TECHNO
Vol.23, No.1, April 2022, Hal. 39~46
P-ISSN: 1410-8607, E-ISSN: 2579-9096

ANALISIS INVESTIGASI CYBER ESPIONAGE PADA FACEBOOK MENGGUNAKAN DIGITAL FORENSICS RESEARCH WORKSHOP (DFRWS)

Joko Triyanto[1], Sunardi[2], Imam Riadi[3]
[1]Program Studi Magister Teknik Informatika, Universitas Ahmad dahlan
[2]Program Studi Teknik Elektro, Universitas Ahmad dahlan
[3]Program Studi Sistem Informasi, Universitas Ahmad dahlan

Informasi Makalah

Dikirim,21 November 2020
Direvisi,20 September 2021
Diterima, 08 Oktober 2021

Kata Kunci*:*

Cyber espionage
DFRWS
Forensics
Facebook

INTISARI

Media sosial sangat bermanfaat untuk mendapatkan informasi atau data dengan mudah dan cepat seiring dengan peningkatan jumlah pengguna *smartphone* terutama pada Android. Di sisi lain, *mobile instant messangging aplications* dan sosial media membuat prospek adanya tindak kejahatan dunia maya atau *Cybercrime* khususnya *cyber espionage* yaitu tindakan mata-mata terhadap data elektronik atau memanfaatkan jaringan internet. Penelitian ini diharapkan dapat membuka barang bukti digital pelaku *cyber espionage* yang ada di aplikasi Facebook berupa gambar dan teks untuk mendukung identifikasi aktivitas yang menuju pada *cyber espionage*. Kerangka kerja untuk menjalankan *digital forensics* pada pengkajian ini menggunakan metode *Digital Forensics Research Workshop (DFRWS)* dengan tahapan *identification* (identifikasi), *Preservation* (Pemeliharaan) *Collection* (Pengumpulan), *Examination* (Pemeriksaan), *Analysis* (Analisis), Presentation (Presentasi) . *Tools* yang digunakan adalah *MobilEdit* dengan cara kerja ektraksi dan analisis. Skenario yang dilakukan adalah kasus *cyber espionage* pada facebook. Harapan dari penelitian ini adalah menghasilkan *Forensis Investigative analysis* pada Facebook memakai metode DFRWS mampu mengungkap *cyber espionage* pada aplikasi Facebook.

Keyword*:*

Cyber espionage
DFRWS
Forensics
Facebook

ABSTRACT

Social media is very useful to get information or data easily and quickly along with the increasing number of smartphone users, especially on Android. On the other hand, mobile instant messaging applications and social media create the prospect of cybercrime, especially cyber espionage, which is spying on electronic data or utilizing the internet network. This research is expected to open digital evidence of cyber espionage actors in the Facebook application in the form of images and text to support the identification of activities that lead to cyber espionage. The framework for carrying out digital forensics in this study uses the Digital Forensics Research Workshop (DFRWS) method with the stages of identification , Preservation, Colecction, Examinaation , Analysis , Presentation. The tools used are MobilEdit by means of extraction and analysis. The scenario is the cyber espionage case on Facebook. The hope of this research is to produce a Forensis Investigative analysis on Facebook using the DFRWS method to reveal cyber espionage on the Facebook application.

Korespondensi Penulis:

Joko Triyanto
Program Studi Magister Teknik Informatika
Universitas Ahmad Dahlan
Jl. Prof. Dr. Soepomo,SH. Umbul harjo, Janturan, Yogyakarta 55164
Email: jokotriyanto19@gmail.com

1. PENDAHULUAN

Jumlah pemakai yang paham *digital savy* atau media digital di Indonesia selalu mengalami perkembangan. Hingga saat ini angka konsumen internet yang menggunakan piranti *mobile* terhitung besar yaitu sampai 171 juta manusia. Kurang lebih 60 juta diantaranya merupakan usia produktif yang menggantikan lebih dari setengah penduduk pemakai internet di Negara Indonesia. Badan hukum pemasaran digital Assosiasi pemasaran seluler/ *Mobile Marketing Association* (MMA) mempublikasikan informasi terkait ekosistem pengguna seluler di negara Indonesia pada tahun 2019. Kurun waktu beberapa tahun kedepan, Negara Indonesia diprediksi akan menjadi negeri pengguna *smartphone* paling besar ketiga dunia atas kalkulasi konsumen hingga 410 juta jiwa pada tahun 2025 mengikuti Cina sebanyak 1,4 miliar serta India sebanyak 930 juta selaku tiga negeri terbesar pasar *smartphone* menurut dunia [1].

