PERANCANGAN DIGITAL FORENSIK PADA APLIKASI TWITTER MENGGUNAKAN METODE *LIVE FORENSICS*

Ikhsan Zuhriyanto [(1)], Anton Yudhana[(2)] dan Imam Riadi [(3)]
[(1)(2)] Program Studi Teknik Informatika, Universitas Ahmad Dahlan
[(3)] Program Studi Sistem Informasi, Universitas Ahmad Dahlan
e-mail : Ikhzann@gmail.com [(1)], imam.riadi@is.uad.ac.id [(2)], eyudhana@mti.ac.id [(3)]

Abstrak
Perkembangan pada era teknologi informasi saat ini semakin pesat dan telah menimbulkan berbagai dampak positif dan juga negatif. Salah satu dampak positif yang dapat diambil dari perkembangan teknologi informasi adalah masyarakat lebih mudah dalam mengakses dan menggunakan informasi, serta lebih mudah berkomunikasi dengan masyarakat lainnya di belahan dunia manapun, disamping itu dampak negatifnya adalah tidak terkontrolnya sikap masyarakat dalam menggunakan aplikas-aplikasi yang dimiliki, sehingga menimbulkan suatu tindak kejahatan di dunia maya (cyber crime). Salah satu aplikasi sosial media yang banyak digunakan adalah aplikasi Twitter, namun belakangan ini aplikasi Twitter menjadi salah satu aplikasi sosial media yang digunakan untuk melakukan ujaran kebencian, pencemaran nama baik dan tindak kejahatan lainnya. Penelitian ini dimaksudkan guna mendapatkan bukti digital dengan menggunakan menerapkan salah satu metode yaitu National Institute of Justice (NIJ) dengan live forensics dimana dikemudian bukti digital tersebut dapat digunakan menjadi bukti pendukung dalam menangani tindak kejahatan.

***Kata Kunci** : Digital Forensik Twitter, Live Forensic, Cybercrime Media Sosial.*

1. PENDAHULUAN

Pada prinsipnya manusia memiliki kebutuhan dan kemampuan serta kebiasaan untuk berkomunikasi dan berinteraksi dengan manusia satu sama lainnya, selanjutnya interaksi ini berbentuk kelompok. Sifat berkelompok ini didasari pada kepemilikan atau kemampuan dalam berkomunikasi, mengungkapkan rasa dan kemampuan untuk saling bekerja sama dan bersosial. Globalisasi telah menjadi pendorong lahirnya era penggunaan teknologi informasi. Pengaruh teknologi memberikan kemudahan kepada manusia dalam hal komunikasi. Selain memberikan dampak positif, kemajuan teknologi informasi dan telekomunikasi juga memberikan dampak negative juga yaitu banyaknya kejahatan yang berkaitan dengan aplikasi internet. Media sosial *Twitter* adalah salah satu bagian yang digunakan sebagai penghubung komunikasi antar manusia di dunia siber (*cyber*). Mudahnya dalam menggunakan media *social Twitter* membuat akun *Twitter* semakin meningkan sehingga memunculkan akun-akun palsu yang selain digunakan untuk berkomunikasi juga digunakan untuk menuliskan berita tidak benar, penipuan dan juga penghinaan terhadap seseorang sehingga pada akhirnya merugikan banyak pihak.

Perkembangan teknologi internet juga di dasari oleh perkembangan *smartphone*, saat ini memudahkan orang-orang dalam mengakses informasi dan diiringi juga dengan banyaknya penggunaan media sosial. Jumlah pengguna aktif media sosial diseluruh dunia mencapai 2,31 Triliun, yang artinya setara dengan 31% dari total populasi penduduk dunia. Pengguna aplikasi Twitter sendiri mencapai nilai 310 Juta pengguna. Banyaknya pengguna menyebabkan Tidak sedikit tindak kejahatan dilakukan menggunakan media social sehingga menimbulkan tindak kejatahan diantaranya penculikan, penipuan, pencemaran nama baik, pemerasan, *cyberbully* dan lainnya. Kejahatan pada media sosial Facebook dan Twitter meningkat sebanyak 780% selama 4 tahun dari tahun 2008 (556 kasus) sampai tahun 2012 (4908) kasus. (Mukti, Masruroh, & Khairani 2017)

Pengambilan bukti digital tindak kejahatan pada penelitian ini dilakukan dengan tahapan penelitian dan analisa mengadaptasi metode forensik dari *National Institute of Justice* (NIJ) untuk mendapatkan bukti digital tindak kejahatan. (Riadi, Umar, & Nasrulloh 2018) Berdasarkan penelitian terdahulu dapat diketahui bukti potensial apa saja yang terdapat pada aplikasi pesan singkat seperti tanggal/waktu, pesan teks, dan gambar/foto (Riadi et al. 2018) yang diharapkan dapat menjadi bukti digital tindak kejahatan di media sosial.

