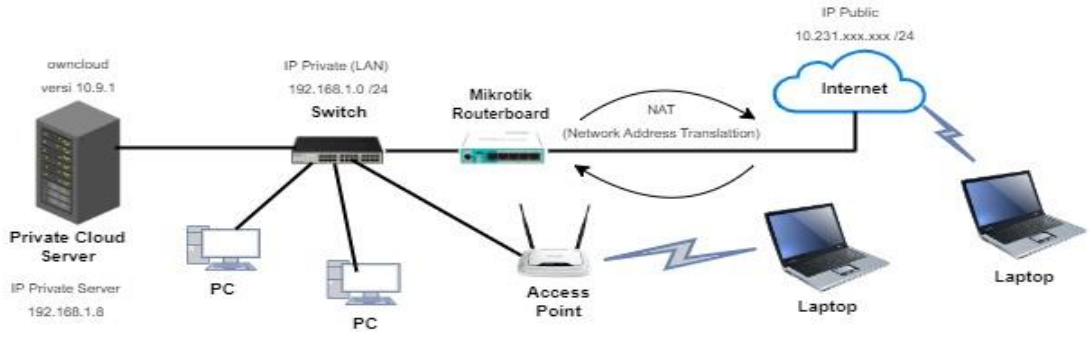

Figure 2. Topology Simulation of Private Cloud Computing Services On Case Studies at Company X

The case study used in the simulation scenario in this study was carried out in a computer network laboratory with the case study being a retail company whose name was disguised as Company X. This case is an example of an insider attack by an employee who falsified the company's financial documents for acts of corruption and divulge confidential company documents to external parties who are competitors of this company and the data is in cloud computing services [15]. In this scenario the investigator is assigned to collect digital evidence potential that exists on the private cloud computing service side, and devices such as personal computer and Laptop used by the company's employees [16]. Based on the condition, every employee in company X can take advantage of private cloud computing service features, Such conditions have the potential to abuse this feature for criminal acts originating from insiders. So that after the digital evidence has been collected by the investigator, it can be concluded who the perpetrators were forging documents and leaking confidential company document [17].

DOI: https://doi.org/10.29207/resti.v7i5.5279

Investigation scenarios for private cloud computing services are carried out using 2 methods including the ADAM method starting from the server service, and then, using tools wireshark software for monitor data traffic leaving or entering to private cloud computing service server on the network side and obtaining digital evidence at the session layer (layer 5 on 7 OSI layer), then conducting an investigation on the client side which consists of personal computer and laptop connected to private cloud computing services. Whereas in the NIST 800-86 method, it begins by collecting all potential sources of digital evidence consisting of the categories of data files, operating systems, network traffic, and applications, then each source of digital evidence is examined and selected to select digital evidence related to the case in question. faced, then digital evidence is analyzed so that conclusions can be drawn regarding what has happened in the case at hand for further reporting [18].

A comparative analysis of the ADAM and NIST 800-86 methods was carried out to see the level of effectiveness of the two methods in determining which method is most effective for use in private cloud computing services. The outcomes of the comparative analysis will thereafter serve as a guide for investigators in the investigation process on private cloud computing services. The parameters that become a comparison in the comparative analysis in this research are in Table 1 [19], [20].

Table 1. Software and Supporting Hardware

Effectiveness Type		Analysis Parameters	Parameter Description
Substance	Procedure	Time	Comparative analysis of the speed of completion of investigations using the ADAM and NIST methods
		Relevance	Comparative analysis of the relevance of using the ADAM and NIST methods for private services cloud computing.
		Accuracy	Comparative analysis of the degree of closeness of results investigative measurement of the use of the ADAM and NIST methods of the true value
		Integrity	Comparative analysis of the completeness from the results of digital evidence collection using the ADAM and NIST methods of private cloud computing services
	Process Stages	Similarities	Comparative analysis of similarity of process stages in the ADAM and NIST methods
		Differences	Comparative analysis of the different process stages in the ADAM and NIST methods

Reports and recommendations are the process of making reports on test results, by providing comprehensive information regarding the process of investigating digital evidence using the ADAM and NIST 800-86 methods as well as the outcomes of a comparison of the effectiveness from methodologies of ADAM and NIST 800-86 based on the aspects investigated, so that can provide recommendations on the methods used in the investigation process on private cloud computing services [21].

3. Results and Discussions

In the process of comparing the effectiveness of the method, it is carried out by applying the ADAM and NIST 800-86 methods in carrying out the investigation starting with operating the system on private cloud computing services on network infrastructure that has been built according to the original conditions at company X as a simulation with the results of verifying client access to private services. cloud computing according to table 2 [22].

Table 2. Verify Client Access To Private Cloud Computing Services

Source	Status	Information
IP LAN 192.168.1.0/24	Connect	Server PC desktop Laptop
IP WLAN 10.231.xxx.xxx/32	Connect	IP Public
IP Router 192.168.1.1/24	Connect	Access settings to router

In the ADAM method the investigation process is carried out in several stages [12], [23].

The initial planning stage which is the stage for reviewing and making an overview of the case at hand to determine the focus of examining potential digital evidence sources related to the misuse of private cloud computing service facilities for criminal acts originating from within by one of the employees so that it can be concluded who the perpetrators are. who forged documents and leaked the company's confidential documents. In this case study, investigators learned that Digital evidence that could be used to identify the offender in this case is in the user access data section of the network traffic connection in private cloud computing services so that the focus of the investigation is on the layer 5 (Session Layer) section. After the case review process is encountered, the investigator first determines the digital forensic team involved in the investigation process on the private cloud computing case study according to the needs of the case study results and consists of 3 people in a team with 1 leader and 2 people. team members each have insight or knowledge in the field of cloud computing technology, server virtualization and have an understanding of system and network security and its devices such as routers, switches and access points such as network switch devices, routers and access-points and understand the structure of folders and files from private cloud computing services in this case on

DOI: https://doi.org/10.29207/resti.v7i5.5279

owncloud as well as the folder and file structures of several operating systems, both linux-based and windows-based operating systems [1].

At The On Site Planning stage, investigators in the form of a team consisting of 3 people divide their tasks in choosing a source location that has the potential to contain digital evidence in it from private cloud computing services. After that, a data acquisition strategy was developed by determining the steps to obtain data either by direct acquisition or write block acquisition [24]. Determination of potential data sources to obtain data from private cloud computing services related to crimes committed in this case include the following :

File *.pcap captured data packet from client 1 (PC Desktop) which is a potential source of data containing captured network packets for analyzing network traffic retrieved from client device 1 on a personal cloud computing service.

File *.pcap captured data packets from client 2 (Laptop) which is a potential data source containing captured network packets to analyze network traffic captured from client 2 devices on personal cloud computing services

Storage media from client 1 and client 2 devices is a potential source of data contained on the client computer's storage media that has the potential to accommodate files retrieved from private cloud computing services.

