Forensic Analysis of Unmanned Aerial Vehicle to Obtain GPS Log Data as Digital Evidence

By Imam Riadi

WORD COUNT 3996
TIME SUBMITTED 18-JUL-2017 04:03PM
PAPER ID 30577583

International Journal of Computer Science and Information Security (IJCSIS),
Vol. 15, No. 3, March 2017

Forensic Analysis of Unmanned Aerial Vehicle to Obtain GPS Log Data as Digital Evidence

Septyan Eka Prastya
Departement of Informatics
Universitas Islam Indonesia
Yogyakarta, Indonesia
septyan_iyas@rocketmail.com

Imam Riadi
Department of Information System
Ahmad Dahlan University
Yogyakarta, Indonesia
imam.riadi@is.uad.ac.id

Ahmad Luthfi
Departement of Informatics
Universitas Islam Indonesia
Yogyakarta, Indonesia
Ahmad.luthfi@uii.ac.id

***Abstract*— In recent years, the use of drones by civilians is increasing rapidly by the presentation of total sales continued to increase rapidly every year. With the increasing possibility of Unmanned Aerial Vehicle (UAV) abuse, crime in the use of UAVs to be larger. Through forensic analysis of data using static forensic and live forensic to obtain data that allows it to be used as digital evidence. To dig up information that could be used as digital evidence in the UAV and controllers, as well as to know the characteristics of digital evidence on a UAV. The results showed that digital evidence on a UAV, the smartphone is used as a controller UAV has a very important role in the investigation. The findings in aircraft has a percentage of 50% and a camera memory card with 16.6%. DJI Phantom 3 Advanced GPS coordinates always store data in flight LOG; the data is always stored even when the flight mode is used does not use GPS signals to stability. Due to DJI Phantom 3 Advanced always use GPS on flights, file, image or video captured by the camera has the best GPS location coordinates to the metadata therein.**

Keywords; UAV; Log; Forensic; GPS; Flight Data

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs) or drones are also called, is a small aircraft without a pilot. This is now the most widely used in the military and those fans the hobby of photography/videography. In recent years, the use of drones by civilians increased rapidly, until it is mentioned by the UK House of Lords that 2014 is the "Year of the drones" [1].

Forbes magazine in 2015 wrote on its Web site sales distribution one trademark holder drones from its inception to the present. At the beginning of sales in 2009 to 2010, the presentation of the annual income more than 50% of overall sales are in North American. Moreover, in 2011 the total annual sales presentation to increase up to 280%, while sales in the North American presentation of only about 30% of total sales. Presentation of total sales continued to increase rapidly every year, the sale of drones in 2020 is expected to touch $ 2.28 Billion [2].

Drone works with two parts; the first is the drone itself and a controller that functions to control the drones. In some types of drones, there is already no longer requires a controller for controlling the aircraft. This type of drone using GPS transmitters installed on the users, so when this is enabled drones, aircraft will automatically follow any direction from people who used the transmitter. Drone with works like this has many sensors on the aircraft, which is useful to keep the drones remain safe from the surrounding environment when flying follow users.

Digital evidence that can be taken from the body of drones and the controller is the ID of the drone itself, the location where the drone ever flew, image or video is taken when drones were flown, log update the software used. While the controller can be found in the form of digital evidence storage of images or videos taken using drones, log the location of the use of drones, the software used to control the drone, the ID of the drones are connected.

Realm of this study is to gather information and conducts an analysis of digital evidence contained on drones along its controller by using static forensic and lives forensic with efforts to help complete the information on the forensic activity that uses GPS on the drone.

II. RELATED WORK

Several studies have been done on a UAV. Research about the small quadcopter demonstrates the utility of UAVs to safely and accurately mapped physical and biological characteristics of the unique habitat[3]. Then research explores the basics of the estimates and the flight controls for small winged UAV remains that covers common sensor and sensor configuration used small UAVs to be estimated[4]. Other studies have also been conducted, which is about the theory and practice of spoofing of Unmanned Aerial Vehicle (UAV) is captured and controlled by using a signal Global Positioning System (GPS)[5].

