**SMARTICS Journal**, Vol.7 No. 1 2021. p7-13
ISSN online: 2476-9754, ISSN print: 2623-0429
DOI : https://doi.org/10.21067/smartics.v7i1.5026


# Laron v2: Pengembangan Aplikasi Forensik Logikal untuk Mengakusisi Percakapan Whatsapp di Android

**Dedy Hariyadi [a,*], Arif Akbarul Huda [b], Kharisma [c], Adri Priadana [d]**
[acd] Universitas Jenderal Achmad Yani Yogyakarta
[b] Universitas Amikom Yogyakarta
[*] correspondence email : dedy@unjaya.ac.id

***Abstract* — Digital forensics can define as an approach to disclosing facts of crime from evidence or electronically using scientific methods to enforce applicable laws. Currently, digital forensics is used as an instrument to uncover crimes or investigations. This influence by the increasing growth and use of information technology. Criminals have used information technology in a crime. Whatsapp, as a popular communication platform, is also used to commit crimes. So in this study, application development was carried out to secure evidence of conversation on Whatsapp. The developed application will release the public with a compatible license with the Free Open Source Software. The hope is that this application can support the process of evidence and investigation by the police with electronic evidence in the form of mobile devices.**

***Index Terms* — Laron, Whatsapp, Digital Forensics, Mobile Forensics, Open Source**

***Abstrak* — Forensik digital dapat diartikan sebagai pendekatan pengungkapan fakta-fakta tindak kejahatan dari barang bukti dan/atau elektronik menggunakan metode ilmiah untuk menegakan perundangan-undangan yang berlaku. Saat ini forensik digital digunakan sebagai instrumen untuk mengungkap tindak kejahatan atau investigasi. Hal ini dipengaruhi meningkatnya pertumbuhan dan penggunaan teknologi informasi. Pelaku tindak kejahatan telah memanfaatkan teknologi informasi pada suatu tindak kejahatan. Whatsapp sebagai platform komunikasi yang populer juga dimanfaatkan untuk melakukan tindak kejahatan. Maka pada penelitian ini dilakukan pengembangan aplikasi untuk melakukan pengamanan barang bukti percakapan pada Whatsapp. Aplikasi yang kembangkan akan dirilis ke publik dengan lisensi yang selaras dengan Free Open Source Software. Harapannya aplikasi ini dapat mendukung proses pembuktian dan investigasi oleh pihak kepolisian dengan barang bukti elektronik berupa perangkat gemerak (*mobile devices*).**

***Kata Kunci* — Laron, Whatsapp, Forensik Digital, Forensik Gemerak, Open Source**

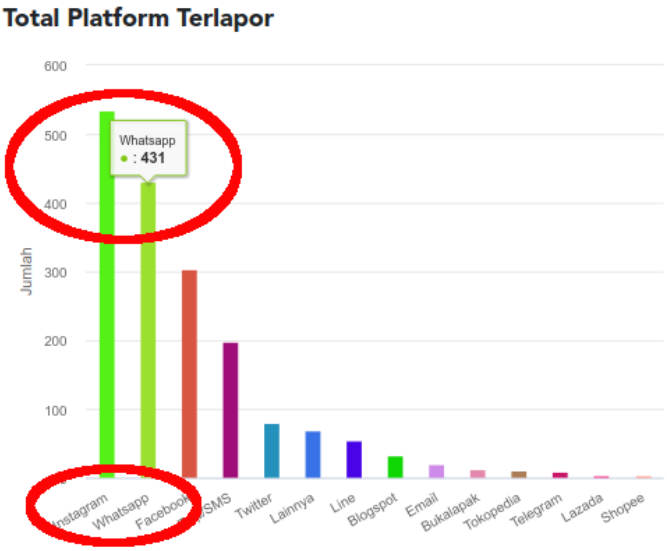
## I. PENDAHULUAN

Pertumbuhan pengguna internet di Indonesia dari tahun ke tahun selalu meningkat. Tercatat pada tahun 2016 pengguna internet di Indonesia persentasenya 51,7%, tahun 2017 54,7% , sedangkan tahun 2018 64,8% [1] [2] [3]. Bahkan penggunaan internet pada tahun 2018 didominasi dari perangkat gemerak (*mobile devices*) dalam hal ini ponsel cerdas sebesar 95,6% [4]. Pada prinsipnya sebuah teknologi bersifat netral tetapi pada kenyataanya memiliki dampak negatif yang perlu menjadi perhatian bersama. Berdasarkan statistik laporan yang masuk ke Direktorat Tindak Pidana Siber Badan Reserse Kriminal Kepolisian Negara Republik Indonesia tindak kejahatan yang menggunakan platform instant messaging terbanyak adalah Whatsapp dengan jumlah 431 aduan, seperti tampak pada gambar 1 [5].