2. TINJAUAN PUSTAKA

Penelitian (Mukti, Masruroh, & Khairani 2017) menggunakan metode simulasi yang telah dilakukan, yaitu bahawa tidak semua proses data dapat tersimpan pada penyimpaan *server* komputer. Data tersebut juga akan tersimpan pada memori internal perangkat Android yang hanya dapat diakses setelah perangkat Android yang digunakan melalui proses *root* pada handphone. Berdasarkan hasil semua skenario pencarian bukti forensik yang telah ditentukan sebelumnya, pada aplikasi media sosial Facebook semua bukti forensik dapat ditemukan. Nama akun data lokasi, nomor telepon, tanggal lahir, *photo profile*, *cover photo*, *posting* berupa teks, *posting* berupa gambar, *private message* berupa teks dan *private message* berupa gambar adalah bukti forensic yang ditemukan pada aplikasi Facebook. Bukti forensik yang ditemukan Pada aplikasi media sosial Twitter sedikit berbeda dikarenakan hanya mendapatkan bukti forensik nama akun, data lokasi, *photo profile*, *cover photo*, *tweet* (*posting*) berupa teks dan *tweet* (*posting*) berupa gambar. Nomor telepon, tanggal lahir, *direct message* berupa teks dan *direct message* berupa gambar tidak berhasil ditemukan pada aplikasi Twitter.

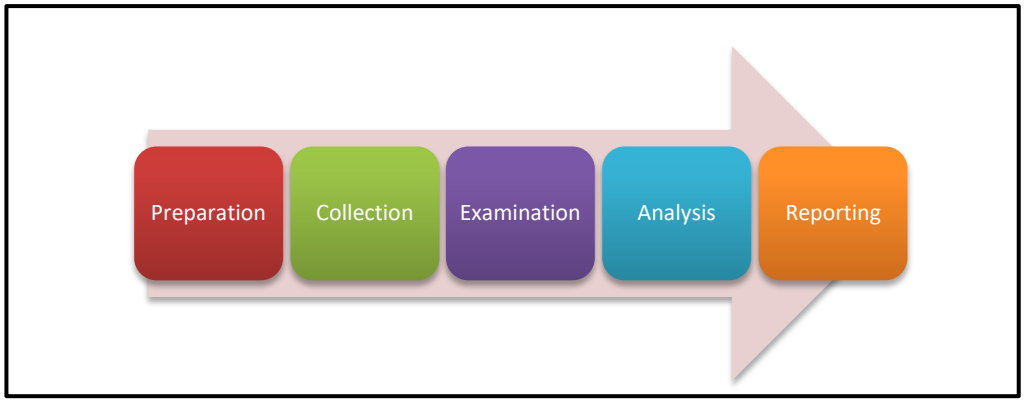
Penelitian (Rauhulloh et al. 2018) mereka menggunakan *National Institute of Justice* (NIJ) sebagai metode, metode ini memiliki beberapa tahapan (Collection, Examinition, Analysis dan Reporting) berikut dijalankan menggunakan perangkat lunak (*tools* FTK Imager) sebagai bahan pendukung untuk mengetahui keamanan masing-masing pada media sosial Facebook, Twitter, dan Instagram. Dalam meyakinkan bahwa akun media sosial Facebook, Twitter dan Instagram menjadi nilai yang merepresentasikan string asli atau akun asli lakukan dengan cloning data dan Hashing data fungsi. Berdasarkan pada tahapan-tahapan metode yang dilakukan, proses analisis mengenai data pada media sosial Facebook, Twitter, dan Instagram berupa barang bukti data yang valid (asli atau palsu). Penelitan (Chang & Chang 2016) melakukan digital forensic pada applikasi twitter pada windows 10 dengan menggunakan *virtual machine* untuk mendapatkan bukti digital.

