JINTEKS (Jurnal Informatika Teknologi dan Sains) ISSN 2686-3359 (Online)
Vol. 5 No. 1, Februari 2023, hlm. 81 – 85

# ANALISIS PENCARIAN DATA *SMARTPHONE* MENGGUNAKAN NIST UNTUK PENYELIDIKAN DIGITAL FORENSIK

**Riya Majalista[1*], Tata Sutabri[2]**
[1,2]Magister Teknik Informatika, Universitas Bina Darma
*email:* riyamajalista@gmail.com*

**Abstrak:** Tujuan dari penelitian ini adalah untuk menganalisis informasi agar dapat digunakan sebagai dasar ilmu forensik dalam membantu penyelesaian kasus kejahatan dunia maya. Penelitian ini membantu penyelidikan digital forensik dengan menganalisis data –data yang hialng dari *smartphone.* Data –data *smartphone* yang dicari diharapkan menjadi bukti suatu tindakan kejahatan yang terjadi di dunia maya. Data yang dominan digunakan adalah data yang tersimpan di aplikasi *WhatsApp* baik kontak, percakapan, gambar/ foto dan yang lainnya. Analisis Pencarian data pada penelitian ini menggunakan metode *National Institute of Standards and Technology (NIST).* Penelitian ini mempelajari dan melaporkan Analisis Forensik pesan instan yaitu jalur. Sistem Android. Selanjutnya, Informasi berdasarkan data-data yang telah dianalisis akan dijadikan dasar pengembangan tindak kejahatan dunia maya. Hasil analisis yang dilaporkan, meliputi uraian tentang kejadian yang terjadi, alat teknis yang digunakan, ada tidaknya prosedur, instruksi, prosedur, peralatan dan lain-lain. Bukti fisik pada penyelidikan digital forensik ini berupa *smartphone*. *Cybercrime* merupakan aktivas yang jelas meskipun terjadi di dunia maya. Jika tindakan *cybercrime* tidak ditindak lanjuti dengan tegas, maka akan semakin banyak yang dirugikan. Dengan adanya hukum tertulis yang jelas , diharapkan mampu menekan angka *cybercrime*. Namun demikian, penyelidikan digital forensik sangat dibutuhkan dalam upaya pembuktian kejahatan *cybercrime*. Maka tentunya diperlukan penelitian-penelitian terkait untuk membantu penyelidikan digital forensik.

**Kata Kunci :** NIST, digital forensik, *cybercrime*

***Abstract:*** *The purpose of this study is to analyze information so that it can be used as a basis for forensic science to assist in solving cybercrime cases. This study helps with digital forensics investigations by analyzing lost smartphone data. The data sought from the smartphone must be evidence of a crime committed in cyberspace. The main data used is the data stored in the WhatsApp application, including contacts, chats, pictures/pictures and others. Analysis Data retrieval for this study used methods from the National Institute of Standards and Technology (NIST). This study investigates and reports forensic analysis of instant messages, i.e. paths. Android system. In addition, the information based on the analyzed data will be the basis for the development of cybercrime. The results of the analysis are reported, including a description of the events that occurred, the technical tools used, whether there are procedures, instructions, procedures, equipment, and others. . The physical evidence in this digital forensic investigation comes in the form of a smartphone. Cybercrime is an overt activity even when it occurs in cyberspace. If cybercriminals are not actively monitored, more and more people using the digital world will be harmed. With a clearly written law, it is hoped that it will be able to reduce the number of cybercrimes. However, digital forensic investigations are essential to prove cybercrime. So, of course, relevant research is needed to support digital forensics investigations.*

***Keywords*** **:** *NIST, digital forensic, cybercrime*

## PENDAHULUAN

Di era global ini, berbicara tentang kejahatan siber tentunya tidak dapat dipisahkan dari masalah keamanan jaringan atau keamanan informasi internet, apalagi jika terkait dengan masalah informasi sebagai komoditas. Informasi sebagai komoditas membutuhkan kehandalan pelayanan agar apa yang diberikan tidak mengecewakan pelanggannya. *Cybercrime* ini terjadi bersamaan dengan pesatnya perkembangan teknologi informasi.