The owncloud directory path which is a potential data source the part of the owncloud directory that can be accessed in the URL and the file part that can be accessed is described in Table 3.

Table 3. Owncloud URL path location

Path name	Path URL
Data folder	*Ip-public/owncloud/apps/files
Delete files	*Ip-public/owncloud/apps/files/?dir=/&view=trashbin
Data account	*Ip-public*/own*cloud*/settings/users

After that the investigator prepares the supporting tools or software that has been determined to assist the investigation process on private cloud computing services according to the requirements required in the case study and some of which shown in Table 4.

Table 4 Software Used in The Investigative Process With ADAM Method

Software	Information
Wireshark	software used to capture data traffic of devices connected to private cloud computing services
Power ISO	Imaging tools for digital evidence found on devices connected to private cloud computing services
Hash calc	Tools used to check the hash value of digital evidence

At the acquisition stage, the investigator divides the acquisition process into two processes including live acquisition and write-block acquisition [25]. Starting from the live acquisitions process flow based on the process flow starting with activating the log system with rules “IP-Firewall-Chain (Forward/Input/Output) – action log” which is on a private cloud computing network infrastructure and data retrieval is at layer 5 (Session Layer) using wireshark software and the files generated with the software are in the form of *.pcap (packet captures) and then the files are then checked to analyze the files as a whole until digital evidence data is found which includes file types, mac-addresses , username, password, log, and time stamp. Furthermore, live acquisitions are based on the process flow described in Figure 3[26].

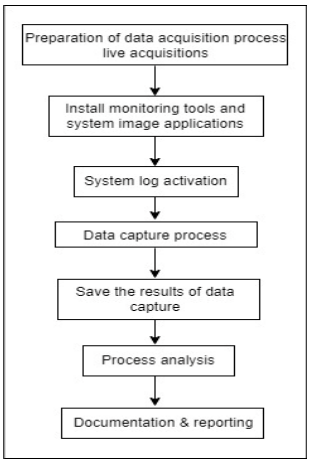

Figure 3. Live Acquisitions Process Flow

In the acquisition process with live acquisitions, it is carried out by capturing data from PC devices (Client 1) and Laptops (Client 2) using Wireshark tools and generating files with *pcap extensions including the following "01_analysis_owncloud_PC_client1.pcap" and "02_analysis_owncloud_Laptop_client2.pcap" for further processing analysis on the file and explained in several processes.

The first process is carried out by checking the MAC address, IP address and port used on the client and server side connected to the private cloud computing service and obtaining address data from each device including client 1 with IP address 192.168.1.12 and MAC address D0:53:49:2D:EA:26 then on client 2 with the IP address 192.168.1.3 and the MAC address C8:21:58:FB:D9:89 then on the server with the IP address 192.168.1.8 while the MAC address which is the destination from client to server uses MAC address on the router with MAC address 58:AE:F1:B7:DF:C0 and port forward settings with dst address 10.231.12.155 on port 80.

DOI: https://doi.org/10.29207/resti.v7i5.5279

The next process, examination and analyze the file "01_analisis_owncloud_PC_client_1.pcap" to see network traffic and activities performed by client 1 on the network in private cloud computing service. Figure 4 explains information related to activities carried out by Client 1, which is a personal computer type Asus All In One V241. In the image, Client 1 can be seen in the capture frame 320 which has MAC address D0:53:49:2D:EA:26 and IP address 192.168.1.12 with port 49843 is seen accessing the owncloud service via an account with the username "karyawan_1" and the password "user123".

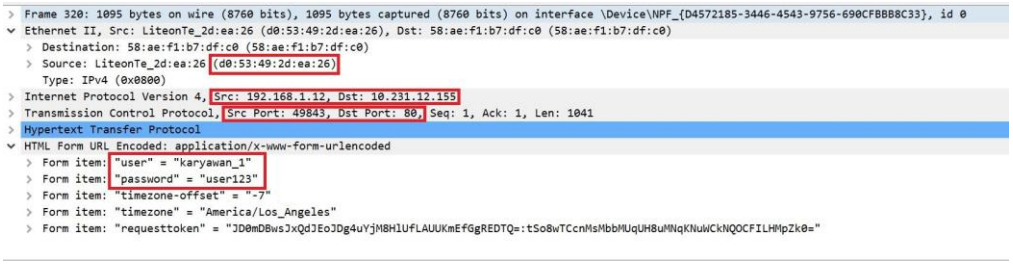

Figure 4. User Credential Client 1

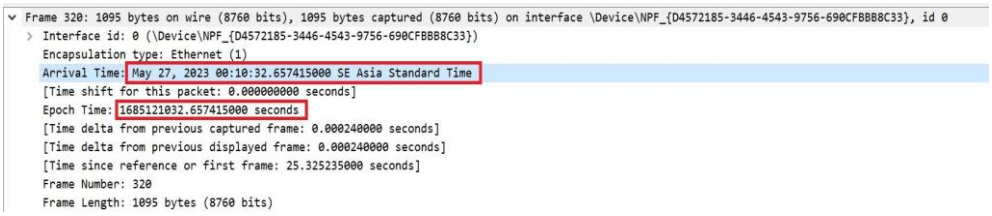

Figure 5. Time Stamp Frame Login Client 1

Figure 5 explains the time of client 1's activity which shows that login access by client 1 using the username "karyawan_1" and the password "user1" has a time stamp of "May 27 2023" with epoch time: 1685121032.657415000.

The next process, examination and analyze the file "02_analisis_owncloud_Laptop_client_2.pcap" to see network traffic and activities performed by client 2 on the network in private cloud computing service.

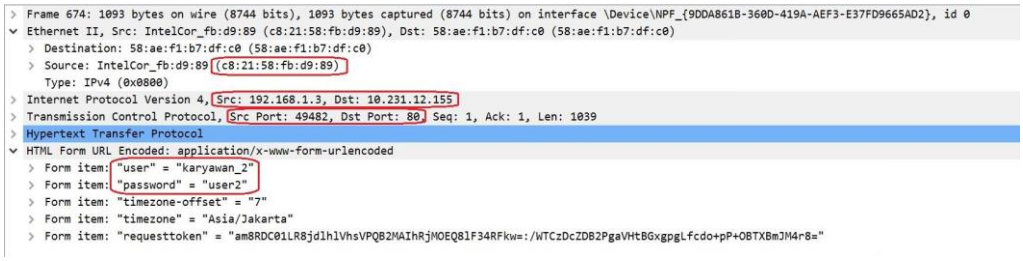

Figure 6. User Credential Client 2

Figure 6 explains information related to activities carried out by Client 2, which is a laptop type HP Pavilion X360 M3. In the image, Client 2 can be seen in the capture frame 674 which has MAC address C8:21:58:FB:D9:89 and IP Address 192.168.1.3 with port 49482 is seen accessing the owncloud service via an account with the username "karyawan_2" and the password "user2".

