Jurnal Riset Teknologi Informasi dan Komputer (JURISTIK)
Vol. 2, No. 2, Des 2022, hlm. 18-25
DOI 10.53863/juristik.v2i2.585

p-ISSN: ....
e-ISSN: 2809-4972

Audio Forensics with the National Institute of Standards and Technology (NIST) Method using Formant and Bandwidth Statistical Analysis

Muhammad Fauzan Gustafi[1], Muhammad Immawan Aulia[2], Panggah Widiandana[3]
[1]Universitas Siber Muhammadiyah (Sistem Informasi, Fakultas Teknologi dan Ilmu Kesehatan)
[2,3]Institut Sains Teknologi dan Kesehatan Mulia Yogyakarta (Informatika)
[1]muhammadfauzangustafi@sibermu.ac.id*, [2]immawan16@istekmulia.ac.id,
[3]panggah.widiandana@istekmulia.ac.id

1. Abstract

Sound recording is one of the digital files that can be used as evidence in a cybercrime case trial. However, sound recordings are vulnerable to manipulation and are changed to hide information in the audio. Audio forensics is a science that analyzes the owner of the sound from the parameters of the pitch, formant, and spectrogram of an audio file. This research analyzes manipulated sound recordings to determine the ownership of audio recordings using formant statistical analysis and bandwidth using the National Institute of Standards and Technology (NIST). The research object used is the original file and the manipulated file, which has mp3 format. Retrieval of data on a smartphone using the live forensic method. The final result of the research succeeded in getting digital evidence on a smartphone with the Oxygen Forensic Suite 2014 application. The results of extracting the application were two audio files. The Analysis of Variance (ANOVA) analysis results can be concluded that nothing is identical because the F ratio value is smaller than F critical, and the probability P-value is more significant than 0.5. The Likehood Ratio (LR) analysis concluded that the sound recording of evidence with sound original limited evidence to against.

Keywords: Audio Forensics, Smartphone, National Institute of Standards and Technology (NIST), Analysis of Variance, Likehood Ratio

2. **Introduction** (10pt, tebal)

In this era of increasingly advanced technology, the digital world is getting closer to the lives of today's people. The ease of sharing information that can be text, audio, or video is getting easier. This is supported by advances in smartphone technology that can make communication more accessible in the digital era. This facility also has a harmful impact, such as crimes committed using digital devices, commonly called cybercrime. In digital crime, there are several cases such as illegal transactions, the spread of fake news, data manipulation, and bullying [1][2].

A message that uses text, voice, and video media is also a digital crime. Digital files in the form of audio can be in the form of a voice message, video recordings that have sound, or wiretapping recordings that have several extensions such as MP3, AAC, OGG, and WAV. With the convenience of today's technology, the audio file is also not safe from manipulation that can change the information in the audio. The ease of manipulation using computer or smartphone software can hide the identity of the owner of the voice by changing the pitch and timbre of the sound recording file [3].

A digital evidence presentation is needed for an authentication process and a correlation to the case in the court process. Evidence acquired by the investigator also requires protection and minimizes damage during the investigation process to maintain the authenticity of the evidence. One of the digital pieces of evidence that can be accepted in a court of law is a voice recording that uses a smartphone as a recording device [4]. Valid and identifiable evidence of the owner of the sound recording is required to solve problems in a court case.

Digital forensics is a science that aims to analyze the suitability or authenticity of a digital file. The analysis carried out on digital evidence in the form of multimedia files such as images, audio, and video is carried out to test the suitability or authenticity of the evidence [5]. Along with the times, digital forensic methods have had various types of methods to solve cybercrime problems; on the other hand, these methods are also used to prevent rife cyber-attacks in the technology world [6].