Informasi data yang diperoleh dari perusahaan *cyber security Surfshark*, sebanyak 1,04 juta akun membocorkan data pada kuartal kedua tahun 2022. Kebocoran data internet Indonesia kuartal kedua tahun 2022 bahkan melonjak 143% dari kuartal pertama tahun 2022.

Informasi di Internet, menurut Badan Siber dan Kriptografi Nasional (BSSN), lebih dari 700 juta serangan *cybercrime* yang terjadi di Indonesia pada tahun 2022. Serangan yang paling sering terjadi adalah ransomware atau malware dengan modus tebusan. Jumlah total kejahatan pada tahun 2022 adalah 714.170.967 dalam bentuk anomali trafik atau serangan dunia maya, dengan puncaknya pada bulan Januari sebanyak 272.962.734, terhitung lebih dari sepertiga dari semua serangan pada paruh pertama tahun2022.

Sepanjang tahun 2022, terdapat kejahatan dunia maya kejahatan dunia maya lainnya, yaitu serangan korupsi online atau metode peretasan yang mengubah konten situs web, seperti B. mengubah font, tata letak (*1ayout)*, menampilkan iklan, dan bahkan mengubah konten umum secara keseluruhan. Peretasan ini juga dapat berupa pencurian data-data penting lainnya yang tentunya merugikan masyarakat di dunia maya.

Bukti yang didapat oleh penyidik biasanya berupa ponse1 yang sudah tidak ada *simcard* dan nomor tersangka dari kebanyakan kasus yang ditangani. Disinilah peran mobile forensik diharapkan dapat membantu memberikan bukti digital yang nantinya dipakai dalam menyelesaikan kasus kriminal yaitu dengan cara menganalisis data yang ada di ponsel.

 ISSN 2686-3359 (Online)

Sejak Januari 2019, ada lebih dari 130 juta pengguna WhatsApp di Indonesia. WhatsApp digunakan sebagai alat komunikasi yang paraktis bagi masyarakat Indonesia. Tidak jarang pengguna WhatsApp menyimpan data- data penting milik pribadi maupun instansi tempat mereka bekerja. Sayangnya, banyak kasus kriminal yang saat ini dominan menggunkan akun WhatsApp sebagai media kejahatan dunia maya, mulai dari percakapan WhatsApp, gambar, rekaman video dan lainnya yang dijadikan barang bukti. Kajian studi ini adalah pencarian data smartphone pada apilakasi whatsApp akibat serangan malware yang merugikan pihak pribadi bahkan instansi yang menggunakan akun WhatsApp sebagai media komunikasi.

Berdasarkan penjelasan permasalahan di atas, diperlukan suatu teknologi yang dapat mencari dan menemukan data agar dapat membatu penyelidikan digital forensik. Sehingga data yangditemukan kembali dapat dijadikan bukti untuk menangani kasus Cyber Crime.

## TINJAUAN PUSTAKA

Menurut Ntantogia dkk. (2014), mobile forensik digital atau mobile forensics adalah cabang dari forensik digital yang merujuk pada pemulihan bukti digital atau data dari perangkat mobile dengan kondisi forensik yang baik. Terdapat tantangan-tantangan dan kesulitan untuk mendapatkan bukti digital di perangkat seluler. Menurut Sai, dkk (2015) adalah perbedaan hardware mobile phone, fitur keamanan, kurangnya sumber daya, seperti kabe1 USB, baterai, dan charger untuk perangkat mobile yang berbeda, teknik anti-forensik, bukti yang dinamis atau dengan mudah berubah, adanya proses reset secara tidak sengaja, perubahan perangkat, pemulihan passcode, dan program malicious.