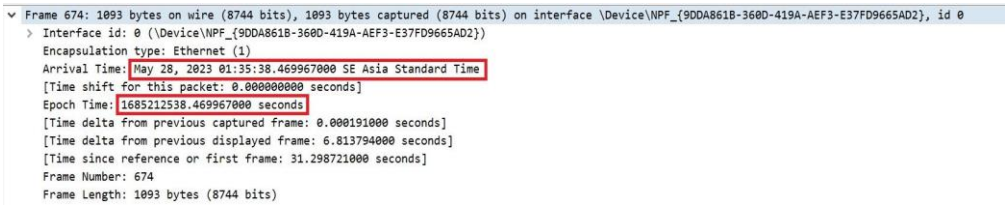

Figure 7. Time Stamp Frame Login Client 2

Figure 7 explains the time of client 1's activity which shows that login access by client 1 using the username "karyawan_2" and the password "user2" has a time stamp of "May 28 2023" with epoch time: 1685212538.469967000.

DOI: https://doi.org/10.29207/resti.v7i5.5279

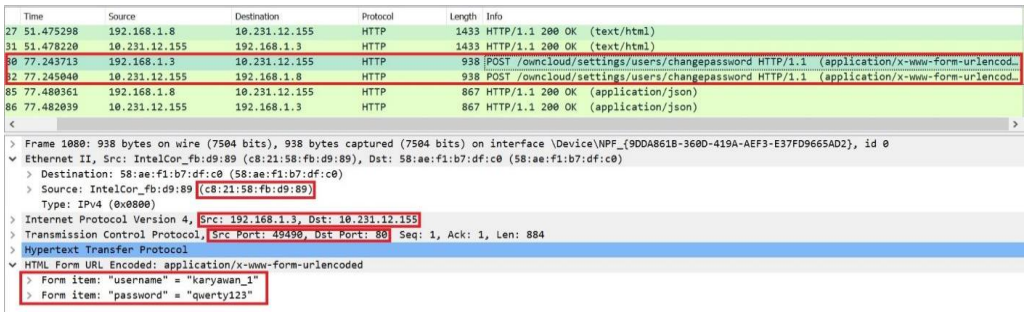

Figure 8. User Setting Activity From Client 2 (Laptop)

Figure 8 managed to found activity from client 2 in the capture frame 1080 results which can be seen by the presence of the MAC address and IP address of client 2 which is known to have changed the password of account “karyawan_1” which was previously shown in figure 7 with the username “karyawan_1” password “user123” In this screenshot, it looks like it has changed to the username “karyawan_1” and the password “qwerty123”.

Furthermore, the activity carried out by client 2 is accessing private cloud computing services by logging in using an account whose password has been changed previously shown in Figure 8 using an account that has been set with the username "karyawan_1" password "qwerty123" so that it can be concluded that the purpose of client 2 is to set a password on the account "karyawan_1" so that client 2 can enter the service and access the contents of files from that account.

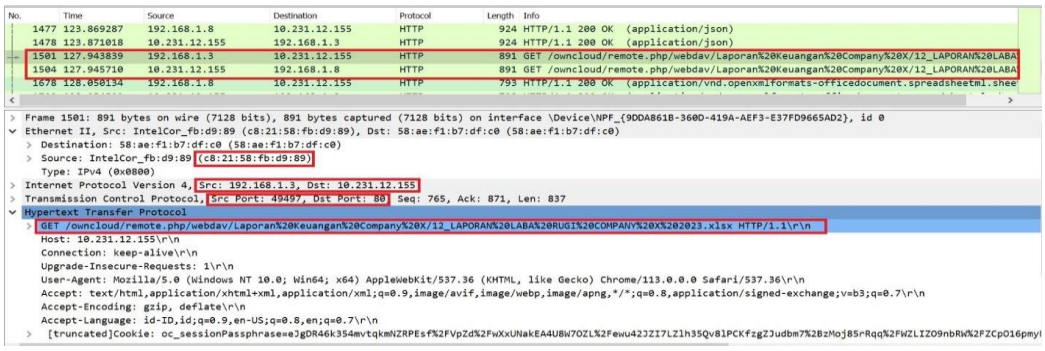

Figure 9. Download File 1 Activity From Client 2

Then in Figure 9 it is found that the packet capture in frame 1501 is in the form of activity from client 2 which can be seen from the address of the MAC address and IP address which shows the address of client 2 using the GET message used by the client to make requests to the server and in the package the activity is client 2 downloads a file with the extension of .xlsx and this file is named “12_PROFIT AND LOSS REPORT COMPANY X 2023.xlsx” which is in the folder of “Laporan Keuangan Company X”.

After that the same activity is carried out again by the client user 2. The activity carried out is to download the second file with the *.docx extension and the file name is “5 Year Corporate Financial Strategic Plan.docx”.

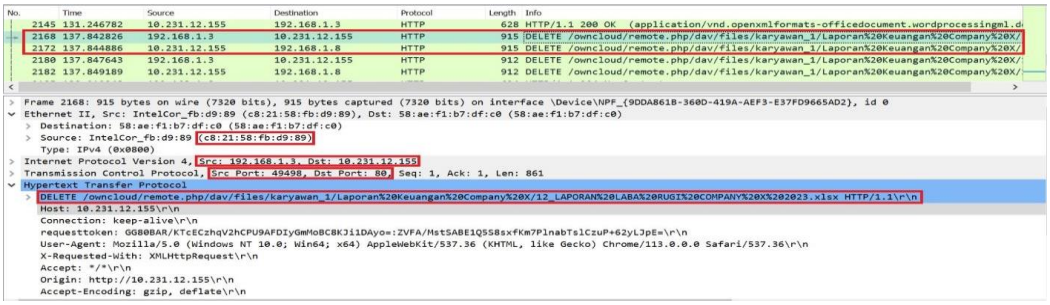

Figure 10. Delete File 1 Activity From Client 2

In Figure 10 it is also found that the packet capture in frame 2168 is in the form of activity coming from client 2 as shown by the MAC address and IP address which shows the address from client 2 using the DELETE

DOI: https://doi.org/10.29207/resti.v7i5.5279

message used by the client to delete data on the server and in the packet the activity is client 2 deletes a file with the extension of .xlsx and the file named is "12_PROFIT AND LOSS REPORT COMPANY X 2023.xlsx" which is in the folder of "Laporan Keuangan Company X" and this file is the file previously downloaded by client 2.

