Design and Develop Forensic Application on Client Server Network

Putu Bayu Suarnata Wahyu Putra[a1], I Made Agus Dwi Suarjaya[a2], Kadek Suar Wibawa[a3]
[a]Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana Bukit Jimbaran, Bali, Indonesia, telp. (0361) 701806
email: [1]bayusuarnatawp@gmail.com, [2]agussuarjaya@it.unud.ac.id, [3]suar_wibawa@unud.ac.id

Abstrak

Jaringan client server memungkinkan untuk terbentuknya efesiensi dan efektivitas dalam aktivitas kelompok yang dimiliki, seperti berbagi sumber daya. Meningkatkan perkembangan teknologi beriringan juga dengan meningkatnya tingkat kejahatan yang disebabkan dengan teknologi. Kejahatan yang menggunakan teknologi tetap meninggalkan jejak yang dapat ditelurusi sehingga dapat disebut dengan digital forensic. Digital forensic biasanya dilakukan satu persatu tiap komputer dan menyebabkan membutuhkan waktu yang lebih lama. Melihat permasalah tersebut maka penelitian ini membahas mengenai rancang bangun aplikasi forensic pada jaringan client server dengan metode live forensic dan socket programming untuk melakukan forensic dengan cara bersamaan dalam satu waktu.Aplikasi menggunakan Java socket untuk membangun hubungan antara server dengan client dan metode life forensic untuk mengumpulkan data ketika client masih dalam keadaan hidup. Hasil yang didapatkan ketika membangun aplikasi adalah aplikasi mampu untuk melakukan pengambilan data dari seluruh client yang berupa data gambar tangkapan layar, data RAM, dan snapshot disk dari client secara bersamaan.

Kata kunci: Aplikasi *Client Server*, *Life Forensic*, Akuisisi Data, Pemgrograman *Socket*, Pemrograman *Desktop*

Abstract

Client server networks allow for creating efficiency and effectiveness in doing activity with teamwork, such as sharing resources. Improving technological development goes hand in hand with increasing crime rates caused by technology. Crimes that use technology still leave a trace that can be traced so that it can be paralleled with digital forensics. Digital forensics are usually done one by one per computer and cause it to take longer time to get evidence in criminal act. Looking at the problem, this study discusses the design of forensic applications on client server networks with live forensic methods and socket programming to perform forensics at the same time. Applications use Java sockets to establish a connection between the server and the client and the elevator method. The result of this study is server can collect data, like data of RAM, captured image, and snapshot disk from clients.

Keywords: *Client Server Application, Life Forensic, Data Acquisition, Socket Programming, Desktop Programming*

1. Introduction

Computer networks and telecommunications are already an important part of life. The utilization of computer networks either wired or wirelessly has been improved and is easy to use [1]. The use of computer networks is useful for increasing effectiveness and efficiency, such as the existence of client and server-based network applications.

The use of client and server-based network applications is widely applied in offices on corporate networks, which makes it possible to share resources between clients [2]. The implementation of a client server network is considered to provide advantages to increase the productivity of network users, with a device that is used as a tool for receive request services sent by client devices [3]. Application creation with client server architecture, can use socket programming technology. Socket is a terminal that connects the client with the server in order to communicate with each other [4]. Socket allows for two nodes to be able to exchange information in two directions. The exchange of information can be carried out with the help of protocols TCP (Transmission Control Protocol). The TCP protocol is a standard or data communication rule used for the process of exchanging data between interconnected computers in a network based on connection oriented [5].

The existence of applications or technologies used can open new gaps to generate risks that can arise [6]. This risk can cause damage to the computer system or computer network system, resulting an unwanted harm. Losses that occur due to the use of loopholes, can be investigated so that the cause can be known and used as a reference to improve computer security [7].

An investigation to obtain evidence when a case occurs in the computer world is called digital forensic [8]. The digital forensic stage is similar to the forensic stage in general, except that the forensic process is carried out on a computer device [9]. There are various types of digital forensics, one of which is live forensic. Live forensic makes it possible to obtain data in the state that a device is still alive, such as from volatile memory to get more evidence to solve the problem that is owned [10]. The existence of Life forensic makes it possible to collect data stored by RAM when the computer is alive, so that the data obtained by the data makes it easier to use it as evidence.

Supriyono et al in a previous study discussed the use of life forensics to collect digital evidence on smart routers [11]. Life forensic is used to conduct investigations to obtain digital evidence on processes occurring on the network through smart routers. Larasati et al in a previous study discussed the use of life forensics to compare conversational applications on the Windows 10 operating system. Evidence was obtained by analyzing RAM data when using conversational applications [6]. Khurniawan et al in a previous study discussed network monitoring tools using Java autonomous agents [12]. The research discussed the formation of applications aimed at monitoring clients with the Java programming language and assistance from the SNMP (Simple Network Management Protocol) protocol. Cordova in previous research discussing designing applications with socket programming [13]. Applications are formed with socket programming technology and Java programming language. The application formed is the OBS (Optel Billing Service) client server application.

Based on previous research and problems regarding the investigation of problems that occur in computer networks that have not been able to carry out investigations of all network devices. The author wants to form a client server-based application to be able to perform live forensics on the client using Java, Java Swing and MySQL server. Java is one of the popular programming languages that can be used to create any kind of application, such as desktop, mobile, IOT [14], Java Swing Java Swing is a Java technology intended to be able to create GUI-based Java applications for the development of desktop applications that can be run cross-platform [15], and MySQL is a DMS (Database Management System) that uses SQL (Structured Query Language) commands to be able to manage database servers to store data [16]. The purpose of forming the application is to be able to collect evidence thoroughly and at the same time and can be controlled from the server.

2. Research Method

Research methods for the formation of applications consist of several stages. An overview of the research method can be seen in Figure 1.