Proses Digital Forensik Menurut NIST SP 800-86 (2006) proses tahapan dalam digital forensik dibagi menjadi empat tahapan. Tahapan- tahapan tersebut ada1ah sebagai berikut.1.Collection, merupakan tahapan pertama dalam proses digital forensik yang bertujuan untuk mengidentifikasi sumber data yang potensial dan mengakuisisi datanya. 2.Examination, merupakan tahapan pemeriksaandata –data yang termasuk didalamnya adalah peni1aian dan pengga1ian informasi dari data yang telah dikumpulkan sebelumnya. 3.Analysis, adalah proses ana1isis dari data yang dapat mengidentifikasi orang, tempat, item, dan peristiwa yag terkait sehingga dapat diambil kesimpulan. 4.Report, adalah proses da1am mempersiapkan dan mempresentasikan informasi yang dihasi1kan dari fase ana1isis. Secara khusus a1ur proses untuk mobi1e forensik sendiri menurut Jones dan Winster (2017) terdiri atas seizure, acquisition, examination/analysis, dan report generating. Seizurebertujuan untuk menjaga barang bukti, acquisition bertujuan untuk mengambi1 data dari perangkat, examination/analysis merupakan proses pemeriksaan dan analisis dari data, dan report generating merupakan pelaporan hasil / informasi dalam bentuk non-technical.

Forensik mobi1e merupakan ilmu yang berawal dari Digital Forensics atau lebih dikenal dengan Computer Forensics. Menurut Riadi dkk. (2018) Forensik digita1 adalah metode ilmiah yang membahas bagaimana bukti digital dari sumber digital disimpan, dikumpulkan, divalidasi, dianalisis, ditafsirkan, didokumentasikan, dan disajikan untuk memfasilitasi rekonstruksi peristiwa kriminal atau untuk membantu memprediksi tindakan yang terbukti melanggar aturan yang telah ditentukan.

Sebuah buku berjudul Sistem Keamanan Komputer mendefinisikan forensik komputer sebagai i1mu penanganan inte1ijen dalam bentuk bukti digital setelah insiden terkait keamanan komputer terjadi. Investigasi forensik berdasarkan forensik digital meliputi penemuan artefak dan pemeriksaan materia1 (data) yang ada pada perangkat digital (komputer, ponsel, tablet, PDA, perangkat jaringan, media penyimpanan dan sejenisnya). Menurut Brown, DeHayes, Hoffer, dan Perkins definisi teknologi informasi merupakan kombinasi teknologi komputer yang terdiri dari perangkat keras dan perangkat lunak yang digunakan untuk mengolah dan menyimpan informasi teknologi komunikas yang kemudian mendistribusikan informasi. Berdasarkan buku Professional Computer Ethics mendefinisikan bahwa Cyber Crime adalah salah satu dampak negatif dari perkembangan teknologi yang menyebabkan kerugian yang banyak pada kehidupan modern saat ini.

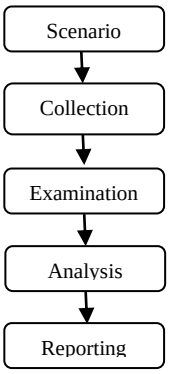
Berdasarkan analisis forensik digital aplikasi Telegram pada *smartphone* berbasis Android. Dalam penelitiannya, penelitian ini melakukan penghilangan bukti digital dari aplikasi Telegram menggunakan MOBILedit Forensic Tool 7.0 dan metode Mobile Forensic yang dikembangkan oleh National Institute of Standards and Technology (NIST).

## METODE

Penelitian ini menggunakan Metode National Institute of Standards and Technology (NIST). Tahapan dalam metode National Institute of Standards and Technology (NIST) di bawah ini adalah sebagai berikut: 1) Collection (Pengumpulan data yang dilakukan adalah mengumpulkan bukti-bukti dengan proses identifikasi, pengumpulan, pengembalian dan pencatatan bukti. 2) Pemeriksaan (Data Acquisition) adalah hasil pengumpulan alat bukti diuji sehingga tidak terjadi adanya perubahan

 ISSN 2686-3359 (Online)

keterangan alat bukti. 3) Analisis Pada tahap yaitu dilakukan pemeriksaan bukti-bukti sehingga mendapatkan bukti-bukti yang berkaitan dengan perkara tersebut. 4) Pelaporan (Reporting) yaitu Pelaporan hasil penyidikan yang didapat dari penyidikan yang memuat hasil analisis barang bukti sehingga barang bukti tersebut membantu proses penyidikan untuk menemukan tersangka.