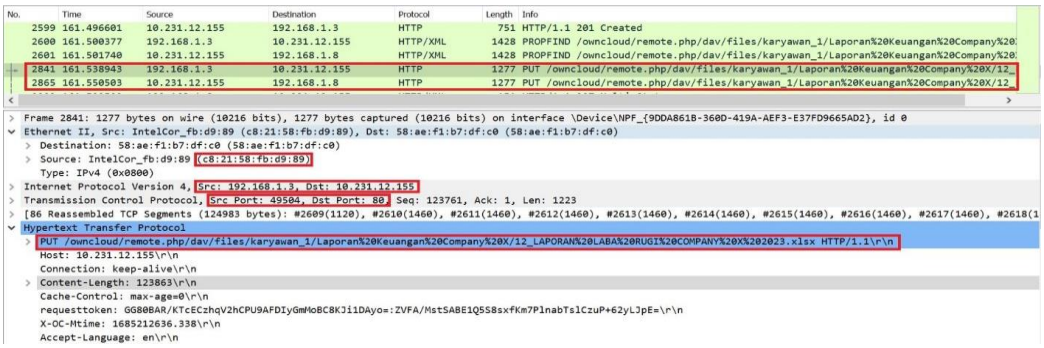

Figure 11. Upload File 1 Activity From Client 2

Furthermore, in Figure 11, it is found that the packet capture in frame 2528 is in the form of activity coming from client 2 as shown by the MAC address and IP address which shows the address from client 2 using the PUT message. The message is used by the client to upload data to the server and on this packet the activity is client 2 uploads a file with the extension of .xlsx and the file is named "12_PROFIT AND LOSS REPORT COMPANY X 2023.xlsx" in the folder of "Laporan Keuangan Company X".

Then for the flow of the write-block acquisitions process, it starts with ensuring that the data to be retrieved is not changed or even eliminated by closing all access that leads to private cloud computing services with the blocking access method from the mikrotik router using rules (IP-Firewall- IP Destinations action drop). Furthermore, the write-block acquisitions are based on the process flow described in Figure 12.

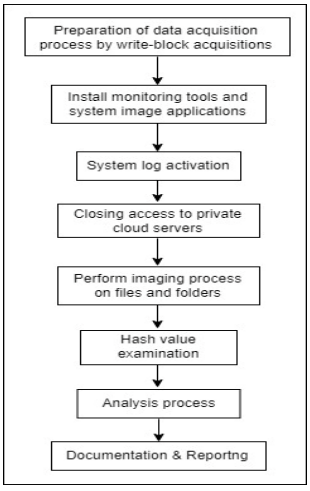

Figure 12. Write-Block Acquisitions Process Flow

In the next process, an explanation of the imaging process with PowerISO tools that can process imaging files (*.iso or *.dd) is installed on a private cloud computing service system and data retrieval can be done remotely to a private cloud computing service machine via LAN.

After knowing the location of the target folder and files on the client side, a case simulation is carried out using the PowerISO software. After that, the personal cloud computing service processes the image file and checks the hash value of the file. Then after the image files are checked and analyzed further to identify which files are the target of misuse for falsification and documents that have been leaked to competitors in the case studies in this study. Then specifically in making documentation and reporting with write-block acquisition using the ADAM method, data can be collected from each device that has the opportunity to contain digital evidence, including servers, PC desktop and laptop as well as network devices such as routers and the process is described as follows.

Starting with the process of examining potential digital evidence contained on the client device 2 because based on *pcap file capture analysis, a potential source of digital evidence related to the crime committed in this case is on the laptop device with the specifications as seen in Figure 13.

Figure 13. The Laptop Allegedly Used by The Suspect

Figure 13 is client 2 which is a laptop device used by the suspect and potential digital evidence inside with brand specifications: HP, Type: HP Pavilion X360 M3, Processor: Intel core i7-7500U, Memory: 12.0 GB (11.9 GB usable), OS: Windows 10 Home 64bit.

DOI: https://doi.org/10.29207/resti.v7i5.5279

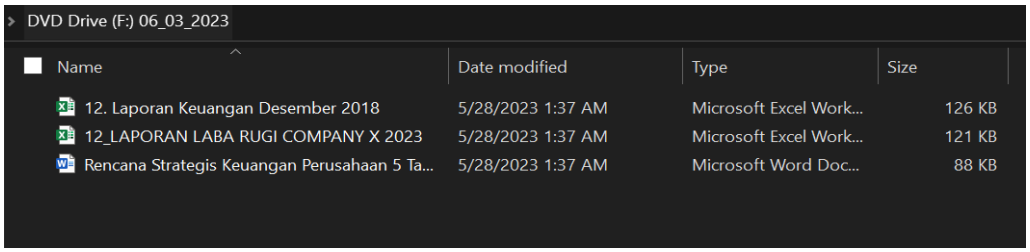

Figure 14. Results Imaging Processes Of Digital Evidence In Client 2

Figure 14 is the result of the digital evidence imaging process in the file folder that is focused on client device 2 because it is based on examining potential sources of digital evidence on client device 2 and found 3 files which are digital evidence related to this case.

Then check on the server side, in this case on the ownCloud path directory to verify the results of network packet traffic analysis based on the *pcap file to find out about what happened, the following facts are obtained.

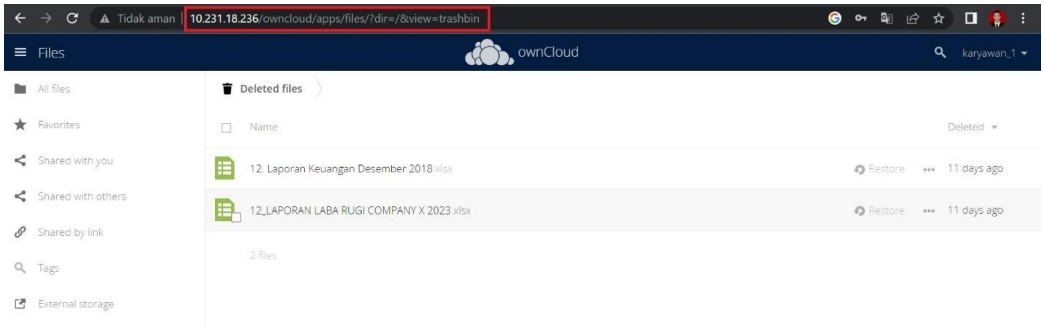

Figure 15. The File Contained In The Owncloud Trashbin of URL Path

Figure 15 is digital evidence of the results obtained at the following path URL of trashbin owncloud "*IP-public/owncloud/apps/files/?dir=/&view=trashbin" which is the original file from the digital evidence which explains that the client 2 user deleted the original file on the owncloud application is then replaced with files that have been manipulated or falsified by the perpetrator. In the process the file was restored then an imaging process was carried out then analyzed and the fact was found that the file was evidence that there was an act of forging documents by client 2 users as evidenced by the different hash values between the files found in the owncloud trashbin and the files contained on the client 2 device which can be find in table 5 which shows the outcomes of the examnination of the MD5 hash value on digital evidence.