Penggunaan *smartphone* semakin meningkat terutama pada *Android*. Di sisi lain, aplikasi *mobile instant messaging* membuka peluang untuk meningkatnya tindakan *cybercrime* atau kejahatan siber. *Cybercrime* muncul seiring dengan perkembangan teknologi informasi yang begitu cepat. Salah satu jenis *cybercrime* adalah *cyber espionage* yaitu *espionase* yang memanfaatkan teknologi informasi berupa internet sebagai medianya [2]. Pidana internet/komputer adalah tindakan kriminal yang bukti kegiatan kriminalnya butuh diselidiki agar menjadi bahan data [3].

Cyber espionage berasal dari kata *cyber* dan *espionage*. *Cyber* artinya adalah internet atau dunia maya, sedangkan *espionage* artinya spionase atau tindakan mata-mata, sehingga *cyber espionage* adalah tindak pidana mata-mata terhadap data elektronik atau kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer [4]. Kasus *cyber espionage* perlu diteliti atau diidentifikasi dengan melakukan analisis forensik. Beberapa *tools* yang dapat digunakan untuk mendapatkan bukti digital diantaranya *KAMAS lite, OXYGEN Forensik, Cellebrite UFED,* dan *MOBILedit Forensic Express*. Selain *tools,* diperlukan juga metode forensik yang tepat untuk penanganan kasus *cyber espionage*.

Kerangka kerja yang dapat digunakan dalam proses pengambilan barang bukti digital diantaranya adalah *Integrated Digital Forensics Identification Framework* (IDFIF), *National Institute of Standards and Technology* (NIST), *National Institute of Justice (NIJ),* dan *Digital Forensics Research Workshop* (DFRWS). Masing-masing metode memiliki proses dan langkah kerja yang berbeda. Penelitian ini menggunakan metode DFRWS sebagai kerangka kerja untuk membantu investigator dalam melakukan *digital forensics.* DFRWS digunakan agar memperoleh atau mendapatkan bukti menurut keilmuan terhadap perawatan, validasi analisis, pengumpulan, identifikasi, dokumentasi, interpretasi, dan presentasi barang bukti digital yang bersumber dari sumber-sumber digital untuk melanjutkan atau memfasilitasi rekontruksi kasus didapatkannya kriminalitas, dan mendukung mengantisipasi perbuatan yang tidak sah mengindikasikan adanya proses yang diagendakan untuk menggangu [5]. Pengangkatan data dapat menggunakan *tool* yang sering digunakan dalam investigasi yaitu *Oxygen Forensik*. *Oxygen Forensik* mengekstrak sebagian besar informasi dengan cara yang efisien [6].

Teknologi informasi dan komunikasi di era globalisasi saat ini telah mengalami perkembangan yang sedemikian pesat. Hal tersebut disertai akibat bertambahnya pemakaian *social media* guna memperoleh data mudah dan cepat. Media sosial merupakan salah satu media yang berkembang paling pesat [7]. Para pengguna lebih gampang berperan serta, membagikan, dan membuat konten berupa wiki, sosial media, blog, dunia virtual dan forum. Akibat baik *social media* diantaranya bisa menjadi inovasi perkembangan pembelajaran pada pendidikan dasar di Indonesia [8], terkait masyarakat dan negara ialah mengeratkan hubungan silaturahim antara satu sama lain [9], memudahkan masyarakat agar berkomunikasi dengan orang banyak, memperbanyak pertemanan, waktu dan jarak sudah bukan masalah, mengekpresikan diri lebih mudah, penyiaran berita bisa lebih cepat, murah biayanya. Tetapi akibat buruk *social media* ialah menurunnya tatap muka, orang-orang yang sudah dekat semakin jauh, internet yang membuat kecanduan banyak orang, semakin meningkatnya konflik dan masalah, mudah mengikuti perilaku buruk orang, dan menyebarnya privasi [10].