Penelitian (Yudhana, Riadi, & Anshori 2018) berdasarkan penelitian mereka menggunakan *Smartphone* Galaxy V+ SM-G31HZ, melakukan proses *Rooting*, install aplikasi Facebook Messenger, pembuatan pesan, melakukan infestigasi menggunakan tool forensic yang bernama Oxigen forensic, kemudian melakukan analisis pada ketiga alat perangkat lunak forensik tersebut, hasil dari analisis akan dilaporkan sebagai barang bukti. Metode yang digunakan untuk melakukan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan metode NIST (*National Institute of Standards Technology*). Hasil yang telah didapatkan adalah text percakapan, gambar dan audio.

Penelitian (Riadi et al. 2017) Dengan menggunakan salah satu teknik digital forensics yakni *live forensics*, data dan informasi yang memungkinkan menjadi barang bukti bisa didapatkan pada RAM yang dianalisa menggunakan *tools* forensik digital. Pada Penelitian ini, kasus akan disimulasi dengan kejahatan penipuan *online shop* yang sering terjadi dan memanfaatkan *tools live forensics* untuk menemukan barang bukti kejahatan. Penelitian (Anwar & Riadi 2017) pada penelitian mereka memperoleh bukti digital pada aplikasi WhatsApp *Messenger* berbasis android dan analisis evidance pada aplikasi WhatsApp *Messenger* berbasis *web* menggunakan metode NIST. Penelitian (Faiz, Umar, & Yudhana 2016) menggunakan metode *live forensic* untuk melihat keamanan pada akun email.

3. METODE PENELITIAN

Penelitian ini mengadaptasi pada proses investigasi metode analisis forensik *National Institute of Justice* (NIJ). Dalam metode tersebut digunakan untuk memudahkan mejabarkan bagaimana gambaran proses penelitian yang sedang dilakukan agar bisa diketahui tahapan penelitian ini secara lebih sistematis sehingga dapat untuk dijadikan referensi pada penelitian selanjutnya. Tahapan metode penelitian dapat dilihat pada Gambar 1. yang menjelaskan proses tahapan penelitian.



Gambar 1. Tahapan Metode Penelitian

Penelitian yang dilakukan oleh Ellick M. Chan tahun 2011 tahapan langkah dalam membantu menangani suatu masalah pada digital forensics yaitu :

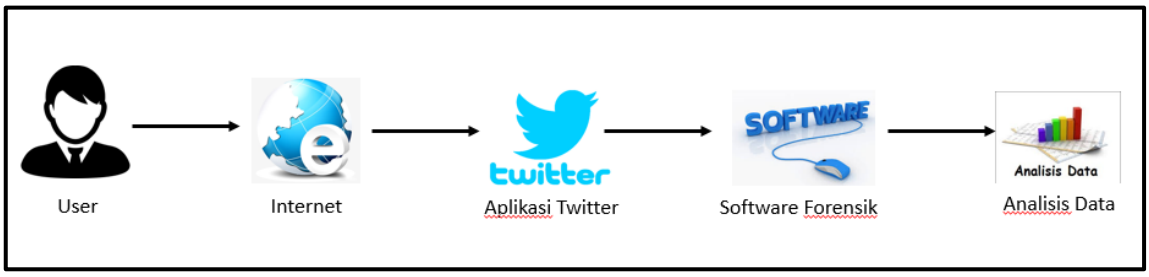
1. Tahapan *Preparation* (Persiapan)
   Dalam tahapan ini yaitu menyiapkan segala peralatan dan alat-alat yang dapat digunakan untuk melakukan tugas-tugas sesuai dengan apa yang diperlukan selama dalam penyelidikan.
2. Tahapan *Collection* (Pengumpulan)
   Melakukan pecarian file dokumen dan mengumpulkan atau membuat salinan dari objek fisik / digital yang berisi bukti elektronik, dan bukti lain didalamnya.
3. Tahapan Examination (Pemeriksaan)
   Tahapan ini merupakan tahapan untuk melakukan pemeriksaan bukti elektronik / bukti digital terlihat dan dokumen dari isi system / direktori. Dalam mengidentifikasi bukti dilakuakn reduksi data.
4. Tahapan *Analysis* (Analisa)
   Setelah mendapatkan bukti-bukti tersebut dari proses sebelumnya maka perlu dilakukan tahapan selanjutnya yaitu analisis data yang bertujuan untuk menentukan bukti signifikan dan nilai dari pembuktian.
5. Tahapan *Reporting* (Pelaporan)
   Pada tahapan ini adalah pembuatan catatan pemeriksaan pada setiap kasus. Dari penelitian tersebut Ellick M. Chan merujuk pada metode *National Institute of Justice* (NIJ). (Faiz, Umar, & Yudhana 2017)