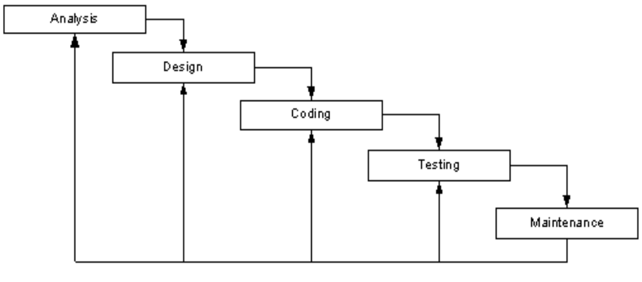


Figure 1 Research Methodology

Figure 1 shows the stages in the formation of an application that is used as a research methodology. The stages of formation of the application consist of five stages. The first stage is the analysis stage, which is the stage of analyzing the needs of the application. The design stage is a stage for designing workflows or process flows and display design for applications. The coding stage is a stage to implement the results of the design into the form of program code and into an application. The testing stage is the stage to try the application when the application has been completed, the type of testing used is black box testing. The last stage is maintenance, the stage of maintaining the application so that it can always be used, if there are additional features or bugs in the application, the stages will repeat to the analysis stage and so on.

3. Material and Method

The analysis and design process produces a method that will be applied to form the application. A general description is an overview that displays the process flow of the application in general. An overview can be seen in Figure 2.

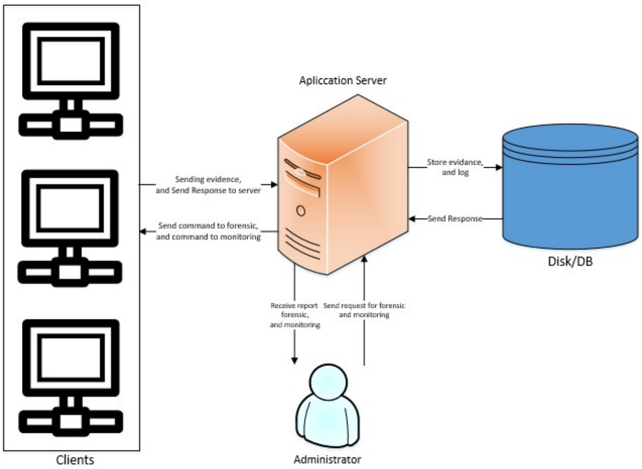


Figure 2 General Overview

The server application serves as a control unit to receive administrator requests and send commands to the entire client, and save data to disk or into a database server. The workflow of the application can be seen in Figure 3.

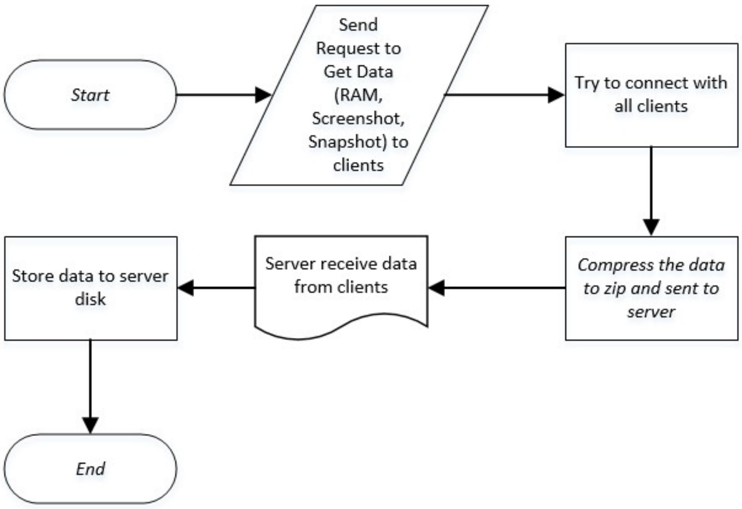

Start
Send Request to Get Data (RAM, Screenshot, Snapshot) to clients
Try to connect with all clients
Compress the data to zip and sent to server
Server receive data from clients
Store data to server disk
End

Figure 3 Flowchart Getting Data from Client

4. Result and Discussion

4.1 System Implementation

The implantation of the system consists of several parts, such as the main menu section, the online client viewing menu, the menu of viewing disk snapshots, viewing the collected data, and viewing log data of activities carried out by the admin.

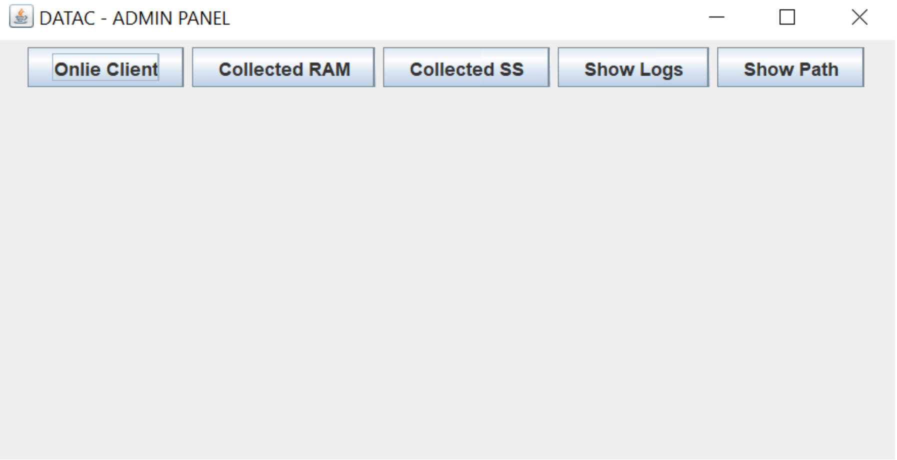
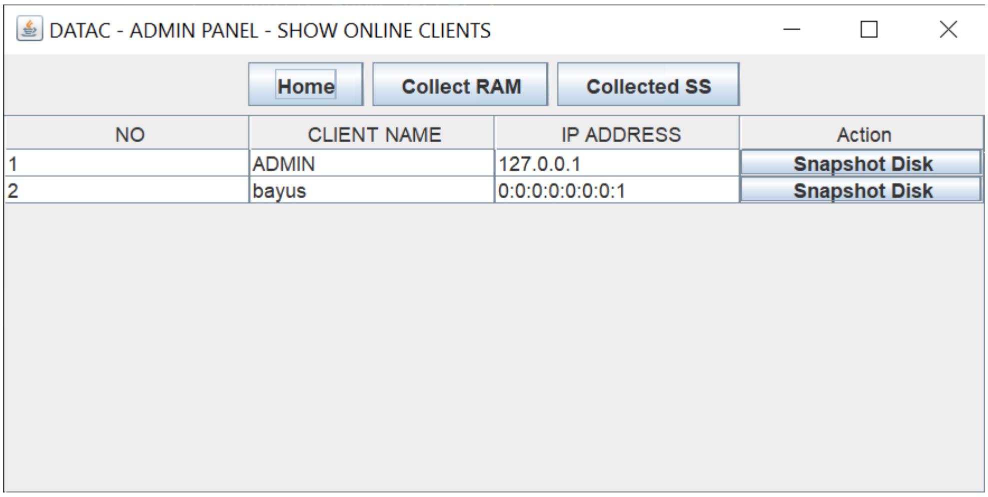