**Gambar 1. Research Method**

Metode penelitian ini dilakukan dengan menginstal ap1ikasi WhatsApp yang terdapat di ponsel. Ponsel yang digunakan dalam penelitian ini tidak di-root/jailbreak. Proses root adalah proses mendapatkan hak istimewa yang tinggi dalam sistem operasi sehingga dapat melakukan hampir semua hal seperti: B. Menghapus sistem file, mematikan proses atau menjalankan perintah tertentu (Nguyen-vudkk, 2017). Proses jailbreaking adalah proses yang memungkinkan pengguna untuk menginstal dan menjalankan aplikasi yang tidak diotorisasi oleh Apple (Ovens and Morison, 2016). Kemudian perankan skenario percakapan yang telah disiapkan. Setelah menjalankan skenario, alat forensik digunakan untuk mencegat dan menguraikan pesan. Kemudian, data yang berhasil diekstraksi akan dianalisis.

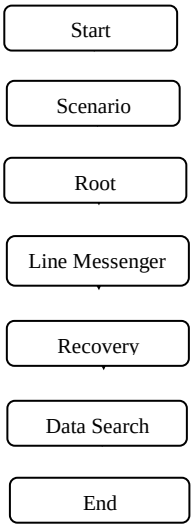
Dalam studi ini dilakukan skenario. Skenario dilakukan untuk memudahkan penyidikan kasus cybercrime malware pada aplikasi whatsApp. Skenario yang dilakukan adalah sebagai berikut :1. Pelaku membuat akun WhatsApp (Akun Pelaku) 2. Selanjutnya pelaku mencari akun-akun whatsApp yang akan dituju 3. pelaku mengirimkan pesan ke akun korban 4. Akun Pelaku mengirimkan pesan yang isi konten tersebut berupa malware sehingga membuat data di akun WhatsApss hilang hanya tinggal akun korban dan pelaku 5. Setelah itu pelaku mengirim kembali percakapan yang berisi meminta imbalan jika data-data di akun korban ingin dipulihkan. 6. percakapan selesai, pelaku menghapus semua data percakapan .

## HASIL DAN PEMBAHASAN

Aplikasi pemulihan digunakan untuk mendapatkan bukti forensik diperlukan, karena forensik WhatsApp Messenger berfokus pada file terkirim dan konten pesan. Aplikasi pemulihan bekerja dengan cara mengemba1ikan kembali data messenger WhatsApp yang dihapus, selanjutnya menganalisis database messenger WhatsApp yang diperoleh dengan DB Browser untuk SQLite

### Proses

1. Penelitian forensik dijalankan sesuai dengan skenario / rancangan yang telah dibuat.
2. Perangkat android yang digunakan sudah melalui proses root.
3. Informasi yang dimasukkan di Line Messenger hanya digunakan untuk tujuan simulasi.
4. Data pada Line messenger dihapus, kemudian dilakukan recovery untuk memulihkan data sebelum mencari bukti data forensik
5. Penelitian ini berfokus pada pencarian informasi forensik dari aplikasi Line Messenger pada platform mobile Android



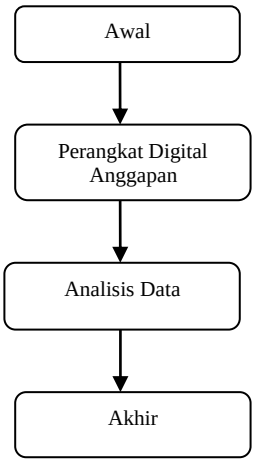

**Gambar 2. Metode Skenario Proses**

### Pencarian Data

Pengolahan data meliputi berbagai kegiatan seperti: pemeriksaan (veryfying), perbandingan (comparing), pemilihan (sorfing), peringkasan (extracfing), dan penggunaan (manipulafing). Pemeriksaan data meliputi pemeriksaan data yang muncul diberbagai daftar yang berkaitan atau yang didapat dari berbagai sumber, untuk mengetahui berbagai sumber dan guna mengetahui perbedaan atau ketidaksesuaian, hal ini dilakukan dengan kegiatan pemeliharaan file (file maintenance)
Metode yang digunakan dalam pencarian data adalah metode forensik digital dengan asumsi perangkat digital digunakan sebagai alat untuk melakukan tindak pidana.