It uses the National Institute of Standards and Technology (NIST) scientific methods to collect, maintain, validate, analyze, document, and present digital evidence from digital sources. This method is carried out to facilitate or continue the reconstruction of events containing crimes by anticipating unauthorized actions that may interfere with the planned operations [7][8]. The method used is one with concise stages but does not leave essential points in an investigation. The use of NIST in the stages of the investigation process using computers or smartphones has four stages, namely Collection, Examination, Analysis, and Reporting. The tools used in this research are Oxygen Forensics Suite 2014 and Praat.

The increase in smartphone users has also led to an increase in cybercrime, so smartphone forensics is needed to overcome this problem [9][10][11]. One of live forensics is mobile forensics [12]. Live forensics is a science that takes data from a digital device while the device is still on [13]. Evidence obtained from a smartphone can be from call logs, contact numbers, messages, emails, audio files, internet history, and other evidence related to the investigated case [14]. Two methods can be used to extract data, namely logical or physical methods.

Audio forensics is a field of science that analyzes the data and information content of an audio file to determine the identity of the audio file [15][16]. One of the audio forensic analysis processes is to analyze the formant value and bandwidth by using the Praat application as a tool for investigation and strengthening evidence in court [17]. By analyzing the data with the parameters of pitch, formant, and spectrogram in the audio file, the identity of the owner of the sound recording can be known [18]. With the current development of audio forensics, the analysis can reduce the possibility of errors in concluding [19].

Formant statistical analysis and bandwidth have two types of analysis, namely analysis of variance and likelihood ratio analysis. Analysis of variance (ANOVA) is an analysis that uses formant values. Likelihood Ratio (LR) analysis is a supporting analysis of ANOVA using the specified hypothesis [20][21][22].

Previous studies used audio samples that were converted to pitch data [18]. Previous research on audio forensics used the Digital Forensics Research Workshop (DFRWS) forensic step and the spectrogram as a parameter [23]. Novelty in this research is voice recordings that have been manipulated with effects such as robotic voices where the recorded voice changes pitch in an irregular pattern. This research use forensic measures of the National Institute of Standards and Technology (NIST), which summarizes several steps of DFRWS and using formant and bandwidth as parameters. This study aims to find the best way to find out the identity of the owner of the sound in an audio file.

3. Metode Penelitian

3.1. Research Material

The research object in the research is two audio files. There are original and manipulated files. The original audio file is 15-seconds long with a file size of 125 KB. Meanwhile, the manipulated audio file is 14-seconds long with a file size of 111 KB. It is manipulated using a voice changer with robotic effects. Both files are in MP3 format, which is encoded in WAV format later. Then, the live forensics method is used to recover the data on a smartphone.

3.2. Research Flow

This study uses a digital forensic method proposed by a United States agency called NIST. The method is a science of measurement, standards, and security technology to help solve cybercrime problems in the jurisdiction. NIST has four stages: collection, examination, analysis, and reporting, as shown in Fig. 1. The first stage is the collection or identification of evidence used in the form of hardware from which the data will be taken to be used as digital evidence of a digital crime case. This process is carried out by following data integrity security measures. The second stage is collecting data on evidence using trusted forensic tools so that the data obtained has high integrity. The third stage is analyzing and re-evaluating the data found from the results of the examination. The last stage is reporting the analysis results, which includes data information that has been found, which is used as the final report of the forensic process carried out. the system flowchart process uses a flow and appearance that is adjusted to the design [24].

3.3. Research Material

The formant and bandwidth statistical analysis stage has two types of analysis: analysis of variance and analysis of likelihood ratio. Analysis of variance, abbreviated as ANOVA, calculates the values of formant 1, formant2, formant 3, and formant 4 from unknown and known voice recordings. The analysis obtained is then seen from the difference in the ratio F, F critical, and probability P values. It can be said that the unknown voice recording is identical to the known voice if the F ratio value is less than F critical and the P probability value is more significant than 0.5 [21].