Aplikasi pesan instant seluler paling populer di konsumen ialah WhatsApp(WA) (97,24%), LINE (88,49), BBM (85,82%), Facebook (77,26%), dan Telegram (0,75%) [11]. Perkembangan ini memberikan kemudahan dalam kehidupan manusia. Namun terdapat hal-hal yang harus diperhatikan dalam pemanfaatannya, yaitu penyalahgunaan hak-hak atas privasi seperti tindakan spionase. Dalam praktiknya, tindakan spionase dilakukan dengan cara yang dianggap ilegal oleh masyarakat, seperti melakukan penyadapan informasi dan pencurian data pribadi. Belakangan hal ini mendapatkan perhatian khusus oleh masyarakat internasional [12]. Penelitian ini memilih objek aplikasi pada Facebook (FB), dikarenakan FB termasuk aplikasi yang digunakan banyak masyarakat yaitu sebesar 77,26%, dan bermaksud untuk menganalisa metode

penyelidikan perkara *cyber espionage* serta menampilkan barang keterangan atau bukti *cyber espionage* yang telah terjadi pada FB.

2. METODOLOGI

Objek riset ialah sebuah sifat dari manusia, objek atau aktivitas yang memiliki ragam tertentu yang dipermanenkan oleh pengkaji atau peneliti untuk dipahami dan selanjutnya di tarik kesimpulannya [13]. Objek pada riset atau penelitian ini yaitu data dari aplikasi Facebook pada perangkat *smartphone* android khususnya pada fitur Facebook *messenger*. Parameter bukti potensial dari DFRWS digunakan untuk mengukur kemampuan masing-masing alat forensik yang digunakan dalam penelitian. Parameter pengukuran disesuaikan dengan simulasi kasus, yaitu bukti potensial terkait *cyber espionage*, yaitu identifikasi pengguna, pesan multimedia, pesan teks, *timestamp*, dan aplikasi.

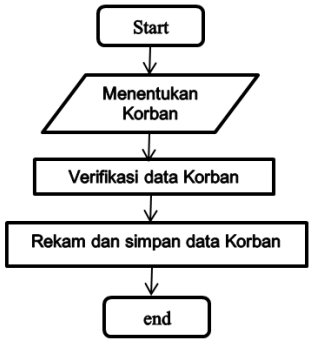
Alat dan bahan yang di butuhkan dalam *digital forensic investigation* ini bisa dilihat pada tabel 2.1.

Tabel 2.1 Alat dan bahan

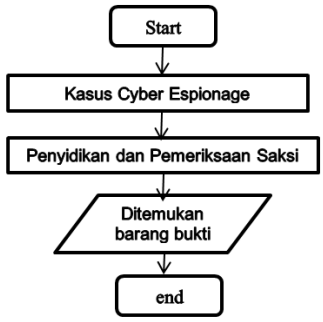
No	Alat dan bahan	Spesifikasi / Deskripsi	Keterangan
1	Sebuah unit Laptop	Merk Acer, dual boot Windows 10	Perangkat Keras
2	Satu unit Smartphone	Merk Vivo Y9, Tipe N1816,Terinstal Facebook	Perangkat Keras
3	*KINGRoot*	Aplikasi yang dipergunakan untuk melakukan *rooting smartphone Android*	Perangkat Lunak
4	MobilEdit	Aplikasi ini dipergunakan untuk mengangkat barang bukti berupa data pada *smartphone*	Perangkat Lunak

2.1. Perancangan Sistem

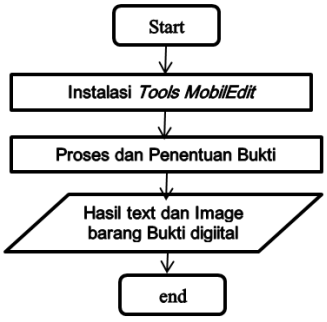
Perancangan sistem pada penelitian ini merupakan kerangka kerja (*framework*) berupa rancangan simulasi kasus, rancangan identifikasi, rancangan akuisisi, rancangan eksaminasi dan rancangan pelaporan bukti digital. Rancangan dibuat *flowchart* secara sistematis sesuai *DFRWS* yang disesuaikan dengan perangkat media *tool* seperti dapat dilihat pada Gambar 2.1 s.d Gambar 2.5.



