**REPOSITOR**, Vol. 2, No. 10, Oktober 2020, Pp. 1400-1405
ISSN : 2714-7975
E-ISSN : 2716-1382 

# Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST

**Salma Azizah[1], Sri Ayu Ramadhona[2], Kenny Willy Gustitio[3]**
[1,2,3]Program Studi Teknik Komputer Universitas Amikom Yogyakarta
e-mail: salma.azizah@students.amikom.ac.id[1] , sri.ramadhona@students.amikom.ac.id[2], kenny.gustitio@students.amikom.ac.id[3]

***Abstrak***

*Kejahatan dunia maya semakin meningkat seiring dengan berkembangnya teknologi yang meningkat. Kasus kejahatan penipuan online shop menjadi salah satu tindak kejahatan yang sering terjadi. Kejahatan ini memanfaatkan salah satu aplikasi Instant Messenger yang cukup populer yaitu Telegram. Telegram berbasis desktop merupakan salah satu aplikasi yang dapat dijalankan pada komputer, khususnya komputer sistem operasi Windows 10. Semua aplikasi yang dijalankan pada komputer meninggalkan data dan informasi pada Random Access Memory (RAM). Data dan informasi tersebut dapat diperoleh dari RAM menggunakan teknik live forensics yang dapat digunakan ketika komputer sedang berjalan dan terkoneksi internet. Penelitian ini bertujuan untuk menemukan bukti digital pada kasus penipuan online shop. Bukti digital tersebut diperoleh dengan menggunakan tools FTK Imager dengan mengakuisisi RAM pada komputer untuk mendapatkan data dan informasi pada RAM. Hasil penelitian ini diperoleh bukti percakapan antara tersangka dan korban menggunakan Telegram untuk mengungkap tindak kejahatan penipuan online shop.*

***Kata kunci:*** *Forensik, NIST, Telegram Messenger, FTK Imager*

***Abstract***

Cybercrime is increasing along with the development of increasing technology. Online shop fraud crime case is one of the crimes that often occurs. This crime makes use of one of the most popular Instant Messenger applications, Telegram. Desktop-based telegram is one application that can run on computers, especially Windows 10 operating system computers. All applications that run on a computer leave data and information in Random Access Memory (RAM). The data and information can be obtained from RAM using live forensics techniques that can be used when the computer is running and connected to the internet. This study aims to find digital evidence on online shop fraud cases. Digital evidence is obtained by using FTK Imager tools by acquiring RAM on a computer to get data and information on RAM. The results of this study obtained evidence of a conversation between the suspect and the victim using Telegram to expose online shop fraud.

***Keywords****: Forensics, NIST, Telegram Messenger, FTK Imager*

## 1. Pendahuluan

Sebelum teknologi berkembang pesat dan kebutuhan ponsel pintar belum cukup diminati, kebanyakan orang masih menggunakan ponsel hanya terbatas untuk penggunaan SMS (*Short Message Service*) dan telepon. Namun seiring dengan kemajuan teknologi yang pesat, berbagai jenis ponsel dikeluarkan oleh perusahaan-perusahaan ternama untuk menarik pengguna dengan fitur-fitur dan spesifikasi luar biasa yang ditawarkan ponsel tersebut. Pembelian ponsel yang meningkat tentunya berdampak pada bertambahnya pengguna telepon seluler, termasuk pengguna telepon seluler dengan sistem operasi Android. Di sisi lain, dengan berkembangnya teknologi yang tidak terkontrol dapat mengakibatkan dampak negatif yang dapat merugikan pengguna, seperti hilangnya privasi dan pihak lain dapat menggunakan kesempatan tersebut untuk melakukan tindak kejahatan yang merugikan.

Telegram menjadi salah satu aplikasi *Instant Messenger* yang saat ini banyak digunakan oleh kebanyakan orang untuk menunjang aktivitas komunikasi jarak jauh dengan pengguna lain. Telegram menjadi salah satu aplikasi *Instan Messenger* yang sering digunakan sebagai

komunikasi dalam melakukan tindakan kriminal seperti penipuan, ujaran kebencian, dan terorisme [1]. Aplikasi ini mungkin menyimpan informasi perangkat dan data pengguna yang dienkripsi dalam *database* perangkat atau di *cloud*. Informasi seperti data pengguna disimpan di *server* mereka daripada menyimpannya diperangkat pengguna [2].