The results of statistical analysis of formant and bandwidth using Likelihood Ratio (LR) analysis with equation (1).

$$\mathrm{LR} = \frac{\mathrm{p(E|H_p)}}{\mathrm{p(E|H_d)}} \quad (1)$$

$\mathrm{p(E|H_p)}$ is a hypothesis request (prosecution); known and unknown samples come from the same person obtained from the p-value ANOVA. $\mathrm{p(E|H_d)}$

is a defense hypothesis; known and unknown samples come from different people.

The value of the LR ratio with the verbal statement for the explanation of the LR value is described in Table 1 and Table 2.

Tabel 1. Demand Hypothesis

LR	LR(log)	Preference Weight (w)	Information
>10000	>4	Very strong evidence to support	Support the demand hypothesis $p(E\|H_p)$
1000-10000	3-4	Strong evidence to support	
100-1000	2-3	Moderately strong evidence to support	
10-100	1-2	Moderate evidence to support	
1-10	0-1	Limited evidence to support	

Tabel 2. Resistance Hypothesis

LR	LR(log)	Preference Weight (w)	Information
1-0.1	0-(-1)	Limited evidence to against	Support the demand hypothesis $p(E\|H_d)$
0.1-0.01	(-1)-(-2)	Moderate evidence to against	
0.01-0.001	(-2)-(-3)	Moderately strong evidence to against	
0.001-0.0001	(-3)-(-4)	Strong evidence to against	
<0.0001	>-4	Very strong evidence to against	

According to Tables 1 and 2, information to support the hypothesis of a significant demand for known and unknown voice values must be LR> 1; the more significant the LR value, the stronger the verbal statement [21].

4. Result and Discussion

4.1. Collection

The collection stage collects physical evidence, namely digital evidence in the form of smartphone devices needed to carry out the research process. This study uses one electronic evidence. Smartphones are evidence, as presented in Figure 1.

Gambar 1. Research Smartphone

The collection process will also record the specifications of the evidence used as a communication tool for drug sales transactions. The following are the specifications of the evidence used, as shown in Table 3.

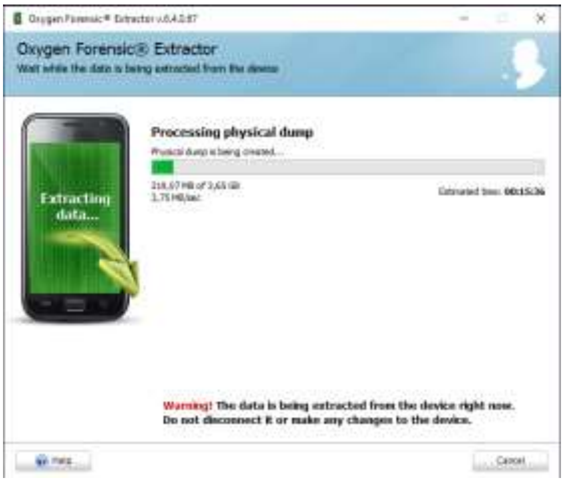
Tabel 3. Resistance Hypothesis

Type	Specifications
Brand	Samsung
Series	Galaxy
Model	Young
Model Number	SM-G130H
IMEI	352716071399351 / 00 352717071399359 / 00
OS	Android
Version	4.4.2 (KitKat)

4.2. Examination

The collection stage is the collection of data taken from digital evidence. The software used to carry out the data extraction process is Oxygen Forensic which can retrieve data directly from smartphones. The data retrieval process carried out on the application is shown in Figure 2. The result of this extraction process is an image file shown in Figure 3.

DOI: https://doi.org/10.53863/juristik.v2i2.585


Oxygen Forensic® Extractor v.6.4.0.87

Oxygen Forensic® Extractor

Wait while the data is being extracted from the device

Processing physical dump

Physical dump is being created...

