
# Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop

Danang Sri Yudhistira

13917111

*Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer*

*Konsentrasi Digital Forensik*

*Program Studi Magister Teknik Informatika*

*Program Pascasarjana Fakultas Teknologi Industri*

*Universitas Islam Indonesia*

*2018*

## Lembar Pengesahan Pembimbing

**Lembar Pengesahan Pembimbing**

**Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop**

Danang Sri Yudhistira

13917111

Yogyakarta, April 2018

Pembimbing

Dr. Imam Riadi, M.Kom

**Lembar Pengesahan Penguji**

**Lembar Pengesahan Penguji**

**Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop**

Danang Sri Yudhistira

13917111

Yogyakarta, April 2018

Tim Penguji,

Dr. Imam Riadi, M.Kom
Ketua

Yudi Prayudi, S.Si.,M.Kom
Anggota I

Dr. Bambang Sugiantoro, M.T
Anggota II

Mengetahui,
Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST., M.Sc

## Abstrak

### Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop

Perkembangan teknologi komputer sekarang ini berdampak pada meningkatnya kasus kejahatan cyber crime yang terjadi baik secara langsung ataupun tak langsung. Kasus cyber crime sekarang ini mampu mencuri informasi digital yang bersifat sensitif dan rahasia. Informasi tersebut dapat berupa user_id, email dan password. Selain tersimpan di cookies browser pada harddisk komputer atau laptop, user_id, email dan password tersebut juga tersimpan pada random access memory (RAM).

Random access memory (RAM) bersifat volatile sehingga dalam melakukan analisa diperlukan metode yang tepat dan efektif. Metode akuisisi data digital pada random access memory dapat dilakukan secara live forensics atau ketika sistem sedang berjalan. Hal ini dilakukan karena jika perangkat komputer atau laptop sudah mati atau shutdown maka informasi yang tersimpan dalam random access memory akan hilang.

Dalam penelitian ini telah dilakukan akuisisi random access memory (RAM) untuk mendapatkan informasi hak akses login berupa user_id, email dan password pada laman website seperti facebook, internet banking, paypal, bitcoin, dan gmail. Tools yang digunakan untuk melakukan akuisisi data yaitu Linux Memory Extractor (LiME) dan FTK Imager.



**Kata kunci**

Live forensics, RAM, laptop, devices

## Abstract

Live Forensics Analysis Method For Random Access Memory
On The Laptop Devices

The development of computer technology now have an impact on the increasing cases of cyber crime crime that occurred either directly or indirectly. Cases of cyber crime now is able to steal digital information is sensitive and confidential. Such information may include email, user_id and password. In addition to browser cookies stored on your computer or laptop harddrive, user_id, email and password are also stored in random access memory (RAM).

Random access memory (RAM) is volatile so that in doing the analysis required an appropriate and effective method. Digital data acquisition method in random access memory can be done live forensics or when the system is running. This is done because if the device or laptop computer is dead or shutdown then the information stored in random access memory will be lost.

In this research has been carried out the acquisition of random access memory (RAM) to get the login permissions information in the form of email, user_id and password on your website such as facebook, paypal, internet banking, bitcoin, and gmail. Tools used to perform data acquisition is Linux Memory Extractor (LiME) and FTK Imager.



Keywords :
Live forensics, RAM, laptop, devices.

# Pernyataan Keaslian Tulisan

**Pernyataan Keaslian Tulisan**

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, April 2018


Danang Sri Yudhistira, S.Kom

## Daftar Publikasi

Tidak ada publikasi yang menjadi bagian dari tesis.

## Halaman Kontribusi

Tidak ada kontribusi dari pihak lain.

## Halaman Persembahan

Segala Puji bagi Allah SWT, ku panjatkan puji syukurku hanya kepada-Mu yang telah memberikan rahmat dan hidayah serta memberikan kesehatan, kekuatan dan kesabaran sehingga pada akhirnya aku bisa menyelesaikan Thesis ini dengan baik.

- Terima kasih kepada Bapak dan Ibu tercinta yang selalu dan tidak pernah bosan memberikan semangat dan motivasi untuk terus belajar. Doamu selalu menyertaiku.
- Terima kasih kepada Bapak Yudi Prayudi dan Bapak Imam Riadi selaku dosen pembimbing yang telah dengan sabar membimbing saya sampai terselesaikannya Thesis ini.
- Untuk teman teman seperjuangan yang selalu saling support dan mau sharing berbagi ilmu. Kalian luar biasa Kawan.
- Special ucapan terima kasih untuk Nurul Hidayati (Thankyou Dear for love and always support me).
- Terima kasih untuk  Geng Bolo Kurowo yang selalu stanby diajak Piknik jika sudah pusing memikirkan Thesis.

## Kata Pengantar

Alhamdulillah, segala puji syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan ridho-NYA, sehingga tesis dengan judul "Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop" ini dapat diselesaikan.

Tesis ini disusun untuk memenuhi salah satu persyaratan memperoleh gelar Magister Komputer (M.Kom.) pada program studi Magister Teknik Informatika Universitas Islam Indonesia dengan sumber dana berasal dari dana mandiri.

Oleh karena itu, pada kesempatan ini penulis menyampaikan rasa hormat dan menghaturkan terima kasih yang sebesar-besarnya, kepada :

1. Bapak Yudi Prayudi, S.Si.Kom atas bimbingan, arahan dan waktu yang diluangkan kepada penulis untuk berdiskusi selama menjadi dosen pembimbing. Terima kasih juga karena selalu memberikan motivasi kepada saya sehingga saya mampu menyelesaikan tesis ini.
2. Bapak Dr. Imam Riadi, M.Kom,. Bapak Dr. Bambang Sugiantoro yang telah memberikan masukan dan saran seminar proposal dan seminar hasil tesis.
3. Ketua Program Studi Pasca Sarjana Fakultas Teknik Industri Bapak Dr. R. Teduh Dirgahayu, ST., M.Sc.
4. Seluruh dosen Pasca Sarjana Program Studi Magister Teknik Informatika khususnya jurusan Digital Forensik.
5. Ayahanda Supardi, Ibunda Marjiyem, My Honey Nurul Hidayati dan seluruh keluarga besar atas segala doa dan supportnya.
6. Bapak Komarudin yang atas training dan sharing ilmunya di Solo.
7. Rekan rekan seperjuangan Grub "Wisuda Bersama". Kalian memang luar biasa kawan.
8. Kepada semua pihak yang sudah membantu yang tidak dapat saya sebutkan satu persatu.

Dengan keterbatasan pengalaman, ilmu maupun pustaka yang ditinjau, penulis menyadari bahwa tesis ini masih banyak kekurangan dan perlu pengembangan lanjutan agar benar benar bermanfaat. Oleh sebab itu, penulis sangat mengharapkan kritik dan saran agar tesis ini lebih sempurna serta sebagai masukan bagi penulis untuk penelitian dan penulisan karya ilmiah di masa yang akan datang.

Akhir kata, penulis berharap tesis ini memberikan manfaat bagi kita semua terutama untuk pengembangan ilmu pengetahuan dalam bidang digital forensik.

Yogyakarta, 2 April 2018

Danang Sri Yudhistira, S.Kom

## Daftar Isi

# Daftar Tabel

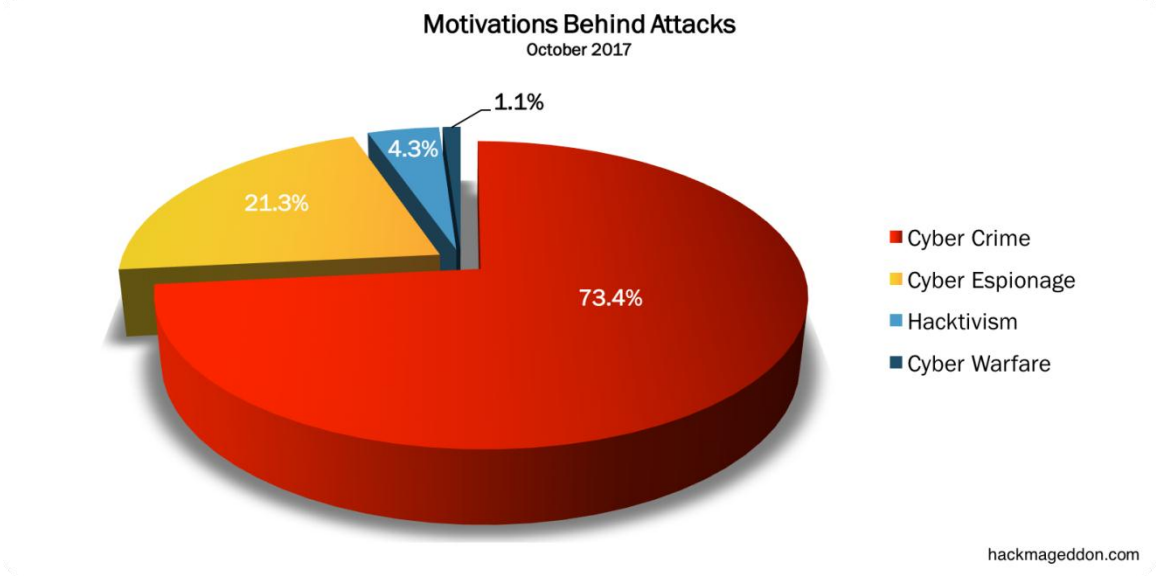
## Daftar Gambar

# BAB 1
# Pendahuluan

## 1.1 Latar Belakang Masalah

Perkembangan teknologi komputer sekarang ini semakin meningkat. Seiring meluasnya penggunaan komputer maka dimungkinkan peluang kejahatan yang melibatkan komputer juga akan semakin meningkat baik secara langsung maupun tidak langsung. Untuk menanggulangi peristiwa tersebut selain dibutuhkan manajemen keamanan yang bertujuan untuk mencegah, diperlukan pula prosedur penanggulangan apabila peristiwa sudah terlanjur terjadi, dimana salah satu prosedur yang dilakukan adalah komputer forensik. Komputer forensik adalah investigasi serta teknik analisis komputer yang melibatkan tahapan identifikasi, persiapan, ekstraksi, dokumentasi dan interpretasi dari data yang ada di komputer yang nantinya dapat berguna sebagai bukti dari peristiwa cyber crime.

Cyber Crime saat ini masih mendominasi dalam peristiwa kejahatan yang terjadi di dunia dibandingkan dengan serangan lain yang melibatkan tindak kejahatan dengan bukti digital. Menurut stastistik yang dikeluarkan oleh hackmageddon, serangan cyber crime masih paling sering terjadi dibandingkan serangan lainnya. Secara lebih jelas persentase seragan tercantum pada Gambar 1.1 :




Gambar 1.1 Cyber Attack Statistic

Berdasarkan hasil analisa serangan seperti yang tercantum Gambar 1.1 diketahui bahwa serangan cyber crime masih mendominasi dengan 84.6 %, cyber espionage 9.9%, hacktivism 4.3%, dan cyber warfare 1.1 %. Dengan semakin meningkatnya serangan cyber crime, perlu dilakukan tindakan pencegahan guna melindungi data data informasi penting milik kita.

Kasus cyber crime yang terjadi sekarang ini sudah mengarah ke pencurian user_id, email dan password yang merupakan informasi pribadi bersifat sensitive bagi sebagian orang. Informasi user_id, email dan password tersebut seperti pada account facebook, internet banking, paypal, bitcoin dan lain sebagainya. User_id, email dan password tersebut bisa saja disalahgunakan oleh orang lain yang tidak bertanggung jawab yang bisa berdampak merugikan. Akibat dari pencurian user_id dan password ini, bisa saja terjadi pencemaran nama baik jika yang dicuri merupakan account social media, sedangkan jika yang dicuri merupakan account internet banking maka dimungkingkan terjadi tindak pidana pencurian uang melaui transfer internet banking ke rekening lain atau pun dengan cara pembebanan biaya kepada si pemilik sah account user_id dan password jika account tersebut digunakan untuk transaksi illegal dengan mengatasnamakan si pemilik sah account internet banking akan tetapi alamat pengiriman ditujukan ke alamat si pencuri.

Informasi berupa user_id, email dan password selain tersimpan pada cookies browser yang kita gunakan untuk melakukan hak akses pada perangkat laptop atau komputer, juga tersimpan didalam random access memory perangkat tersebut. Untuk itu diperlukan teknik atau metode yang tepat guna melakukan analisis terhadap random access memory pada perangkat laptop. Hal ini dikarenakan data yang ada di random access memory bersifat volatile. Data akan hilang jika computer dimatikan atau mengalami restart. Akuisisi informasi digital yang ada dirandom access memory hanya bisa dilakukan ketika sistem sedang berjalan (Dave, Mistry, & Dahiya, 2014).

Data volatile yang tersimpan dalam random access memory menggambarkan seluruh kegiatan yang sedang terjadi pada sistem komputer atau laptop yang sedang digunakan. Penanganan data pada random access memory harus hati-hati sebab selain datanya dapat hilang jika sistem dimatikan, penggunaan tools akan meninggalkan footprint yang kemungkinan dapat menimpa bukti berharga yang ada ada di dalam random access memory. Oleh karena itu diperlukan metode yang tepat guna yaitu metode live forensics yang mampu menjamin integritas data volatile tanpa menghilangkan data yang berpotensi menjadi barang bukti.

Dengan kerawanan tersebut, telah banyak menginspirasi developers untuk mengembangkan metode beserta tools yang dapat digunakan untuk menganalisis random access memory. Salah satunya dalam sistem operasi Linux (Anand, 2016). Didalamnya terdapat berbagai macam tools yang bisa digunakan untuk hacking dan juga forensik. Selain itu ada juga beberapa tools untuk akuisisi memory yang bisa digunakan di sistem operasi windows.

Namun apakah semua metode dan tools yang telah diciptakan memang layak digunakan untuk melakukan analisis forensics memory? Oleh karenanya diperlukan penelitian yang dapat memberikan gambaran mengenai kinerja metode tersebut serta akan lebih baik jika bisa memberikan rekomendasi metode terbaik yang dapat digunakan oleh investigator dalam melakukan analisa terhadap barang bukti di random access memory.

## 1.2 Permasalahan

Berdasarkan latar belakang yang telah dipaparkan terdapat beberapa permasalahan yang terjadi diantaranya : belum diketahui cara mendapatkan akses untuk melakukan capture data yang tersimpan dalam random access memory pada perangkat laptop; belum dilakukan investigasi secara live forensics dalam melakukan akusisi data random access memory; data apa saja yang tersimpan di random access memory yang bisa dijadikan sebagai barang bukti digital.