Analisis forensik sering menghadapi masalah yang berkaitan dengan aplikasi tersebut, seperti peningkatan keamanan dan fitur baru yang dirilis dengan versi yang lebih baru seperti dapat menghapus pesan pada perangkat penerima, ukuran maksimum file dikirim, dan panggilan suara melalui data [3].

RAM merupakan tempat penyimpanan sementara ketika komputer dijalankan. Penggunaan aplikasi pada komputer meninggalkan data dan informasi pada *Random Access Memory* (RAM) [4]. Data dan informasi yang terdapat pada RAM dapat hilang jika sistem mati, maka diperlukan penanganan data dan informasi pada RAM harus dilakukan dengan hati-hati [5]. Data dan informasi yang terdapat pada RAM dapat dijadikan sebagai bukti digital untuk dilakukan proses investigasi.

Forensik digital merupakan ilmu untuk kepentingan bukti hukum yang bertujuan untuk membuktikan kejahatan komputer untuk mendapatkan bukti digital yang valid [6]. Melalui *live forensics* bukti tersebut didapatkan untuk menangani kejahatan komputer dengan menggunakan pendekatan ketika komputer sedang berjalan dan terkoneksi internet [7]. *Live forensics* bergantung pada saat komputer sedang berjalan karena membutuhkan data dan informasi yang terdapat pada RAM [8]. Proses pengambilan data dan informasi harus dilakukan dengan cepat setelah barang bukti digital ditemukan [9]. Teknik tersebut juga menjamin integritas data tanpa harus kehilangan bukti digital yang potensial [10]

## 2. Metode Penelitian

Metode penelitian ini menggunakan metode yang dijelaskan oleh Ravneet Kaur dan Amandeep Kaur dalam penelitiannya yang mengacu pada tindak kejahatan digital [11]. Metode yang digunakan adalah metode NIST (*National Institute of Standard Technology*) sebagai tahapan untuk mendapatkan informasi dari bukti digital yang ada [12]. Proses investivigasi pada forensik digital ini dilakukan melalui beberapa tahapan yaitu Collection, Examination, Analysis, dan Reporting. Lihat gambar 1.


*Gambar 1 Tahap NIST*

Berdasarkan gambar 1, dapat dijelaskan bahwa:

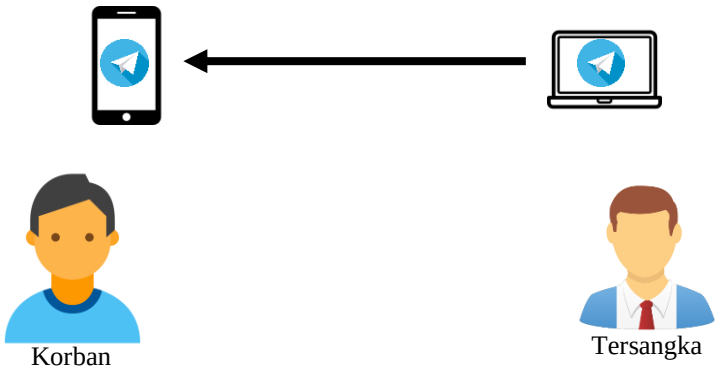
a. *Collection* merupakan tahap mengumpulkan data dari sumber yang terkait namun tetap menjaga integritas data tersebut.
b. *Examination* merupakan tahap pemrosesan data yang dikumpulkan untuk dilakukan ke proses selanjutnya.
c. *Analysis* merupakan tahap melakukan analisis sesuai dengan teknik dan hukum yang dibenarkan untuk mendapatkan informasi dan menjawab pertanyaan-pertanyaan
d. *Reporting* merupakan hasil laporan analisis meliputi penjelasan tindakan yang dilakukan sehingga dapat mengidentifikasi data yang dijadikan barang bukti pada kasus penipuan *online shop.*

Alat dan bahan yang dibutuhkan untuk mendapatkan bukti digital adalah laptop ASUS tipe X441B dengan sistem operasi Windows 10 yang telah terpasang aplikasi *Instant Messenger* Telegram berbasis desktop versi 2.1.13.0 dan *smartphone* Realme 5 pro yang telah terpasang aplikasi Telegram. Kasus yang digunakan adalah penipuan pada *online shop* dan menggunakan *tools* forensik FTK Imager untuk mengambil, menggandakan, menganalisis bukti digital.