 ISSN 2686-3359 (Online)

Metode forensic digital yang berfokus pada penanganan dan analisis data yang telah diperoleh




**Gambar 3. Metode Skenario Pencarian Data**

### Analisis

Analisis forensik aplikasi perpesanan instan Android terenkripsi. Tujuan penelitian ini adalah menganalisis ruang penyimpanan aplikasi pesan instan yang sering dipakai di perangkat Android. Penelitian dilakukan pada ponsel Android yang menjalankan beberapa versi OS Android. Alat yang digunakan pada penelitian ini yaitu Universal ADB Driver, WhatsApp KeyDB Extractor, WhatsApp Viewer dan SQLiteSpy, Analisis forensik LINE Messenger di Android. Dalam penelitian ini menggunakan virtual machine dengan default instalasi Windows OS 10. Aplikasi BlueStacks terinstall di Windows 10. Kemudian BlueStacks kita root. BlueStacks App Player dirancang untuk menjalankan aplikasi Android di PC Windows dan Macintosh. Penelitian ini menunjukkan bahwa penggunaan baris untuk Android dapat meninggalkan materi berdasarkan fakta bahwa itu sangat berguna dalam memori yang mudah menguap dan memori yang tidak mudah menguap. Dalam penelitian ini, mempelajari dan melaporkan Analisis Forensik pesan instan yaitu jalur Sistem Android.

### Reporting

Setelah dari analisis selesai, selanjutnya tahap pelaporan, yaitu tahap terakhir dari metode NIST, hasil analisis dilaporkan, meliputi uraian tentang kejadian yang terjadi, alat teknis yang digunakan, ada tidaknya prosedur, instruksi, prosedur, peralatan dan lain-lain. aspek investigasi tahap Pelaporan di sini dalam penelitian. Bukti fisik pada penelitian ini yaitu *smartphone* berbasis Android dengan tampilan digital berupa profil pengguna, kontak, emai1, chat dan foto terdapat pada seluruh 75% data *smartphone*. Karena keterbatasan biaya uji coba, penelitian ini menggunakan BlueStacks untuk meniru sistem OS Android. Imp1ementasi dapat bervariasi antara pengembang akhir yang berbeda.

## KESIMPULAN DAN SARAN

Meskipun aktivitas dunia maya bersifat virtual, namun bisa diklasifikasikan sebagai suatu perbuatan dan tindakan hukum nyata. Dari sisi hukum, dalam pengertian dunia maya, tidak tepat lagi untuk mengklasifikasikan sesuatu sebagai objek dan fungsi menurut penjelasan konvensional/moral untuk digunakan.

Aktivitas siber merupakan aktivitas virtual yang dampaknya nyata, walaupun buktinya berupa elektronik. Oleh karena itu, target pelaku haruslah orang yang benar-benar melakukan pelanggaran hukum.

Berdasarkan kasus yang disimulasikan, ada dua aspek hukum yang harus diperhatikan, yang pertama adalah kejahatan malware menurut hukum positif Indonesia yaitu Pasal 34 UU ITE, digunakan untuk menyalahgunakan perangkat keras atau perangkat lunak. Untuk kasus kedua, yaitu hilangnya barang bukti, berlaku Pasal 282 KUHP.

Dengan menggunakan metode dalam, penelitian ini, dapat disimpu1kan bahwa data dapat dicari berdasarkan asumsi data dan analisis data, sehingga data dapat ditemukan dalam sistem meskipun data tersebut dihapus atau disembunyikan. Analisis pencarian data pada smartphone ini dapat dijadikan bahan pendukung untuk penyelidikan digital forensik, bahkan dapat menjadi bukti dari kejahatan yang terjadi di dunia maya.

Masih perlunya dilakukan penelitian-penelitian terkait. Karna masih banyak tindakan *cybercrime* yang masih dianggap bias. Penelitian ini juga dapat dilakukan kembali dengan menggunakan metode digital foreksik lainnya.

## DAFTAR PUSTAKA

[1] A. Wirara, B. Hardiawan and M. Salman, 2020, *Identifikasi Bukti Digita1 pada Akuisisi Perangkat Mobile dari Ap1ikasi Pesan Instan "WhatsApp",* Jurnal Teknoin, 26(1), 66-74, https://journal.uii.ac.id/jurnal-teknoin/article/view/15549/pdf

[2] Sutabri, Tata, 2012, *Konsep Sistem Informas*, Andi, Yogyakarta.