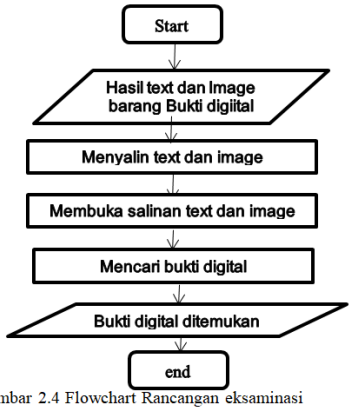
Gambar 2.1 Flowchart Rancangan Simulasi Kasus



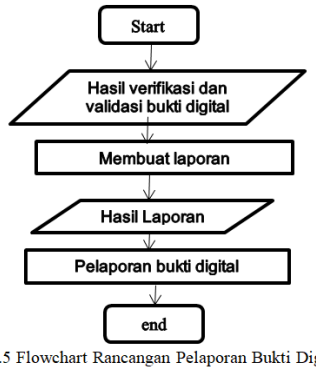
Gambar 2.2 Flowchart Rancangan identifikasi



Gambar 2.3 Flowchart Rancangan akuisisi



Gambar 2.4 Flowchart Rancangan eksaminasi



Gambar 2.5 Flowchart Rancangan Pelaporan Bukti Digital

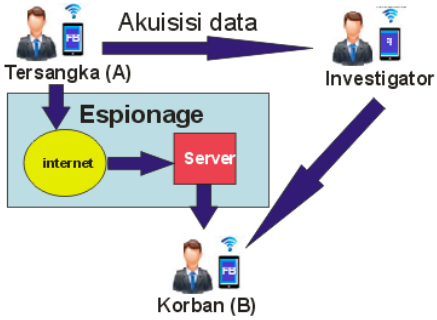
Skenario Aktivitas harus dijalankan agar mendapatkan barang bukti digital [14]. Penelitian ini membuat skenario rekayasa komprehensif dari kegiatan yang dijalankan pada Facebook. Tujuan diadakannya skenario ini untuk mempermudah investigasi dari kasus *cyber espionage*. Skenario tersebut sebagai berikut:

a. Tersangka membuat akun Facebook (Akun A)
b. Tersangka mencari dan menentukan akun korban di Facebook (Akun B)
c. Akun A mengirimkan memverifikasi data pengguna akun B
d. Akun A merekam data akun B
e. Akun A menyimpan semua data akun B

Pesan yang disimpan dari Facebook akan di bedah dari piranti atau perangkat aktor menggunakan *tools.* Skenario aktivitas dapat dilihat pada Gambar 2.6.

Gambar 2.6 Skenario Aktivitas

Proses investigasi yang dilakukan dari skenario kasus espionase dari Tersangka (Akun A) kepada Korban (Akun B) seperti pada Gambar 2.7. Pada proses ini, tersangka melakukan penyadapan/mata-mata kepada korban berupa pesan dan gambar. Setelah tersangka (akun A) melakukan penyadapan kepada korban (akun B), tersangka menyimpan data pesan dan gambar dari perangkat komunikasi yang digunakan yakni *smartphone*.



Gambar 2.7 Skenario Investigasi

Kasus *cyber espionage* pada penelitian ini dilakukan berdasarkan skenario kasus, dengan tujuan jika terjadi sesuai kasus yang sama tinggal mengikuti simulasi yang telah dibuat. Perkara yang disketsakan pada riset ini adalah data *espionage* teman Facebook. Kejahatan ini terkait penghapusan barang bukti dokumen penting dari skenario kasus di Facebook. Dari kasus ini ditemukan barang bukti komputer, *smartphone* beserta media penyimpanan Facebook. *Smartphone* dan Facebook menjadi instrumen kasus kejahatan.