Metode *live forensics* pada dasarnya memiliki beberapa kesamaan pada teknik forensik tradisional yaitu identifikasi, penyimpanan, analisis, kemudian presentasi. Metode *live forensics* merupakan respon dari kekurangan teknik forensik tradisional yang tidak bisa mendapatkan informasi dari data dan informasi yang hanya dilakukan ketika sistem sedang berjalan/bekerja misalnya aktivitas *Memory*, aktivitas *Network proses*, aktivitas *Swap file* dan aktivitas *running sistem prose.* Informasi dari file sistem ini menjadi kelebihan dari teknik *live forensics*, dimana teknik *live forensics* telah berkembang dalam beberapa dekade terakhir, seperti analisis *content memory* untuk mendapatkan gambaran yang lebih baik mengenai aplikasi dan proses yang sedang berjalan. (Riadi 2017)

Pada metode *live forensics* bertujuan untuk penanganan insiden lebih cepat, integritas data lebih terjamin, teknik enkripsi lebih memungkinkan bisa dibuka dan kapasitas memori yang lebih rendah bila dibandingkan dengan metode forensik tradisional. Banyak tools untuk digunakan *live forensics* untuk analisis data. Tools yang dibandingan pada metode *live forensics* yaitu dari kemampuan penggunaan memory, waktu, jumlah langkah dan akurasi paling baik dalam melakukan *live forensic*.(Dwi et al. 2017)

3.1 Simulasi Perancangan Sistem

Sebuah rancangan untuk mendapatkan suatu bukti digital untuk dilakukan analisis. Pada penelitian ini menganalisa dari ketiga media sosial tersebut sehingga mengeluarkan data analisis. Tahapan Gambar 2. menjelaskan tentang rancangan yang digunakan dalam penelitian.



Gambar 2. Tahapan Analisis

Pada Gambar 2 menjelaskan tahapan analis yaitu dilakukan tahapan analisis terhadap media sosial Aplikasi Twitter dimana tahap akhir nanti mengeluarkan suatu data analisis dari perangkat lunak FTK *imager*.

4. HASIL DAN PEMBAHASAN

Dalam melakukan analisis forensik media sosial pada perangkat laptop atau komputer di butuhkan sebuah metode dan tools guna membantu peneliti guna memcari data untuk di investigasi

forensik. Penelitian ini diawali dengan membuat akun media sosial Twitter, Selanjutnya penelitian ini melakukan pemilihan tools untuk mengambil data pada akun media sosial berikut. Pada tahap ini tools yang akan digunakan menggunakan tools FTK Imager sebagai pengelola pada data yang akan di analisis. Selanjutnya pada saat membuat akun media sosial Twitter di lakukan dengan cloning data dan Hashing data fungsi nya yaitu meyakinkan bahwa akun media sosial Twitter menjadi nilai yang merepresentasikan string asli atau akun asli. Tahapan berikutnya yaitu akun media sosial tersebut akan di analisis untuk mendapatkan data yang dapat menjadi barang bukti data forensik yang valid. Pada tahapan terakhir dilakukan *reporting* atau laporan hasil penelitian mengenai data pada media sosial berupa barang bukti data yang valid pada media sosial tersebut, dalam *reporting* juga menjelaskan tahapan-tahapan atau proses yang digunakan untuk mendapatkan barang bukti yang dibutuhkan agar data tersebut terbukti asli atau valid.

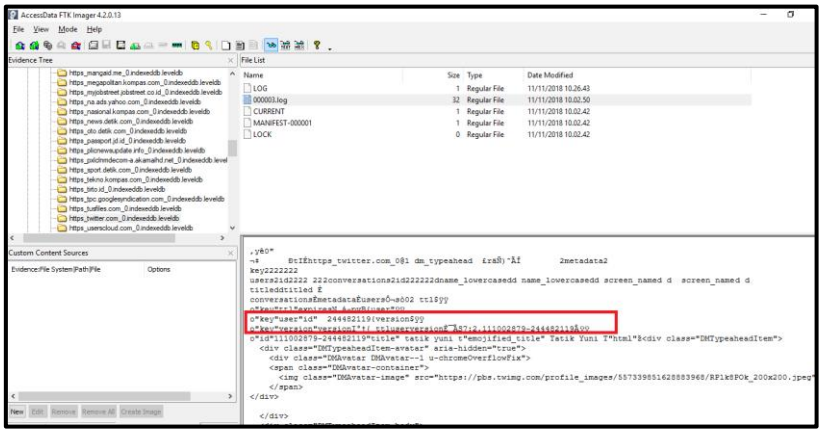
4.1 Analisis Bukti Digital

Pada Tahapan ini dilakukan pengumpulan bukti digital pada program browse google chrome di direktori leptop dengan menggunakan program TFK Imager, sehingga didapatkan data berupa file dan log pada Tabel 1 yang menjelaskan type file, storange location dan file name.