## 1.3 Rumusan Masalah

Berdasarkan uraian latar belakang masalah yang telah diuraikan diatas, maka dibuat rumusan permasalahan sebagai berikut :

1. Bagaimana cara melakukan akuisisi data dengan metode live forensics pada random access memory di perangkat laptop ?
2. Informasi artefak digital apa saja yang tersimpan pada random access memory yang bisa dijadikan sebagai barang bukti digital oleh investigator ?

## 1.4 Batasan Masalah

Untuk lebih memfokuskan penelitian yang sedang dilakukan agar sesuai dengan rumusan masalah yang telah dijelaskan diatas, maka peneliti memberikan batasan masalah dalam penelitian sebagai berikut :

1. Menganalisa random access memory pada perangkat laptop berbasis linux dan windows.
2. Kegiatan akuisisi data pada random access memory dilakukan secara live forensics.

3. Tools menggunakan Linux Memory Extractor (LiME) dan FTK Imager.
4. Fokus analisis bukti digital yang ingin dicari pada random access memory yaitu informasi mengenai user_id, email dan password pada facebook, internet banking, paypal, account gmail dan bitcoin.

## 1.5 Tujuan Penelitian

Adapun tujuan penelitian yang ingin dicapai dalam penelitian ini yaitu :

1. Mencari dan menemukan informasi artefak yang tersimpan pada random access memory pada perangkat laptop.
2. Mengetahui tahapan / langkah-langkah dalam proses akuisisi bukti digital yang terdapat pada random access memory di perangkat laptop berbasis linux dan windows dengan menggunakan metode live forensics.

## 1.6 Manfaat Penelitian

Berdasarkan latar belakang, rumusan masalah, batasan masalah dan tujuan dari penelitian yang telah disampaikan pada bagian sebelumnya, adapun manfaat penelitian yang ingin dicapai dalam penelitian ini yaitu :

1. Memudahkan investigasi dalam menemukan informasi digital baik berupa user_id, email, dan password serta informasi digital lainnya yang tersimpan dalam random access memory pada perangkat laptop.
2. Berkontribusi dalam penanganan barang bukti digital yang tersimpan di random access memory pada perangkat laptop.

## 1.7 Review Penelitian

Pada bagian ini akan dibahas ulasan tentang penelitian yang telah dilakukan sebelumnya berkaitan dengan penelitian yang akan dilakukan mengenai metode live forensics untuk analisis random access memory pada perangkat laptop.

Pada penelitian yang dilakukan oleh (Faiz, 2017), dijelaskan tentang perbandingan beberapa tools yang digunakan secara live forensics untuk analisis data. Faktor yang menjadi acuan dalam perbandingan tersebut yaitu kemampuan penggunaan memory, waktu, jumlah langkah dan akurasi paling baik dalam melakukan live forensics.

Pada penelitian yang dilakukan oleh (Anand, 2016) dilakukan akses ke random access memory untuk menemukan logs, informasi tentang sistem yang sedang berjalan, user yang sedang login, namun masih terkendala kernel module yang belum sesuai atau

belum cocok. Untuk itu pada paper ini menjabarkan bagaimana cara menemukan informasi digital dengan melakukan akses ke random access memory laptop.

Pada penelitian sebelumnya yang dilakukan oleh (Nisbet, 2016) menjelaskan bahwa akusisi data yang terdapat pada laptop biasanya dilakukan hanya untuk mengakuisisi harddisk namun kali ini bisa dilakukan untuk mengakuisisi random access memory. Dalam penelitian ini dikhususkan untuk meneliti file yang terenkripsi.

Fokus lain dari penelitian tentang akuisisi random access memory dengan metode live forensics pada perangkat laptop berbasis linux tidak hanya pada account yang tersimpan pada random access memory saja, melainkan pada kernel /boot/config-3.13.0-61-generic. Untuk bisa menjalankan perintah kernel tersebut harus melalui kompilasi dengan spesifikasi random access memory. Akuisisi random access memory pada laptop linux tidak semudah yang dibayangkan karena haruslah memakai perintah command line dalam menjalankannya. (Socała & Cohen, 2016).

Pada penelitian yang dilakukan oleh (Gruhn & Freiling, 2016) membahas tentang teknik akuisisi memory dengan menggunakan 12 tools berbeda. Spesifikasi komputer untuk akusisi data menggunakan sistem operasi windows 7 64 bit, i5 2400 dan RAM 2GB. Dalam penelitian ini ditemukan kendala pada ProcDump yang menghambat proses akusisi data sehingga integritas capture memory kurang sempurna.

Pada penelitian lain yang dilakukan oleh (Stüttgen, Vömel, & Denzel, 2015) tidak lagi berfokus pada sistem kernel yang digunakan untuk akusisi memory. Melainkan pada firmware yang belakangan ini menjadi sasaran dalam serangan malware. Firmware juga digunakan untuk mengenali program berbahaya yang sudah terinstal dalam sistem operasi linux.

Penelitian dengan metode live forensics untuk menganalisa random access memory membutuhkan kecermatan dalam menemukan bukti digital yang ada. Terdapat komplektifitas dalam mempelajari random access memory. Untuk mempermudah dalam penanganan metode live forensics serta menjaga nilai integritas barang bukti maka akan diakses dengan bahasa python scripting (Bharath & R, 2015).

Penelitian lain mengenai analisis random access memory pada perangkat laptop berbasis linux dengan metode live forensics selain digunakan untuk menganalisa password yang tersimpan pada random access memory juga digunakan untuk analisa malware. Penelitian mengenai computer forensics tidak lagi terfokus pada analisa harddisk saja (Dave et al., 2014).

Investigasi forensik yang dilakukan secara live forensics memudahkan investigator dalam mengbongkar sebuah kasus yang melibatkan barang bukti dalam jumlah banyak dan mempunyai kapasitas penyimpanan yang lebih 1 TB. Investigator hanya fokus bagaimana mengumpulkan data yang diduga sebagai bukti digital. Tidak semua data dikumpulkan melainkan hanya metadata saja. Metode live forensics sangat memudahkan dalam penelitian random access memory (Panchal, 2013).

Pada penelitian sebelumnya dilakukan perbandingan antara tradisional forensik dan live forensics. Diketahui live forensics lebih banyak memberikan keuntungan. Akuisisi data live forensics tidak perlu melakukan cloning data yang punya kapasitas penyimpanan besar (Gupta, 2013).

Penelitian lain yang dilakukan oleh (Vömel, 2013) menjelaskan tentang teknik akusisi data pada random access memory guna mendapatkan gambaran tentang bagaimana melakukan perlindungan terhadap data pribadi yang tersimpan di random access memory dikarenakan sudah banyak akses ilegal yang mencoba mendapatkan informasi pribadi tersebut. Penelitan ini juga mengembangkan tools RKfinder dengan algoritma untuk memeriksa integritas data dan mendeteksi adanya indikasi ancaman pada sistem komputer.

Pada penelitian yang dilakukan oleh (Divyang Rahevar, 2013) membuktikan bahwa random access memory menyimpan informasi yang bersifat sensitive seperti contohnya user_id dan password. Karena informasi ini bersifat sensitive atau private maka akan sangat merugikan jika hak akses atas informasi tersebut disalahgunakan oleh orang yang tidak berhak.

(Richard Carbone, 2012) melakukan penelitian untuk menguji 2 tools yaitu LiME dan Fmem untuk mendapatkan hasil perbandingan dalam melakukan akuisisi random access memory pada perangkat pc berbasis sistem operasi linux dengan menggunakan framework volatility memory analysis.

Penelitian lain dilakukan oleh (Karayianni & Katos, 2012) dengan melakukan penyelidikan tentang data yang bersifat privasi menyangkut informasi data pribadi. Informasi tersebut berupa password yang tersimpan didalam random access memory. Proses analisa pada random access memory dilakukan ketika komputer dalam kondisi beroperasi atau running karena jika komputer dalam kondisi mati maka data yang tersimpan didalam random access memory akan menghilang.

Rangkuman dari literature review terhadap penelitian-penelitian yang telah dilakukan, secara singkat dapat dilihat pada Tabel 1.1

Tabel 1.1 Literatur Review

| No | Paper Utama | RAM | OS Linux | Live Forensics | OS Windows | Yang Diuji | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Email | Password | User_id | Link Url | Lainnya |
| 1 | (Anand, 2016) | √ | √ | - | - | - | - | - | - | Log, system informasi |
| 2 | (Nisbet, 2016) | √ | - | - | - | - | - | - | - | File Enkripsi |
| 3 | (Socała & Cohen, 2016) | √ | √ | √ | - | - | - | - | - | Kernel /boot/config-3.13.0-61-generic |
| 4 | (Stüttgen et al., 2015) | √ | √ | √ | - | - | - | - | - | Firmware |
| 5 | (Bharath & R, 2015) | √ | - | √ | - | - | - | - | - | Python scripting |
| 6 | (Dave et al., 2014) | √ | √ | √ | - | √ | √ | √ | - | Malware |
| 7 | (Panchal, 2013) | √ | - | √ | - | - | - | - | | Metadata |
| 8 | (Divyang Rahevar, 2013) | √ | | √ | √ | - | √ | √ | - | - |
| 9 | (Richard Carbone, 2012) | √ | √ | √ | - | - | - | - | - | Memory Analysis Framework |
| 10 | (Karayianni & Katos, 2012b) | √ | - | - | - | - | √ | - | - | - |
| Usulan Penelitian | | Peneliti akan melakukan akuisisi pada random access memory di perangkat laptop berbasis OS Linux dan OS Windows secara live forensics. | | | | Yang akan dijadikan fokus penelitian adalah untuk menguji apakah didalam random access memory menyimpan informasi terkait user_id,email, password, dan informasi digital lainnya. | | | | |

Berbeda dengan penelitian terdahulu, dalam penelitian ini berada pada kategori analisis random access memory dengan metode live forensics.

Paparan singkat mengenai penelitian ini tertulis pada tabel 1.2 tentang penelitian yang diusulkan :

Tabel 1.2 Penelitian Yang Diusulkan

| Judul | Uraian Singkat Masalah Penelitian | Solusi | Hasil Yang Diharapkan |
|---|---|---|---|
| Metode Live Forensics Untuk Analisa Random Access Memory Pada Perangkat Laptop | Bagaimana cara mengambil dan mengolah data informasi yang tersimpan dirandom access memory pada perangkat laptop berbasis sistem operasi linux dan windows dengan kondisi perangkat on power atau menyala. | 1. Akusisi data menggunakan Linux Memory Extractor (LiME) yang bisa melakukan capture data secara lengkap<br>2. Akusisi data dilakukan secara live forensics.<br>3. Analisa data menggunakan tools FTK Imager. | Memberikan gambaran secara jelas tentang cara akuisisi random access memory pada perangkat laptop berbasis linux dan windows dan hasil apa saja yang bisa didapatkan. |

## 1.8 Metodologi Penelitian

Adapun langkah langkah yang akan ditempuh selama melakukan penelitian ini adalah sebagai berikut :

1. Studi Pustaka

Penelitian ini dilakukan dengan melakukan studi kepustakaan yaitu dengan mengumpulkan bahan bahan referensi yang terkait dengan penelitian, baik melalui buku, artikel, paper, jurnal, makalah, dan mengunjungi beberapa situs yang terdapat pada internet terkait dengan random access memory, live forensics, linux, windows, user_id, email dan password serta beberapa referensi lain yang dapat menunjang kegiatan penelitian yang dilakukan.

2. Persiapan Alat dan Bahan Penelitian

Tahapan ini melakukan persiapan tools yang akan dipakai untuk melakukan analisa live forensics pada perangkat laptop.

3. Skenario Kasus

Tahapan ini melakukan pembuatan skenario dengan beberapa simulasi kasus yang dapat dihadapi dalam melakukan random access memory forensics.

4. Simulasi Kasus

Tahapan simulasi kasus yaitu melakukan akuisisi random access memory dengan teknik live forensics yang berkaitan tentang suatu kasus.

5. Olah TKP

Pada tahapan ini dilakukan olah tempat kejadian perkara dan pengamanan terhadap barang bukti yang ditemukan.

6. Akuisisi Data

Tahap akuisisi pada penelitian ini dilakukan secara live forensics, untuk melakukan akuisisi secara langsung pada perangkat laptop.

7. Analisis Hasil

Pada tahapan ini dilakukan analisa terhadap hasil capture memory yang sudah dilakukan pada random access memory laptop.

8. Laporan

Tahapan ini melakukan pembahasan dan pembuatan laporan atas hasil yang telah diperoleh pada tahap analisis.

## 1.9 Sistematika Penulisan

Tahapan ini merupakan gambaran secara umum terkait sistematika penulisan, Dengan tujuan memberikan gambaran secara ringkas terkait kerangka penulisan.

BAB I Pendahuluan

Tahapan ini merupakan tahapan awal yang dilakukan dalam penelitian. Pada tahapan ini berisikan penjelasan terkait latar belakang masalah penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II Landasan Teori

Pada tahapan ini berisikan penjelasan mengenai beberapa teori yang mendukung penelitian yang sedang dilakukan. Teori tersebut terkait Random Access Memory, Live Forensics, Linux, Windows, Email, Username, Password dan Link Url.

BAB III Metodologi Penelitian

Bab ini berisikan gambaran secara umum tentang analisa yang dilakukan terhadap proses dan mekanisme live forensics, serta melakukan implementasi terhadap akuisisi data pada random access memory perangkat laptop.

BAB IV Hasil dan Pembahasan

Pada tahapan ini membahas tentang hasil implementasi dari proses akuisisi data pada random accces memory di perangkat laptop dengan menggunakan metode live forensics.

BAB V Kesimpulan dan Saran

Tahapan ini merupakan tahapan akhir yang dilakukan peneliti dengan memaparkan kesimpulan dari keseluruhan uraian pada setiap bab sebelumnya, serta saran untuk pengembangan penelitian berikutnya.

Daftar Pustaka

Daftar pustaka berisi referensi yang terkait dengan penelitian, baik melalui buku, artikel, paper, jurnal, makalah, situs yang terkait yang dapat menunjang kegiatan penelitian yang dilakukan.

# BAB 2

# Tinjauan Pustaka

## 2.1 Komputer

Istilah komputer (computer) berasal dari bahasa Latin computare yang berarti alat hitung. Karena awalnya komputer lebih digunakan sebagai perangkat bantu dalam hal perhitungan angka angka sebelum akhirnya menjadi perangkat multifungsi. Berikut ini definisi komputer yang didapat dari beberapa buku komputer.

Menurut buku Computer Annual (Robert H.Blissmer), komputer adalah suatu alat elektronik yang mampu melakukan beberapa tugas sebagai berikut :

1. Menerima input
2. Memproses input tadi sesuai dengan programnya
3. Menyimpan perintah-perintah dan hasil dari pengolahan
4. Menyediakan output dalam bentuk informasi2

Menurut buku Computer Today (Donald H.Sanders), komputer adalah sistem elektronik untuk memanipulasi data yang cepat dan tepat serta dirancang dan diorganisasikan supaya secara otomatis menerima dan menyimpan data input, memprosesnya, dan menghasilkan output dibawah pengawasan suatu langkah langkah instruksi instruksi program yang tersimpan di memori (stored program).