Penanganan tindak kejahatan yang melibatkan perangkat gemerak (*mobile device)* seperti ponsel memerlukan tindakan khusus. Berdasarkan studi terkait perbandingan penanganan barang bukti elektronik dan/atau digital di Pusat Laboratorium Forensik Kepolisian Negara Republik Indonesia bahwa standar operasional prosedur penanganan barang bukti atau akuisisi ponsel dan sim card perlu penanganan secara khusus [6]. Sehingga dalam proses penangangan barang bukti elektronik berupa ponsel perlu hati-hati dan cermat serta memperhatikan kaidah-kaidah forensik yang berlaku pada SNI ISO/IEC 27037:2014 yang diterbitkan oleh Badan Standarisasi Nasional. SNI ini juga menjadi referensi pengembangan standar operasional standar penanganan barang bukti di Kementerian Komunikasi dan Informatika Republik Indonesia [7]. Pada standar ini dapat diterapkan di bidang forensik gemerak atau ponsel cerdas karena

Received November 11, 2020; Revised December 21, 2020; Accepted January 4, 2021

terdapat prosedur yang mengatur akuisis barang bukti digital dengan barang bukti elektronik dalam kondisi menyala [8].




**Gambar 1. Statistik Platform Terlapor Tahun 2019**

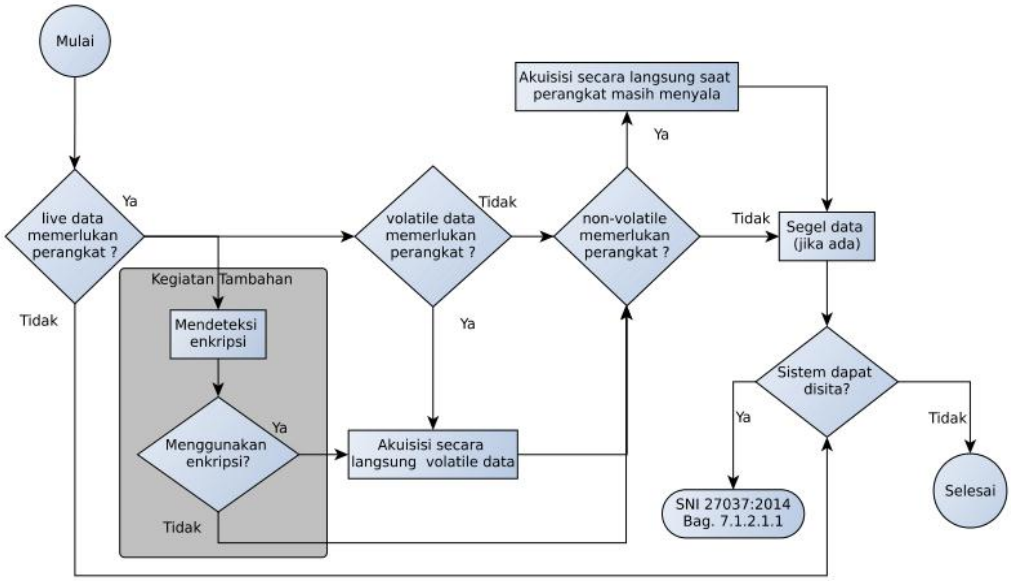
Penelitian sebelumnya terkait penanganan barang bukti digital pada ponsel cerdas pada Laron versi pertama belum membahas secara khusus tentang barang bukti digital berupa percakapan pada Whatsapp, walaupun telah mengikuti standarisasi SNI ISO/IEC 270237:2014. Pada penelitian tersebut fokus pada akusisi seluruh barang bukti berupa berkas basis data sqlite dari aplikasi yang terpasang pada ponsel cerdas bersistem operasi Android [8]. Pada perkembangannya Whatsapp yang terpasang pada fitur clone apps atau dual apps memiliki karakteristik sedikit berbeda dalam menyimpan berkas basis data sqlite [9]. Pada tulisan ini dikembangkan Laron versi dua yaitu aplikasi yang dapat melakukan akuisisi barang bukti digital khusus Whatsapp baik yang terpasang pada *single system* maupun *clone apps*.