Proses Akuisisi bukti digital ini berdasarkan pada metode DFRWS yaitu metode ilmiah yang memiliki dasar dan terbukti untuk pemeliharaan, mengumpulkan, Identifikasi, validasi, interpretasi, analisis, dokumentasi dan presentasi barang bukti digital yang bersumber dari sumber-sumber digital bertujuan melanjutkan atau memfasilitasi pemulihan kasus yang mengandung pidana, atau mendukung untuk mengantisipasi aktivitas yang ilegal yang terbukti mengganggu untuk operasi yang telah diprogramkan. Hasil penelitian yang telah dilakukan dapat menjalankan proses pengangkatan data untuk mengungkap bukti digital pada pelaku di fitur Facebook berupa teks menggunakan *MobilEdit* dengan kerangka kerja DFRWS.

2.2. Pengujian Sistem

Tujuan dari pengujian sistem adalah untuk mengetahui apakah sistem yang dikerjakan sudah layak untuk digunakan dan sesuai dengan tujuan awal pembuatan [15]. Proses ini dijalankan memakai skenario yang telah ditetapkan pada tahap sebelumnya. Pengujian dilakukan sesuai dengan parameter berupa bukti potensial terkait *cyber espionage*. Sebelum pengujian sistem dioperasikan, dilaksanakan beberapa persiapan seperti *rooting* piranti *smartphone*, pemasangan aplikasi *Kingtool*, pemasangan aplikasi database browser, dan pembuatan akun Facebook.

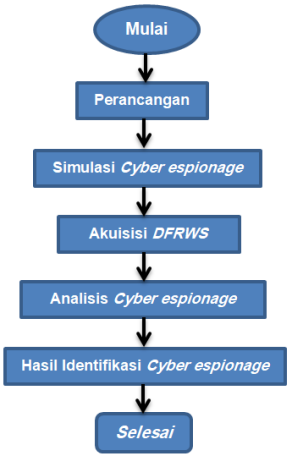
Kriteria keberhasilan dilihat dari terangkatnya bukti digital pada Facebook dan proses investigasi yang benar di perangkat *smartphone*. Analisis hasil akan diambil dari bukti digital yang telah diakuisisi oleh alat forensik *MOBILedit Forensic*. Analisis meliputi analisis percakapan (teks dan multimedia) ada aplikasi Facebook yang dianggap sebagai bukti potensial. Analisis hasil tidak mempertimbangkan isi dari pesan perundungan namun fokus pada pesan yang dikirimkan oleh pelaku. Bukti digital tersebut kemudian akan divalidasi melalui aspek *repeatability, reproducibility*, dan *hashing*.

Repeatability adalah proses forensik dilakukan secara berulang dalam waktu yang berdekatan menggunakan metode, objek, dan alat penelitian yang sama dan hasil tes diharapkan memberikan hasil yang sama. *Reproducibility* adalah Proses forensik dilakukan secara berulang dalam waktu yang berdekatan menggunakan metode dan objek penelitian yang sama dan alat penelitian yang berbeda. Hasil tes *reproducibility* diharapkan memberikan hasil yang sama. *Hashing* dilakukan untuk melihat integritas hasil yang diperoleh. Tidak semua alat forensik melakukan komputasi *Hashing.* Pada kondisi seperti itu, kalkulasi *Hashing* secara terpisah perlu dilakukan. Kalkulasi *Hashing* dilakukan pada *image* setelah proses akuisisi selesai dilakukan. Kalkulasi *Hashing* menghasilkan yang dijadikan acuan integritas data [16]

Analisis kinerja alat forensik juga diuji dengan perhitungan pada aspek akurasi (kecermatan, ketelitian, ketepatan). pengujian ini harus menggambarkan petunjuk dari kasus yang sedang didalami yaitu *cyber espionage*.