Menurut buku Computer Organization (VC. Hamacher, ZG. Vranesic, SG.Zaky), komputer adalah mesin penghitung elektronik yang cepat dapat menerima informasi input digital, memprosesnya sesuai dengan suatu program yang tersimpan di memorinya (stored program) dan menghasilkan output informasi

Dari beberapa definisi yang didapat dari berbagai buku, dapat disimpulkan bahwa komputer adalah :

1. Alat elektronik
2. Dapat menerima input data
3. Dapat mengolah data
4. Dapat memberikan informasi
5. Menggunakan suatu program yang tersimpan di memori computer (stored program)
6. Dapat menyimpan program dan hasil pengolahan
7. Bekerja secara otomatis

## 2.2 Sistem Operasi

Sistem Operasi (Operating System) adalah komponen pengolah peranti lunak dasar (essential component) tersistem sebagai pengelola sumber daya perangkat keras komputer, dan menyediakan layanan umum untuk aplikasi perangkat lunak. Sistem operasi adalah jenis yang paling penting dari perangkat lunak sistem dalam sistem komputer. Tanpa sistem operasi, pengguna tidak dapat menjalankan program aplikasi pada komputer mereka, kecuali program booting.

Sistem operasi mempunyai penjadwalan yang sistematis mencakup perhitungan penggunaan memori, pemrosesan data, penyimpanan data, dan sumber daya lainnya. Secara umum sistem operasi dibagi menjadi beberapa bagian, antara lain:

1. Booting, meletakan karnel kedalam memori
2. Kernel, bagian inti dari sebuah sistem operasi
3. Command Interpreter atau shell, membaca input dari pengguna
4. Pustaka-pustaka, menyediakan kumpulan fungsi dasar dan standar yang dapat dipanggil oleh perangkat lunak lain

Untuk fungsi-fungsi perangkat keras seperti sebagai masukan dan keluaran dan alokasi memori, sistem operasi bertindak sebagai perantara antara program aplikasi dan perangkat keras komputer, meskipun kode aplikasi biasanya dieksekusi langsung oleh perangkat keras dan seringkali akan menghubungi sistem operasi atau terputus oleh itu. Ada beberapa definisi yang dapat diberikan untuk sistem operasi, antara lain :

1. Software yang mengontrol hardware, hanya berupa program biasa. Seperti : beberapa file pada DOS (Disk Operating System).
2. Program yang menjadikan hardware lebih mudah untuk digunakan.
3. Kumpulan program yang mengatur kerja hardware. Seperti : permintaan user.
4. Resource manager/Resource allocator. Seperti : mengatur memori, printer, Dll.
5. Sebagai program pengenal. Program yang digunakan untuk mengontrol program yang lainnya.
6. Sebagai Kernel, yaitu program yang terus menerus berjalan selama computer dihidupkan.
7. Sebagai Guardian, yaitu mengatur atau menjaga komputer dari berbagai kajahatan komputer.

Dalam pemakaian sehari hari sistem operasi berfungsi mengatur jalannya sumber daya perangkat dalam kebutuhan sehari hari. Berikut merupakan berbagai macam sistem operasi yang sering digunakan dalam keseharian kita seperti pada Gambar 2.1 :


Gambar 2.1 Berbagai Macam Sistem Operasi Komputer

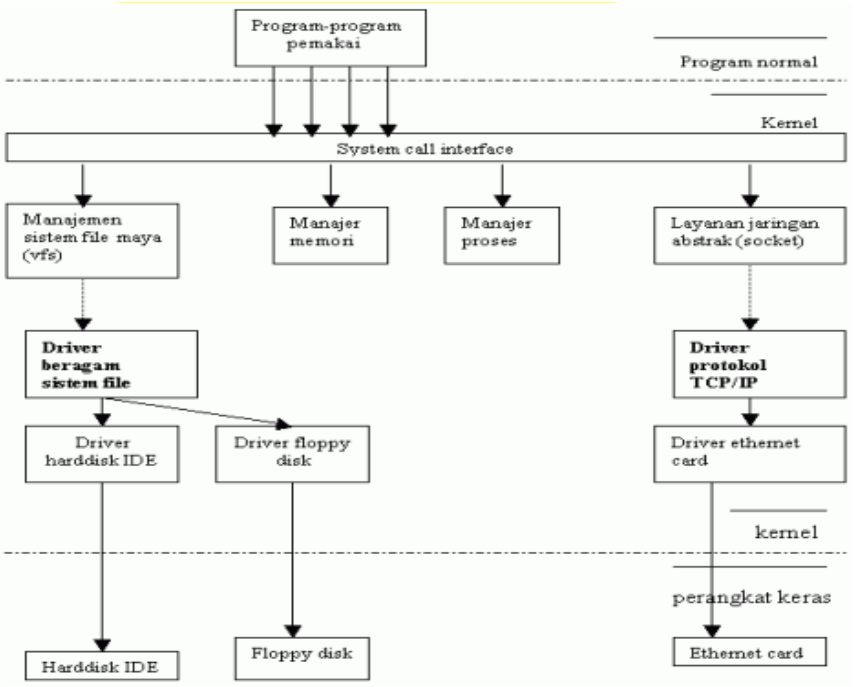
Sistem operasi dilihat dari metode pengembangannya sendiri bisa dibagi menjadi dua. Pertama adalah sistem operasi dengan metode pengembangan tertutup seperti Windows dimana tidak bisa melihat dan mengubah source code dari sistem operasi tersebut dan yang kedua adalah sistem operasi open source dimana pengguna bisa memakai dan melihat kode penyusun dari sistem operasi tersebut. Contoh sistem operasi open source yaitu Linux, Minix dan FreeBSD.

Namun, sistem operasi free yang paling populer untuk saat ini adalah Linux. Linux bisa berjalan diatas arsitektur prosesor yang berbeda beda, dari super komputer, server, komputer pribadi, handled device sampai embedded system.

### 2.2.1 Sistem Operasi Linux

GNU/Linux adalah sistem operasi yang dibuat oleh Linus Benedict Torvalds dan disebarkan secara bebas di internet dimana orang lain bisa mengembangkan dan menggunakan untuk keperluannya sendiri. Namun, perlu dijelaskan bahwa GNU/Linux disini bisa bermakna ganda. Pertama, GNU/Linux berarti kernel linux. Pengertian kedua berarti sebuah sistem yang didalamnya sudah terdapat kernel, shell dan program pendukung lain yang siap di distribusikan dan dipakai. GNU/Linux dalam penelitian ini mengacu pada pengertian yang kedua. GNU/Linux adalah sistem operasi yang bebas dipakai, didistribusikan dan dikembangkan kembali. Oleh karena itu, GNU/Linux mempunyai banyak varian yang lebih dikenal dengan istilah distro.

Sistem operasi GNU/Linux terdiri atas kernel linux (inti), program sistem, dan beberapa program aplikasi. Kernel linux merupakan inti dari sistem operasi. Program sistem dan semua program-program lainnya yang berjalan di atas kernel disebut user mode. Perbedaan antara program sistem dan program aplikasi adalah program sistem dibutuhkan agar suatu sistem operasi dapat berjalan sedangkan program aplikasi adalah program yang dibutuhkan untuk menjalankan suatu aplikasi tertentu. Struktur system operasi linux tercantum pada Gambar 2.2 :




Gambar 2.2 Arsitektur Sistem Operasi Linux

Sistem Linux terdiri atas tiga badan kode utama, dengan isi pada barisnya merupakan implementasi UNIX paling tradisional :

1. Kernel

Kernel Linux adalah potongan orisinil dari perangkat lunak yang dibuat dari serpihan oleh komunitas Linux. Sedangkan sistem Linux merupakan gabungan dari komponen-komponen. Sistem Linux basic adalah lingkungan standar untuk aplikasi dan program user.

2. System libraries

System libraries mendefinisikan set standar dari fungsi untuk melewatkan aplikasi agar dapat berinteraksi dengan kernel. Implementasi dari fungsifungsi ini sedikit banyak ada pada fungsionalitas sistem operasi yang tidak membutuhkan hak keseluruhan atas kode kernel. System libraries menyediakan banyak tipe dari fungsionalitas. Pada level paling

sederhana, system libraries mengijinkan aplikasi untuk membuat permintaan kernel-system-service. System libraries juga menjaga dan mengoleksi argument system call dan jika diperlukan mengatur argumenargumen tersebut ke dalam suatu bentuk khusus untuk melakukan system call.

3. System utilities

System utilities adalah program yang menunjukkan tugas manajemen yang individual dan terspesialisasi. Beberapa system utilities dapat dilibatkan hanya sekali saja untuk menginisialisasi dan mengatur beberapa aspek dari sistem secara permanen, memegang tugas seperti merespon pada koneksi jaringan yang masuk. Sistem Linux termasuk di dalamnya bermacam-macam user-mode program, baik system utilities maupun user utilities. Pada system utilities terdapat seluruh program yang dibutuhkan untuk menginisialisasi sistem.

### 2.2.2 Sistem Operasi Windows

Microsoft Windows atau lebih dikenal dengan sebutan Windows merupakan sistem operasi komputer yang dikembangkan oleh Microsoft menggunakan antarmuka dengan pengguna berbasis grafik (graphical user interface). Sistem operasi ini banyak digunakan oleh kalangan masyarakat, dari kalangan menengah ke atas hingga ke bawah. Sistem operasi Windows telah berevolusi dari MS-DOS, sebuah sistem operasi yang berbasis modus teks dan command-line. Windows versi pertama, Windows Graphic Environment 1.0 pertama kali diperkenalkan pada 10 November 1983, tetapi baru keluar pasar pada bulan November tahun 1985 yang dibuat untuk memenuhi kebutuhan komputer dengan tampilan bergambar. Windows 1.0 merupakan perangkat lunak 16-bit tambahan (bukan merupakan sistem operasi) yang berjalan di atas MS-DOS (dan beberapa varian dari MS-DOS), sehingga ia tidak akan dapat berjalan tanpa adanya sistem operasi DOS. Versi 2.x, versi 3.x juga sama. Beberapa versi terakhir dari Windows (dimulai dari versi 4.0 dan Windows NT 3.1) merupakan sistem operasi mandiri yang tidak lagi bergantung kepada sistem operasi MS-DOS. Microsoft Windows kemudian bisa berkembang dan dapat menguasai penggunaan sistem operasi hingga mencapai 90%.

## 2.3 Random Access Memory

Random access memory merupakan memori yang berfungsi untuk menyimpan sementara perintah dan data pada saat sebuah program dijalankan. Perintah dan data tersebut mencakup data yang akan dibaca dari hardisk, data-data yang dimasukkan melalui alat

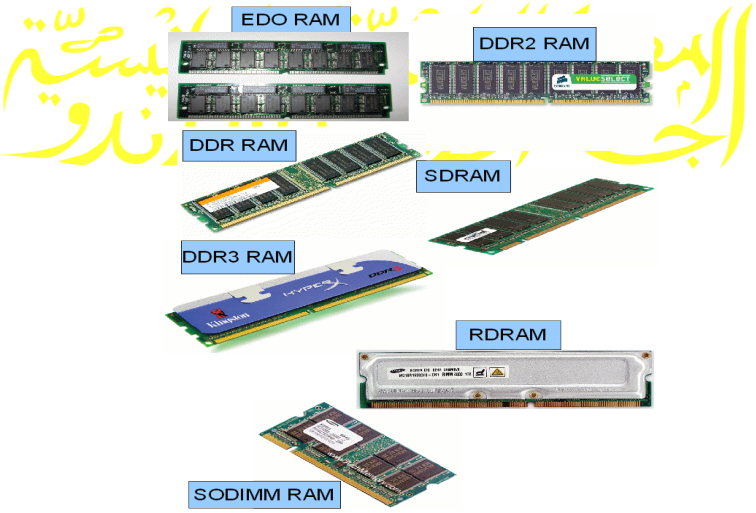
input komputer dan juga data-data hasil pemrosesan sebuah program. Kebanyakan dari random access memory disebut sebagai barang yang volatile yang artinya jika daya listrik tidak ada atau power off maka semua konten yang ada di dalam random access memory akan segera hilang secara permanen.

Dalam memproses sebuah data yang masuk dalam inputan user, beberapa bagian random access memory saling membantu proses pengolahan data tersebut. Berikut bagian utama random access memory yang mengelola data dari inputan hingga output:

1. Input Storage, digunakan untuk menampung input yang diguakann lewat alat input.
2. Program Storage, dipakai untuk menyimpan semua instruksi instruksi program yang akan diproses.
3. Working Storage, digunakan untuk menyimpan data yang akan diolah dan hasil pengolahan.
4. Output Storage, digunakan untuk menampung hasil akhir dari pengolahan data yang akan ditampilkan ke alat output.

Berdasarkan proses kerja random access memory dalam melakukan penyimpanan data dalam sebuah komputer dari awal penyimpanan hingga pengeluaran data yang akan di tampilkan. Karena hal yang menjadi alasan mengapa proses forensik digital dapat dilakukan pada sebuah random access memory dengan hasil yang spesifik dan bisa dipertanggung jawabkan.

Dalam media penyimpanan, random access memory memiliki berbagai macam jenis yang biasa digunakan, jenis jenis random access memory yang biasa digunakan untuk perangkat komputer dan lainnya tercantum pada Gambar 2.3




Gambar 2.3 Jenis Random Access Memory

## 2.4 Live Forensics

Live forensics yaitu suatu teknik analisis dimana menyangkut data yang berjalan pada sistem atau data volatile yang umumnya tersimpan pada random access memory atau transit pada jaringan. Teknik live forensics memerlukan kecermatan dan ketelitian, dikarenakan data volatile pada random access memory dapat hilang jika sistem mati, dan adanya kemungkinan tertimpanya data penting yang ada pada random access memory oleh aplikasi yang lainnya. Karena itu diperlukan metode live forensics yang dapat menjamin integritas dan keaslian data volatile tanpa menghilangkan data yang berpotensial menjadi barang bukti.

Live forensics pada dasarnya memiliki kesamaan pada teknik forensik tradisional dalam hal metode yang dipakai yaitu identifikasi, penyimpanan, analisis, dan presentasi, hanya saja live forensics merupakan respon dari kekurangan teknik forensik tradisional yang tidak bisa mendapatkan informasi dari data dan informasi yang hanya ada ketika sistem sedang berjalan misalnya aktifitas memory, network proses, swap file, running system proses, dan informasi dari file sistem.