## II. METODOLOGI PENELITIAN

Keilmuan forensik digital dalam perkembangan tidak hanya terkait komputer tetapi semua perangkat elektronik yang terdapat barang bukti digital yang berpotensial. Adapun cabang keilmuan forensik digital diantaranya: forensik komputer (*computer forensics*), forensik gemerak (*mobile forensics*), forensik audio (*audio forensics*), forensik video (*video forensics*), forensik citra (*image forensics*), forensik siber (*cyber forensics*), forensik memori (*memory forensics*), forensik jaringan (*network forensics*), forensik komputasi awan (*cloud forensics*), forensik malware (*malware forensics*), dan forensik sistem operasi (*OS forensics*) [10] [11]. Teknik mengamankan barang bukti digital dari barang bukti elektronik disebut akuisisi. Teknik Akuisisi pada ponsel cerdas diantaranya [12]:

1. Akuisisi Manual, teknik akuisisi yang dilakukan penyidik dengan melakukan kontak langsung dengan barang bukti elektronik karena kondisi tertentu. Pada teknik ini harus dilakukan proses perekaman saat melakukan kontak langsung dengan barang bukti elektronik.
2. Akuisisi Logikal, teknik akuisisi barang bukti digital pada partisi logikal selayaknya proses menyalin berkas yang mengedepankan prinsip dan etika forensik digital. Maka pada teknik barang bukti digital yang telah terhapus tidak dapat ditemukan.
3. Akuisisi Fisikal, teknik akuisisi ini biasa disebut *bit-by-bit copy* pada media penyimpan dari barang bukti elektronik. Istilah lain dari istilah teknik ini adalah kloning media penyimpanan. Tentu teknik tetap mengedepankan integritas dari barang bukti elektronik dan/atau digital.
4. Akuisisi *Chip-off*, teknik akuisisi yang perlu pengetahuan tentang elektronika karena mengambil barang bukti elektronik dari *printed circuit board* (PCB). Selanjutnya barang bukti tersebut dibaca menggunakan alat pembaca khusus.

Pada SNI ISO/IEC 27037:2104 juga telah mengatur prosedur akuisisi logikal yang dapat diterapkan pada akuisisi ponsel cerdas karena memerlukan ponsel cerdas dalam kondisi menyala. Walaupun data pada ponsel cerdas bersifat *non-volatile* tetapi untuk mengakuisisinya memerlukan perangkat sehingga dapat dilakukan akuisisi secara logikal, hal tersebut alur akuisisi dapat dilihat pada gambar 2 [13].



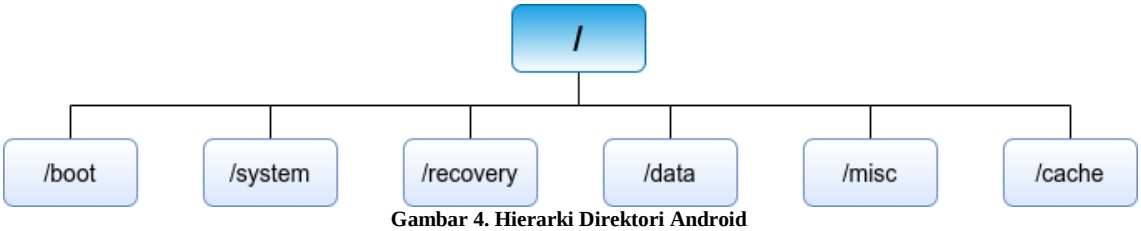

**Gambar 1. Prosedur Akuisisi Perangkat dalam Kondisi Menyala**


**Gambar 3. Alur Pengembangan Laron**

Maka pengembangan aplikasi forensik ini menyesuaikan dengan kebutuhan yaitu melakukan akuisisi barang bukti digital berupa percakapan Whatsapp dari aplikasi sebelumnya, yaitu Laron. Pengembangan sebelumnya aplikasi Laron telah disesuaikan dengan SNI ISO/IEC 27037:2014. Namun, terdapat perbedaan alur dengan aplikasi sebelumya yaitu prasyarat penggunaan aplikasi disebutkan diawal, terdapat pilihan menyimpan hasil kompresi menggunakan password, dan teknik pencarian spesifik ke obyek percakapan Whatsapp, seperti tampak pada gambar 3.