Figure 4 Main Menu

Figure 4 shows the main menu of the application. The main menu consists of several components that serve to make it easier for administrators to use the application. The online client button serves to see the client connected to the server. The collected RAM and collected SS buttons serve to see the data that has been collected. Show logs button to view data collection activity log and show path button to view and configure excluded path data.

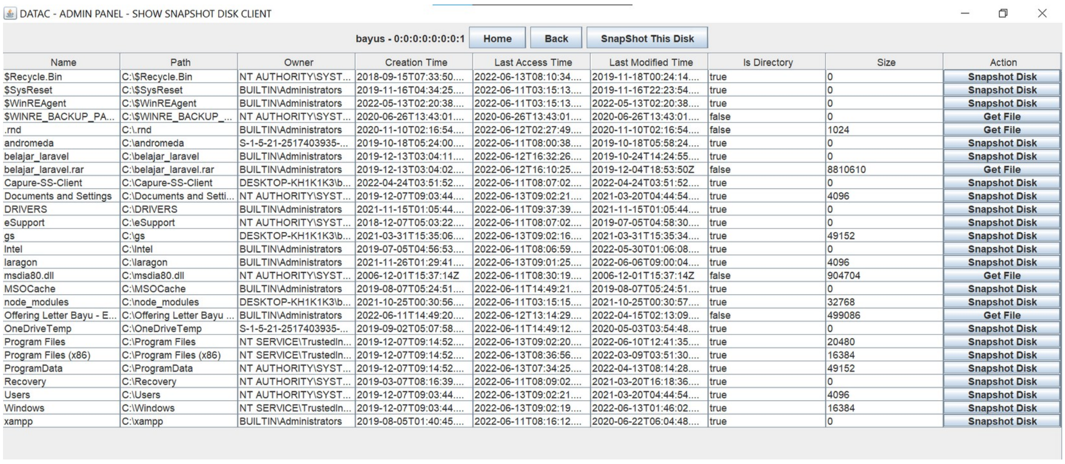


NO	CLIENT NAME	IP ADDRESS	Action
1	ADMIN	127.0.0.1	Snapshot Disk
2	bayus	0:0:0:0:0:0:0:1	Snapshot Disk

Figure 5 Online Client

Figure 5 shows the online client menu. The online client menu consists of several constituent components that aim to display clients connected to the server. There is a table that displays the number information, the name of the client, the IP address of the client and the action button to perform disk snapshot commands on the selected client. There is a home button that functions to return to the main menu, a collect RAM button which functions to collect

RAM data from all clients connected to the server, and a collected SS button to collect screenshot data from all clients connected to the server.