218,67 MB of 3,65 GB

1,75 MB/sec

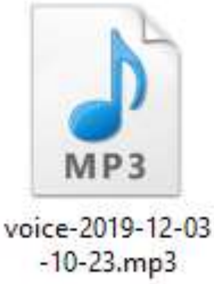
Estimated time: 00:15:36

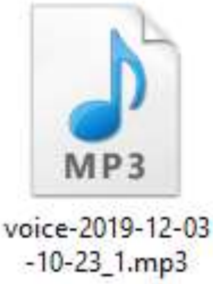
Warning! The data is being extracted from the device right now. Do not disconnect it or make any changes to the device.

Gambar 2. Smartphone Extraction Process

Gambar 3. Smartphone Extraction Result

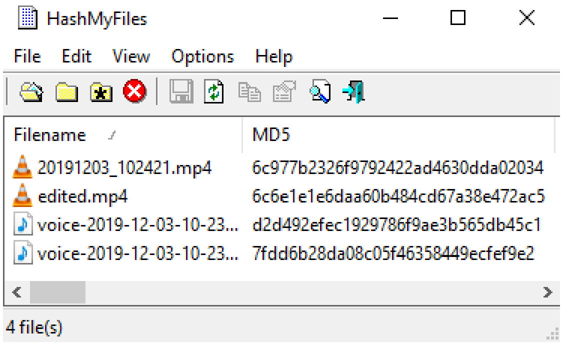
The resulting data retrieval is in the form of two audio files as evidence. The two data that were successfully obtained were then processed by hashing to determine the hash value in the file shown in Figure 4.


voice-2019-12-03-10-23.mp3


voice-2019-12-03-10-23_1.mp3

Gambar 4. Extraction Result

Extraction results that have been stored and then the hashing process is carried out to determine the hash value in the file shown in Figure 5.


HashMyFiles

Filename	MD5
20191203_102421.mp4	6c977b2326f9792422ad4630dda02034
edited.mp4	6c6e1e1e6daa60b484cd67a38e472ac5
voice-2019-12-03-10-23...	d2d492efec1929786f9ae3b565db45c1
voice-2019-12-03-10-23...	7fdd6b28da08c05f46358449ecfef9e2

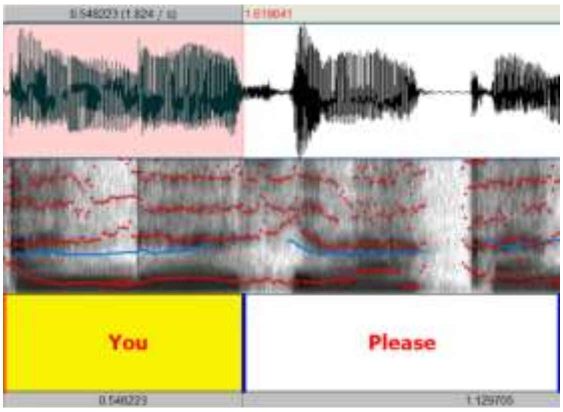
4 file(s)

Gambar 5. Hashing Process

The hash value obtained from the HashMyFile application is shown in Figure 6. The results of the hash on the original audio file (d2d492efec1929786f9ae3b565db45c1) and the edited audio file (7fdd6b28da08c05f46358449effef9e2). The results can be said that the original file and the fake file have changed or are different.

4.3. Analysis

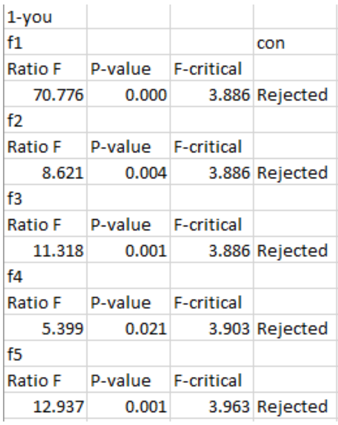
In the audio file that has been obtained, it is necessary to cut every word in the sound recording and then process it as data. The voice recording contains the words "You, please make a transfer of twenty million after that the ordered goods will be sent three days later after transfer.". Praat software is used to cut the recorded sound in each syllable, as shown in Figure 6.