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 yang bisa digunakan dalam 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 forensics.

Dalam melakukan analisis akuisisi data pada random access memory di perangkat laptop berbasis sistem operasi linux dan windows dengan metode live forensics yang merupakan bagian dari komputer forensik, maka peneliti berpedoman pada framework NIST 800-86. Tahapan analisis forensik yang dijabarkan sesuai dengan framewoek NIST 800-86 dalam hal ini untuk penanganan barang bukti yang tersimpan di random access memory adalah sebagai berikut :

1. Collect :

   Tahapan ini dilakukan untuk mengenali, mengupulkan dan memberikan label terhadap barang bukti yang diketemukan di tempat kejadian perkara. Selanjutnya barang bukti didokumentasikan dan memastikan integritas data.

2. Examine :

   Pada tahapan ini dilakukan proses pemeriksaan dan mengklasifikasi terhadap barang bukti yang sudah dikumpulkan terkait dengan kasus tindak kejahatan yang terjadi.

3. Analyze :

   Pada tahapan ini dilakukan analisa terhadap barang bukti yang sudah dikumpulkan terkait dengan kasus yang terjadi. Dalam tahap ini juga dilakukan analisa barang bukti dengan tools terkait untuk selanjutnya dibuat laporan.

4. Report :

   Tahapan ini adalah melaporkan hasil akhir dari semua tahapan yang sudah dilalui. Dalam laporan disertakan tindakan yang diambil, peralatan hardware dan software yang digunakan, serta metode yang digunakan dalam pemecahan kasus tindak kejahatan yang terjadi. Dalam tahapan ini juga disimpulkan dan diberikan saran agar tidak terjadi lagi kasus yang sama di masa mendatang.

## 2.5 Linux Memory Extractor (LiME)

LiMe merupakan *loadable kernel module* yang dapat digunakan untuk melakukan akuisisi volatile memory pada perangkat bersistem operasi berbasis linux. Untuk dapat mempergunakan LiMe dibutuhkan privilege sebagai root. LiME merupakan tools pertama yang mampu mengcapture random access memory secara keseluruhan.

## 2.6 FTK Imager

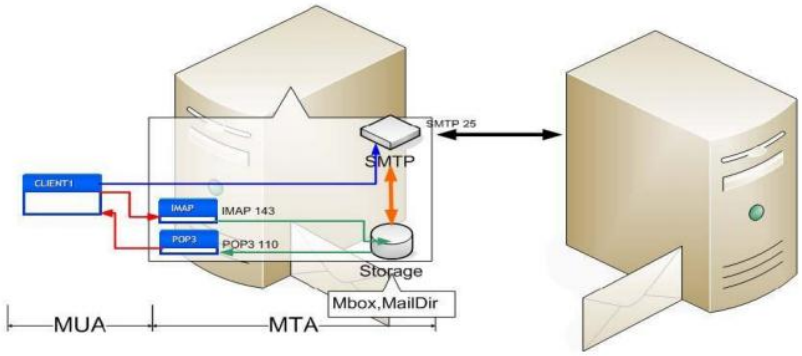
FTK Imager atau bahasa lengkapnya adalah “Forensic Toolkit Imager” merupakan sebuah aplikasi stand-alone untuk disk imaging besutan Access Data. Access Data merupakan sebuah perusahaan yang bergerak di bidang forensik digital dan menyediakan solusi dari kelas stand-alone sampai kelas enterprise untuk proses investigasi digital.

## 2.7 Email

Email adalah singkatan dari Electronic Mail . Email berfungsi sebagai sarana untuk mengirim surat atau pesan melalui jaringan Intenet. Dengan email kita hanya membutuhkan beberapa menit agar surat/pesan kita sampai tujuan tidak perlu menunggu berhari-hari seperti mengirim surat/pesan biasa (pos) dan dengan email isi surat/pesan dapat kita isi dengan konten gambar/suara dan video. Email bukan hanya untuk mengirim surat/pesan, jaman sekarang apa-apa yang berhubungan internet seperti mendaftar

facebook, twitter, blogger dan lain-lain pasti memerlukan email utuk mendaftar. Sebuah pesan elektronis terdiri dari isi, alamat pengirim, dan alamat-alamat yang dituju.

Sistem email beroperasi diatas jaringan berbasis pada model store and forward. Sistem ini mengaplikasikan sebuah sistem server email yang menerima, meneruskan, mengirimkan, serta menyimpan pesan pesan user, dimana user hanya perlu untuk mengkoneksikan pc mereka kedalam jaringan. Email dapat dianalogikan dengan kotak surat yang ada di kantor POS sedangkan server email dapat diibaratkan sebagai kantor POS. Dengan analog ini sebuah mail server dapat memiliki banyak account email yang ada didalamnya. Cara kerja email tersebut tercantum pada Gambar 2.4




Gambar 2.4 Cara Kerja Email

Cara kerja email yang dapat dilihat berdasarkan Gambar 2.4 menunjukkan bahwa email yang dikirim belum tentu akan diteruskan ke komputer penerima (end user), tetapi disimpan/dikumpulkan dahulu dalam sebuah computer server (host) yang akan online secara terus menerus (continue) dengan media peyimpanan (storange) yang relative besar dibanding computer biasa. Hal ini bisa diibaratkan dengan sebuah kantor pos, jika seseorang mempunyai alamat (mailbox), maka dia dapat memeriksa secara berkala jika dia mendapatkan surat. Komputer yang melayani penerimaan email secara terus menerus tersebut biasa disebut dengan mailserver atau mailhost.

## 2.8 User_id dan Password

User_id atau username merupakan serangkaian huruf yang merupakan tanda pengenal untuk masuk dan mengakses sistem. Apabila kita sudah mendaftarkan diri ke ISP maka secara otomatis akan diberikan user_id dan password yang digunakan untuk mengakses sistem. Password merupakan serangkaian huruf atau angka yang merupakan sandi untuk dapat mengakses sistem. Password bersifat rahasia, sehingga kita tidak diperkenankan memberitahukanya kepada orang lain. Ketika pengguna memasukan password, maka yang

terlihat pada tampilan komputer hanya berupa karakter huruf (A-Z) sehingga tidak akan terbaca dalam bentuk angka maupun tulisan. Search Engine (mesin pencari) juga menyediakan kata bantu apabila user lupa akan password.

## 2.9 Link URL

URL atau Uniform Resource Locator adalah rangkaian karakter menurut suatu format standar tertentu, yang digunakan untuk menunjukkan alamat suatu sumber seperti dokumen dan gambar di internet. URL merupakan suatu inovasi dasar bagi perkembangan sejarah Internet. URL pertama kali diciptakan oleh Tim Berners-Lee pada tahun 1991 agar penulis dokumen dokumen dapat merujuk pranala ke World Wide Web. Sejak 1994. Konsep URL telah dikembangkan menjadi istilah Uniform Resource Identifier (URI) yang lebih umum sifatnya. Walaupun demikian, istilah URL masih tetap digunakan secara luas.

URL/URI terdiri atas nama domain plus protocol yang digunakan untuk membuka domain tersebut. Sebagai contoh, travelwisatajogja.com adalah domain, sedangkan http://travelwisatajogja.com adalah URL/URI.

# BAB 3
# Metodologi Penelitian

## 3.1 Studi Pustaka

Studi Pustaka merupakan kegiatan untuk mengkaji dan mempelajari berbagai sumber literature dan teori-teori yang mendukung tentang penelitian yang dilakukan. Sumber pembelajaran pada studi pustaka dapat bersumber dari jurnal, paper, artikel, buku buku, website, dan sumber pembelajaran lainnya yang membahas tentang laptop, random access memory, live forensics, user_id, password, linux memory extractor (LiME) dan FTK Imager.

## 3.2 Tempat dan Waktu Penelitian

Dalam penelitian ini menggunakan metode kualitatif yaitu metode dengan pendekatan studi kasus yang tempat penelitiannya pada kantor Travel Wisata Jogja. Travel Wisata Jogja bergerak dibidang layanan jasa wisata dan transportasi. Sebagai biro jasa yang bergerak dibidang tersebut maka integritas dan nama baik menjadi hal utama dalam menarik client untuk menggunakan jasa kami.

## 3.3 Persiapan Alat dan Bahan

Untuk mendukung implementasi dalam penelitian ini diperlukan adanya perangkat keras dan perangkat lunak sebagai alat dan bahan penelitian, berikut ini alat dan bahan yang dipakai dalam melakukan penelitian :

1. Hardware

Spesifikasi komputer yang dibutuhkan untuk analisa bukti digital pada kasus ini adalah sebagai berikut :

Tabel 3.1 Spesifikasi Laptop Dengan Sistem Operasi Linux Santoku

| | |
|---|---|
| Processor | Intel ® Core™ i3 - 2330M |
| Chipset | Intel® Core™ i3 Chipset |
| Memory | 4GB DDR3 1600MHz |
| Graphic | 1GB NVIDIA® GeForce® GT 520M |
| Baterai | 6-cell Li-ion Batteray |
| Drive Optic | DVD-Super Multi DL drive |
| Storage | ATA 500GB HDD |

| | |
|---|---|
| Networking and Interface | Wi-Fi, Bluetooth, HDMI port, Webcam |

Tabel 3.2 Spesifikasi Laptop Dengan Sistem Operasi Linux Ubuntu / Virtual

| | |
|---|---|
| Processor | AMD A8-4500M APU with Radeon(TM) HD Graphics |
| Chipset | AMD Radeon Graphics Prosesor |
| Memory | 1019 MB DDR3 1600MHz |
| Graphic | AMD Radeon HD7640G |
| Baterai | 6-cell (48Whr): up to 6 hrs |
| Drive Optic | DVD +/- RW |
| Storage | ATA 15GB |
| Networking and Interface | HDMI, USB3.0, Bluetooth, Camera |

Tabel 3.3 Spesifikasi Laptop Dengan Sistem Operasi Linux Mint

| | |
|---|---|
| Processor | Intel ® CoreTM i5-7200U |
| Chipset | Intel® Core™ i5 Chipset |
| Memory | 8GB DDR4 |
| Graphic | NVIDIA GeForce 920MX |
| Baterai | 2 Cell Li-Polymer |
| Drive Optic | DVD Recordable |
| Storage | SSD 240GB |
| Networking and Interface | Bluetooth, Wifi 802 11.ac, Lan 10/100/1000 gigabit Ethernet. |

Tabel 3.4 Spesifikasi Laptop Dengan Sistem Operasi Windows

| | |
|---|---|
| Processor | Intel ® CoreTM i3 - 2330M |
| Chipset | Intel® Core™ i3 Chipset |
| Memory | 4GB DDR3 1600MHz |
| Graphic | 1GB NVIDIA® GeForce® GT 520M |
| Baterai | 6-cell Li-ion Batteray |
| Drive Optic | DVD-Super Multi DL drive |
| Storage | ATA 500GB HDD |
| Networking and Interface | Wi-Fi, Bluetooth, HDMI port, Webcam |

2. Software

Adapun spesifikasi perangkat lunak / software yang digunakan untuk analisa bukti digital pada kasus ini adalah sebagai berikut :

Tabel 3.5 Kebutuhan Perangkat Lunak

| No | Software | Fungsionalitas |
|---|---|---|
| 1 | Linux Distro Santoku | Sistem Operasi Laptop |
| 2 | Linux Distro Mint | Sistem Operasi Laptop |
| 3 | Linux Distro Ubuntu | Sistem Operasi Laptop |
| 4 | Windows 7 Ultimate | Sistem Operasi Laptop |
| 5 | Linux Memory Extractor | Kernel Module untuk akusisi random access memory pada sistem operasi linux |
| 6 | FTK Imager | Tools untuk analisa hasil akuisisi data yang berekstensi .lime dan capture memory windows. |

## 3.4 Skenario Kasus

Skenario kasus dalam penelitian tentang metode live forensics untuk analisa random access memory pada perangkat laptop berbasis linux dan windows adalah sebagai berikut :

Telah terjadi complain terhadap Travel Wisata Jogja. Isi complain tersebut adalah tentang layanan order yang fiktif. Bentuk complain layanan order tersebut diantaranya, beberapa pengguna jasa sudah order dan transfer uang muka ke pihak travel akan tetapi pada hari yang sudah terjadwal ternyata pihak travel tidak memenuhi kewajiban yang sudah disepakati. Dari pihak travel tenyata tidak ada jadwal sesuai dengan order dari tersebut diatas.

Kasus tersebut berakibat pada ketidakpuasan pelanggan yang mengakibatkan menurunnya order pengguna travel. Oleh karena itu manajemen travel berencana melakukan investigasi terkait kasus yang terjadi. Dugaan sementara ada pihak tertentu yang menggunakan account travel wisata jogja secara illegal untuk akses account sosial media serta dilakukan juga investigasi terkait bocornya account bagian keuangan seperti pada internet banking dan paypal.

## 3.5 Simulasi Kasus

Simulasi kasus digunakan 4 laptop dengan spesifikasi yang berbeda beda untuk mendapatkan akusisi data yang lebih variasi sehingga menghasilkan analisa yang akurat.

Simulasi bertujuan untuk melakukan pembuktian terhadap dugaan yang telah diskenariokan pada kasus penyalahgunaan account. Simulasi ini dilakukan karena kasus yang sebenarnya tidak mungkin untuk dilakukan. Tahap pembuatan simulasi juga untuk mendukung proses pengambilan data agar penelitian yang dirancang mendapat hasil sesuai dengan rumusan yang dibuat.

### 3.6 Olah TKP dan Pengamanan Barang Bukti

Pada tahapan ini dilakukan olah tempat kejadian perkara yang menjadi lokasi ditemukannya barang bukti. Selanjutnya dilakukan pengamanan terhadap barang bukti tersebut sebelum dilakukan akusisi data untuk menemukan informasi digital terkait dengan kasus yang terjadi. Dalam kasus ini adalah penyalahgunaan account secara illegal.