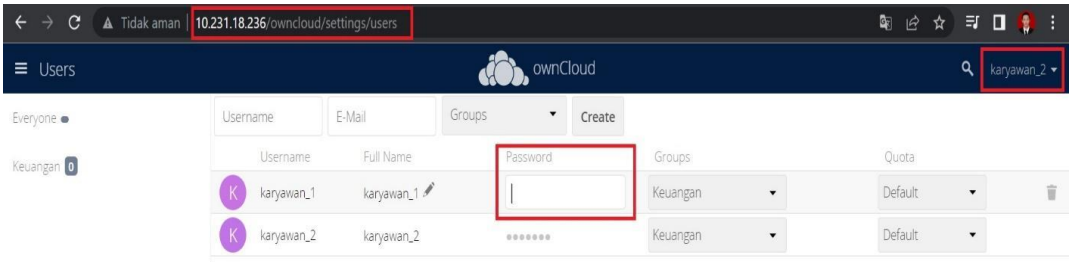

Figure 16. Bug Owncloud Version 10.9.1

In Figure 16 a bug is found in the path URL of owncloud as follows "IP-public/owncloud/settings-/users" which is the owncloud user account data. It can be seen that the account of "karyawan_2" can change the password via the account of "karyawan_1". This is a bug or weakness of the application owncloud version 10.9.1. The problem with this bug is that one user and another user in the same group can change each other's passwords. this is what causes user client 2 to be able to change the account used by user client 1 which was previously seen in the *pcap file analysis results.

After an imaging process on several digital evidence files that were found, a time stamp examination was carried out and it was found that the document file was modified on 28/05/2023 right after the file was downloaded from the account of "karyawan_1", thereby strengthening evidence that the file was used for falsification and then an examination of the MD5 hash value was also carried out using tool of Hash Calc and the outcomes of the examination that shown in Table 5.

DOI: https://doi.org/10.29207/resti.v7i5.5279

Table 5. Examination of Hash Value MD5 on Digital Evidence

Nama file	Hash value
12_PROFIT AND LOSS REPORT COMPANY X 2023.xlsx	6bf01a43ad9ae48c93524ead761157c5
5 Year Corporate Financial Strategic Plan.docx	f4a7c9562c15780d7eaaedd7e53792de
12_PROFIT AND LOSS REPORT COMPANY X 2023 (restored).xlsx	f69050a40f30848cc834619f070a7dff

Then at the reporting stage it was explained that client 1 as the legal owner of the account " Karyawan _1" last accessed the account on May 27 2023 after that on May 28 2023 user client 2 changed the account password "Karyawan_1" so that it could not be accessed by user client 1 as the legal owner an account that led to a complaint to the server administrator and after an investigation process it can be concluded that the user from client 2 is suspected of being the perpetrator in a case of forging documents for the purpose of corruption and leaking confidential documents to competitors. This is based on the outcomes of an analysis of the *pcap file which is the result of capturing network traffic packets on client 1 and client 2. The results of the analysis explain that user client 2 falsified documents and leaked confidential documents on client 1's account on May 28, 2023 by changing the account password used by client 1 then log in with the account used by client 1 to access important documents on that account including 1 document file that will be falsified due to corruption and 1 confidential document file that will be leaked. Document falsification is done by deleting the original file on owncloud and replaced with a manipulated file and in the file that was leaked to competitors, no other actions were found besides the download process because this file was indeed targeted by perpetrators as a confidential document that was leaked to competitors. Based on the outcomes of an investigation using the ADAM method, The conclusion that causes the abuse of private cloud computing service facilities at Company X is due to a weakness in the owncloud application version 10.9.1, in the form of a bug in the user management section as described in figure 16.

In the NIST 800-86 method the investigation process is carried out with several stages.

At the Collection stage, it starts with determining the location sources that have the opportunity to have digital evidence in them and the data collection process in the NIST method is divided into several categories, including based on the categories of data files, operating systems, network traffic and applications by collecting data from the four coverage categories, then carried out backup on collected data for further review.

The first step in the collection process stage is to determine potential data sources related to crimes committed in private cloud computing services and in this case there are virtual servers, client 1 (PC desktop), client 2 (laptop) and router (mikrotik) to then collect potential digital evidence in the category of data files that are on the device.

Then collect data from the operating system category used to obtain volatile and non-volatile data relating to cases that occur including configuration files, application files, logs, dump files, swap files, hibernation files and temporary files [27].

After that, collect data from the network traffic category by installing network traffic monitoring with Wireshark on client devices that are connected to private cloud computing services and obtain digital evidence in the form of files captured by network traffic data packets with the *pcap extension, including the file captured 01_analysis_owncloud_PC_client_1.pcap" from client 1 and 02_analysis_owncloud_Laptop_client_1.pcap from client 2.

Finally, data collection in the application category is based on case studies, the application used by owncloud and the type of private cloud computing service used is of the PAAS (Platform As A Service) type so that what can be collected and identified from the server is only at the owncloud URL path location which is part from the owncloud directory which can be accessed via the URL and the collected data is the same as the URL path previously collected in the ADAM method described in table 3.

The examination process is the process of examining the data that has been collected to extract more in-depth information and sorting or selecting data related to the case at hand because not all the data obtained is needed in the forensic analysis process. After selecting and obtaining data related to the case at hand, an imaging process is carried out on the file using PowerISO with the *iso extension so as not to damage the original file, then the file is examined for the MD5 hash value using Hashcalc tools and digital evidence related to the case. encountered include files originating from network traffic capture from clients 1 and 2, data files from client 2, and application data obtained from the owncloud URL path with the results of examining the same MD5 hash value as was done in the ADAM method in table 5.

At the Analysis stage an analysis of digital evidence has been examined and selected to be studied in more depth so that conclusions can be drawn about what has happened from the digital evidence. The digital evidence analysis process carried out is explained as follows.

Examination of device addresses including MAC addresses, IP addresses and ports used on the client and server sides connected to private cloud computing services on the NIST method is the same as that carried out on the ADAM method which aims to verify the

DOI: https://doi.org/10.29207/resti.v7i5.5279

results of file capture analysis of network traffic packets on *pcap file related to what activities are carried out by the device in the private cloud computing service, the information obtained is in accordance with Figure 4, Figure 5, and Figure 6 which consists of client 1 using IP address 192.168.1.12 and MAC D0:53:49:2D :EA:26 then on client 2 using the IP address 192.168.1.3 and MAC C8:21:58:FB:D9:89 and on the server with the IP address 192.168.1.8 while the MAC address that is the destination from client to server uses the MAC on the router with MAC 58:AE:F1:B7:DF:C0 and port forward settings with dst address 10.231.12.155 and port 80.

Then the analysis process on the file capture of network traffic which include of files "01_analysis-_owncloud_PC_client_1.pcap" and "02_analysis-_owncloud_Laptop_client_1.pcap" the analysis process on the two files is the same as the analysis process in the adam method to see what activities each device performs when connected to the private cloud computing service with the same results with the discovery of document forgery and leaking of confidential documents allegedly carried out by users from client devices 2.

Then the process of data analysis in the category of data files that are on the client 2 device which consists of 2 files.