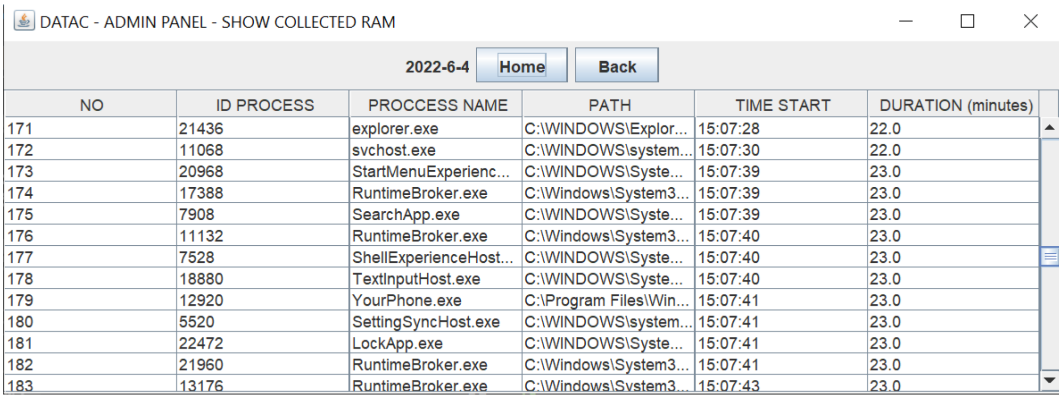
DATAC - ADMIN PANEL - SHOW SNAPSHOT DISK CLIENT

bayus - 0:0:0:0:0:0:0:1

Name	Path	Owner	Creation Time	Last Access Time	Last Modified Time	Is Directory	Size	Action
$Recycle.Bin	C:\$Recycle.Bin	NT AUTHORITY\SYST...	2018-09-15T07:33:50....	2022-06-13T08:10:34....	2019-11-18T00:24:14....	true	0	Snapshot Disk
$SysReset	C:\$SysReset	BUILTIN\Administrators	2019-11-16T04:34:25....	2022-06-11T03:15:13....	2019-11-16T22:23:54....	true	0	Snapshot Disk
$WinREAgent	C:\$WinREAgent	BUILTIN\Administrators	2022-05-13T02:20:38....	2022-06-11T03:15:13....	2022-05-13T02:20:38....	true	0	Snapshot Disk
$WINRE_BACKUP_PA...	C:\$WINRE_BACKUP_...	NT AUTHORITY\SYST...	2020-06-26T13:43:01....	2020-06-26T13:43:01....	2020-06-26T13:43:01....	false	0	Get File
.rnd	C:\.rnd	BUILTIN\Administrators	2020-11-10T02:16:54....	2022-06-12T02:27:49....	2020-11-10T02:16:54....	false	1024	Get File
andromeda	C:\andromeda	S-1-5-21-2517403935-...	2019-10-18T05:24:00....	2022-06-11T08:00:38....	2019-10-18T05:58:24....	true	0	Snapshot Disk
belajar_laravel	C:\belajar_laravel	BUILTIN\Administrators	2019-12-13T03:04:11....	2022-06-12T16:32:26....	2019-10-24T14:24:55....	true	0	Snapshot Disk
belajar_laravel.rar	C:\belajar_laravel.rar	BUILTIN\Administrators	2019-12-13T03:04:02....	2022-06-12T16:10:25....	2019-12-04T18:53:50Z	false	8810610	Get File
Capure-SS-Client	C:\Capure-SS-Client	DESKTOP-KH1K1K3\b...	2022-04-24T03:51:52....	2022-06-11T08:07:02....	2022-04-24T03:51:52....	true	0	Snapshot Disk
Documents and Settings	C:\Documents and Setti...	NT AUTHORITY\SYST...	2019-12-07T09:03:44....	2022-06-13T09:02:21....	2021-03-20T04:44:54....	true	4096	Snapshot Disk
DRIVERS	C:\DRIVERS	BUILTIN\Administrators	2021-11-15T01:05:44....	2022-06-11T09:37:39....	2021-11-15T01:05:44....	true	0	Snapshot Disk
eSupport	C:\eSupport	NT AUTHORITY\SYST...	2018-12-07T05:03:22....	2022-06-11T08:07:02....	2019-07-05T04:58:30....	true	0	Snapshot Disk
gs	C:\gs	DESKTOP-KH1K1K3\b...	2021-03-31T15:35:06....	2022-06-13T09:02:16....	2021-03-31T15:35:34....	true	49152	Snapshot Disk
Intel	C:\Intel	BUILTIN\Administrators	2019-07-05T04:56:53....	2022-06-11T08:06:59....	2022-05-30T01:06:08....	true	0	Snapshot Disk
laragon	C:\laragon	BUILTIN\Administrators	2021-11-26T01:29:41....	2022-06-13T09:01:25....	2022-06-06T09:00:04....	true	4096	Snapshot Disk
msdia80.dll	C:\msdia80.dll	NT AUTHORITY\SYST...	2006-12-01T15:37:14Z	2022-06-11T08:30:19....	2006-12-01T15:37:14Z	false	904704	Get File
MSOCache	C:\MSOCache	BUILTIN\Administrators	2019-08-07T05:24:51....	2022-06-11T14:49:21....	2019-08-07T05:24:51....	true	0	Snapshot Disk
node_modules	C:\node_modules	DESKTOP-KH1K1K3\b...	2021-10-25T00:30:56....	2022-06-11T03:15:15....	2021-10-25T00:30:57....	true	32768	Snapshot Disk
Offering Letter Bayu - E...	C:\Offering Letter Bayu ...	BUILTIN\Administrators	2022-06-11T14:49:20....	2022-06-12T13:14:29....	2022-04-15T02:13:09....	false	499086	Get File
OneDriveTemp	C:\OneDriveTemp	S-1-5-21-2517403935-...	2019-09-02T05:07:58....	2022-06-11T14:49:12....	2020-05-03T03:54:48....	true	0	Snapshot Disk
Program Files	C:\Program Files	NT SERVICE\TrustedIn...	2019-12-07T09:14:52....	2022-06-13T09:02:20....	2022-06-10T12:41:35....	true	20480	Snapshot Disk
Program Files (x86)	C:\Program Files (x86)	NT SERVICE\TrustedIn...	2019-12-07T09:14:52....	2022-06-13T08:36:56....	2022-03-09T03:51:30....	true	16384	Snapshot Disk
ProgramData	C:\ProgramData	NT AUTHORITY\SYST...	2019-12-07T09:14:52....	2022-06-13T07:34:25....	2022-04-13T08:14:28....	true	49152	Snapshot Disk
Recovery	C:\Recovery	NT AUTHORITY\SYST...	2019-03-07T08:16:39....	2022-06-11T08:09:02....	2021-03-20T16:18:36....	true	0	Snapshot Disk
Users	C:\Users	NT AUTHORITY\SYST...	2019-12-07T09:03:44....	2022-06-13T09:02:21....	2021-03-20T04:44:54....	true	4096	Snapshot Disk
Windows	C:\Windows	NT SERVICE\TrustedIn...	2019-12-07T09:03:44....	2022-06-13T09:02:19....	2022-06-13T01:46:02....	true	16384	Snapshot Disk
xampp	C:\xampp	BUILTIN\Administrators	2019-08-05T01:40:45....	2022-06-11T08:16:12....	2020-06-22T06:04:48....	true	0	Snapshot Disk

Figure 6 Snapshot Disk

Figure 6 shows a menu for performing a disk snapshot process on one of the clients that connect to the server. The disk snapshot menu is a menu that functions to view and collect file data owned by the selected client directly. The disk snapshot menu displays the client name and IP address accompanied by file or directory information owned by the client. The information displayed is the name of the file or directory (file), the path the file was saved, the owner of the file or directory, the time the file was formed, the last time to access the file, the last time to modify the file, whether the file is a directory, the size of the file in bytes and the action buttons to enter the directory or take the file to be used as evidence. There is also a snapshot this disk button that functions to store a log of directory information displayed by the disk snapshot menu.