Tabel 1. Hasil Eksplorasi pada direktori Laptop

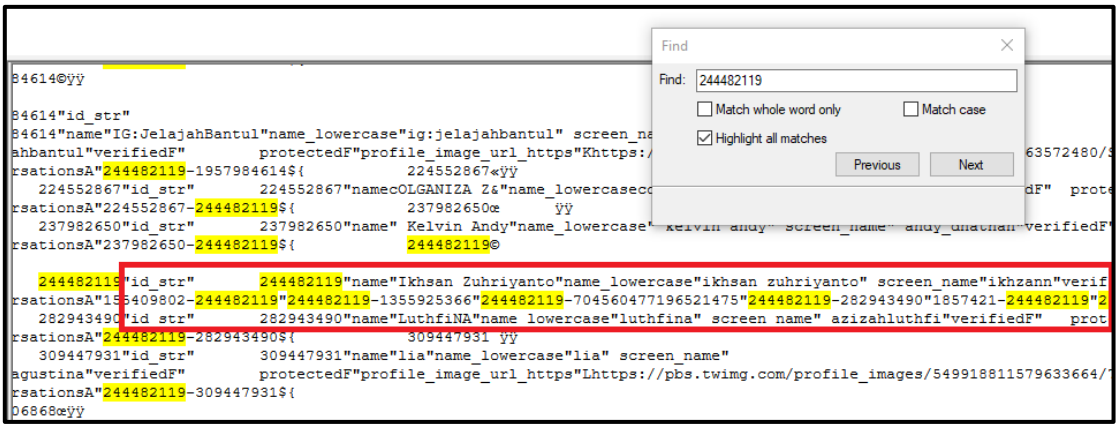
File Type	Storage Location	File Name
Log File	C:\Users\IkhzannPC\AppData\Local\Google\Chrome\User Data\Default\IndexDB\https_twiter.com_0.indexeddb.leveldb	000003.log
Chace	C:\Users\IkhzannPC\AppData\Local\Google\Chrome\User Data\Default\Cache\	f_0022f5

Berdasarkan data pada Tabel 1 log file pada aplikasi Twitter sudah dapat diketahui, untuk mengakses log file tersebut dapat dilakukan dengan program FTK Imager seperti pada gambar 3.



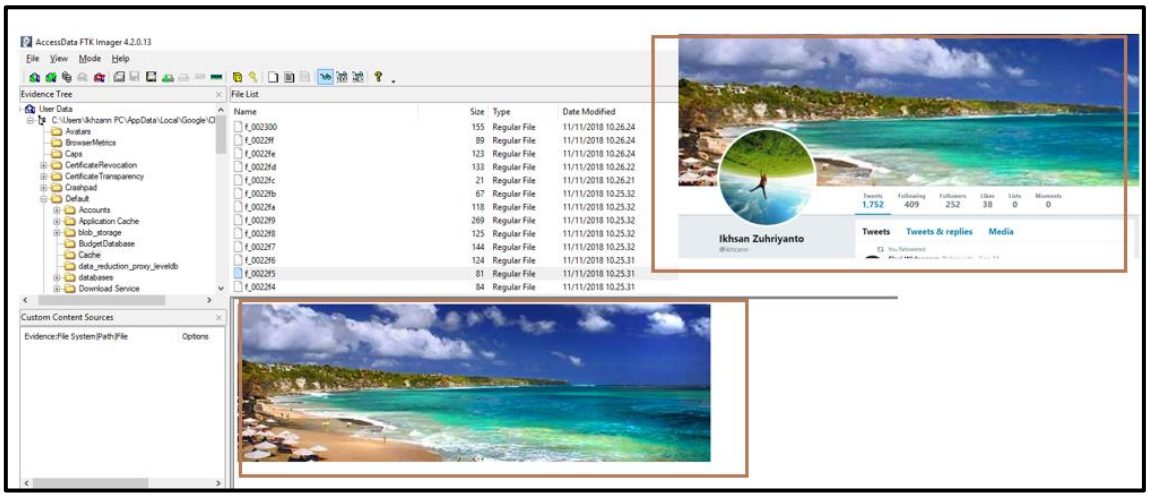
Gambar 3. Log File

Dalam log file terdapat user id / akun Twitter yang dipakai yaitu dengan id 244482119, yang kemudian dilakukan analisis untuk mengetahui id tersebut, Gambar 4. Menjelaskan pencarian user id pada log file Twitter.