## III. HASIL DAN PEMBAHASAN

Pada manajemen penyimpanan ponsel cerdas bersistem operasi android terbagi menjadi beberapa partisi diantaranya: /boot, /system, /recovery, /data, /misc, dan /cache. Aplikasi yang terinstall pada sistem operasi Android tersimpan pada partisi /data. Begitu pula data pengguna yang terkait aplikasi juga tersimpan pada /data. Gambar gambar 4 merupakan hierarki dari sistem operasi Android [14]. Maka pada pengembangan Laron fokus pencarian barang bukti digital pada direktori /data.




**Gambar 4. Hierarki Direktori Android**

Pencarian barang bukti digital percakapan Whatsapp sesuai yang diteliti oleh Cosimo Anglano seperti tampak pada Table 1 [15]. Hasil dari penelitian tersebut dituangkan dalam pengembangan Laron sebagai aplikasi yang berfungsi melakukan akuisisi barang bukti percakapan Whatsapp.

**Table 1. Barang Bukti Digital Whatsapp**

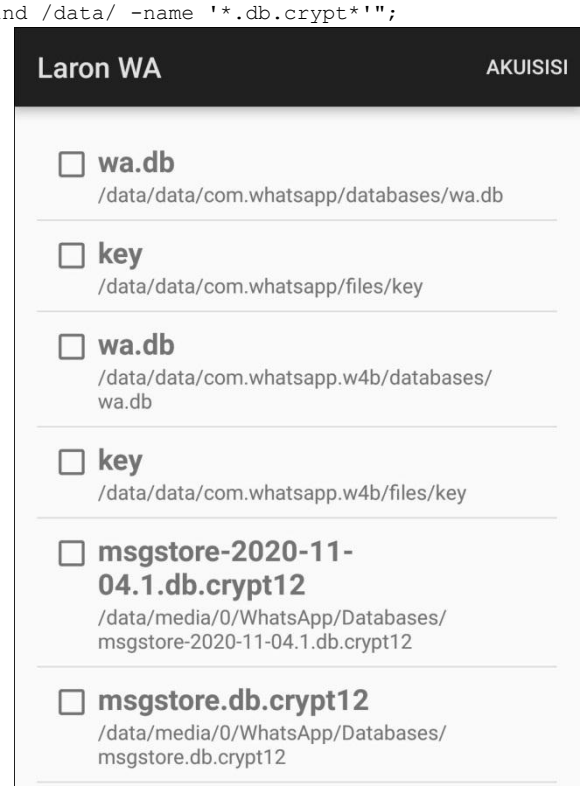
| *Tipe Whatsapp* | *Konten* | *Direktori* | *Berkas* |
|---|---|---|---|
| Whatsapp Orisinal | Basis data kontak | /data/data/com.whatsapp/databases | wa.db |
| Whatsapp Orisinal | Basis data percakapan | /data/data/com.whatsapp/databases | msgstore.db |
| Whatsapp Orisinal | Cadangan basis data percakapan | /storage/emulated/0/Whatsapp/Databases | msgstore.db.crypt12 msgstore-<tanggal>.crypt12 |
| Whatsapp Orisinal | Kunci enkripsi | /data/data/com.whatsapp/files | key |
| Whatsapp Business | Basis data kontak | /data/data/com.whatsapp.w4b/databases | wa.db |
| Whatsapp Business | Basis data percakapan | /data/data/com.whatsapp.w4b/databases | msgstore.db |
| Whatsapp Business | Cadangan basis data percakapan | /storage/emulated/0/Whatsapp/Databases | msgstore.db.crypt12 msgstore-<tanggal>.crypt12 |
| Whatsapp Business | Kunci enkripsi | /data/data/com.whatsapp.w4b/files | key |
| Whatsapp Dual Apps | Basis data kontak | /data/user/999/com.whatsapp/databases | wa.db |
| Whatsapp Dual Apps | Basis data percakapan | /data/user/999/com.whatsapp/databases | msgstore.db |
| Whatsapp Dual Apps | Cadangan basis data percakapan | /storage/emulated/999/Whatsapp/Databases | msgstore.db.crypt12 msgstore-<tanggal>.crypt12 |
| Whatsapp Dual Apps | Kunci enkripsi | /data/user/999/com.whatsapp/files | key |