3. HASIL DAN PEMBAHASAN

Pada penelitian ini bertujuan untuk dapat membantu investigasi *cyber espionage* dengan melihat frekuensi *term key* yang terkandung pada bukti digital. Proses pengujian sistem dioperasikan memakai sketsa atau skenario yang sudah ditetapkan pada tahap sebelumnya. Pengujian dilakukan sesuai dengan parameter berupa bukti potensial terkait *cyber espionage*. Sebelum pengujian sistem dijalankan akan dilakukan beberapa persiapan seperti *rooting* piranti *smartphone*, pemasangan aplikasi *Kingtool*, pemasangan aplikasi database *browser*, dan pembuatan akun Facebook. Diagram alur pada tahapan penelitian analisis investigasi forensik *cyber espionage* pada Facebook menggunakan metode *DFRWS* dapat dilihat pada Gambar 3.1.



Gambar 3.1 Diagram alur penelitian

Tahapan–tahapan dalam diagram alur penelitian yaitu sebagai berikut:

1. Perancangan, merupakan tahapan untuk menganalisis kebutuhan sebelum dilakukan penelitian dan membuat kerangka kerja dari penelitian tersebut. Kerangka kerja digunakan untuk membantu *investigator* dalam melakukan *digital forensics.*
2. Simulasi *cyber espionage*, merupakan tahap dilakukan simulasi antara pelaku *cyber espionage* dengan korban *cyber espionage* dengan menggunakan beberapa kata atau kalimat, agar dapat terindentifikasi

tindakan *cyber espionage*. Parameter pengukuran disesuaikan dengan simulasi kasus, yaitu bukti potensial terkait *cyber espionage*, yaitu identifikasi pengguna, pesan multimedia, pesan teks, *timestamp*, dan aplikasi.

3. Akuisisi digital forensik dengan menggunakan metode DFRWS merupakan tahap akuisisi digital forensik menggunakan metode DFRWS akan dilakukan forensik dengan menggunakan metode *DFRWS* yaitu *identification, preservation, collection, examination, analysis, dan presentation* sehingga dari tahap ini dapat menghasilkan barang bukti berupa chat Facebook dengan menggunakan *tools MobilEdit.* Analisis hasil akan diambil dari bukti digital yang telah diakuisisi oleh alat forensik yaitu tool *MOBILedit Forensic*.
4. Analisis *cyber espionage* dilakukan degan melihat kata atau kalimat yang ditemukan pada pesan Facebook kemudian di analisis agar dapat di identifikasi tindakan *cyber espionage.* Analisis kinerja alat forensik juga diuji dengan perhitungan pada aspek akurasi (kecermatan, ketelitian, ketepatan). Pengujian ini harus menggambarkan petunjuk dari kasus yang sedang didalami yaitu *cyber espionage*.
5. Hasil Identifikasi *cyber espionage* adalah hasil analisis dari tahapan sebelumnya dan berisi kesimpulan. Hasil tidak mempertimbangkan isi dari pesan perundungan namun fokus pada pesan yang dikirimkan oleh pelaku. Bukti digital tersebut kemudian akan divalidasi melalui aspek *repeatability, reproducibility, hashing.*

Tahapan selanjutnya dilakukan pemberitahuan hasil pengkajian yang mencakup penjelasan mengenai *tools* , gambaran aktivitas yang dilakukan, dan metode yang dipakai, penetapan aktivitas pendukung yang dilakukan, dan menyampaikan rekomendasi untuk perbaikan kebijakan, metode, *tool*, atau aspek pendukung lainnya pada proses tindakan forensik digital [17]. Tahap terakhir adalah tahap presentasi yaitu mempresentasikan dan melaporkan hasil analisis sehingga bisa dipahami oleh kalayak umum [18].

Kriteria keberhasilan dilihat dari terangkatnya bukti digital pada Facebook dan proses investigasi yang benar pada perangkat *smartphone*. Analisis hasil akan diambil dari bukti digital yang telah diakuisisi oleh alat forensik *Oxygen Firensic, MobilEdit Forensic*, dan *Autopsy*. Analisis meliputi analisis percakapan (teks dan multimedia) ada aplikasi Facebook yang dianggap sebagai bukti potensial.