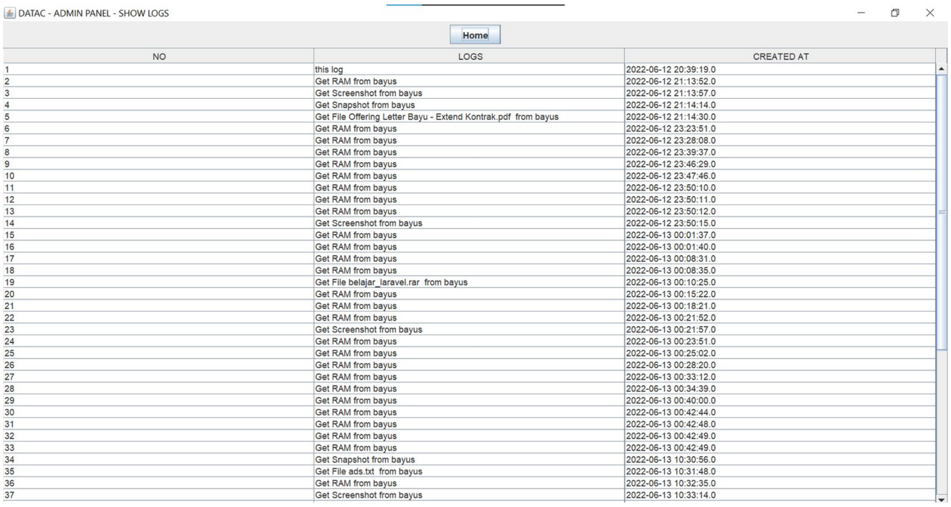
DATAC - ADMIN PANEL - SHOW COLLECTED RAM

2022-6-4

NO	ID PROCESS	PROCCESS NAME	PATH	TIME START	DURATION (minutes)
171	21436	explorer.exe	C:\WINDOWS\Explor...	15:07:28	22.0
172	11068	svchost.exe	C:\WINDOWS\system...	15:07:30	22.0
173	20968	StartMenuExperienc...	C:\WINDOWS\Syste...	15:07:39	23.0
174	17388	RuntimeBroker.exe	C:\Windows\System3...	15:07:39	23.0
175	7908	SearchApp.exe	C:\WINDOWS\Syste...	15:07:39	23.0
176	11132	RuntimeBroker.exe	C:\Windows\System3...	15:07:40	23.0
177	7528	ShellExperienceHost...	C:\WINDOWS\Syste...	15:07:40	23.0
178	18880	TextInputHost.exe	C:\WINDOWS\Syste...	15:07:40	23.0
179	12920	YourPhone.exe	C:\Program Files\Win...	15:07:41	23.0
180	5520	SettingSyncHost.exe	C:\WINDOWS\system...	15:07:41	23.0
181	22472	LockApp.exe	C:\WINDOWS\Syste...	15:07:41	23.0
182	21960	RuntimeBroker.exe	C:\Windows\System3...	15:07:41	23.0
183	13176	RuntimeBroker.exe	C:\Windows\System3...	15:07:43	23.0

Figure 7 Collected Data RAM

Figure 7 is a menu to view RAM data from one of the clients on a certain date that has been collected previously. The menu displaying RAM data is intended to show RAM data information that has been successfully collected by the server. The information displayed on the menu is the number of service, the process id of the running application service, the name of the process, where the process was run, the time the process was run, and the length of time the process ran in units of minutes.



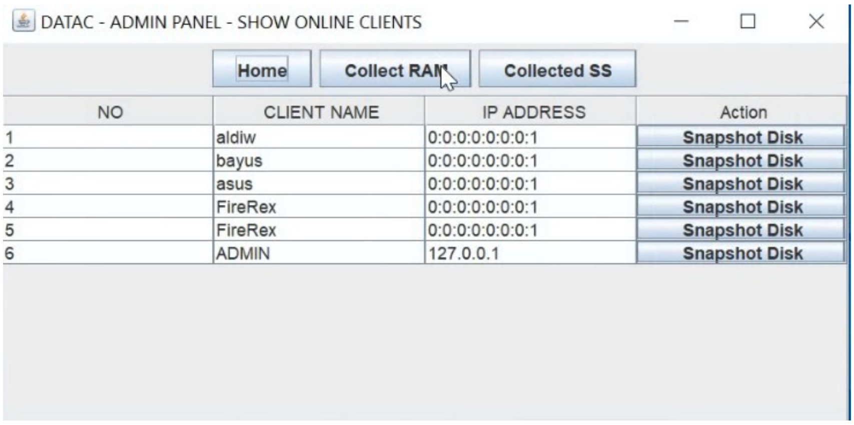
NO	LOGS	CREATED AT
1	this log	2022-06-12 20:39:19.0
2	Get RAM from bayus	2022-06-12 21:13:52.0
3	Get Screenshot from bayus	2022-06-12 21:13:57.0
4	Get Snapshot from bayus	2022-06-12 21:14:14.0
5	Get File Offering Letter Bayu - Extend Kontrak.pdf from bayus	2022-06-12 21:14:30.0
6	Get RAM from bayus	2022-06-12 23:23:51.0
7	Get RAM from bayus	2022-06-12 23:28:08.0
8	Get RAM from bayus	2022-06-12 23:39:37.0
9	Get RAM from bayus	2022-06-12 23:46:29.0
10	Get RAM from bayus	2022-06-12 23:47:46.0
11	Get RAM from bayus	2022-06-12 23:50:10.0
12	Get RAM from bayus	2022-06-12 23:50:11.0
13	Get RAM from bayus	2022-06-12 23:50:12.0
14	Get Screenshot from bayus	2022-06-12 23:50:15.0
15	Get RAM from bayus	2022-06-13 00:01:37.0
16	Get RAM from bayus	2022-06-13 00:01:40.0
17	Get RAM from bayus	2022-06-13 00:08:31.0
18	Get RAM from bayus	2022-06-13 00:08:35.0
19	Get File belajar_laravel.rar from bayus	2022-06-13 00:10:25.0
20	Get RAM from bayus	2022-06-13 00:15:22.0
21	Get RAM from bayus	2022-06-13 00:18:21.0
22	Get RAM from bayus	2022-06-13 00:21:52.0
23	Get Screenshot from bayus	2022-06-13 00:21:57.0
24	Get RAM from bayus	2022-06-13 00:23:51.0
25	Get RAM from bayus	2022-06-13 00:25:02.0
26	Get RAM from bayus	2022-06-13 00:28:20.0
27	Get RAM from bayus	2022-06-13 00:33:12.0
28	Get RAM from bayus	2022-06-13 00:34:39.0
29	Get RAM from bayus	2022-06-13 00:40:00.0
30	Get RAM from bayus	2022-06-13 00:42:44.0
31	Get RAM from bayus	2022-06-13 00:42:48.0
32	Get RAM from bayus	2022-06-13 00:42:49.0
33	Get RAM from bayus	2022-06-13 00:42:49.0
34	Get Snapshot from bayus	2022-06-13 10:30:56.0
35	Get File ads.txt from bayus	2022-06-13 10:31:48.0
36	Get RAM from bayus	2022-06-13 10:32:35.0
37	Get Screenshot from bayus	2022-06-13 10:33:14.0

Figure 8 Log Activity

Figure 8 is a menu to show logs of data collection activities from clients carried out by the admin. The logs feature is intended to show the history of admin activities when retrieving data, so that the data retrieved can be accounted for and the admin does not retrieve data arbitrarily. The logs are stored in a database that stores data on RAM data ownership activities, screenshots, disk snapshots, and one of the files obtained from the client.