In 2014 conducted research to discover forensic methods in the search for artifacts that may be used for digital evidence on the device Garmin and Tom Tom satnav. The results obtained in the form of the acquisition method and the analysis and comparison of data obtained in the navigation system Garmin and Tom Tom[6]. Similar research is also done by exploration of digital evidence on Android Smartphone with through several stages. Results obtained in the form of technical image acquisition and analysis of digital evidence GPS on Android Smartphone, the application framework for the investigation, and provides several options framework that can be used[7].

Another study conducted on GPS data are based on a study reported in the relevant publication and focuses on variable directly to a GPS device such as clouds, weather, obstructions,

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

signal split and user preferences, and test the accuracy of three GPS devices[8].

III. Basic Theory

A. Log

Log files become a standard part of large and very important applications in the operating system, computer networks, and distributed systems. The log file is the only way how to identify and locate faults in the software because the log file analysis is not affected by the issues based on the time known as the probe effect. This contrasts with the analysis of the program when the analytical process can disrupt critical condition time or critical resources in the program being analyzed.

Log files are often very large and can have a very complex structure. Although the process of generating a log file is quite simple and straightforward, log file analysis can be a tremendous task requires very large computational resources, long and sophisticated procedures. This often leads to a common situation, when the log file is generated and continues to occupy precious space on a storage device, but no one uses them and utilizes the enclosed information [9]. The log has a large size. Therefore it is necessary steps to facilitate the process of storage and retrieval of information in databases [10].

Log (record keeping) is a file that records events in the computer program. Meanwhile, according to the definition of the log is a record of daily activities. Activities that are recorded directly called the transaction log. The log file can be used as a support in the process of cyber forensics to obtain digital evidence during the investigation stage [11].

While the GPS log is a collection of GPS points, each GPS point containing latitude, longitude, and timestamp [12].

B. GPS Forensics

The GPS-enabled device uses satellite readings to determine the geocentric receiver. Coordinates associated with the center of the earth, and the information to be read by some satellites, which optimally at least four satellites. Gps is defined as a group of satellites in earth orbit that sends the right signal, to enable GPS receivers to calculate and display accurate location, time and speed information to the user [8].

GPS evidence is digital evidence capable of determining a particular geographic location with incredible accuracy. It shows directly to a user's location, so it is easy to find, as well as with a particular user is sought in criminal cases. Evidence in the form of data GPS latitude and longitude [7].

C. Unmanned Aerial Vehicles (UAVs)

Unmanned Aerial Vehicles (UAV) is an unmanned flying vehicle. As for civilian purposes, UAVs can be used for mapping isolated areas, volcano monitoring, monitoring of congestion or shooting area after the tsunami disaster. UAV system consists of the air vehicle (aircraft), payload and control station [13].

Hartmann and Steup [14] describes the flow of information between system components UAV with its ground station that shows in Figure 1.

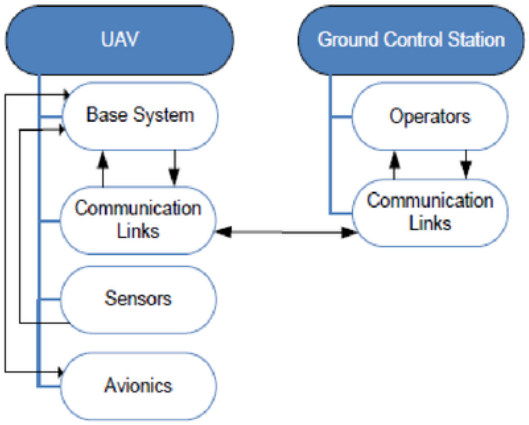

Figure 1 Flow of Information between UAV with Ground Station

"UAV base system" is the basis of the UAV, linking together the components UAV. It is necessary to allow inter-component communication and sensor control, navigation, avionics and communication systems. This can be considered as a UAV "operating system" [14].

D. Flight Data

Jiang and Huang [15] explains that in a conventional aircraft identification system, the various testing technology required for flight data. In general, these technologies can be divided into two methods that measure the parameters of the external and internal parameter measurements. Instantaneous position, trajectory, velocity, and acceleration, etc. can be measured with an external parameter measurement. This data can then be compared with data measured by the air system to test the accuracy of the air system. Measurement parameters of external equipment include photography, radar measurements, laser measurement and others. Measurement parameters include the internal apparatus of global positioning system (GPS) receiver, angular velocity gyroscope, accelerometer, an angular accelerometer, altimeter, airspeed meters and beyond.