Dalam kasus penipuan *online shop* ini kami melakukan simulasi secara lengkap untuk mendapatkan bukti digital yang dijalankan pada aplikasi Telegram. Simulasi ini menjadi petunjuk untuk menganalisis informasi sebagai penipuan. Simulasi tersebut dimulai dengan membuat akun Telegram tersangka dan korban, korban melanjutkan komunikasi dengan tersangka untuk negoisasi barang yang akan dibeli dengan mengirimkan gambar barang yang akan dibeli,

tersangka melakukan penipuan terhadap korban, dan isi percakapan tersebut dihapus dari akun tersangka.

Pesan Telegram yang dihapus oleh tersangka akan diinvestigasi menggunakan laptop tersangka menggunakan alat forensik. Gambar 2 menunjukkan simulasi yang akan dijalankan.




*Gambar 2 Simulasi penipuan online shop*

## 3. Hasil Penelitian dan Pembahasan

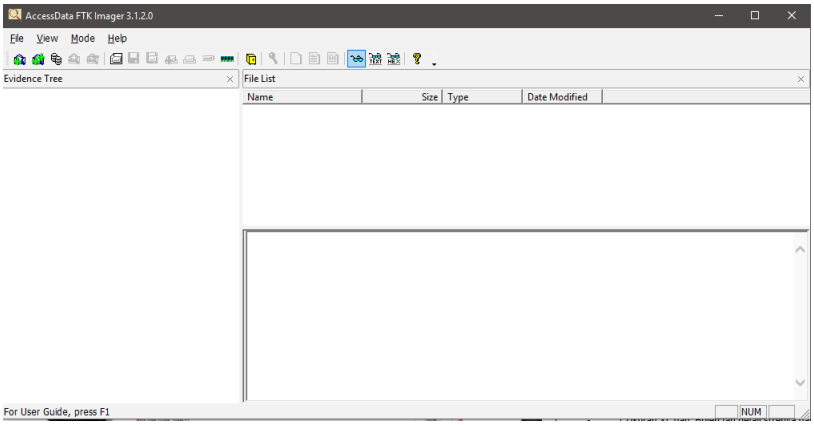
Penelitian ini menggunakan laptop dengan sistem operasi Windows 10 64 bit yang sudah terinstall aplikasi *Instant Messenger* Telegram berbasis desktop versi 2.1.13.0. pada kasus ini penyidik menemukan barang bukti laptop yang sudah dimatikan oleh tersangka dan isi percakapan yang terdapat dalam Telegram sudah dihapus untuk menghilangkan barang bukti.

### 3.1. Pengumpulan dan Pemrosesan Barang Bukti

Melalui tahap ini barang bukti dikumpulkan oleh penyidik untuk dilakukan investigasi mendapatkan bukti digital dari tersangka atas kasus tindak kejahatan penipuan *online shop.* Tindak kejahatan penipuan yang dilakukan oleh tersangka digunakan sebagai barang bukti penyidik untuk menemukan barang bukti terkait. Proses investigasi pada proses ini bertujuan untuk membantu proses selanjutnya dalam investigasi. Penemuan barang bukti berupa laptop ASUS tipe X441B dengan sistem operasi Windows 10 yang sudah terinstall aplikasi Telegram. Aplikasi Telegram tersebut sudah dalam kondisi ditutup dan laptop dalam keadaan mati.

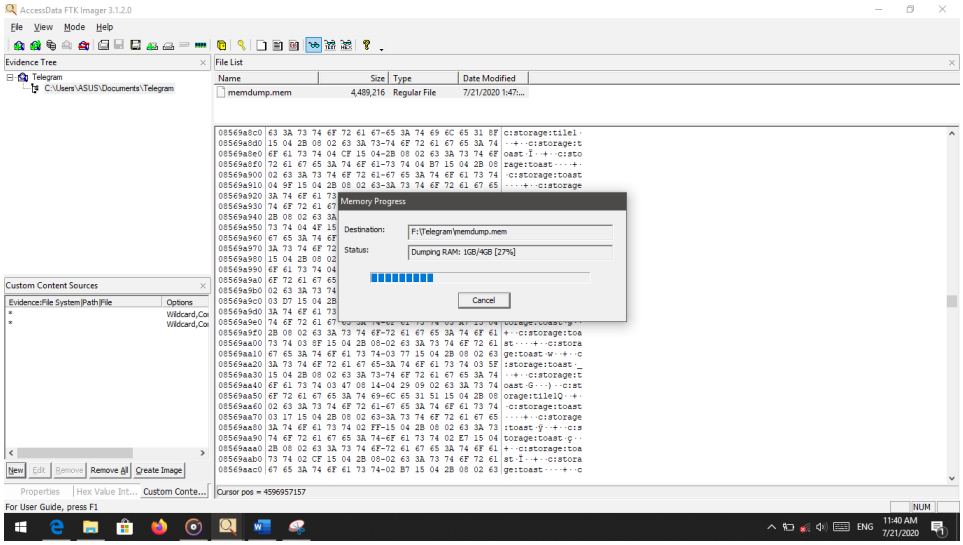
Pada tahap ini aplikasi Telegram akan dijalankan menggunakan teknik *live forensics* untuk memproses bukti digital yang terdapat pada RAM.