### 3.7 Akuisisi Data

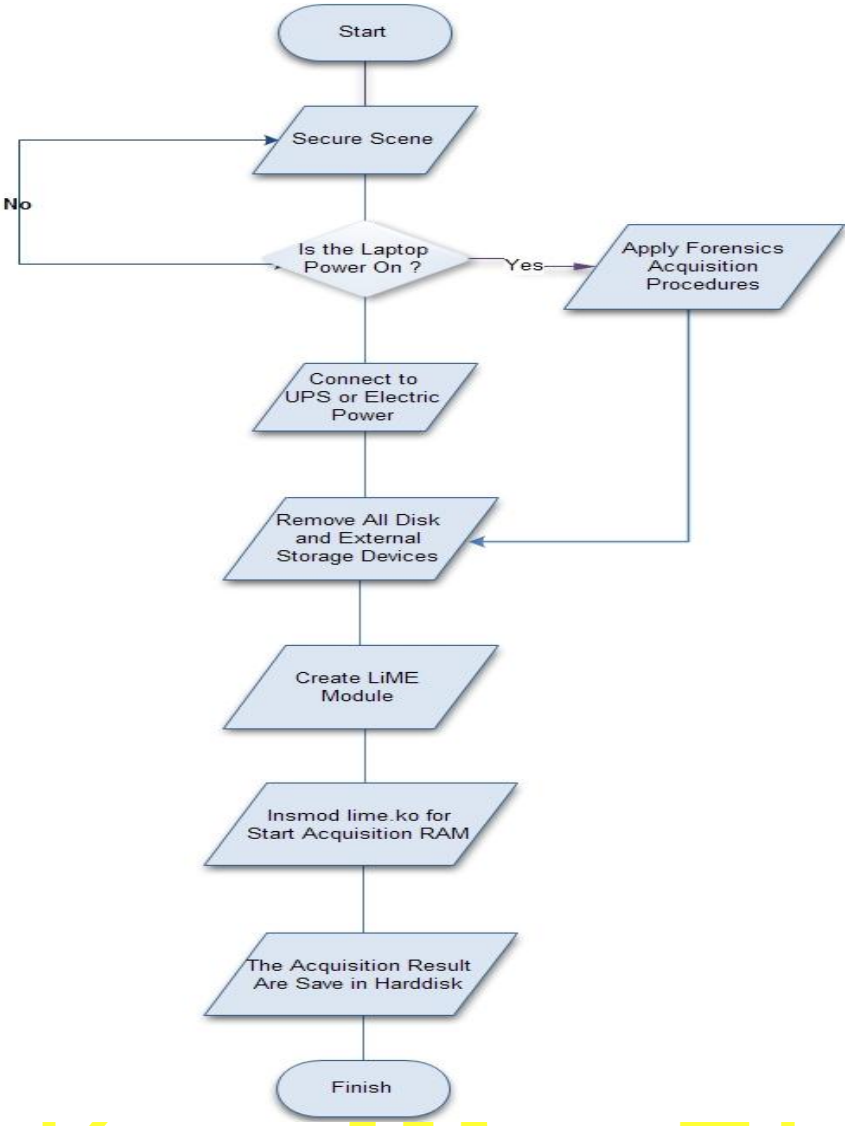
Tahap akuisisi data pada penelitian ini dilakukan secara live forensics, Tahapan akuisisi data secara live forensics mengacu pada penelitian yang dilakukan sebelumnya oleh (Karayianni & Katos, 2012). Pada penelitian lainnya yang dilakukan oleh (Divyang Rahevar, 2013) dilakukan akuisisi terhadap random access memory windows untuk menemukan user_id dan password. Dalam penelitian kali ini selain meneliti random access memory untuk mendapatkan informasi terkait user_id, password, email serta informasi lainnya juga untuk meneliti bagaimana karakteristik random access memory dan bagaimana kondisi random access memory pada perangkat laptop setelah dilakukan hibernate.

#### 3.7.1 Akuisisi Data Live Forensics

Kondisi utama yang harus dipenuhi dalam live forensics adalah sistem dalam kondisi running atau beroperasi dikarenakan beberapa data dan informasi pada random access memory bersifat volatile artinya jika komputer mati atau reebot maka data akan hilang. Untuk itu perlu dilakukan penanganan secara khusus dalam melakukan akusisi data yang bersifat volatile.

### 3.8 Rancangan Akuisisi Random Access Memory

Untuk melakukan penanganan barang bukti laptop diperlukan suatu tahapan yang akan menggabarkan alur proses penanganan barang bukti tersebut serta bagaimana tahapan untuk melakukan akusisi data guna mendapatkan bukti informasi digital. Tahapan tersebut tercantum pada Gambar 3.1.




Gambar 3.1 Flowchart Proses Akuisisi Random Access Memory

Berdasarkan Gambar 3.1 diketahui bahwa sebelum melakukan akusisi data pada barang bukti laptop terlebih dahulu amankan lokasi tempat ditemukannya barang bukti. Selanjutnya jika yang ditemukan laptop dalam kondisi menyala atau running maka proses forensics akusisi data bisa dilanjutkan. Untuk melakukan akusisi data pada random access memory, sebelumnya lepaskan semua perangkat external storage dan kemudian create modul lime untuk memulai proses capture memory.

# BAB 4
# Hasil dan Pembahasan

## 4.1 Data

### 4.1.1 Sumber Data

Dalam melakukan penelitian ini, sumber data diperoleh dari random access memory pada perangkat laptop. Studi kasus dalam hal ini menggunakan metode live forensics, Dimana untuk memperoleh data dilakukan dengan cara akuisisi data dari laptop yang masih aktif, karena data yang diperoleh dari sumbernya bersifat volatile. Adapun sistem operasi yang berjalan pada laptop tersebut yaitu berbasis sistem operasi windows dan berbasis sistem operasi linux.

### 4.1.2 Proses Mendapatkan Data

Proses mendapatkan data diperoleh dengan metode live forensics, dimana proses dilakukan saat laptop dalam keadaan aktif kemudian dilakukan akuisisi data dari random access memory menggunakan tools Linux Memory Extractor (LiME) untuk laptop yang menggunakan sistem operasi linux, sedangkan untuk laptop berbasis sistem operasi windows capture memory menggunakan tools FTK Imager. Data yang diperoleh dari random access memory yang sudah diakuisisi menggunakan tools LiME berekstensi *.lime sedangkan hasil capture memory menggunakan tools FTK Imager berekstensi *.mem.

Setelah peneliti melakukan akuisisi dan ekstraksi terhadap random access memory di barang bukti laptop yang diduga digunakan dalam tindak kejahatan penyalahgunaan account selanjutnya dilakukan verifikasi nilai hash hasil imaging untuk menjaga nilai integritas barang buki. Karena integritas data dapat memastikan keakuratan, konsistensi, dan kualitas dari sebuah data.

Tabel 4.1 Sumber Data Akusisi Random Access Memory

| No | Barang Bukti | Nilai Hash |
|---|---|---|
| 1 | Laptop Linux Santoku | 9743d3a18e7b7a8cbe92f6f5fd9c9061 |
| 2 | Laptop Linux Mint | 65e993e702890df6f2a5480324c8b1e7 |
| 3 | Laptop Linux Ubuntu | 02915553b49842b484d2b340dc458d55 |
| 4 | Laptop Windows Normal | 7160aa08f7cbf4a604cd6ed01fed3100 |

| No | Barang Bukti | Nilai Hash |
|---|---|---|
| 5 | Laptop Windows Ada Aktifitas | 06ad24c01063b6876d7a3cfe38ede1de |
| 6 | Laptop Windows Setelah Hibernate | f16eb7a5259d71113ca571d3015f3bd6 |

## 4.2 Skenario dan Simulasi Kasus

Pada tahapan ini dilakukan penerapan skenario sesuai yang telah dirancang di Bab 3 dimana telah terjadi penyalahgunaan account secara illegal. Dalam skenario ini digunakan 4 laptop dengan spesifikasi laptop 1 dengan sistem operasi linux santoku, laptop 2 dengan sistem operasi linux ubuntu, laptop 3 dengan sistem operasi linux mint, dan laptop 4 dengan sistem operasi windows 7. Dugaan sementara bocornya account ini karena kelalaian atau tidak terkontrolnya penggunaan account.

Dalam penelitian ini dugaan sementara pencurian account melalui data yang berada dalam random access memory pada saat komputer masih hidup, dugaan ini muncul dikarenakan setiap menggunakan account untuk login facebook, akses login internet banking, dan akses login paypal tidak pernah melakukan save password pada browser dan selalu log out.

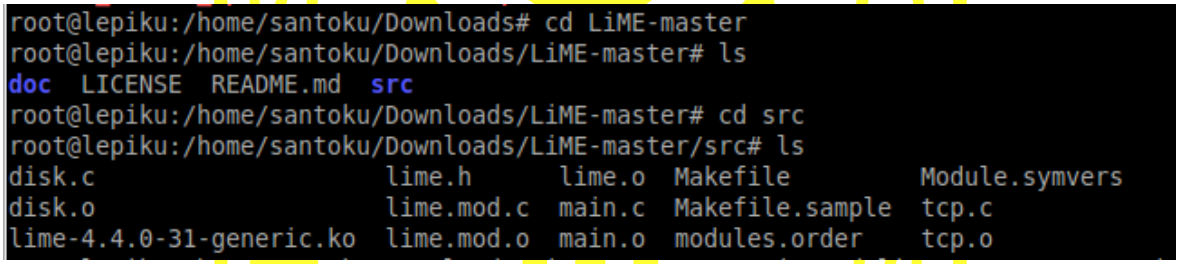
## 4.3 Akuisisi Data

Data penelitian diperoleh dari hasil akuisisi random access memory pada perangkat laptop yang masih aktif. Alur atau tahapan akuisisi data mengacu pada Gambar 3.1. Pada alur tersebut dijelaskan bahwa ditemukan laptop dalam kondisi menyala, yang diduga menyimpan barang bukti digital dalam kasus yang sedang diselidiki, selanjutnya persiapkan prosedur untuk melakukan tahapan akusisi data. Jika alat bukti tersebut berupa laptop pastikan mempunyai cadangan baterray, jika komputer koneksikan dengan UPS sebagai cadangan listrik atau power. Sebelum melakukan akuisisi jangan pernah melepas power kabel. Selanjutnya cabut semua external device yang menancap pada alat bukti laptop atau komputer. Lakukan akuisisi data pada random access memory secara live forensics dengan cara insmod / menginstal module LiME (Linux Memory Extractor) sebagai tools untuk capture memory pada laptop berbasis sistem operasi linux. Jika proses akusisi pada random access memory sudah selesai maka selanjutnya dilakukan analisis terhadap hasil capture memory tersebut dengan menggunakan tools FTK Imager.

## 4.4 Analisa Random Access Memory Laptop Berbasis Sistem Operasi Linux

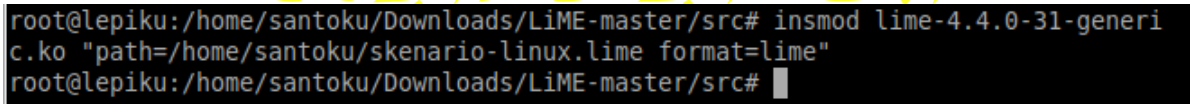
Berdasarkan analisa yang dilakukan, karakteristik random access memory antara sistem operasi berbasis windows dan sistem operasi berbasis linux hampir sama, yaitu random access memory tidak akan menyimpan informasi apapun jika laptop belum digunakan untuk akses data file atau digunakan untuk melakukan login dan browsing internet. Dalam hal ini belum ditemukan informasi digital yang bisa dicurigai untuk digunakan sebagai bukti digital dari suatu kasus. Berbeda dengan random access memory dari perangkat laptop yang sudah digunakan untuk akses file atau login aplikasi di internet. Maka informasi yang sudah diakses akan tersimpan dalam random access memory selama laptop belum dimatikan.

Untuk melakukan akuisisi atau capture random access memory pada perangkat laptop berbasis sistem operasi linux digunakan tools linux memory extractor (LiME). Sebelumnya lakukan akses ke direktori */src* pada LiME-master yang terletak di folder Downloads dengan mengetikkan perintah pada terminal linux seperti Gambar 4.1




Gambar 4.1 Akses lime-4.4.0.31-generic.ko pada direktori src

Gambar 4.1 menjelaskan tentang bagaimana melakukan akses ke direktori /src guna menemukan kernel modul lime-4.4.0-31-generic.ko. Modul ini digunakan untuk melakukan proses capture memory. Untuk memulai proses capture memory pada random access memory pada perangkat laptop berbasis system operasi linux terlebih dahulu ketikkan perintah di command line terminal linux sesuai pada Gambar 4.2




Gambar 4.2 Proses Capture Memory Pada Random Access Memory

Gambar 4.2 menjelaskan tentang perintah apa yang harus diinputkan pada terminal linux guna memulai proses capture memory. Hasil dari akusisi data pada random access memory akan tersimpan pada direktori /home/"Nama Hasil Akuisisi".

Hasil dari akusisi terdapat file dengan ekstensi *.lime. File ini bisa dianalisa menggunakan tools FTK Imager. Dari hasil analisa diperoleh beberapa informasi yang bisa dijadikan sebagai barang bukti digital. Artefak bukti informasi digital diperoleh dari hasil pengujian 3 distro linux pada barang bukti laptop diantaranya sebagai berikut :

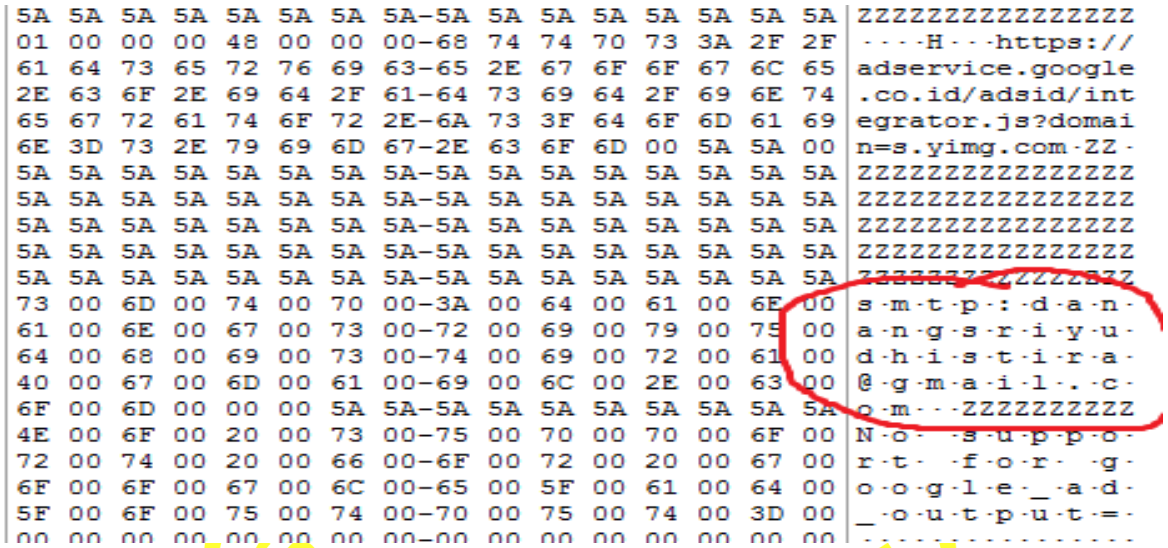
### 4.4.1 Analisa Random Access Memory Laptop Linux Santoku