IV. Research Methods

To support experiment on this research, hardware, and software that necessary used is listed below:

- DJI Phantom 3 Advanced and controller.
- Android smartphone and PC.
- DJI GO for Android version 2.8.4(415)
- FTK Imager version 3.4.2
- DatCon version 2.3.0
- PhotoMe version 0.79R17

To simulate the scenario created from the use of drones, while the UAV usage scenarios in this study will be described as a Figure 2.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

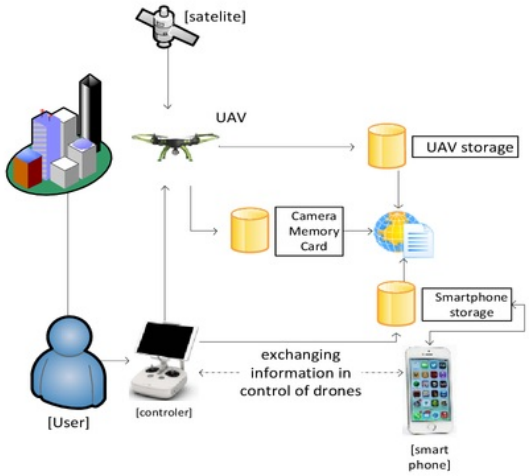

Figure 2 usage scenario of UAV

Scenarios designed in this study are operated a drone to do some flying with different flying mode and taking pictures and video on the site. In each of these locations, when flown navigation sensors inside drone receive location data from GPS and GLONASS satellites which then stored into the database on drones. Controller and smartphone as a ground station are used as a controller and video signal receiver of aircraft. All data received from the UAV ground station then stored in a database on the smartphone as a signal receiver

V. RESULT

A. Scenario

Scenarios used in this study through the multiple activities carried out using three different modes during the flight. The first flight is done by using the P-mode (Positioning), which in this mode using GPS and Vision Position System works together. In this mode, there are three circumstances that are automatically selected by DJI Phantom 3 Advanced based on the signal strength of GPS and Vision Positioning Sensor. As for the form of three circumstances:

- P-GPS: GPS Positioning and Vision sensors are available in this mode UAV using GPS for the position.
- P-OPTI: Vision Positioning available but GPS signal strength is not sufficient, in this mode using only UAV Vision Positioning System for the position.
- P-ATTI: GPS signal and Vision Positioning is not available in this mode using only UAV barometer for the position, so only the height that can be stabilized.

B. Acquisition

The process of acquisition of the UAV performed in three parts, the first of the aircraft used during flight. The second camera storage media used in flight. Moreover, the third is on the controller or ground station that is here is to use a smartphone Lenovo P70.

The acquisition process is in aircraft storage and the memory card found on the aircraft done by way of physical (sectors per sector or bit-stream copy) so that the imaging results will be the same as physical evidence. Imaging files saved with the extension .dd.

C. Analysis

1) GPS evidence extraction

In this study, it was found that the logs that contain GPS information data have the file extension DAT on aircraft storage and file with a .txt extension on the smartphone. Log data on storage UAV with DAT extension that contains GPS information stored in the directory /root/FLY019.DAT. Whereas the log results on a smartphone with a .txt extension stored in the directory /root/DJI/dji.pilot/FlightRecord/DJIFlightRecord_2016-08-29_[16-25-49].txt.

a) P-mode (Position)

In the log found on the aircraft analyzed by reading the file FLY019.log.txt outcome use of the DatCon application on file FLY019.DAT known flight mode, the location of the home point recorded, and the duration of the flight. For more detail can be seen in Figure 3.

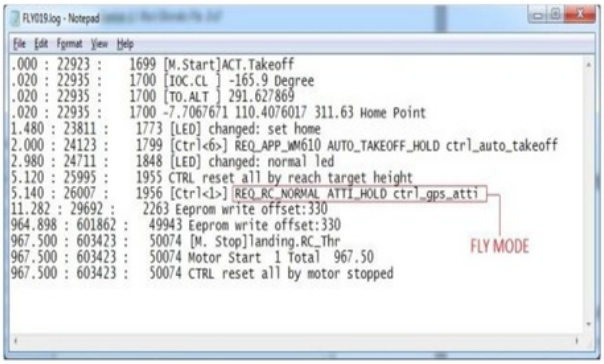

Figure 3 Results Event Log on File FLY019.DAT

In the logs found on the UAV's storage media can be seen the collection of coordinates and flight path conducted by uploading a log file FLY019.DAT to web applications based on https://www.mapsmadeeasy.com/log_viewer to get a list of coordinates to a .csv file. The examples of GPS log data can be seen in Table 1.