Gambar 6. Dividing Audio Process

The formant and bandwidth statistical analysis method analyze the components in the sound recording, namely the formant and bandwidth values that compare the p-value statistics using one-way ANOVA, which will later be supported by the Likehood Ratio (LR) [25]. The use of the Gnumeric tool is carried out for this analysis using existing functions.

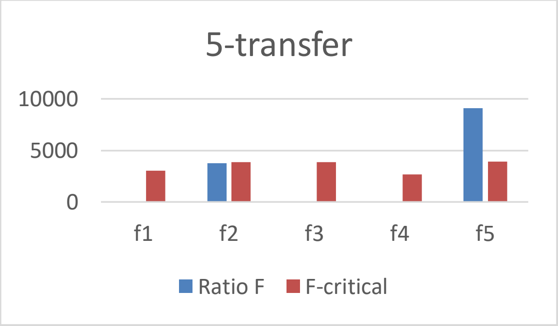
In ANOVA, the first stage is to get the formant value using the Praat application on each word; then, the data results are then processed using the Gnumeric application shown in Figure 7. The stipulation is that if the value of the F ratio is less than F critical and the probability value of P is greater than 0.5, it can be concluded that from the analysis of the known and unknown voices, it can be said to be accepted [21].



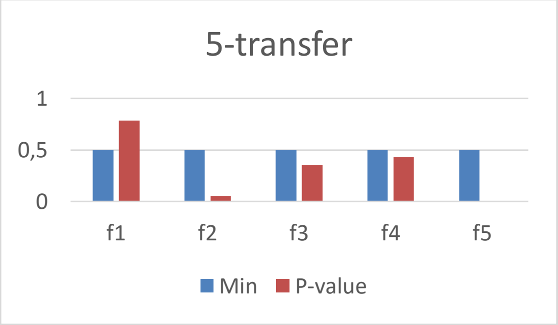
1-you			
f1			con
Ratio F	P-value	F-critical	
70.776	0.000	3.886	Rejected
f2			
Ratio F	P-value	F-critical	
8.621	0.004	3.886	Rejected
f3			
Ratio F	P-value	F-critical	
11.318	0.001	3.886	Rejected
f4			
Ratio F	P-value	F-critical	
5.399	0.021	3.903	Rejected
f5			
Ratio F	P-value	F-critical	
12.937	0.001	3.963	Rejected

Gambar 7. Calculation of ANOVA Results

The results of the ANOVA analysis concluded that the sound recording of the evidence with the original sound is not identical with a 100% percent because the value of the F ratio is smaller than the critical F and the probability value of P is greater than 0.5, which is shown in Figure 8 and Figure 9.



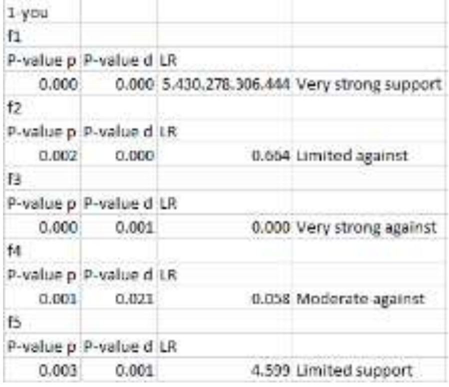
Gambar 8. The Difference between Ratio F and F-Critical



Gambar 9. P-Value with Minimum Limit

Figure 8 shows the difference between the F and F-critical ratio values, it is known that f1, f2, f3, and f4 are included in the identical vote criteria, but f5 shows the opposite; the F ratio value is greater than the F-critical value. Figure 9 shows the P-value with a minimum limit to prove that the votes are identical. The f1 value is included in the identical vote criteria because the P-value is greater than 0.5. In the final result of the analysis, the "5-transfer" sound sample is said to be not identical because only f1 can be accepted as a requirement for voice identification, while f2, f3, f4, and f5 do not qualify as identical.