Berdasarkan hasil akuisisi data di random access memory pada laptop berbasis sistem operasi linux santoku menggunakan tools LiME (Linux Memory Extractor) dengan metode live forensics diperoleh hasil akusisi dengan format file berekstensi *.lime. File tersebut selanjutnya dilakukan analisa menggunakan tools FTK Imager dan diperoleh beberapa informasi digital diantaranya user_id, account email, password, dan link url. Tahapan akusisi data pada random access memory pada perangkat laptop berbasis sistem operasi linux santoku didokumentasikan dengan menggunakan tabel validasi seperti yang tercantum pada tabel 4.2 :

Tabel 4.2 Validasi Hasil Analisa Random Access Memory Laptop Linux Santoku

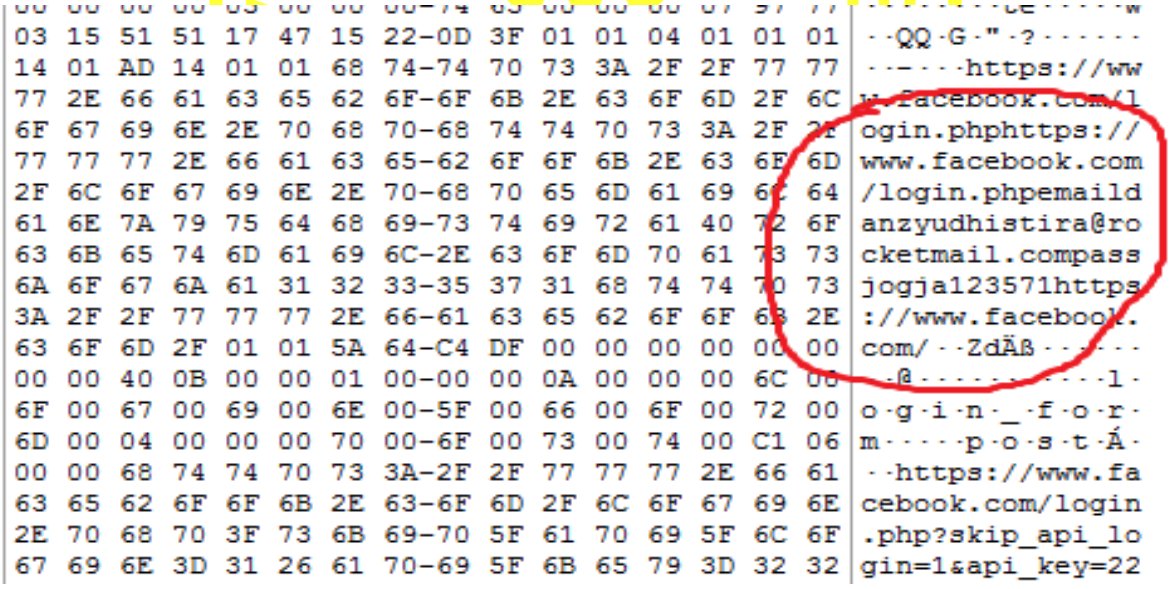
| No | Aktivitas | OS | Alat | Tools | Tanggal | Waktu | Hasil |
|---|---|---|---|---|---|---|---|
| 1 | Pencarian Email | Linux Santoku | Laptop | LiME FTK Imager | 30 Januari 2018 | 3.04 PM | Gambar 4.3 |
| 2 | Pencarian Password | Linux Santoku | Laptop | LiME FTK Imager | 30 Januari 2018 | 3.04 PM | Gambar 4.4 |
| 3 | Pencarian Username | Linux Santoku | Laptop | LiME FTK Imager | 30 Januari 2018 | 3.04 PM | Gambar 4.5 |
| 4 | Link Url | Linux Santoku | Laptop | LiME FTK Imager | 30 Januari 2018 | 3.04 PM | Gambar 4.6 |
| 5 | Account Internet Banking | Linux Santoku | Laptop | LiME FTK Imager | 16 Maret 2018 | 11.56 PM | Gambar 4.7 |
| 6 | Account Bitcoin | Linux Santoku | Laptop | LiME FTK Imager | 16 Maret 2018 | 11.56 PM | Gambar 4.8 |

Berikut ini merupakan bukti hasil dari analisa random access memory pada perangkat laptop berbasis sistem operasi linux santoku. Ditemukan beberapa bukti informasi yang bisa dijadikan sebagai barang bukti digital. Informasi pertama yang berhasil ditemukan yaitu bukti account email seperti tercantum pada Gambar 4.3. Account email ini merupakan email yang biasa digunakan oleh user dalam berkomunikasi via internet.



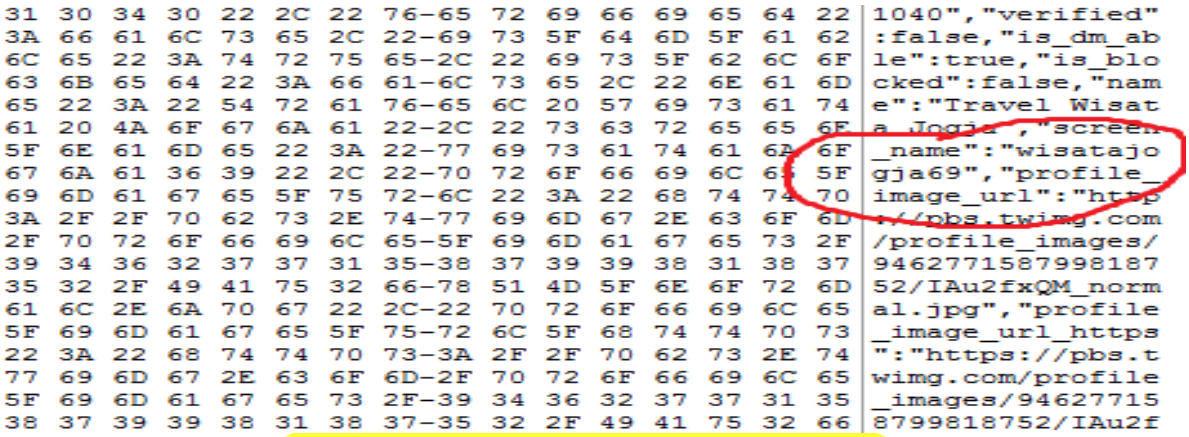

Gambar 4.3 Bukti Email pada Laptop Linux Santoku

Gambar 4.3 merupakan bukti dari hasil analisa random access memory pada perangkat laptop berbasis sistem operasi linux santoku. Pada random access memory terbukti menyimpan informasi terkait account email yang jika dikonversi dari nilai heksa menjadi nilai teks maka diketahui alamat email tersebut "danangsiyudhistira@gmail.com". Bukti lainnya yang berhasil ditemukan dari hasil analisa random access memory yaitu email dan password untuk login facebook. Bukti tersebut tercantum pada Gambar 4.4



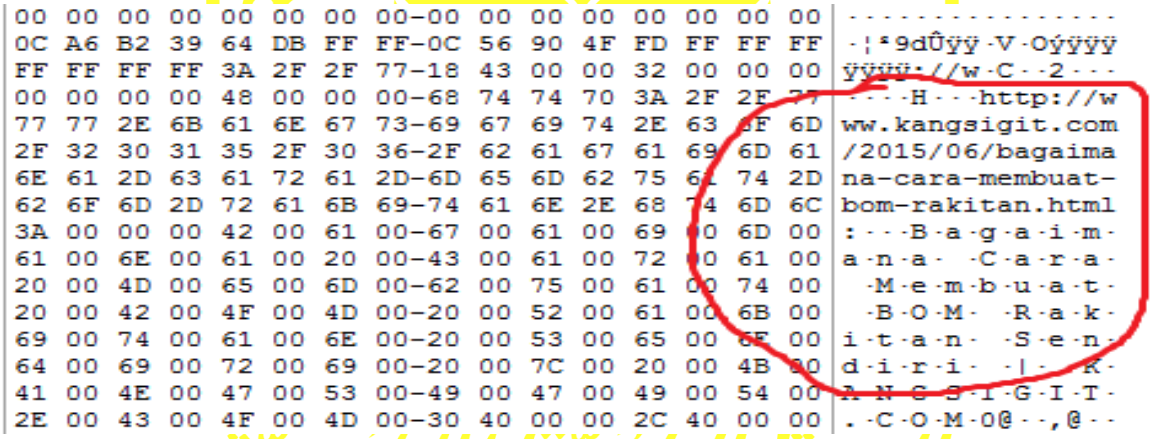

Gambar 4.4 Bukti Password pada Laptop Linux Santoku

Berdasarkan analisa random access memory sesuai dengan Gambar 4.4 terdapat informasi bukti akses login facebook menggunakan email danzyudhistira@rocketmail.com dan password jogja123571. Bukti lainnya terdapat account username seperti pada Gambar 4.5



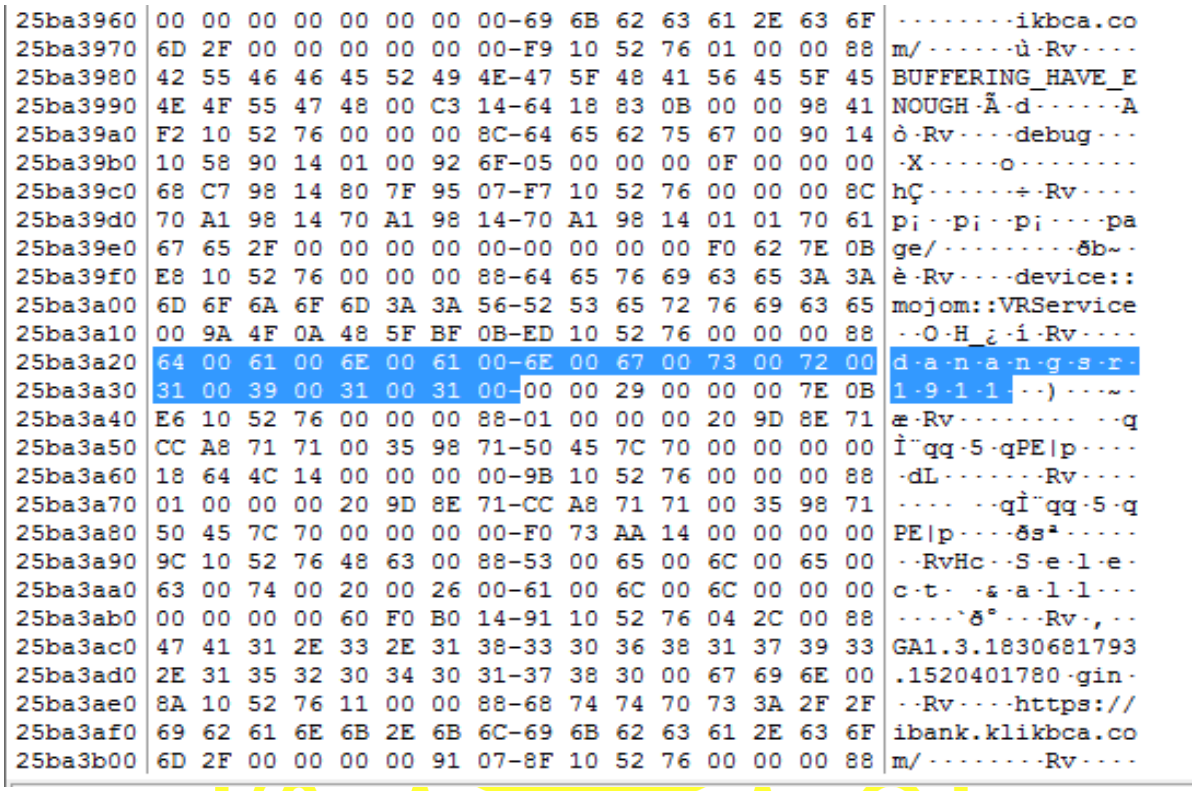

Gambar 4.5 Bukti Username pada Laptop Linux Santoku

Gambar 4.5 merupakan hasil analisa dari random access memory pada perangkat laptop berbasis sistem operasi linux santoku. Diketahui terdapat username dari sebuah profile dengan nilai heksa -77 69 73 61 74 61 6A 6F 67 6A 61 36 39 jika dikonversi ke nilai teks menjadi “wisatajogja69”. Username ini digunakan untuk akses login sosial media twitter. Bukti lain yang berhasil ditemukan dari hasil analisa random access memory yaitu bukti link url seperti pada Gambar 4.6