a. Langkah pertama yaitu proses pengambilan bukti digital. Proses ini menggunakan teknik *live forensics* untuk mendapatkan bukti digital percakapan Telegram yang terdapat pada RAM. Pada penelitian ini mengguna FTK Imager sebagai *tools live forensics* karena FTK Imager mendukung teknik *live forensics* yaitu fitur *Capture Memory.* Fitur tersebut dapat mengambil data dan informasi yang terdapat pada RAM, termasuk data percakapan Telegram. Gambar 3 menampilkan fitur *Capture Memory* yang terdapat pada FTK Imager.




*Gambar 3 Fitur FTK Imager*

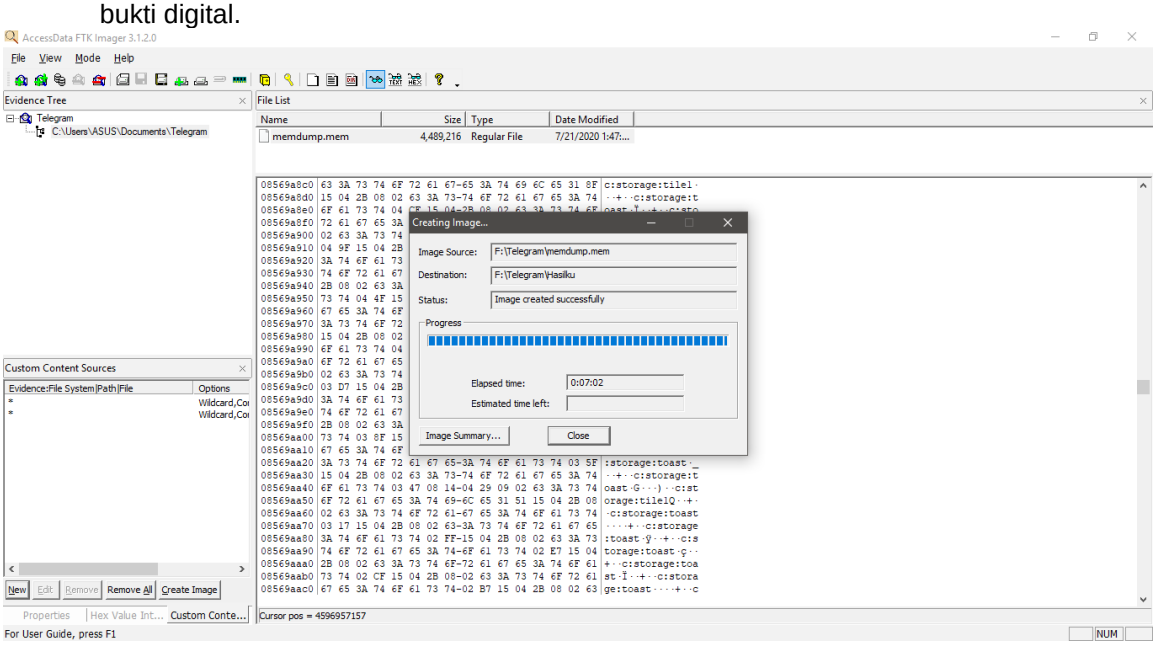
Aplikasi Telegram yang sedang berjalan pada laptop dapat digunakan untuk mengambil data dan informasi termasuk data percakapan pada Telegram yang telah dihapus dengan menggunakan FTK Imager. Gambar 4 menunjukkan proses pengambilan data pada RAM.