Untuk mendapatkan barang bukti digital berupa wa.db, key, dan msgstore.db memerlukan akses *root* pada ponsel Android. Sedangkan untuk mendapatkan barang bukti digital berupa msgstore-<tanggal>.crypt12 lebih mudah karena tanpa akses *root*. Namun, untuk membukanya memerlukan kunci berupa berkas key. Oleh sebab itu pada pengembangan aplikasi Laron versi 2 ini memerlukan akses *root*. Adapun kode dalam bahasa Java untuk mendeteksi ponsel Android yang telah ter-*root* seperti dibawah ini.

```
if(RootTools.isRootAvailable()){
    if (RootTools.isBusyboxAvailable()) {
        searchDatabase();
    } else {
        showDialogInstalBusyBox();
         }
}else{
    showDialogDeviceNeedRootAccess()
}
```

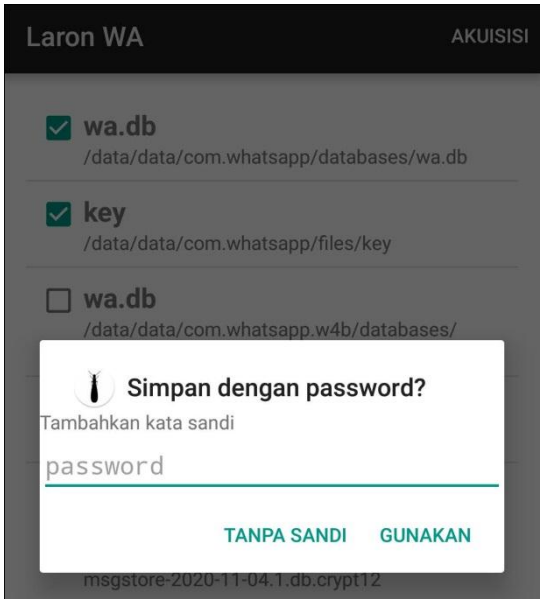
Dengan ponsel Android dalam kondisi ter-*root* maka akan mempermudah proses pencarian. Dalam proses pencarian memerlukan modul BusyBox yang membutuhkan kondisi ponsel Android harus dalam kondisi ter-*root*. Artinya kondisi ponsel Android ter-*root* merupakan syarat mutlak. Penggunaan modul BusyBox dalam proses pencarian dapat dilihat pada kode dibawah ini. Hasil dari pencarian barang bukti digital ditunjukan pada gambar 5.

```
String cmd="busybox find /data/data/com.whatsapp -type f -name 'wa.db' && " +
        "busybox find /data/data/com.whatsapp -name key &&"+
        "busybox find /data/data/com.whatsapp.w4b -type f -name 'wa.db' && " +
        "busybox find /data/data/com.whatsapp.w4b -name key &&"+
        "busybox find /data/ -name '*.db.crypt*'";
```




**Gambar 5. Hasil Pencarian Barang Bukti Digital**

Akuisisi atau proses pengamanan barang bukti digital tersebut dikompres menggunakan format .zip. Proses kompresi yang dapat diproteksi menggunakan password ataupun tidak. Tujuan dikompresi merupakan upaya menjaga keutuhan barang bukti digital sesuai dengan SNI ISO/IEC 27037:2014 ataupun standarisasi forensik lainnya. Adapun tampilan pilihan proteksi kompresi menggunakan password seperti pada gambar 6.




**Gambar 6. Proteksi Proses Akuisisi**

## IV. KESIMPULAN

Aplikasi Laron versi 2 atau Laron WA ini lebih efektif dibandingkan versi sebelumnya dalam proses pencarian barang bukti digital. Hal ini disebabkan pencarian berfokus pada barang bukti digital percakapan Whatsapp saja. Saat ini Laron WA hanya dapat digunakan pada ponsel cerdas bersistem operasi Android. Aplikasi Laron baik versi 1 atau versi 2 dapat dikategorikan sebagai aplikasi forensik digital yang berbasis agen [16]. Walaupun berbasis agen aplikasi Laron dapat membantu Kepolisian dalam proses investigasi dan pembuktian suatu tindak kejahatan dengan barang bukti elektronik ponsel cerdas.

Kelemahan aplikasi berbasis agen ini diantaranya memerlukan akses *root*. Begitu pula pada aplikasi Laron versi 1 atau versi 2. Kelemahan ini harapannya dapat diperbaiki pada penelitian selanjutnya dengan fitur yang lebih disempurnakan.

## REFERENSI

[1] Asosiasi Penyelenggara Jasa Internet Indonesia, "Penetrasi dan Perilaku Pengguna Internet Indonesia 2016," Jakarta, 2017.