[3] Nasirudin, Sunardi, Riadi I, 2020, *Ana1isis Forensik Smartphone Android Menggunakan Metode NIST dan Too1 MOBILedit Forensic Express*, Jurnal Informatika Universitas Pamulang, ISSN, 5(1), 89-94, https://core.ac.uk/download/pdf/337610185.pdf

[4] Aisyah, Nuru1., Putra Syah, Arman., Valentino, V.H., Prasetyo, B.S., Susanti, Daru., Nurhayati, Zikriah., 2022, *Ana1isa Perkembangan Digita1 Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic*, Jurnal Esensi Infokom, 6(1), 22-27, https://ibn.e-journal.id/index.php/KOMPUTASI/article/view/452/351

*[5]* Kurniawan, T.A., Putra, A.S., Aisyah Nurul, 2022, *Ana1ysis Search Data Using The National Institute*

 ISSN 2686-3359 (Online)

*Of Standard And Techno1ogy (Nist) Method On Cybercrime*, Bajang Jornal, ISSN, 1(12), 1767-1774, https://bajangjournal.com/index.php/JIRK/article/view/2231

[6] Nafila, F.L., Prayudi, Yudi., 2022, *Analisis Digital Artifak Ap1ikasi Signal Messenger Pada Sistem Operasi Android dengan metode NIST*, J-SAKTI, ISSN, 6(1), 532-543, http://www.tunasbangsa.ac.id/ejurnal/index.php/jsakti/article/view/466/443

[7] Yuliana, Dina., Yuniati, Trihastuti., Zen, B.P., A, Iqsyahiro Kresna., 2022, *Ana1isis Bukti Digital Cyberbullying Pada Media Sosia1 Menggunakan Metode Nationa1 Institut Of Standard And Technology (Nist) 800-101 (Studi Kasus : Instagram Dan Whatsapp)*, Journal Informatic and Information Technology, ISSN, 1(3), 113-123, https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=NALISIS+BUKTI+DIGITAL+CYBERBULLYING+PADA+MEDIA+SOSIAL+MENGGUNAKAN+METODE+NATIONAL+INSTITUT+OF+STANDARD+AND+TECHNOLOGY+%28NIST%29+800-101+%28Studi+Kasus+%3A+Instagram+dan+WhatsApp%29&btnG=

[8] Kusumadewa, Bramesta, Rendi., 2022, *Analisis Perbandingan Bukti Digita1 Forensik Pada Instant Messaging Berbasis Smartphone Android Menggunakan Framework Nist*, UMM Institutional Repository , https://eprints.umm.ac.id/87624/

[9] P. K. Dhamarsa, Safrizal, . S. P. Arman and Suyanto, 2019, *Perancangan Aplikasi ITBU Career Center Berbasis Website Menggunakan PHP dan MYSQL*, TEKINFO UPI YAI, https://journals.upi-yai.ac.id/index.php/TEKINFO/article/download/1765/1465

[10] P. Sukamto, A. S. Putra, N. Aisyah and R. Toufiq, 2022, *Forensic Digital Ana1ysis for CCTV Video Recording*, International Journal of Science, Technology & Management, 3 (1), 284-291

[11] Sutabri, Tata., 2013, *Komputer dan Masyarakat*, *Andi*, Yogyakarta.

[12] Wahyudi, Erfan., Zulpahmi,M., Gunawan, Karya.,Imran bahtiar., 2020, Analisis Bukti Digital Whatsapp Pada Android Smartphone Menggunakan Metode Live Forensic, EXPLORE, 10(2), https://utmmataram.ac.id/ojs/index.php/explore/article/download/428/pdf

*[13]* Zaenuddin, Imam,. Simorangkir. Y.N., Putra, A.S., 2022, *National Institute Of Standards And Technology (Ninst) Method For Cyber Crime Using Forensic Data On Smartphone*, *IJISTECH*, ISSN, 6(1), 145-151, *https://ijistech.org/ijistech/index.php/ijistech/article/view/222*