Gambar 4.6 Bukti Link URL pada Laptop Linux Santoku

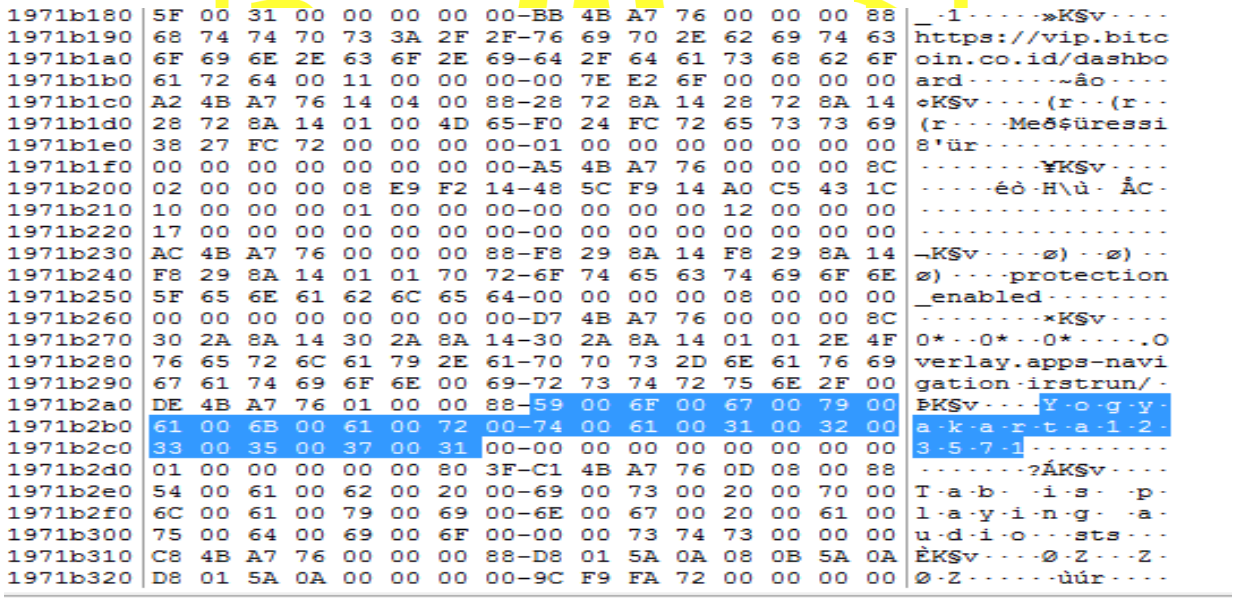
Gambar 4.6 merupakan hasil dari analisa file akusisi random access memory pada perangkat laptop dengan sistem operasi distro linux santoku dengan format *.lime. Dari hasil analisa tersebut diketahui bahwa apa yang kita akses di browser selain historinya tersimpan di cookies browser ternyata random access memory juga menyimpan alamat url yang kita akses. Bukti yang tersimpan di cookies browser dan random access memory akan identik sama. Selama laptop atau komputer belum mati maka informasi berupa alamat url tersebut akan tetap tersimpan dalam random access memory. Bukti lain yang berhasil dianalisa yaitu adanya account internet banking. Bukti account tersebut tercantum pada Gambar 4.7



```
25ba3960 00 00 00 00 00 00 00 00-69 6B 62 63 61 2E 63 6F ........ikbca.co
25ba3970 6D 2F 00 00 00 00 00 00-F9 10 52 76 01 00 00 88 m/......ù.Rv....
25ba3980 42 55 46 46 45 52 49 4E-47 5F 48 41 56 45 5F 45 BUFFERING_HAVE_E
25ba3990 4E 4F 55 47 48 00 C3 14-64 18 83 0B 00 00 98 41 NOUGH.Ã.d......A
25ba39a0 F2 10 52 76 00 00 00 8C-64 65 62 75 67 00 90 14 ò.Rv....debug...
25ba39b0 10 58 90 14 01 00 92 6F-05 00 00 00 0F 00 00 00 .X.....o........
25ba39c0 68 C7 98 14 80 7F 95 07-F7 10 52 76 00 00 00 8C hÇ......÷.Rv....
25ba39d0 70 A1 98 14 70 A1 98 14-70 A1 98 14 01 01 70 61 p¡..p¡..p¡....pa
25ba39e0 67 65 2F 00 00 00 00 00-00 00 00 00 F0 62 7E 0B ge/.........ðb~.
25ba39f0 E8 10 52 76 00 00 00 88-64 65 76 69 63 65 3A 3A è.Rv....device::
25ba3a00 6D 6F 6A 6F 6D 3A 3A 56-52 53 65 72 76 69 63 65 mojom::VRService
25ba3a10 00 9A 4F 0A 48 5F BF 0B-ED 10 52 76 00 00 00 88 ..O.H_¿.í.Rv....
25ba3a20 64 00 61 00 6E 00 61 00-6E 00 67 00 73 00 72 00 d.a.n.a.n.g.s.r.
25ba3a30 31 00 39 00 31 00 31 00-00 00 29 00 00 00 7E 0B 1.9.1.1...).....~.
25ba3a40 E6 10 52 76 00 00 00 88-01 00 00 00 20 9D 8E 71 æ.Rv........ ..q
25ba3a50 CC A8 71 71 00 35 98 71-50 45 7C 70 00 00 00 00 Ì¨qq.5.qPE|p....
25ba3a60 18 64 4C 14 00 00 00 00-9B 10 52 76 00 00 00 88 .dL.....Rv....
25ba3a70 01 00 00 00 20 9D 8E 71-CC A8 71 71 00 35 98 71 .... ..qÌ¨qq.5.q
25ba3a80 50 45 7C 70 00 00 00 00-F0 73 AA 14 00 00 00 00 PE|p....ðsª.....
25ba3a90 9C 10 52 76 48 63 00 88-53 00 65 00 6C 00 65 00 ..RvHc..S.e.l.e.
25ba3aa0 63 00 74 00 20 00 26 00-61 00 6C 00 6C 00 00 00 c.t. .&.a.l.l...
25ba3ab0 00 00 00 00 60 F0 B0 14-91 10 52 76 04 2C 00 88 ....`ð°...Rv.,..
25ba3ac0 47 41 31 2E 33 2E 31 38-33 30 36 38 31 37 39 33 GA1.3.1830681793
25ba3ad0 2E 31 35 32 30 34 30 31-37 38 30 00 67 69 6E 00 .1520401780.gin.
25ba3ae0 8A 10 52 76 11 00 00 88-68 74 74 70 73 3A 2F 2F ..Rv....https://
25ba3af0 69 62 61 6E 6B 2E 6B 6C-69 6B 62 63 61 2E 63 6F ibank.klikbca.co
25ba3b00 6D 2F 00 00 00 00 91 07-8F 10 52 76 00 00 00 88 m/........Rv....
```

Gambar 4.7 Bukti Akses Account Internet Banking Laptop Linux Santoku

Berdasarkan Gambar 4.7 pada laptop dengan sistem operasi linux santoku, telah berhasil ditemukan informasi terkait penggunaan akses login internet banking klikbca.com dengan user_id dalam nilai heksa yaitu 64 00 61 00 6E 00 61 00-6E 00 67 00 72 00 72 00 31 00 39 00 31 00 21 00 kemudian dikonversi ke nilai teks menjadi “danangsr1911”. Bukti lainnya yang berhasil dianalisa yaitu ditemukan account bitcoin seperti tercantum pada Gambar 4.8



```
1971b180 5F 00 31 00 00 00 00 00-BB 4B A7 76 00 00 00 88 _.1.....»K§v....
1971b190 68 74 74 70 73 3A 2F 2F-76 69 70 2E 62 69 74 63 https://vip.bitc
1971b1a0 6F 69 6E 2E 63 6F 2E 69-64 2F 64 61 73 68 62 6F oin.co.id/dashbo
1971b1b0 61 72 64 00 11 00 00 00-00 7E E2 6F 00 00 00 00 ard......~âo....
1971b1c0 A2 4B A7 76 14 04 00 88-28 72 8A 14 28 72 8A 14 ¢K§v....(r..(r..
1971b1d0 28 72 8A 14 01 00 4D 65-F0 24 FC 72 65 73 73 69 (r....Með$üressi
1971b1e0 38 27 FC 72 00 00 00 00-01 00 00 00 00 00 00 00 8'ür............
1971b1f0 00 00 00 00 00 00 00 00-A5 4B A7 76 00 00 00 8C ........¥K§v....
1971b200 02 00 00 00 08 E9 F2 14-48 5C F9 14 A0 C5 43 1C .....éò.H\ù. ÅC.
1971b210 10 00 00 00 01 00 00 00-00 00 00 00 12 00 00 00 ................
1971b220 17 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
1971b230 AC 4B A7 76 00 00 00 88-F8 29 8A 14 F8 29 8A 14 ¬K§v....ø)..ø)..
1971b240 F8 29 8A 14 01 01 70 72-6F 74 65 63 74 69 6F 6E ø).....protection
1971b250 5F 65 6E 61 62 6C 65 64-00 00 00 00 08 00 00 00 _enabled........
1971b260 00 00 00 00 00 00 00 00-D7 4B A7 76 00 00 00 8C ........×K§v....
1971b270 30 2A 8A 14 30 2A 8A 14-30 2A 8A 14 01 01 2E 4F 0*..0*..0*.....O
1971b280 76 65 72 6C 61 79 2E 61-70 70 73 2D 6E 61 76 69 verlay.apps-navi
1971b290 67 61 74 69 6F 6E 00 69-72 73 74 72 75 6E 2F 00 gation.irstrun/.
1971b2a0 DE 4B A7 76 01 00 00 88-59 00 6F 00 67 00 79 00 ÞK§v....Y.o.g.y.
1971b2b0 61 00 6B 00 61 00 72 00-74 00 61 00 31 00 32 00 a.k.a.r.t.a.1.2.
1971b2c0 33 00 35 00 37 00 31 00-00 00 00 00 00 00 00 00 3.5.7.1.........
1971b2d0 01 00 00 00 00 00 80 3F-C1 4B A7 76 0D 08 00 88 .......?ÁK§v....
1971b2e0 54 00 61 00 62 00 20 00-69 00 73 00 20 00 70 00 T.a.b. .i.s. .p.
1971b2f0 6C 00 61 00 79 00 69 00-6E 00 67 00 20 00 61 00 l.a.y.i.n.g. .a.
1971b300 75 00 64 00 69 00 6F 00-00 00 73 74 73 00 00 00 u.d.i.o...sts...
1971b310 C8 4B A7 76 00 00 00 88-D8 01 5A 0A 08 0B 5A 0A ÈK§v....Ø.Z...Z.
1971b320 D8 01 5A 0A 00 00 00 00-9C F9 FA 72 00 00 00 00 Ø.Z.....úùr....
```

Gambar 4.8 Bukti Akses Account Bitcoin Laptop Linux Santoku

Berdasarkan analisa random access memory sesuai dengan bukti pada Gambar 4.8 di perangkat laptop dengan sistem operasi linux santoku, telah berhasil ditemukan informasi terkait penggunaan akses login bitcoin.co.id dengan nilai heksa dari password yaitu 59 00 6F 00 67 00 79 00 61 00 6B 00 61 00 72 00-74 00 61 00 31 00 32 00 33 00 35 00 37 00 31 jika dikonversi ke nilai teks menjadi "Yogyakarta123571".

Untuk analisa account paypal pada random access memory di perangkat laptop dengan sistem operasi linux santoku tidak berhasil diketemukan user_id dan password yang digunakan untuk login paypal, dengan kata lain bahwa account paypal secara otomatis tidak tersimpan dalam random access memory.

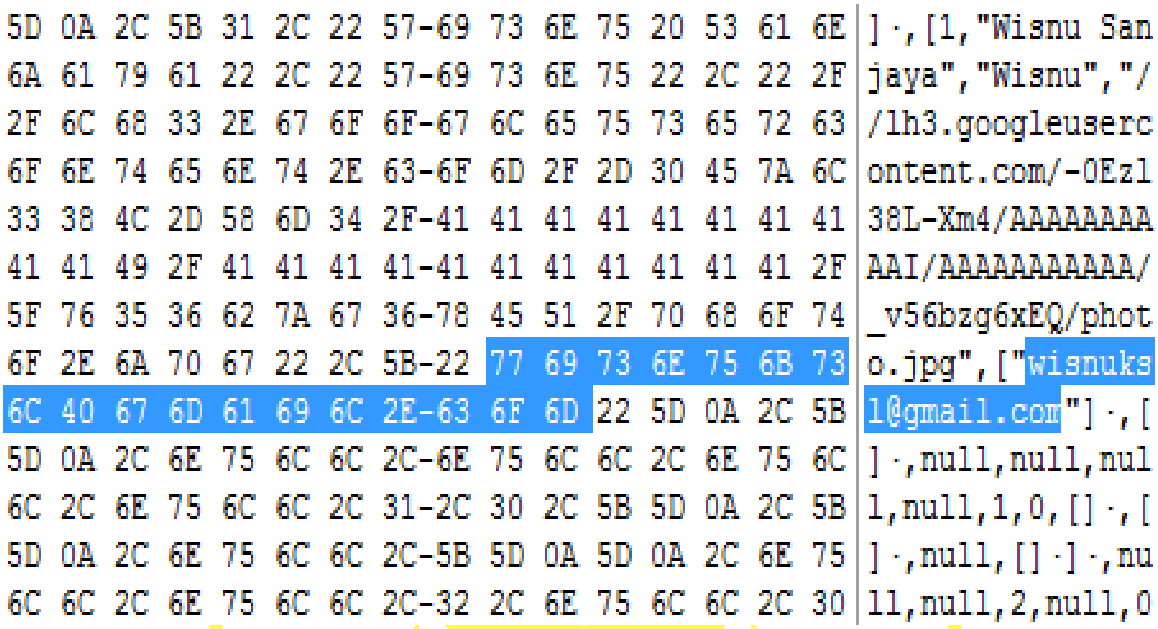
### 4.4.2 Analisa Random Access Memory Pada Laptop Linux Mint

Pada tanggal 31 Januari telah dilakukan akuisisi dari random access memory pada perangkat laptop berbasis sistem operasi linux mint dengan menggunakan tools LiME (linux memory extractor). Dari hasil akusisi dihasilkan file dengan ekstensi *.lime. Selanjutnya file hasil akusisi tersebut dianalisa menggunakan tools FTK Imager untuk mengetahui bukti informasi digital apa saja yang tersimpan di random access memory pada perangkat laptop berbasis sistem operasi linux mint. Tahapan akusisi data pada random access memory didokumentasikan dengan menggunakan tabel validasi seperti yang tercantum pada Tabel 4.3

Tabel 4.3 Validasi Hasil Analisa Random Access Memory Laptop Linux Mint

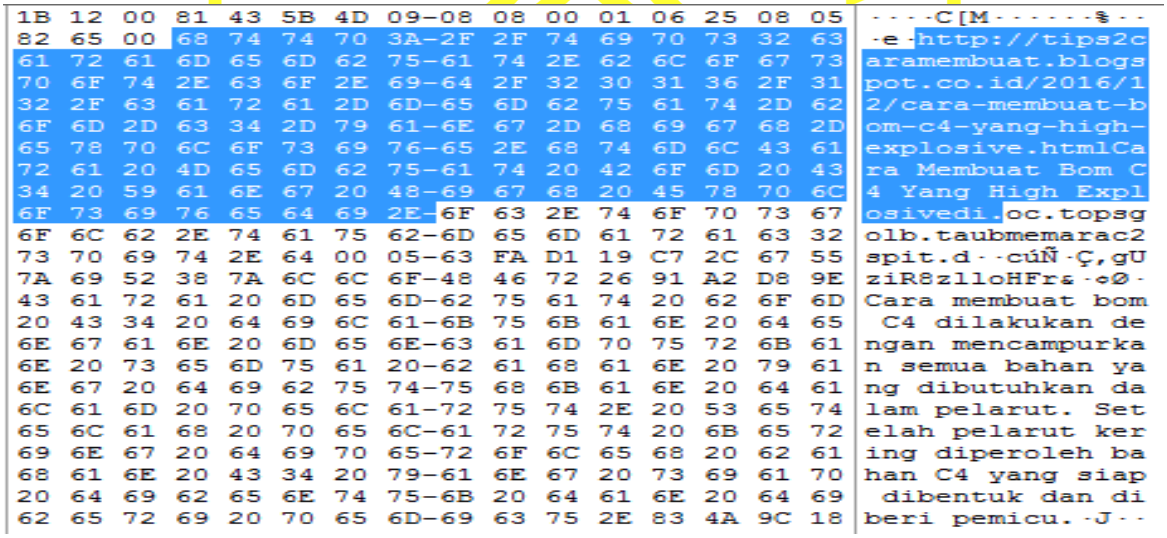
| No | Aktivitas | OS | Alat | Tools | Tanggal | Waktu | Hasil |
|---|---|---|---|---|---|---|---|
| 1 | Pencarian Email | Linux Mint | Laptop | LiME FTK Imager | 31 Januari 2018 | 01.07 AM | Gambar 4.9 |
| 2 | Pencarian Link Url | Linux Mint | Laptop | LiME FTK Imager | 31 Januari 2018 | 01.07 AM | Gambar 4.10 |
| 3 | Pencarian Username | Linux Mint | Laptop | LiME FTK Imager | 31 Januari 2018 | 01.07 AM | Gambar 4.11 |
| 4 | Pencarian Password | Linux Mint | Laptop | LiME FTK Imager | 31 Januari 2018 | 01.07 AM | Gambar 4.12 |
| 5 | Account Internet Banking | Linux Mint | Laptop | LiME FTK Imager | 16 Maret 2018 | 11.59 PM | Gambar 4.13 |
| 6 | Account Bitcoin | Linux Mint | Laptop | LiME FTK Imager | 16 Maret 2018 | 11.59 PM | Gambar 4.14 |