4.2 Testing

Testing is a process to try applications that have been made. Testing is aimed at ensuring that the application is running properly. The type of testing used in this study was using black box testing. Testing is done by connecting several clients on the server and trying to run the features possessed by the application. The following are the results of testing and scenarios from the process of trying the application that has been created.



NO	CLIENT NAME	IP ADDRESS	Action
1	aldiw	0:0:0:0:0:0:0:1	Snapshot Disk
2	bayus	0:0:0:0:0:0:0:1	Snapshot Disk
3	asus	0:0:0:0:0:0:0:1	Snapshot Disk
4	FireRex	0:0:0:0:0:0:0:1	Snapshot Disk
5	FireRex	0:0:0:0:0:0:0:1	Snapshot Disk
6	ADMIN	127.0.0.1	Snapshot Disk

Figure 9 All Client Connected to Server

Figure 9 shows several clients that have successfully connected to the server. The image shows five clients connected to the server that the data will be tried to retrieve as digital evidence.

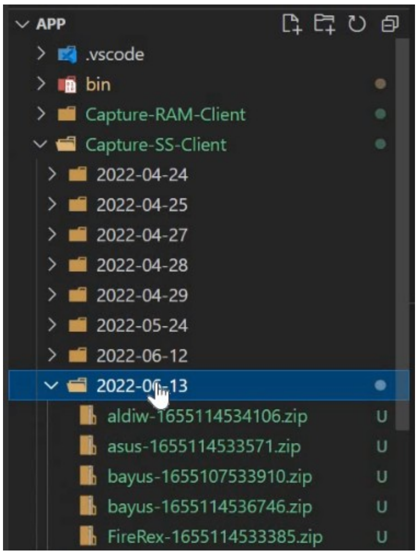


Figure 10 Collected Images

Figure 10 shows that it has successfully collected image data obtained from all clients at the same time. Image data collection is carried out by pressing the SS collect button. Image data is grouped into a directory called from the date of capture of the image data and is named according to the client who owns the image data. Image data is compressed into a zip file so that it is easier to send data from the client to the server because the number of images collected is more than one.

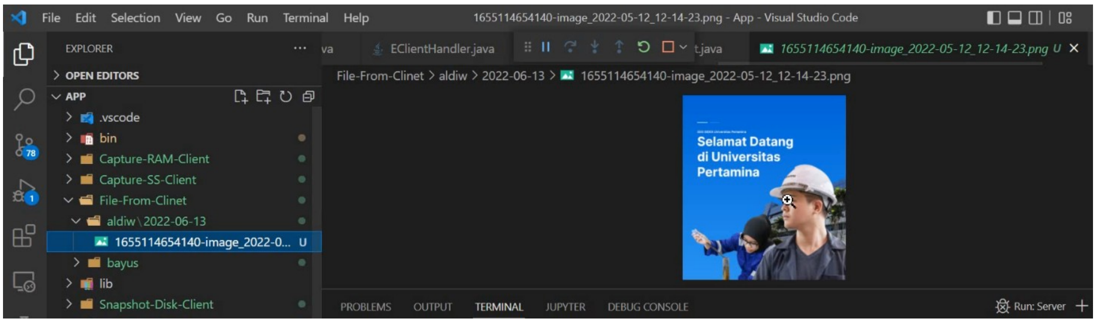
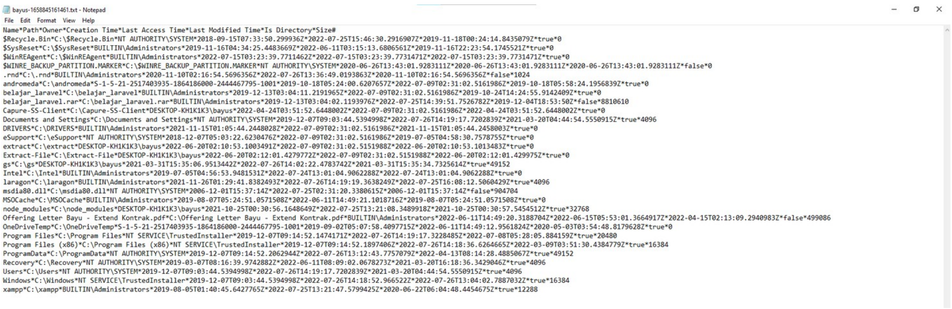

File Edit Selection View Go Run Terminal Help
1655114654140-image_2022-05-12_12-14-23.png - App - Visual Studio Code
EXPLORER
OPEN EDITORS
APP
.vscode
bin
Capture-RAM-Client
Capture-SS-Client
File-From-Clinet
aldiw \ 2022-06-13
1655114654140-image_2022-0... U
bayus
lib
Snapshot-Disk-Client
EClientHandler.java
1655114654140-image_2022-05-12_12-14-23.png U
File-From-Clinet > aldiw > 2022-06-13 > 1655114654140-image_2022-05-12_12-14-23.png
Selamat Datang di Universitas Pertamina
PROBLEMS OUTPUT TERMINAL JUPYTER DEBUG CONSOLE
Run: Server