Gambar 4. Id User Twitter

Berdasarkan temuan pada gambar 4. Id User Twitter yaitu user id 244482119 dengan dilakukan pencarian menggunakan find text maka didapatkan nama user id yang bernama Ikhsan Zuhriyanto dan menggunakan nama akun Twitter Ikhzann. Pada Tahap selanjutnya yaitu dilakukan analisis pada chace file yang telah ditemukannya file chace f_0022f5 dimana file tersebut dijelaskan pada Gambar 5. Yang dapat dilihat menggunakan FTK Imager.



Gambar 5. File Chace Twitter

Hasil pada file chace pada Gambar 5. menunjukan bahwa ada identik atau kesamaan dengan profil yang didapat pada akun Twitter Ikhzann. Sehingga dapat dikatakan untuk file yang didapat merupakan file asli / bukti digital yang dapat digunakan dalam digital forensik.

5. KESIMPULAN

Penelitian ini menggunakan *National Institute of Justice* (NIJ) sebagai metode, metode ini memiliki beberapa tahapan yaitu (*Collection, Examinition, Analysis* dan *Reporting).* Metode tersebut kemudian dijalankan menggunakan perangkat lunak (*FTK Imager*) sebagai bahan pendukung untuk mengetahui keamanan pada aplikasi Twitter. Dalam meyakinkan bahwa akun media sosial menjadi nilai yang merepresentasikan string asli atau akun asli dilakukan dengan analisis data pada direktori leptop. Berdasarkan beberapa hasil dari tahapan-tahapan metode yang telah dilakukan, proses analisis mengenai data pada media sosial Twitter dapat dikatakan bahwa bukti digital berupa barang bukti data yang valid.

DAFTAR PUSTAKA

Anwar, Nuril, & Riadi, I. 2017. "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web." *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika* 3(1): 1. http://journal.uad.ac.id/index.php/JITEKI/article/view/6643.

Chang, Ming Sang, & Chih Yen Chang. 2016. "Twitter Social Network Forensics on Windows 10." 3(9): 55–60.

Dwi, Tayomi et al. 2017. "Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10." (November).

Faiz, Muhammad Nur, Umar,R., & Yudhana, A. 2016. "Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary." *Jurnal Ilmiah ILKOM* 8(3): 242–47. https://www.researchgate.net/publication/316274410_Implementasi_Live_Forensics_untuk_Perbandingan_Browser_pada_Keamanan_Email.

Faiz, Muhammad Nur, Umar, R., & Yudhana, A. 2017. "Implementasi Live Forensics Untuk Perbandingan Browser Pada Keamanan Email." *JISKA (Jurnal Informatika Sunan Kalijaga)* 1(3): 108. http://ejournal.uin-suka.ac.id/saintek/JISKA/article/view/13-02.

Rauhulloh Ayatulloh, K.N.B., Umar,R., & Yudhana, A.2018. "Prosiding SNST Ke-9 Tahun 2018 Fakultas Teknik Universitas Wahid Hasyim 121." : 121–24.

Mukti, Wisnu Ari, Siti Ummi Masruroh, & Dewi Khairani. 2017. "Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial." *Jurnal Teknik Informatika* 10(1): 73–84.

Riadi, I.,Sunardi, Rauli, M.E. 2017. "Analisis Live Forensics Aplikasi Whatsapp Dan Line Pada Sistem Operasi Windows 8." : 1–6.

Riadi, I., Sunardi, & Muhammad Ermansyah Rauli. 2017. "Investigasi *Live Forensics* Dari Sisi Pengguna Untuk Menganalisa Investigasi *Live Forensics* Dari Sisi Pengguna Untuk Menganalisa Serangan Man in the Middle Attack Berbasis Evil Twin." 9(April): 1–8.

Riadi, I., Umar,R., & Nasrulloh, I.M. 2018. "Analisis Forensik Digital Pada Frozen Slod State Drive Dengan Metode National Institute of Justice (Nij)." 3(May): 70–82.

Riadi, I.,Yudhana, A., Muhamad Caesar, & Febriansyah Putra. 2018. "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)." 4(September): 219–27.

Yudhana, A., Riadi, I., & Anshori,I. 2018. "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist." 3(1): 13–21.