The Likehood Ratio (LR) analysis is a supporting analysis of the statistical analysis of the formant and bandwidth of the ANOVA analysis with the demand hypothesis and the resistance hypothesis derived from the ANOVA analysis. If the LR value is > 1, it is known that the value is supported by the claimant's hypothesis; the greater the LR value, the stronger the verbal statement [21]. The calculation of the LR analysis can be seen in Figure 10.

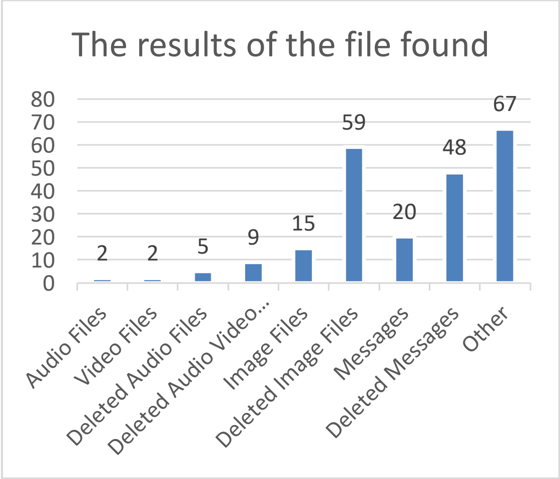


1 you			
f1			
P-value p	P-value d	LR	
0.000	0.000	5.430.278.306.444	Very strong support
f2			
P-value p	P-value d	LR	
0.002	0.000	0.664	Limited against
f3			
P-value p	P-value d	LR	
0.000	0.001	0.000	Very strong against
f4			
P-value p	P-value d	LR	
0.001	0.021	0.058	Moderate against
f5			
P-value p	P-value d	LR	
0.003	0.001	4.599	Limited support

Gambar 10. Calculation of ANOVA Results

4.4. Reporting

The final stage is the presentation stage done by redisplaying that information generated from the previous stage once obtained evidence from the inspection process. The Oxygen Forensic application can retrieve data from evidence in the form of a smartphone can be seen in Figure 11.



Gambar 11. The Difference between Ratio F and F-Critical

It is known that Oxygen Forensic is able to retrieve existing files and files that have been deleted. From Figure 9 above, Oxygen Forensic can retrieve 227 data in the form of two audio files, two video files, five deleted audio files, nine deleted video files, 15 image files, 59 deleted images, 20 message files 48 deleted message files, and 67 other files.

The final results of the voice sample ANOVA are shown in Table 4.

Tabel 4. ANOVA Results

Syllables	ANOVA
You	Unmatched
Please	Unmatched
Make a	Unmatched
Transfer	Unmatched
Of	Unmatched
Twenty	Unmatched
Million	Unmatched
After	Unmatched
That	Unmatched
The	Unmatched
Ordered	Unmatched
Goods	Unmatched
Will	Unmatched
Be	Unmatched
Sent	Unmatched
Three	Unmatched
Days	Unmatched
Later	Unmatched
After2	Unmatched
Transfer2	Unmatched

The results of the ANOVA analysis, as shown in Table 4, can be concluded that none of them are identical because the value of the F ratio is smaller than the critical F, and the probability value of P is greater than 0.5.

The results of the LR analysis concluded that the sound recording of the evidence with the original voice was limited evidence against the original voice in accordance with equation (1) and the hypothesis of Table 1 and Table 2. Table 5 is the result of the entire analysis.