Figure 11 Result Image from Client

Figure 11 shows the results of one of the images successfully received by the server. The image indicates that the server has succeeded in asking the client to collect data according to the administrator's request which will later be used as digital evidence. The result of the collection of disk snapshots can be seen in Figure 12



```
Name*Path*Owner*Creation Time*Last Access Time*Last Modified Time*Is Directory*Size#
$Recycle.Bin*C:\$Recycle.Bin*NT AUTHORITY\SYSTEM*2018-09-15T07:33:50.299936Z*2022-07-25T15:46:30.2916907Z*2019-11-18T00:24:14.8435079Z*true*0
$SysReset*C:\$SysReset*BUILTIN\Administrators*2019-11-16T04:34:25.4483669Z*2022-06-11T03:15:13.6806561Z*2019-11-16T22:23:54.1745521Z*true*0
$WinREAgent*C:\$WinREAgent*BUILTIN\Administrators*2022-07-15T03:23:39.7711462Z*2022-07-15T03:23:39.7731471Z*2022-07-15T03:23:39.7731471Z*true*0
$WINRE_BACKUP_PARTITION.MARKER*C:\$WINRE_BACKUP_PARTITION.MARKER*NT AUTHORITY\SYSTEM*2020-06-26T13:43:01.9283111Z*2020-06-26T13:43:01.9283111Z*2020-06-26T13:43:01.9283111Z*false*0
.rnd*C:\.rnd*BUILTIN\Administrators*2020-11-10T02:16:54.5696356Z*2022-07-26T13:36:49.0193863Z*2020-11-10T02:16:54.5696356Z*false*1024
andromeda*C:\andromeda*S-1-5-21-2517403935-1864186000-2444467795-1001*2019-10-18T05:24:00.6207657Z*2022-07-09T02:31:02.5161986Z*2019-10-18T05:58:24.1956839Z*true*0
belajar_laravel*C:\belajar_laravel*BUILTIN\Administrators*2019-12-13T03:04:11.2191965Z*2022-07-09T02:31:02.5161986Z*2019-10-24T14:24:55.9142409Z*true*0
belajar_laravel.rar*C:\belajar_laravel.rar*BUILTIN\Administrators*2019-12-13T03:04:02.1193976Z*2022-07-25T14:39:51.7526782Z*2019-12-04T18:53:50Z*false*8810610
Capure-SS-Client*C:\Capure-SS-Client*DESKTOP-KH1K1K3\bayus*2022-04-24T03:51:52.6448002Z*2022-07-09T02:31:02.5161986Z*2022-04-24T03:51:52.6448002Z*true*0
Documents and Settings*C:\Documents and Settings*NT AUTHORITY\SYSTEM*2019-12-07T09:03:44.5394998Z*2022-07-26T14:19:17.7202839Z*2021-03-20T04:44:54.5550915Z*true*4096
DRIVERS*C:\DRIVERS*BUILTIN\Administrators*2021-11-15T01:05:44.2448028Z*2022-07-09T02:31:02.5161986Z*2021-11-15T01:05:44.2458003Z*true*0
eSupport*C:\eSupport*NT AUTHORITY\SYSTEM*2018-12-07T05:03:22.6230476Z*2022-07-09T02:31:02.5161986Z*2019-07-05T04:58:30.7578755Z*true*0
extract*C:\extract*DESKTOP-KH1K1K3\bayus*2022-06-20T02:10:53.1003491Z*2022-07-09T02:31:02.5151988Z*2022-06-20T02:10:53.1013483Z*true*0
Extract-File*C:\Extract-File*DESKTOP-KH1K1K3\bayus*2022-06-20T02:12:01.4279772Z*2022-07-09T02:31:02.5151988Z*2022-06-20T02:12:01.429975Z*true*0
gs*C:\gs*DESKTOP-KH1K1K3\bayus*2021-03-31T15:35:06.9513442Z*2022-07-26T14:02:22.4783742Z*2021-03-31T15:35:34.7325614Z*true*49152
Intel*C:\Intel*BUILTIN\Administrators*2019-07-05T04:56:53.9481531Z*2022-07-24T13:01:04.9062288Z*2022-07-24T13:01:04.9062288Z*true*0
laragon*C:\laragon*BUILTIN\Administrators*2021-11-26T01:29:41.8382493Z*2022-07-26T14:19:19.3638249Z*2022-07-25T16:08:12.5060429Z*true*4096
msdia80.dll*C:\msdia80.dll*NT AUTHORITY\SYSTEM*2006-12-01T15:37:14Z*2022-07-25T02:31:20.3380615Z*2006-12-01T15:37:14Z*false*904704
MSOCache*C:\MSOCache*BUILTIN\Administrators*2019-08-07T05:24:51.0571508Z*2022-06-11T14:49:21.1018716Z*2019-08-07T05:24:51.0571508Z*true*0
node_modules*C:\node_modules*DESKTOP-KH1K1K3\bayus*2021-10-25T00:30:56.1648649Z*2022-07-25T13:21:08.3489918Z*2021-10-25T00:30:57.5454512Z*true*32768
Offering Letter Bayu - Extend Kontrak.pdf*C:\Offering Letter Bayu - Extend Kontrak.pdf*BUILTIN\Administrators*2022-06-11T14:49:20.3188704Z*2022-06-15T05:53:01.3664917Z*2022-04-15T02:13:09.2940983Z*false*499086
OneDriveTemp*C:\OneDriveTemp*S-1-5-21-2517403935-1864186000-2444467795-1001*2019-09-02T05:07:58.4097715Z*2022-06-11T14:49:12.9561824Z*2020-05-03T03:54:48.8179628Z*true*0
Program Files*C:\Program Files*NT SERVICE\TrustedInstaller*2019-12-07T09:14:52.1474171Z*2022-07-26T14:19:17.3228485Z*2022-07-08T05:28:05.884159Z*true*20480
Program Files (x86)*C:\Program Files (x86)*NT SERVICE\TrustedInstaller*2019-12-07T09:14:52.1897406Z*2022-07-26T14:18:36.6264665Z*2022-03-09T03:51:30.4384779Z*true*16384
ProgramData*C:\ProgramData*NT AUTHORITY\SYSTEM*2019-12-07T09:14:52.2062944Z*2022-07-26T13:12:43.7757079Z*2022-04-13T08:14:28.4885067Z*true*49152
Recovery*C:\Recovery*NT AUTHORITY\SYSTEM*2019-03-07T08:16:39.9742882Z*2022-06-11T08:09:02.0678273Z*2021-03-20T16:18:36.3429046Z*true*4096
Users*C:\Users*NT AUTHORITY\SYSTEM*2019-12-07T09:03:44.5394998Z*2022-07-26T14:19:17.7202839Z*2021-03-20T04:44:54.5550915Z*true*4096
Windows*C:\Windows*NT SERVICE\TrustedInstaller*2019-12-07T09:03:44.5394998Z*2022-07-26T14:18:52.966522Z*2022-07-26T13:04:02.7887032Z*true*16384
xampp*C:\xampp*BUILTIN\Administrators*2019-08-05T01:40:45.6427765Z*2022-07-25T13:21:47.5799425Z*2020-06-22T06:04:48.4454675Z*true*12288
```