TABLE I SAMPLE COORDINATES GPS LOG RESULTS ON FILE FLY19.DAT

Longitude	Latitude	Altitude (m)
110.407602	-7.70676706	292.17404
110.407602	-7.70676696	291.9357
110.407603	-7.70676250	378.17572
110.407603	-7.70676783	400.34015
110.407602	-7.70676827	408.8675
110.407606	-7.70676712	387.056

b) A-mode (Attitude)

In the log found on the aircraft analyzed by reading the file FLY021.log.txt outcome use of the DatCon application on file FLY021.DAT known flight mode, the location of the home point recorded, and the duration of the flight. For more detail can be seen in Figure 4.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

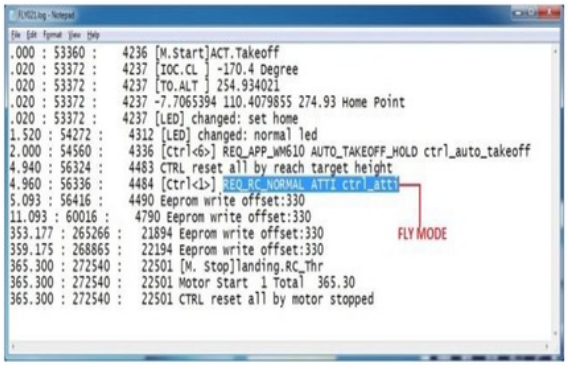

Figure 4 Results Event Log on File FLY021.DAT

For the flight path with this mode can still be found using the same process as before. This is by uploading a log file FLY021.DAT to web applications based on https://www.mapsmadeeasy.com/log_viewer address to get a list of coordinates to a .csv file. The examples of GPS log data can be seen in Table 2.

TABLE II SAMPLE COORDINATES GPS LOG RESULTS ON FILE FLY021.DAT

Longitude	Latitude	Altitude (m)
110.407974	-7.70653814	256.1733
110.407877	-7.70667488	280.66656
110.407814	-7.70676682	279.22858
110.407825	-7.70669853	281.3734
110.407841	-7.70661924	282.16977
110.407827	-7.70658926	282.1325

c) F-mode (Function)

For a flight path with this mode can still be found using the same process as before. That is by uploading a log file FLY022.DAT to web applications based on https://www.mapsmadeeasy.com/log_viewer address to get a list of coordinates to a .csv file. The examples of GPS log data can be seen in Table 3.

TABLE III SAMPLE COORDINATES GPS LOG RESULTS ON FILE FLY022.DAT

Longitude	Latitude	Altitude (m)
110.407070	-7.70664311	271.31238
110.407070	-7.70664396	277.22327
110.407069	-7.70664478	277.67554
110.407073	-7.70664458	286.21893
110.407111	-7.70661816	286.2421
110.407074	-7.70650167	283.9515

2) GPS evidence conversion

Further analysis done is to convert log files other than that contained in aircraft storage, camera memory cards, and smartphones. This method is done by reading the file containing metadata or GPS location information; the file may include images, video, and others. In this process, after the captured image files in the storage UAV, and smartphones are found. The file exported using FTK Imager application to read metadata therein by using the application PhotoMe. In detail, the information on file .dd GPS coordinates can be seen in Figure 5.

Figure 5 GPS Information on File Image

From the result of the conversion files from storage media both the drone and controller Investigators can strengthen the evidence obtained from the GPS information found in the case of crime in the use of drones.

D. Analysis Result

After going through the process of extraction and conversion of digital evidence the GPS, the next stage performed is present in the form of presentation. Digital forensic presentation in a series of activities carried out by forensic experts in demonstrating his findings in court to explain a case in assisting judges in making decisions. Presentation of GPS digital evidence for a different shape GPS presented visually using Google maps or applications that are relevant in presenting the coordinates of the location.