Tabel 5. ANOVA Results

Syllables	ANOVA
You	Limited against
Please	Strong support
Make a	Moderate against
Transfer	Moderately strong against
Of	Moderate support
Twenty	Moderate against
Million	Moderate against
After	Moderately strong against
That	Limited against
The	Moderately strong support
Ordered	Moderate support
Goods	Moderate support
Will	Moderate against
Be	Strong against
Sent	Very strong against
Three	Strong against
Days	Strong against
Later	Moderately strong against
After2	Very strong support
Transfer2	Moderately strong support

Table 5 is the result of the Likehood Ratio analysis; it is concluded that the limited evidence against the original vote is taken from the average of the total existing likelihood ratio values.

5. Conclusion

Sound recording is one of the digital files that can be used in uncovering a case. However, a sound recording is a file that is very easy to manipulate to hide information in it. Forensic methods are needed for this matter of problems. NIST is one of the existing digital forensic methods. Using scientific methods based on collection, examination, analysis, and reporting originating from cybercrime cases.

Based on the results obtained, the study succeeded in obtaining two digital pieces of evidence in the form of audio files from a smartphone using the Oxygen Forensic Suite 2014 software. The hashing process was carried out on both files that were proven to be authentic. The process of statistical analysis of formant and bandwidth, which has two stages, namely ANOVA and LR, has shortcomings in this study. ANOVA concluded that most of the calculation results were rejected, as seen from the F ratio value greater than F critical and the probability P value less than 0.5. The results of the ANOVA analysis can be concluded that they are not identical. The results of the LR analysis concluded that the sound recording of the evidence with the original voice was limited evidence to against or limited evidence against the original voice in accordance with formula 2.1 and the hypothesis of Table 2.2. The points obtained are that formant and bandwidth analysis are not suitable for the case of sound recordings that have been manipulated with irregular pitch waves.

There is a suggestion for further research related to audio forensics. Future research can use other forensic methods in the forensics analysis, such as pitch statistical analysis, graphical distribution analysis, spectrogram analysis, Mel-frequency Cepstrum (MFCC), or the Itakura-Saito Distance method.

6. Daftar Pustaka

[1] A. P. Utama Siahaan, "Pelanggaran Cybercrime Dan Kekuatan Yurisdiksi Di Indonesia," *J. Tek. dan Inform.*, vol. 5, no. 1, pp. 6–9, 2018.

[2] W. Y. Sulistyo, I. Riadi, and A. Yudhana, "Penerapan Teknik SURF pada Forensik

Citra untuk Analisa Rekayasa Foto Digital," *JUITA J. Inform.*, vol. 8, no. 2, p. 179, 2020, doi: 10.30595/juita.v8i2.6602.

[3] H. Wu, Y. Wang, and J. Huang, "Identification of electronic disguised voices," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 3, pp. 489–500, 2014, doi: 10.1109/TIFS.2014.2301912.

[4] V. A. Hadoltikar, V. R. Ratnaparkhe, and R. Kumar, "Optimization of MFCC parameters for mobile phone recognition from audio recordings," *Proc. 3rd Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2019*, pp. 777–780, 2019, doi: 10.1109/ICECA.2019.8822177.

[5] R. Böhme, F. C. Freiling, T. Gloe, and M. Kirchner, "Multimedia forensics is not computer forensics," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5718 LNCS, pp. 90–103, 2009, doi: 10.1007/978-3-642-03521-0_9.

[6] A. C. K. Wardana, R. Pedrason, and T. B. Prasetyo, "Implementasi digital forensik brunei darussalam dalam membangun keamanan siber implementation of digital forensic brunei darussalam in building cyber security," *J. Prodi Perang Asimetris*, vol. 4, no. 1, pp. 1–22, 2018.

[7] I. Riadi, S. Sunardi, and Sahiruddin, "Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 30, pp. 1–8, 2020, doi: 10.25126/jtiik.202071921.

[8] Imam Riadi, Rusydi Umar, and M. I. Syahib, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 45–54, 2021, doi: 10.29207/resti.v5i1.2626.

[9] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic Tools Performance Analysis on Android-Based Blackberry Messenger using NIST Measurements," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.