Figure 12 Result of Snapshot Disk

The result of the disk snapshot is in the form of file or directory name information in a path that collected. The purpose of taking a disk snapshot is to record the activity of a file or directory owned by the client. Information that is felt to be strange, such as strange activity dates, can be stored and used as evidence. The testing scenarios carried out can be seen in Table 1.

Table 1 Scenario Testing

Testing Activities	Test Scenarios	Expected results	Test Results	Conclusion
View client data connected to the server	Enter the Show Client Online menu	Can see all clients connected to the server along with personal data from the client	*Can see all* clients connected to the server along with personal data from client	Fulfilled
Retrieve screen capture data that has been collected by each Client	Pressing the Collect SS button	Get all the screenshot data that has been collected by each client	Get all the screenshot data that has been collected by each client	Fulfilled
Take a disk snapshot data from one of the clients	Pressing the Snapshot This Disk button	Get information about the specified disk path from one of the clients	Get information about the specified disk path from one of the clients	Fulfilled

5. Conclusion

The conclusion of this study is that the application can provide information about the client connected to the server accompanied by name and IP address information. The server through the application is able to collect RAM data, screenshots, and disk snapshots owned by the connected client. Administrators can view data that has been collected by the server through the application or is arranged by the application to a predefined directory for the data that has been stored. The results of data collection carried out by the server are expected to be able to be used as digital evidence in digital forensic activities.

Reference

[1] A. Fadlil, I. Riadi, and A. Nugrahantoro, “Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology,” *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 11, no. 3, p. 155, 2020.

[2] C. Rizal, M. Zen, and M. Eka, “Perancangan Server Kantor Desa Tomuan Holbung Berbasis Client Server,” vol. 3, no. 1, pp. 27–33, 2022.

[3] R. A. Yusda, “Rancang Bangun Jaringan Client Server Berbasis Linux Debian 6.0,” *Semin. Nas. R.*, vol. 1, no. 1, p. 311, 2018.

[4] U. M. Wahyuni and F. Fitrilina, “Implementasi Client-Server Pada Sistem Informasi Pengolahan Nilai Siswa Menggunakan Object-Oriented Programming,” *J. Amplif. J. Ilm. Bid. Tek. Elektro Dan Komput.*, vol. 10, no. 1, pp. 26–32, 2020.

[5] I. F. Anshori, “Implementasi Socket Tcp/Ip Untuk Mengirim Dan Memasukan File Text Kedalam Database,” *Responsif*, vol. Vol 1 No 1, no. 1, pp. 1–5, 2019.

[6] N. R. Maulana, P. Dewonoto, L. Santoso, and R. D. Fajri, “Edukasi Bahaya Software Bajakan Serta Pengenalan Aplikasi Freewere Sebagai Alternatif,” vol. 2, pp. 301–303, 2021.

[7] V. Rosalina and D. Herli, “Pengembangan Model Tahapan Digital Forensic Untuk

Mendukung Serang Sebagai Kota Bebas Cybercrime," *Semin. Nas. Ris. Terap.*, vol. 12, pp. 0–5, 2015.

[8] T. E. WIJATMOKO, "DIGITAL FORENSIC READINES INDEX (DiFRI) UNTUK MENGUKUR KESIAPAN PENANGGULANGAN CYBERCRIME PADA KANTOR WILAYAH KEMENTERIAN HUKUM DAN HAM DIY," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 18–23, 2021.

[9] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Perancangan Digital Forensik pada Aplikasi Twitter Menggunakan Metode Live Forensics," *Semin. Nas. Inform. 2008 (semnasIF 2008)*, vol. 2018, no. November, pp. 86–91, 2018.

[10] T. D. Larasati and B. C. Hidayanto, "Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10," *Sesindo*, vol. 6, no. November, pp. 456–256, 2017.

[11] A. R. Supriyono, B. Sugiantoro, and Y. Prayudi, "Eksplorasi Bukti Digital Pada Smart Router Menggunakan Metode Live Forensics," *Infotekmesin*, vol. 10, no. 2, pp. 1–8, 2019.

[12] E. S. Khurniawan, L. A. S. I. A, and I. B. K. Widiartha, "Perancangan Network Monitoring Tools Menggunakan Autonomous Agent Java," vol. 7, no. 2, pp. 115–121, 2016.

[13] R. Cordova, "Design and Implementation of Client-Server Based Application using Socket Programming in a Distributed Computing Environment," no. January 2018, 2017.

[14] A. P. C. Udaksana and W. R. Kusaeri, "Rancang Bangun Aplikasi Digital School Dengan Java NetBeans IDE 8.1," *Irons*, pp. 332–336, 2018.

[15] A. R. Ni Luh Ayu Widary, Halimatus Sa'diah, "RANCANG BANGUN SISTEM INFORMASI ADMINISTRASI MANAJEMEN PADA SALON CAPTUS BERBASIS JAVA," *Syntax Idea*, vol. 2, no. August, pp. 458–470, 2020.

[16] M. S. Novendri, A. Saputra, and C. E. Firman, "Aplikasi Inventaris Barang Pada MTS Nurul Islam Dumai Menggunakan PHP Dan MySQL," *Lentera Dumai*, vol. 10, no. 2, pp. 46–57, 2019.