1) Data log on smartphone

This research presentation made by using the website address https://healthydrones.com/ to display flight information stored in log files DJIFlightRecord_2016-08-31_[17-00-34].txt contained in smartphones. For more details, flight information can be seen in Figure 6.

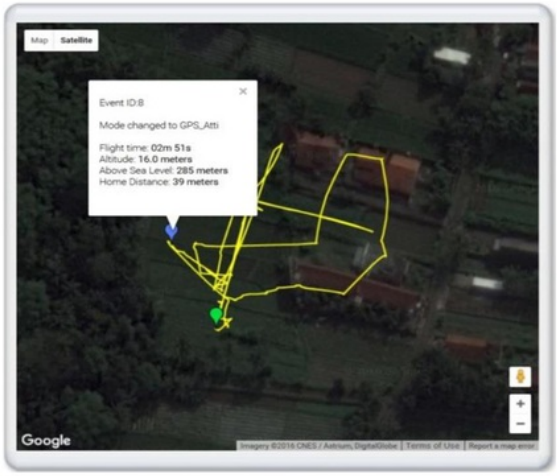

Figure 6 Presentation Log File DJIFlightRecord_2016-08-31_[17-00-34].txt

Presentation of the results can be known UAV flight path. In a green dot "F-mode" is executed and the function Follow me on UAV work, and on the blue dots altitude of 16 meters

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

and as much distance as 39 meters from the home point, the F-mode switched off and changed using P-mode.

2) Data log on UAV storage

To log file with the extension DAT contained in the storage UAV can use https://www.mapsmadeeasy.com/log_viewer site address in the presenting location, flight path, speed, altitude, and a wide range of useful information as evidence UAV. For more details log FLY021.DAT data presentation can be seen in Figure 7.

Figure 7 Presentation Log File FLY021.DAT

In the log data with the extension DAT, the information displayed are still not rich when compared with the information obtained from the log of the controller (smartphone) which is used to control the flight.

3) The result of image conversion on UAV

For GPS information, the presentation of the results of conversion image files taken by UAVs camera, use the Google Maps app. In Figure 8 can be seen results location of the coordinates contained in the metadata file org_a8ccc30f7ce0c44f_1472617871000.jpg

Figure 8 presentations of Information GPS Data File org_a8ccc30f7ce0c44f_1472617871000.jpg

Results of the presentations can be known location coordinates of -7.706890, 110.408255. The location of the pictures taken is in Sardonoharjo, Nganglik, Sleman Regency, and Special Region of Yogyakarta.

E. Characteristics of Digital Evidence

The characteristics of GPS digital evidence from the UAV is known in detail as follows:

Evidence of digital GPS is very susceptible to changes in migration; a little movement can influence the change point of latitude and longitude.

In the DJI Phantom 3 Advance, GPS coordinates and flight data information is always written into the log in aircraft storage and smartphone. Data will continue to be written and saved even used flight mode does not use GPS signals to aircraft stability.

On aircraft storage, flight log information is stored in the file with the extension DAT, while the flight log information on the controller is stored in the application folder DJI with a .txt extension.

At the camera's memory card found on the UAVs, GPS digital evidence that must be obtained through a process conversion of metadata from the pictures or video files contained therein. Digital evidence in storage is only in the form of latitude and longitude coordinates of the location at the time of an image or video was taken.

Digital evidence information obtained from a smartphone as a controller has a wealth of information that is more than the information obtained from the aircraft storage or a memory card in the camera UAVs.

As the result of analysis, a detailed comparison of the information obtained from the UAV storage, camera memory cards, and storage media within DJI applications on smartphones can be seen in Table 4.

TABLE IV COMPARISON OF DIGITAL EVIDENCE IN UAV

Digital Evidence Informations	Storage		
	UAV	Memory Card	Smartphone
Acquisition Method	Live	Static	Live / Static
Type of Image	Physical	Physical	Logical
Image Format	.dd	.dd	.ad1
Acquisition Tool	FTK Imager	FTK Imager	FTK Imager
GPS Location	√	√	√
Log coordinate flight path	√	-	√
UAV configuration information	√	-	√
Pictures/ Videos	-	√	√
Flight Mode Information	√	-	√
UAV user information	-	-	√
UAV flight data information	√	-	√
Directions shooting	-	-	√
UAV signal strength information	-	-	√
Information UAV sensor condition	-	-	√
UAV power condition information	√	-	√
Information condition UAV controller	-	-	√

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Information included in the storage controller (smartphone) has more potential as digital evidence. To obtain digital evidence UAV flight path can be found in the storage UAV and smartphones.