[10] A. Al-Sabaawi and E. Foo, "A Comparison Study of Android Mobile Forensics for Retrieving Files System," *Int. J. Comput. Sci. Secur.*, no. 13, pp. 2019–148, 2019.

[11] A. Wirara, B. Hardiawan, and M. Salman, "Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan 'WhatsApp,'" *Teknoin*, vol. 26, no. 1, pp. 66–74, 2020, doi: 10.20885/teknoin.vol26.iss1.art7.

[12] R. Umar, A. Yudhana, and M. N. Faiz, "Experimental Analysis of Web Browser Sessions Using Live Forensics Method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 2951–2958, 2018, doi: 10.11591/ijece.v8i5.pp.2951-2958.

[13] W. Jansen and R. Ayers, "Guidelines on Cell Phone Forensics Recommendations of the National Institute of Standards and Technology," *Nist Spec. Publ.*, vol. 800, no. 101, pp. 1–104, 2007, doi: 10.6028/NIST.SP.800-124.

[14] I. Riadi, S. Sunardi, and P. Widiandana, "Investigasi Cyberbullying pada WhatsApp Menggunakan Digital Forensics," vol. 1, no. 10, pp. 730–735, 2020.

[15] R. R. Huizen, N. K. D. A. Jayanti, and D. P. Hostiadi, "Model Evaluasi Rekaman Percakapan Di Audio Forensik," pp. 133–140, 2017.

[16] A. G. Boyarov and I. S. Siparov, "Forensic Investigation of MP3 Audio Recordings," *Theory Pract. Forensic Sci.*, vol. 14, no. 4, pp. 125–136, 2020, doi: 10.30764//1819-2785-2019-14-4-125-136.

[17] E. Gural and M. Pazarc, "A supporting method to detect manipulated zones in digitally edited audio files," *Med. Sci. | Int. Med. J.*, p. 1, 2017, doi: 10.5455/medscience.2017.06.8699.

[18] V. R. C. Putri and Sunarmo, "Analisis Rekaman Suara Menggunakan Teknik Audio Forensik Untuk Keperluan Barang Bukti Digital," vol. 3, no. 1, pp. 7–13, 2014.

[19] S. Camacho, D. M. Ballesteros L, and D. Renza, "A cloud-oriented integrity verification system for audio forensics," *Comput. Electr. Eng.*, vol. 73, pp. 259–267, 2019, doi: 10.1016/j.compeleceng.2018.11.022.

[20] A. Subki, B. Sugiantoro, and Y. Prayudi, "Membandingkan Tingkat Kemiripan Rekaman Voice Changer Menggunakan Analisis Pitch, Formant dan Spectogram," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 1, p. 17, 2018, doi: 10.25126/jtiik.201851500.

[21] M. Al-Azhar Nuh, "Audio Forensic : Theory and Analysis," pp. 1–38, 2011.

[22] P. Rose, *Forensic Speaker Identification.* New York: cRc Press, 2002.

[23] Sunardi, I. Riadi, R. Umar, and M. F. Gustafi, "Audio Forensics on Smartphone with Digital Forensics Research Workshop (DFRWS) Method," *CommIT (Communication Inf. Technol.*, vol. 15, no. 1, pp. 41–47, 2021, doi: https://doi.org/10.21512/commit.v15i1.6739.

[24] A. Yudhana, A. Fadlil, and M. Rosidin, "Indonesian words error detection system using nazief adriani stemmer algorithm," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12,

pp. 219–225, 2019, doi: 10.14569/ijacsa.2019.0101231.

[25] B. S. Deva and I. Mardianto, "Teknik Audio Forensik Menggunakan Metode Analisis Formant Bandwidth, Pitch dan Analisis Likelihood Ratio," *Ultimatics*, vol. 10, no. 2. pp. 67–72, 2019. doi: 10.31937/ti.v10i2.936.