*Gambar 4 Proses Pengambilan Data*

Besarnya kapasitas RAM menentukan lamanya proses pengambilan data pada RAM. Proses pengambilan bukti digital akan semakin lama jika kapasitasnya besar, begitu juga sebaliknya. Hasil dari proses pengambilan data pada RAM menghasilkan file berekstensi .mem. FTK Imager menjadi salah satu *tools* yang mendukung ekstensi file ini untuk dapat membuka dan menganalisis file tersebut.

b. Tahap kedua merupakan tahap *imaging*. *Imaging* merupakan proses untuk menggandakan bukti digital yang bertujuan untuk mengurangi resiko kehilangan atau kerusakan barang bukti digital asli pada saat proses analisis. Perbedaan barang bukti digital dari proses imaging akan berdampak pada hasil analisis, maka barang bukti hasil *imaging* harus sama dengan barang bukti asli. Gambar 5 menunjukkan proses *imaging* bukti digital.

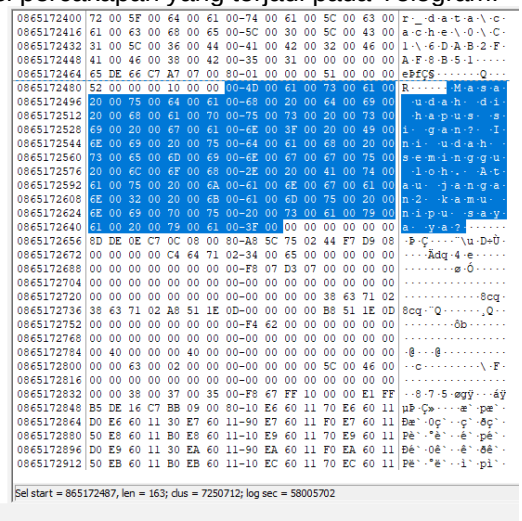



*Gambar 5 Proses Imaging*

Hasil *imaging* tersebut akan digunakan untuk proses analisis pada tahap selanjutnya. Untuk mengantisipasi kesalahan saat proses analisis, maka bukti digital yang asli akan disimpan.

### 3.2. Analisis

Proses analisis dari hasil pengambilan data yang dilakukan oleh penyidik menggunakan FTK Imager menemukan rekaman data percakapan yang terjadi pada Telegram. Data tersebut ditemukan berupa teks percakapan, seperti yang ditunjukkan pada Gambar 6. Gambar 6 menunjukkan salah satu isi percakapan yang terjadi pada Telegram.




*Gambar 3 Data Digital*

Dalam percakapan tersebut hanya ditemukan satu tipe data. Tidak ditemukan nomor telepon pengirim, nomor telepon penerima, dan waktu percakapan, hanya ditemukan teks percakapan dari data percakapan tersebut. pada percakapan yang disimulasikan terdapat 1 file gambar. Saat proses proses analisis tidak ditemukan file gambar tersebut.

Berdasarkan hasil analisis data digital, teks percakapan akan dibandingkan dengan percakapan yang terdapat pada *smartphone* korban. Hasil tersebut dapat disimpulkan bahwa isi percakapan Telegram korban dengan tersangka memiliki beberapa kesamaan, namun penyidik harus menyelidiki lebih lengkap lagi untuk memastikan apakah data percakapan tersebut dapat digunakan sebagai barang bukti digital dalam kasus penipuan *online shop.*

*Table 1 Perbandingan Percakapan*

| Offset | Isi Percakapan | Kesimpulan |
|---|---|---|
| 0164562832 | Masih ready gan? | Sama dan terbukti |
| 0935959216 | Masih kak, mau ukuran berapa? | Sama dan terbukti |
| - | Ukuran XL gan. Boleh tau detail sizenya gak? | Tidak ditemukan |
| - | Ukuran XL: PB 140, LB 110 | Tidak ditemukan |
| - | Harganya berapa ya gan? | Tidak ditemukan |
| - | Harganya 240.000 kak | Tidak ditemukan |
| 0206256096 | Oke gan. Langsungku order | Tidak ditemukan |
| 0206256192 | No rekening 5423-02-021097-54-6 An. Salma Azizah | Tidak ditemukan |
| 0206256416 | Kirim alamat lengkapnya kak | Sama dan terbukti |
| 11127ca0 | Nama: Nurma Erlyna<br>Alamat: Bukit Rivaria Indah, blok b, no 108 rt5/12, sawangan, Depok | Sama dan terbukti |
| 1351500736 | Sudah ku transfer gan. Berapa hari paketnya sampe gan? | Sama dan terbukti |
| - | Kira" 3 sampai 4 hari kak. Ditunggu aja, makasih | Tidak ditemukan |
| - | Gan boleh minta resinya? Kok paket udah seminggu blm sampe ya? | Tidak ditemukan |