The first file is "12_PROFIT AND LOSS REPORT COMPANY X 2023.xlsx" which is digital evidence of document falsification and the analysis process for the file is carried out by looking at the time stamp of the file first to find out when the file was created or modified and matched with when the incident occurred and in the document file found when the file was made on 28/05/2023 and modified still on the same date on 28/05/2023 at 1:37:16 AM and the time is right on the date where the incident occurred in the catch analysis network traffic packets related to activities caught on client 2's device regarding unauthorized logins and the time is right after the file is downloaded from the employee_1 account thereby strengthening the evidence that the file was used for document forgery. Then an examination of the MD5 hash value is carried out and the results are the same as those carried out in the ADAM method and are contained in the table 5.

The second file is "5 Year Corporate Financial Strategic Plan.docx" which is digital evidence of leaking confidential documents to competitors and the analysis process checks the time stamp first and the time stamp in this document file is different from the previous document because it was found that the time the file was made was on the 24th /01/2019 and modified it is still on the same date on 01/24/2019 at 12:53:32 PM and based on the time stamp there is no visible file modification activity since about 4 years ago meaning the file was only downloaded from the account employee_1 and has nothing to do with the act of falsifying documents but based on the search results this file is a confidential company document so it can be concluded that this document file is a document file that was leaked to competitors. then an examination of the MD5 hash value was carried out and the results were the same as those carried out in the ADAM method and are listed in Table 5.

After that, further analysis is carried out on the application data category which consists of several URL paths in the owncloud application including "*Ip-public/owncloud/apps/files/?dir=/&view=trashbin" which is the URL path to view deleted data but it can still be recovered and at the URL path the original document is found which can be used as digital evidence explaining that the client 2 user deleted the original file on the owncloud application with the aim of replacing it with a file that has been manipulated or falsified by the perpetrator, this can be concluded because of the hash value from document file at this URL path is different from that found in the data files on the client 2 device which can be seen in the table 5.

Then analyze the next URL path in the owncloud application, namely "IP-public/owncloud/settings-/users" which is the URL path for user management and in that URL path it is found that there are bugs or weaknesses in the owncloud application version 10.9.1 where the problem is user one with other users in the same group can change each other's passwords. this is what causes users on client 2 to be able to change the account password used by users on client 1 as shown in the Figure 16.

Reporting process started after the investigation process was carried out, some information related to the process and the results of the investigation was obtained starting from information about the tools used and because the use of tools in the NIST 800-86 method is the same as those used in the ADAM method, the list of tools can be seen in table 4. Then after the investigation process was carried out, some information was obtained regarding the process and the results of the investigation starting from information about the tools used and because the use of tools in the NIST 800-86 method is the same as those used in the ADAM method, the list of tools is as shown in the table 4. Then related the outcomes of the investigation carried out which have conclusions regarding what happened, the results are the same as those carried out in the ADAM method which explains that client 2 users forged documents and leaked confidential documents in the account on client 1 on May 28, 2023 by changing the account password used client 1 then enters the account used by client 1 to access important documents in the account including 1 document file that will be falsified for corruption and 1 confidential document file that will be leaked. Based on the facts obtained from the results of the investigation,

DOI: https://doi.org/10.29207/resti.v7i5.5279

it can be concluded that the cause of the abuse of private cloud computing service facilities at Company X was due to a weakness in the owncloud version 10.9.1 application in the form of a bug in user management as described in Figure 16.

Comparative analysis of digital evidence supporting parameters obtained from network traffic capture between the ADAM and NIST 800-86 methods includes several parameters which obtained and are shown in Table 6.

Table 6. Comparison Of Parameters Supporting Digital Evidence Obtained

Parameters supporting digital evidence	ADAM		NIST 800-86	
	Client 1	Client 2	Client 1	Client 2
IP Source	√	√	√	√
Mac Address Source	√	√	√	√
IP Destination	√	√	√	√
Mac Address Destination	√	√	√	√
Struktur Folder dan File	√	√	√	√
Log Activity	√	√	√	√
Username and Password	√	√	√	√
Time Stamp	√	√	√	√
Data Locations	√	√	√	√
Protocol and Port Access	√	√	√	√

Table 6 analyzed the comparison of the ADAM and NIST 800-86 methods in obtaining the supporting parameters of digital evidence shows that both have the same value because both of them succeeded in obtaining all the supporting parameters needed to strengthen digital evidence in network traffic.

Comparison of time parameters after being analyzed from the ADAM and NIST 800-86 methods is known from the activities carried out at the two processing stages which shown in Table 7 and Table 8.

Table 7. The Activity Process Flow Through The ADAM Method

Process Stages	Activity
Initial Planning	Study the cases at hand
	Assign a team
	Define supporting tools
The On Site Planning	Determining the focus of potential digital evidence sources
	Dividing tasks on the team in identifying sources of digital evidence
	Create a data collection strategy plan
Acquisition Digital Data	Acquisition process with live acquisitions technique
	Acquisition process with write-block acquisitions technique and imaging process
	Preparation of investigative reports

Table 8. The Activity Process Flow Through The NIST 800-86 Method

Process Stages	Activity
Collection	Determination of potential digital evidence sources from the side of each device connected to private cloud computing services
	The stage of identifying digital evidence sources in the scope of the data files category
	The stage of identifying digital evidence sources in the scope of the operating systems category
	The stage of identifying digital evidence sources in the scope of the network traffic category
	The stage of identifying digital evidence sources in the scope of the application category
Examination	Examination of data collected from all sources on private cloud computing services so that in-depth information mining can be carried out
	Selection or sorting of data collected as digital evidence related to the case that occurred.
	Perform imaging processes on digital evidence data that has been selected
	Examination of the hash value on digital evidence data that has been carried out by the imaging process.
Analysis	Analyze the file selection results that have been carried out by the imaging process
Reporting	The Stages of reporting study findings, information obtained from analysis findings based on other reasonable explanations, audience considerations, and information that can be sought

Based on table 7 and table 8 which is a table showing the process flow of the activities encountered in this case, the ADAM method involved 9 activities, while in the NIST 800-86 method there were 11 activities used in the investigation process in this case study, so that from a comparison the activities of both can be concluded that the ADAM method is more effectively used than the time parameter in this case because the activity carried out in the ADAM method is less than the NIST 800-86 method so that the time used in the investigation process in the ADAM method is faster than the NIST 800-86 method.

Comparison of the relevance parameters between the ADAM and NIST 800-86 methods used with the case at hand can be seen from the data collected to be used as digital evidence in this case which explains whether digital evidence is relevant to the case that occurred or not and the comparison can be seen in Table 9 and Table 10.