4. KESIMPULAN

Analisis Investigasi forensik *cyber espionage* pada Facebook menggunakan metode DFRWS diharapkan dapat membantu investigator untuk menyelidiki kasus *cyber espionage* yang terjadi selama ini. Metode DFRWS digunakan untuk membantu proses pengangkatan barang bukti dari pelaku tindak *cyber espionage.* Penelitian ini bertujuan agar bisa memberikan gambaran umum terkait bagaimana teknik yang bisa dipergunakan untuk memulihkan barang bukti digital berupa gambar dan teks yang ada di *smartphone.*

Penelitian ini menggunakan alat dan metodologi penelitian yang diharapkan bisa dipergunakan untuk *analisys forenscis* pada aplikasi Facebook dan mendapatkan hasil yang dapat digunakan dalam mendukung proses penyelidikan kasus. Dari metode forensik yang sudah ditingkatkan, pastinya masih dibutuhkan pengembangan sehingga metode ini bisa lebih baik dari sebelumnya. Saran untuk pengembangan *tools* yang telah di uji keakuratannya, sehingga data - data yang hilang dapat dikembalikan.

DAFTAR PUSTAKA

[1] www.makasardigitalvalley.id., " *Pengguna Perangkat Mobile Indonesia diprediksi jadi ketiga terbesar di dunia,"* 2019.
[2] Nawawi, B.A.,"*Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*," Rajawali Pers, Jakarta, 2005.
[3] Widiandana, P. dkk. ," *Analisis Investigasi Forensik Cyberbullying pada Whatsapp Menggunakan Metode NIST,"* Jakarta 17 Juli 2019.
[4] Nicko, S.," Tindak Pidana Cyber Espionage," Perpustakaan Universitas Airlanggar, 2010.
[5] Altheide, C. dan Carvey Harlan," Digital Forensics with Open Source Tools," 2011.
[6] Riadi, I. dkk," *Analisis Recovery Bukti Digital Instagram Messengers Menggunakan Metode National Institute of Standard and Technology (NIST)*,"Seminar Nasional Teknologi Informasi dan Komunikasi, SEMANTIKOM 2017.
[7] Anwar, F.," *Perubahan dan Permasalahan Media Sosial. Jurnal Muara Ilmu Sosial, Humaniora, dan Seni*,"Vol. 1, No. 1, April 2017: hlm 137-144
[8] Sulidar, F. ,"*Dampak Positif Dan Negatif Sosial Mediaterhadap Perubahan Sosial Anak*," Naturalistic, April 2017: 118-123
[9] Hakeem, L.," *Media Sosial dan Dampak Positif Menurut Islam,"* Seminar Sains Teknologi dan Manusia 2019 (SSTM'19) UTM. Akademi Tamadun Islam pada 15 Desember 2019.
[10] Sugeng, A.,"*Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat di Indonesia,"* PUBLICIANA: Universitas Tulungagung, 2016.
[11] https://dailysocial.id/post/laporan-dailysocial-survey-instant-messaging-2017

[12] Mansur, M.A. dkk," *Cyber Law Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung. 2005.
[13] Sugiyono.,"*Metode Penelitian Kuantitatif, Kualitatif, dan R&D.* Bandung : Alfabeta, CV. 2017.
[14] Fauzan, A. dkk," *Analisys Forensikcs Digital Pada Line Messenger untuk Penanganan Cybercrime,"* Desember 2016, Volume 2 Nomor 1. Ilkom Unisri.ac.id
[15] Hanifah, U. ," *Penggunaan Metode Black Box pada Pengujian Sistem Informasi Surat Keluar Masuk,"* Scan Vol. Xi Nomor 2 Juni 2016
[16] Hadi, A. dkk," *Analisis Bukti Digital Fitur TRIM Pada SSD NVMe Menggunakan Metode Static Forensics," JUITA: Jurnal Informatika Volume 8, Nomor 1, Mei 2020*
[17] Yudhana, A. dkk ," *Analisis Live Forensics Aplikasi Media Sosial pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS),"* Vol.20, No.2, Oktober 2019, Hal. 125~130
[18] Suryana, dkk ,"*Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS)*," J. Edukasi dan Penelit. Inform., vol. 2, no. 2, pp. 111–117. 2016.