[2] Asosiasi Penyelenggara Jasa Internet Indonesia and Teknopreneur Indonesia, "Penetrasi & Perilaku Pengguna Internet Indonesia - Survey 2017," Jakarta, 2018.

[3] Asosiasi Penyelenggara Jasa Internet Indonesia, "Penetrasi dan Perilaku Pengguna Internet Indonesia 2018," Jakarta, 2019.

[4] D. Hariyadi, M. R. Jinan, N. S. Bayuaji, and A. S. Hasan, "Analisis Jaringan pada Aplikasi Pengamanan Akses Internet," *Cybersecurity dan Forensik Digit.*, vol. 2, no. 1, pp. 16–23, 2019.

[5] Direktorat Tindak Pidana Siber Badan Reserse Kriminal Kepolisian Negara Republik Indonesia, "Statistik Laporan Polisi 2019," 2020. https://patrolisiber.id/statistic (accessed Jan. 08, 2020).

[6] D. Hariyadi, "Komparasi Penangangan Barang Bukti Elektronik dan/atau Barang Bukti Digital sesuai SOP Pusat Laboratorium Forensik Polisi Republik Indonesia." pp. 1–5, 2014.

[7] S. Kurniawan, "Perancangan Prosedur Operasional Standar Penanganan Alat Bukti Digital: Studi Kasus Kementerian Komunikasi dan Informatika," Universitas Indonesia, 2014.

[8] D. Hariyadi and A. A. Huda, "Laron: Aplikasi Akuisisi Berbasis SNI 27037:2014 pada Ponsel Android," *Indonesia Security Conference 2015*. Cirebon, pp. 1–10, 2015, doi: 10.13140/RG.2.1.3819.9520.

[9] I. Y. Pasa and D. Hariyadi, "Identifikasi Barang Bukti Percakapan Aplikasi Dual Apps Whatsapp Pada Ponsel Xiaomi Menggunakan Metode NIST Mobile Forensics," *J. INTEK Univ. Muhammadiyah Purworejo*, vol. 1, pp. 1–7, 2018, [Online]. Available: http://ejournal.umpwr.ac.id/index.php/intek/article/view/4815/4641.

[10] M. N. Al-Azhar, *Digital Forensic: Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek, 2012.

[11] S. Dogan and E. Akbal, "Analysis of Mobile Phones in Digital Forensics," *2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2017 - Proc.*, pp. 1241–1244, 2017, doi: 10.23919/MIPRO.2017.7973613.

[12] K. A. Alghafli, A. Jones, and T. A. Martin, "Forensics data acquisition methods for mobile phones," *2012 Int. Conf. Internet Technol. Secur. Trans. ICITST 2012*, pp. 265–269, 2012.

[13] Badan Standarisasi Nasional, "Teknologi Informasi - Teknik Keamanan-Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital (SNI ISO/IEC 27037:2014)," Jakarta, 2014.

[14] N. L. Htun, M. Mie, and S. Thwin, "Proposed Workable Process Flow with Analysis Framework for Android Forensics in Cyber-Crime Investigation," *Int. J. Eng. Sci.*, vol. 6, no. 1, pp. 82–92, 2017.

[15] C. Anglano, "Forensic analysis of WhatsApp Messenger on Android smartphones," *Digit. Investig. J.*, vol. 11, no. 3, pp. 201–213, Sep. 2014, doi: 10.1016/j.diin.2014.04.003.

[16] M. P. Aji, D. Hariyadi, and T. Rochmadi, "Logical Acquisition in the Forensic Investigation Process of Android Smartphones based on Agent using Open Source Software," in *IOP Conference Series: Materials Science and Engineering*, Mar. 2020, vol. 771, p. 012024, doi: 10.1088/1757-899X/771/1/012024.

**Dedy Hariyadi**, Meraih gelar sarjana teknik (S.T) dari Universitas Pembangunan Nasional Veteran Yogyakarta pada tahun 2004. Kemudian meraih gelar Master (M.Kom) dari Universitas Islam Indonesia pada tahun 2016. Saat ini Penulis menjadi dosen program studi Teknologi Informasi di Universitas Jenderal Achmad Yani Yogyakarta.

Arif Akbarul Huda, Meraih gelar sarjana (S.Si) dari Universitas Gadjah Mada pada tahun 2011. Kemudian meraih gelar Master (M.Eng) dari Universitas Gadjah Mada pada tahun 2015. Saat ini Penulis menjadi dosen program studi Informatika di Universitas Amikom Yogyakarta.