Table 9. The Relevance of Using Digital Evidence In The ADAM Method To The Case at Hand

Types of Digital Evidence	Relevant	
	Yes	No
Network traffic packet layer 5 - Session Layer (file *.pcap)	√	
Storage media for data files Client 1 & client 2 devices	√	
Path direktori owncloud	√	

DOI: https://doi.org/10.29207/resti.v7i5.5279

Table 10. The Relevance of Using Digital Evidence In The NIST 800-86 Method To The Case at Hand

Types of Digital Evidence	Relevant	
	Yes	No
Storage media for data files from Client 1 & client 2 devices, virtual servers and routers	√	
Volatile and non-volatile operating system data		√
Network traffic capture data from network traffic coverage (file *.pcap)	√	
The data from the scope of the application is in the form of the owncloud directory path	√	

Considering the comparing outcomes from table 9 and table 10, shows there are 3 types of digital evidence collected by ADAM method and each of the three is related to the case study in this research while in the NIST 800-86 method contains 4 types of digital evidence collected with 3 types of digital evidence being related with case study while 1 type of digital evidence is not relevant to the case study in this research so that the results of the analysis of this relevance parameter can be concluded that the ADAM method is more relevant to use than the NIST 800-86 method in the case of private cloud computing services. After analyzing the stage of collecting digital evidence in determining potential sources of digital evidence between the ADAM method and the NIST 800-86 method, in the ADAM method, which first reviews the cases at hand so that the process of collecting digital evidence can be focused on sources related to the case at hand, while the NIST method 800-86 collection of digital evidence is taken from all related sources first but digital evidence that has been collected from all potential sources is re-selected in the examination process.

Furthermore, a comparison of the accuracy parameters between the ADAM and NIST 800-86 methods is used to obtain strong evidence that can explain what happened, who was involved, when the incident occurred, and explain how the chronology of the crime was committed and the results are shown in the table furthermore, a comparative of the accuracy parameters between the ADAM and NIST 800-86 methods is used to obtain strong evidence that can explain what happened, who was involved, when the incident occurred, and explain how the chronology of the crime was committed and the outcomes are shown in Table 11.

Table 11. Comparison of Process Flow Accuracy In Uncovering The Facts Of The Case at Hand

The facts found from digital evidence are based on the process that has been passed	ADAM	NIST 800-86
Facts what happened	√	√
Facts who was involved	√	√
Facts when it happened	√	√
Facts where the incident occurred	-	-
Facts how the chronology of events	√	√

After being analyzed, the ADAM and NIST 800-86 methods have a balanced level of effectiveness on the accuracy parameter because the two methods accurately reveal the facts that occurred in this case and obtain strong evidence that can explain what happened, who was involved. , when the incident occurred, as well as explaining how the chronology of the crime was committed. However, the facts about where the perpetrators committed the crime were located cannot be determined accurately considering the condition of private cloud computing services that can be accessed from anywhere.

In the integrity parameter, it can be seen from the quality of digital evidence resulting from the investigations carried out by the two methods, both of them obtained digital evidence that can be said to be of high quality and intact because it can be seen from the hash value of digital evidence from the two methods that the value is the same and 100% has not changed since from digital evidence taken from the original source, which means that both methods provide adequate techniques that can maintain digital evidence intact until the reporting process and comparison of digital evidence obtained as well as comparison of hash values is shown in Table 12.

Table 12. Comparison of Hash Values From Digital Evidence Between The ADAM Method and The NIST 800-86 Method

File Name	MD5 Hash Value	ADAM	NIST 800-86
12_PROFIT AND LOSS REPORT COMPANY X 2023.xlsx	6bf01a43ad9ae48c93524ead761157c5	√	√
5 Year Corporate Financial Strategic Plan.docx	f4a7c9562c15780d7eaaedd7e53792de	√	√
12_PROFIT AND LOSS REPORT COMPANY X 2023 (restored).xlsx	f69050a40f30848cc834619f070a7dff	√	√

Based on the outcomes of the analysis which includes the similarity of stages between the ADAM method and the NIST 800-86 method, it can be seen in Table 13.

DOI: https://doi.org/10.29207/resti.v7i5.5279

Table 13. Analysis of similarities in process stages between ADAM and NIST 800-86 methods

ADAM method stages	NIST 800-86 method stages
The on Site Planning	Collection
Acquisition Digital Data	Examination Analisys

At the on site planning stage in the ADAM method and collection in the NIST 800-86 method, the basic similarity possessed by the two methods is to make preparations in determining potential data sources to be identified.

The similarity in the next stages of the ADAM and NIST 800-86 methods is to carry out the data acquisition process and carry out a detailed examination of potential data sources for further analysis so that conclusions can be drawn about what has happened. However, in the ADAM method, all of these processes are summarized in one stage, namely "Acquisition Digital Data", while in the NIST 800-86 method it is divided into 2 stages, including "Examination" for the acquisition and examination process and "Analysis" for the analysis process in concluding what happened in the case.

Table 14 Analysis of Differences In Process Stages Between ADAM and NIST 800-86 Methods

ADAM method stages	NIST 800-86 method stages
Initial Planning	-
-	Reporting

In Table 14, the conclusions from the analysis results include the differences in stages between the ADAM method and the NIST 800-86 method as follows.

The first difference between the ADAM and NIST 800-86 methods is that in the ADAM method there are stages that discuss initial preparation starting with understanding the task to be carried out in the case at hand then having to form a team with the required skill criteria according to the task criteria to be faced in that case as well as understanding the overall picture of the case at hand and this stage is called "Initial Planning" while the NIST 800-86 method does not discuss this process.

The next difference between the ADAM and NIST 800-86 methods is related to the reporting stage, he reporting stage discusses and describes the process of collecting and giving information on the findings of the conducted investigation. The reporting stages are not discussed in detail in the ADAM method. The reporting process in the ADAM method is explained according to the standards of the investigator, while the NIST 800-86 method is discussed in detail, including preparing several scenarios and several factors that influence reporting in this case based on the explanation. alternatives, audience considerations and actionable information.

4. Conclusion

Based on the research findings from the comparative study between the ADAM method and the NIST 800-86 method in investigating cloud computing case studies, the conclusion from these facts is that the ADAM method outperforms the NIST 800-86 method in terms of measuring time parameters. The superiority of the ADAM method in this aspect is attributed to its "Initial Planning" stage, where the process of identifying the source of digital evidence focuses directly on specific aspects relevant to the case in this research. On the other hand, the NIST 800-86 method lacks a similar preparatory stage, leading to a more time-consuming process of obtaining and examining all sources before selecting potential sources of digital evidence. Additionally, the ADAM method also demonstrates superiority in terms of relevance compared to the NIST 800-86 method. Once again, this advantage is due to the "Initial Planning" stage in the ADAM method, which ensures that the digital evidence collected is highly relevant to the specific case being investigated. Therefore the results of this study can answer existing problems including those related to standardization of the use of methods that are suitable for investigations in cloud computing which are problems that can be answered in this study with proposed recommendations and the results of an analysis of the advantages and disadvantages of the two methods when used in case studies cloud computing which can be a reference and consideration for investigators.

To build upon this research, future studies could explore and compare other investigative methods related to cloud computing, utilizing different scenarios for case studies. It is important to recognize that the effectiveness of these methods varies based on the type and characteristics of the cloud computing service being used.