VI. Conclusion

Forensics on the UAV can be done by using a static method on a forensic acquisition UAV storage media devices. Except for aircraft storage can not use static methods forensics because the system is turned on in order to be accessible.

GPS data which could potentially be used as digital evidence is always stored in the system log UAV contained on aircraft storage, memory cards and smartphones. GPS data is always stored information even if the system uses UAV flight mode without using GPS. From this research, it has been known to the potential of the whole digital evidence contained information on the device UAV. Percentage of digital evidence found in the storage UAVs has 50% of the overall findings and on the memory cards has 16.6% of the overall findings.

While most digital evidence found to exist on the storage of smartphones used as UAV controllers. In the smartphone storage media found almost the whole information that can be obtained from the UAV.

References

[1] G. Horsman, "Unmanned aerial vehicles: A preliminary analysis of forensic challenges," *Digit. Investig.*, vol. 16, pp. 1–11, 2016.

[2] H. Shao, "Drone Overlord Frank Wang On DJI's Milestones, Miscarried GoPro Partnership & Corporate Espionage," *Forbes Asia*, 2015.

[3] A. Nishar, S. Richards, D. Breen, J. Robertson, and B. Breen, "Thermal infrared imaging of geothermal environments and by an unmanned aerial vehicle (UAV): A case study of the Wairakei – Tauhara geothermal field, Taupo, New Zealand," *Renew. Energy*, vol. 86, pp. 1256–1264, 2016.

[4] J. D. Barton, "Fundamentals of Small Unmanned Aircraft Flight," *Johns Hopkins Apl Tech. Dig.*, vol. 31, no. 2, pp. 132–149, 2012.

[5] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," *J. F. Robot.*, vol. 31, no. 4, pp. 617–636, 2014.

[6] A. Arbelet, "Garmin satnavs forensic methods and artifacts : An exploratory study School of Computing," no. August, 2014.

[7] Sukriadi and Y. Prayudi, "Analysis of Digital Evidence of Global Positioning System (GPS) On Android Smartphone," *Kns&I Stikom*, no. 11, 2014.

[8] D. Huang, "Evidential Problems with GPS Accuracy : Device Testing," 2013.

[9] J. Valdman, "Log File Analysis," 2001.

[10] A. Iswardani and I. Riadi, "Denial Of Service Log Analysis Using Density K-Means Method," vol. 83, no. 2, pp. 299–302, 2016.

[11] M. Zulfadhilah, "Cyber Profiling using Log Analysis and K-Means Clustering A Case Study Higher Education in Indonesia," vol. 7, no. 7, pp. 430–435, 2016.

[12] Y. Lou and W. Wang, "Map-Matching for Low-Sampling-Rate GPS Trajectories," no. c, 2009.

[13] M. A. Lukmana and H. Nurhadi, "Design of Unmanned Aerial Vehicle (UAV)," pp. 1–5.

[14] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks - An approach to the risk assessment," *Cyber Confl. (CyCon), 2013 5th Int. Conf.*, pp. 1–23, 2013.

[15] T. Jiang, J. Li, and K. Huang, "Longitudinal parameter identification of a small unmanned aerial vehicle based on modified particle swarm optimization," *Chinese J. Aeronaut.*, vol. 28, no. 3, pp. 865–873, 2015.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Forensic Analysis of Unmanned Aerial Vehicle to Obtain GPS Log Data as Digital Evidence

ORIGINALITY REPORT

4%

SIMILARITY INDEX

PRIMARY SOURCES

1	M.N. Noorhuzaimi. "An analysis of network services using association rules", 2009 2nd IEEE International Conference on Computer Science and Information Technology, 08/2009 Crossref	67 words — 2%
2	dl.djicdn.com Internet	51 words — 1%
3	www-kiv.zcu.cz Internet	39 words — 1%
4	www.scribd.com Internet	9 words — < 1%

EXCLUDE QUOTES OFF
EXCLUDE MATCHES OFF
EXCLUDE BIBLIOGRAPHY OFF