| | | |
|---|---|---|
| - | Resinya udah aku hapus kak, kemarin kan udah aku kirim resinya | Tidak ditemukan |
| 0865172480 | Masa udah di hapus si gan? Ini udah seminggu loh. Atau jangan2 kamu nipu saya ya? | Sama dan terbukti |
| - | Beneran kemarin udah saya kirim kak, gak percaya kalo udah saya kirim ya kak | Tidak ditemukan |
| - | Ya gimana gan, buktinya paket aja ga sampe. Kalo ga gini aja deh, balikin aja uang saya | Tidak ditemukan |
| 1290330544 | Maaf banget kak, uang yang udah dikirim gak bisa dikembalikan, mungkin paketnya nyasar di tengah jalan | Sama dan terbukti |
| - | Gw laporin polisi lu gan | Tidak ditemukan |
| - | Terserah, saya gak takut polisi, gak ada bukti juga | Tidak ditemukan |

## 4. Kesimpulan

Teknik *live forensics* dapat diterapkan untuk mendapatkan bukti digital pada Telegram berbasis desktop dengan sistem operasi Windows 10 menggunakan FTK Imager, meskipun data yang dihasilkan tidak sama persis dengan data percakapan yang terdapat pada *smartphone* korban.

Untuk penelitian selanjutnya diharapkan hasil data yang didapatkan lebih akurat dengan data asli. Untuk mendukung *live forensics* dapat dikombinasikan dengan *tools* yang lebih berkualitas sehingga hasil data yang didapatkan dapat memudahkan penyidik mengungkap tindak kejahatan yang terjadi.

## Referensi

[1] M. S. Asyaky, “Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android,” *J. Penelit. Tek. Inform.*, vol. Vol. 3 No, no. 1, pp. 220–231, 2019.

[2] J. Gregorio, B. Alarcos, and A. Gardel, “Forensic analysis of Telegram Messenger Desktop on MacOS,” vol. 6, no. 8, pp. 39–48, 2018.

[3] J. Gregorio, A. Gardel, and B. Alarcos, “Forensic analysis of Telegram Messenger for Windows Phone,” *Digit. Investig.*, vol. 22, pp. 88–106, 2017, doi: 10.1016/j.diin.2017.07.004.

[4] H. K. Mann, “Volatile Memory Forensics : A Legal Perspective,” vol. 155, no. 3, pp. 11–15, 2016.

[5] D. S. Yudhistira, I. Riadi, and Y. Prayudi, “Live Forensics Analysis Method For Random Access Memory On Laptop Devices,” no. May, 2018.

[6] I. Riadi and A. Firdonsyah, “Identification Of Digital Evidence On Android ’ s Blackberry Messenger Using Identification Of Digital Evidence On Android ’ s Blackberry Messenger Using NIST Mobile,” no. June, pp. 1–7, 2017.

[7] M. N. Faiz and P. N. Cilacap, “ANALISIS LIVE FORENSICS UNTUK PERBANDINGAN KEMANANAN EMAIL,” no. April, 2017, doi: 10.33096/ilkom.v8i3.79.242-247.

[8] M. I. Mazdadi, “Live Forensics on RouterOS using API Services to Investigate Network Attacks,” no. March, 2017.

[9] T. Rochmadi, “Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser,” no. October, 2017.

[10] R. Umar, A. Yudhana, and M. N. Faiz, “ANALISIS KINERJA METODE LIVE FORENSICS UNTUK INVESTIGASI RANDOM ACCESS MEMORY PADA SISTEM PROPRIETARY,” pp. 207–211.

[11] R. Kaur and A. Kaur, “Digital Forensics,” *Int. J. Comput. Appl.*, vol. 50, no. 5, pp. 5–9, 2012, doi: 10.5120/7765-0844.

[12] A. Yudhana, I. Riadi, and I. Anshori, “Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist,” *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.