Reference

[1] Dwi Kurnia Wibowo, Ahmad Luthfi, Yudi Prayudi, Erika Ramadhani, and Muhamad Maulana, “Faux Insider Hazard Investigation on Non-Public Cloud Computing by Using ADAM’s Technique,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 6, no. 6, pp. 1028–1036, 2022, doi: 10.29207/resti.v6i6.4714.

[2] T. Sianturi and Kalamullah Ramli, “A Security Framework for Secure Host-to-Host Environments,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 6, no. 3, pp. 380–386, 2022, doi: 10.29207/resti.v6i3.4018.

[3] Y. Khan and S. Varma, *Development and Design Strategies of Evidence Collection Framework in Cloud Environment*. 2020. doi: 10.1007/978-981-15-2071-6_3.

[4] H. Ernita, Y. Ruldeviyani, D. Nurul Maftuhah, and R. Mulyadi, “Strategy to Improve Employee Security Awareness at Information Technology Directorate Bank XYZ,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 6, no. 4, pp. 577–584, 2022, doi: 10.29207/resti.v6i4.4170.

[5] F. Fataftah and B. Isong, “Case Study Analysis of the Use of Cloud Computing for Assessing Big Data Risks,” vol. 5, no. 2,

DOI: https://doi.org/10.29207/resti.v7i5.5279

pp. 445–466, 2023, doi: 10.51519/journalisi.v5i2.478.
[6] P. Jain and A. Mahalkari, "Review of Cloud Forensics: Challenges, Solutions and Comparative Analysis," *Int. J. Comput. Appl.*, vol. 178, no. 34, pp. 28–34, 2019, doi: 10.5120/ijca2019919220.
[7] C.-Y. Cheng, E. Colbert, and H. Liu, "Experimental Study on the Detectability of Man-in-the-Middle Attacks for Cloud Applications," in *2019 IEEE Cloud Summit*, 2019, pp. 52–57. doi: 10.1109/CloudSummit47114.2019.00015.
[8] Bita Parga Zen, Anggi Zafia, and Iwan Nofi Yono Putro, "Network Security Analysis Simulation at the GCS in the UCAV to support the Indonesian Defense Area," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 6, no. 5, pp. 824–831, 2022, doi: 10.29207/resti.v6i5.4412.
[9] N. Widiyasono, I. Riadi, and A. Luthfi, "Investigation on the services of private cloud computing by using ADAM Method," *Int. J. Electr. Comput. Eng.*, vol. 6, no. 5, pp. 2387–2395, 2016, doi: 10.11591/ijece.v6i5.11527.
[10] N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal," *J. Reliab. Intell. Environ.*, Jun. 2021, doi: 10.1007/s40860-020-00115-0.
[11] M. H. Hersyah, "A Proposed Model of Digital Forensic on Cloud Computing Security Infrastructure," *Int. J. Innov. Enterp. Syst.*, vol. 2, no. 02, pp. 18–23, 2018, doi: 10.25124/ijies.v2i02.21.
[12] S. Simou, C. Kalloniatis, S. Gritzalis, and V. Katos, "A framework for designing cloud forensic-enabled services (CFeS)," *Requir. Eng.*, 2019, doi: 10.1007/s00766-018-0289-y.
[13] D. Sudyana and N. Lizarti, "Forensic Investigation Framework on Server Side of Private Cloud Computing," vol. 10, no. 3, pp. 181–192, 2019, doi: 10.24843/LKJITI.2019.v10.i03.p06.
[14] E. E.-D. Hemdan and D. H. Manjaiah, "An efficient digital forensic model for cybercrimes investigation in cloud computing," *Multimed. Tools Appl.*, vol. 80, no. 9, pp. 14255–14282, 2021, doi: 10.1007/s11042-020-10358-x.
[15] G. S. Pandi, S. Shah, and K. H. Wandra, "Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 163–173, 2020, doi: 10.1016/j.procs.2020.03.194.
[16] A. Alenezi, H. F. Atlam, and G. B. Wills, "Experts reviews of a cloud forensic readiness framework for organizations," *J. Cloud Comput.*, vol. 8, no. 1, 2019, doi: 10.1186/s13677-019-0133-z.
[17] S. Yuan, "Deep Learning for Insider Threat Detection : Review , Challenges and Opportunities," 2020, doi: https://doi.org/10.48550/arXiv.2005.12433.
[18] T. Morrow, K. Pender, C. Lee, D. Faatz, and N. Richmond, *Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud*. apps.dtic.mil, 2020. doi: 10.1184/R1/12363569.v2.
[19] M. Malatji, A. Marnewick, and S. Von Solms, "Computers & Security Validation of a socio-technical management process for optimising cybersecurity practices," *Comput. Secur.*, vol. 95, p. 101846, 2020, doi: 10.1016/j.cose.2020.101846.
[20] M. Khanafseh, M. Qatawneh, and W. Almobaideen, "A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 8, pp. 610–629, 2019, doi: 10.14569/ijacsa.2019.0100880.
[21] S. Siddiqui, M. Darbari, and D. Yagyasen, "A comprehensive study of challenges and issues in cloud computing," *... Comput. Signal Process.*, 2019, doi: 10.1007/978-981-13-3600-3_31.
[22] D. C. Le and A. N. Zincir-Heywood, "Evaluating insider threat detection workflow using supervised and unsupervised learning," *Proc. - 2018 IEEE Symp. Secur. Priv. Work. SPW 2018*, pp. 270–275, 2018, doi: 10.1109/SPW.2018.00043.
[23] R. Adams, V. Hobbs, G. Mann, V. Hobbs, and G. Mann, "Journal of Digital Forensics , Security and Law The Advanced Data Acquisition Model (Adam): A Process Model for Digital Forensic Practice THE ADVANCED DATA ACQUISITION MODEL (ADAM): A PROCESS MODEL FOR," vol. 8, no. 4, 2013, doi: https://doi.org/10.15394/jdfsl.2013.1154.
[24] F. Yuan, Y. Cao, Y. Shang, Y. Liu, J. Tan, and B. Fang, *Insider threat detection with deep neural network*, vol. 10860 LNCS. Springer International Publishing, 2018. doi: 10.1007/978-3-319-93698-7_4.
[25] M. N. F. Rusydi Umar, Anton Yudhana, "Experimental Analysis of Web Browser Sessions Using Live Forensics Method," *Int. J. Electr. Comput. Eng.*, vol. 8, 2018, doi: 10.11591/ijece.v8i5.pp2951-2958.
[26] Z. A. Al-Sharif, M. I. Al-Saleh, L. M. Alawneh, Y. I. Jararweh, and B. Gupta, "Live forensics of software attacks on cyber–physical systems," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 1217–1229, 2020, doi: 10.1016/j.future.2018.07.028.
[27] R. A. Ramadhan, P. Rachmat Setiawan, and D. Hariyadi, "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework," *IT J. Res. Dev.*, vol. 6, no. 2, pp. 162–168, 2022, doi: 10.25299/itjrd.2022.8968.

DOI: https://doi.org/10.29207/resti.v7i5.5279