Bukti pertama yang berhasil ditemukan pada hasil analisa akusisi data pada random access memory laptop linux mint yaitu account email. Bukti tersebut tercantum pada Gambar 4.9



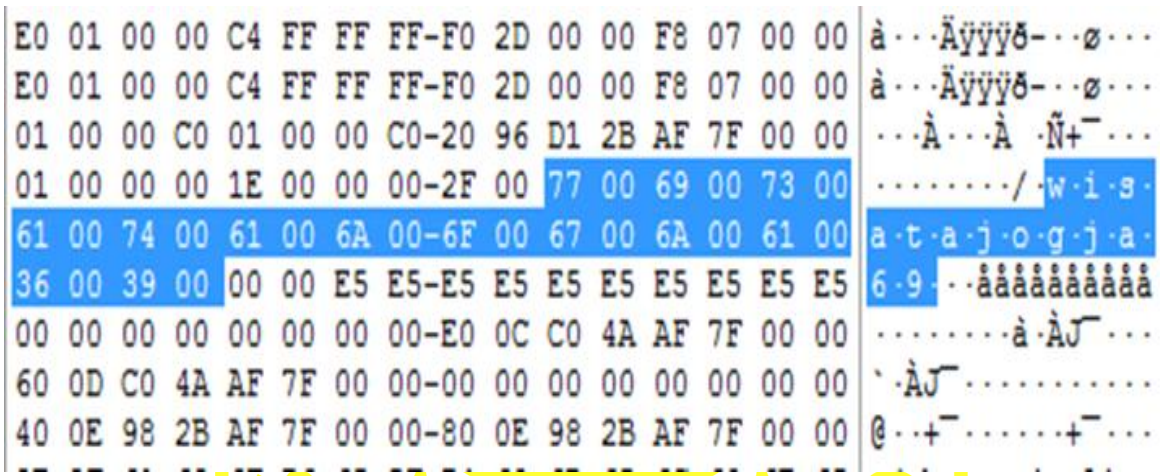

Gambar 4.9 Bukti Email pada Laptop Linux Mint

Gambar 4.9 menunjukkan bahwa dalam random access memory pada perangkat laptop dengan sistem operasi linux mint menyimpan informasi terkait account email yang sudah digunakan. Account email tersebut jika dikonversi dari nilai heksa 77 69 73 6E 75 6B 73 6C 40 67 6D 61 69 6C 2E-63 6F 6D ke nilai teks, maka akan muncul account email "wisnuksl@gmail.com". Bukti lainnya yang berhasil diakusisi yaitu link url. Bukti tersebut tercantum pada Gambar 4.10



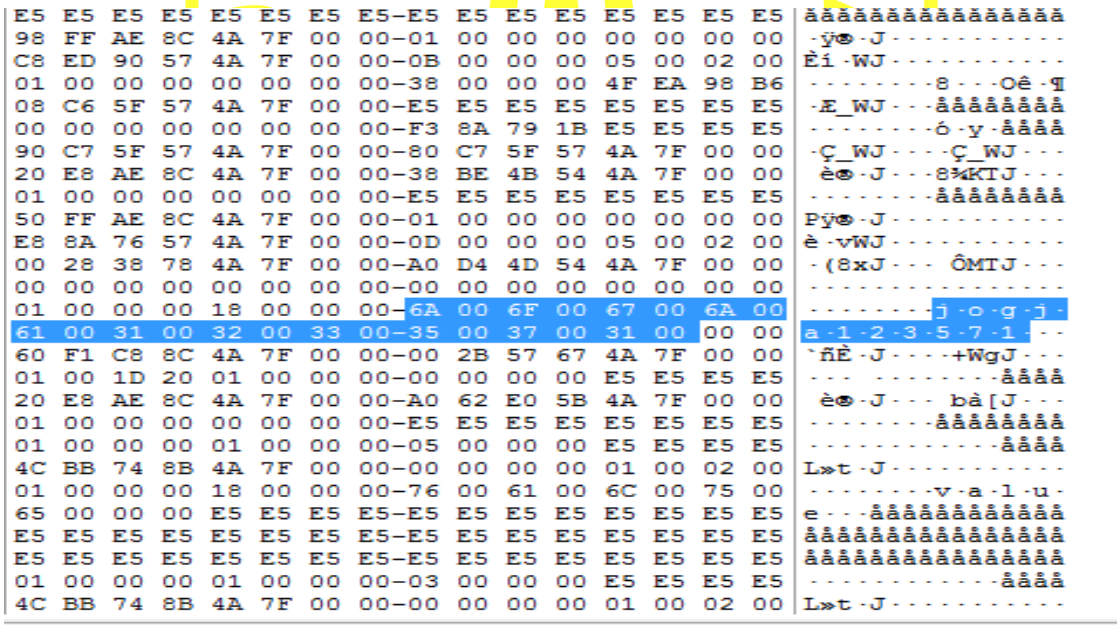

Gambar 4.10 Bukti Alamat URL pada Laptop Linux Mint

Gambar 4.10 merupakan bukti analisa dari hasil akuisisi random access memory pada laptop berbasis sistem operasi linux mint menggunakan LiME (Linux Memory Extractor). Berdasarkan hasil konversi dari nilai heksa ke nilai teks diketahui bahwa alamat url tersebut memuat content “cara membuat bom c4 yang high explisove”. Bukti lainnya yang berhasil didapatkan yaitu account twitter seperti tercantum pada Gambar 4.11



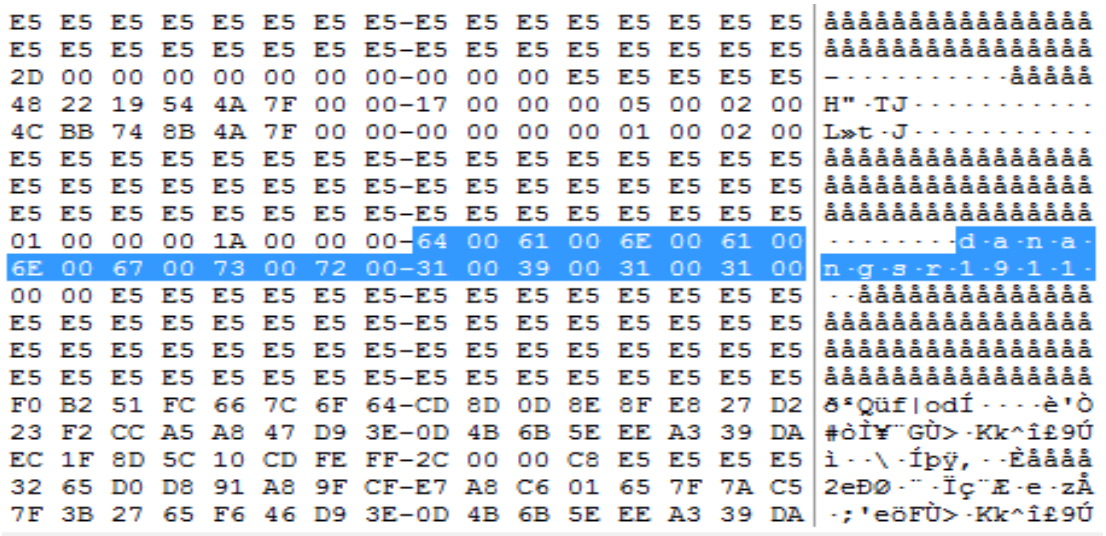
Gambar 4.11 Bukti Username pada Laptop Linux Mint

Berdasarkan Gambar 4.11 yang merupakan hasil analisa random access memory pada perangkat laptop berbasis sistem operasi linux mint berhasil ditemukan informasi terkait dengan bukti username yang sering digunakan untuk melakukan akses ke sosial media. Nilai heksa dari username tersebut yaitu 77 00 69 00 73 00 61 00 74 00 61 00 6A 00-6F 00 67 00 6A 00 61 00 26 00 39 00 jika dikonversi ke nilai teks menjadi “wisatajogja69”.



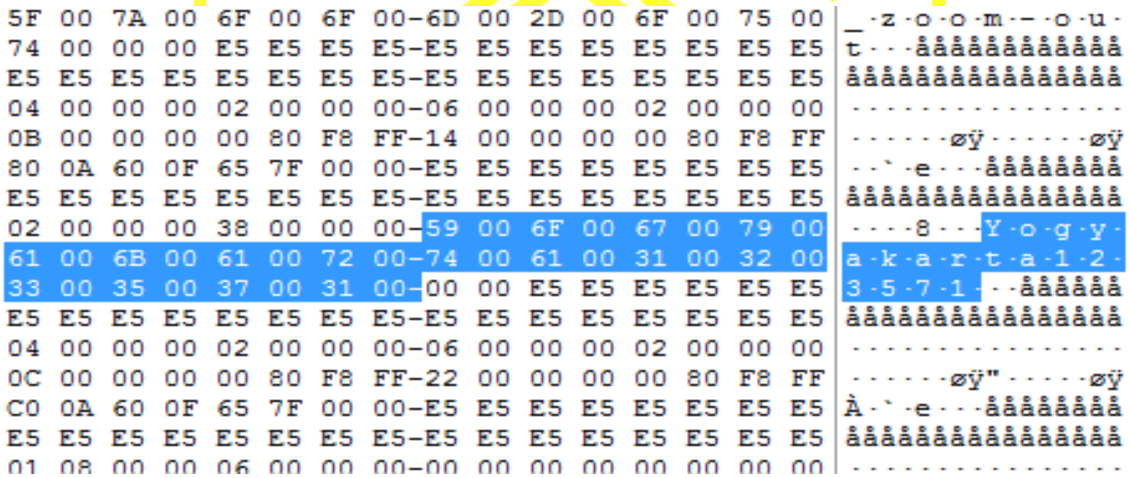
Gambar 4.12 Bukti Analisa Password pada Laptop Linux Mint

Berdasarkan Gambar 4.12 diketahui nilai heksa 6A 00 6F 00 67 00 6A 00 61 00 31 00 32 00 33 00-35 00 37 31 00 yang jika dikonversi ke nilai teks menjadi “jogja123571”. Nilai teks ini sesuai dengan nilai teks pada gambar 4.4 yang merupakan password untuk akses login media social facebook. Bukti lainnya yang berhasil diakusisi pada laptop linux mint yaitu account internet banking seperti tercantum pada Gambar 4.13




Gambar 4.13 Bukti Analisa Internet Banking pada Laptop Linux Mint

Berdasarkan analisa random access memory sesuai dengan Gambar 4.13 diketahui nilai heksanya 64 00 61 00 6E 00 61 00 6E 00 67 00 73 00 72 00-31 00 39 00 31 00 31 00 yang jika dikonversi ke nilai teks menjadi “danangsr1911”. Hasil nilai teks tersebut sesuai dengan gambar 4.7 yang diketahui merupakan user_id untuk melakukan akses login internet banking Bank BCA.




Gambar 4.14 Bukti Analisa Bitcoin pada Laptop Linux Mint

Berdasarkan hasil anasila Gambar 4.14 diketahui nilai heksa 59 00 6F 00 67 00 79 00 61 00 6b 00 61 00 72 00-74 00 61 00 31 00 32 00 33 00 35 00 37 00 31 00 jika dikonversi ke nilai teks menjadi "Yogyakarta123571". Nilai teks ini sesuai atau ada kecocokan dengan nilai teks pada gambar 4.8 yang merupakan hasil analisa password untuk akses login account bitcoin pada laptop linux mint.

Hasil analisa lainnya masih belum bisa menemukan user_id maupun password yang diduga bisa digunakan untuk melakukan akses login paypal. Hal ini serupa dengan kondisi pada analisa random access memory diperangkat laptop berbasis linux santoku.

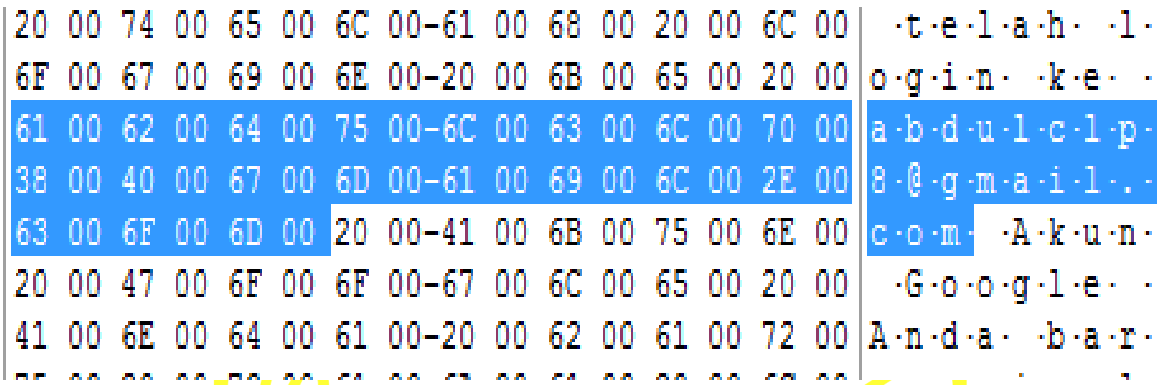
### 4.4.3 Analisa Random Access Memory Pada Laptop Linux Ubuntu

Pada tanggal 30 Januari telah dilakukan akuisisi dari random access memory pada perangkat laptop berbasis sistem operasi linux ubuntu dengan menggunakan tools LiME (Linux Memory Extractor). Dari hasil akusisi tersebut dihasilkan file dengan ekstensi *.lime. Selanjutnya file hasil akusisi tersebut dianalisa menggunakan tools FTK Imager untuk mengetahui bukti informasi digital apa saja yang tersimpan di random access memory laptop linux ubuntu. Tahapan akusisi data di dokumentasikan dengan menggunakan tabel validasi seperti yang tercantum pada Tabel 4.4

Tabel 4.4 Validasi Hasil Akuisisi Random Access Memory Linux Ubuntu

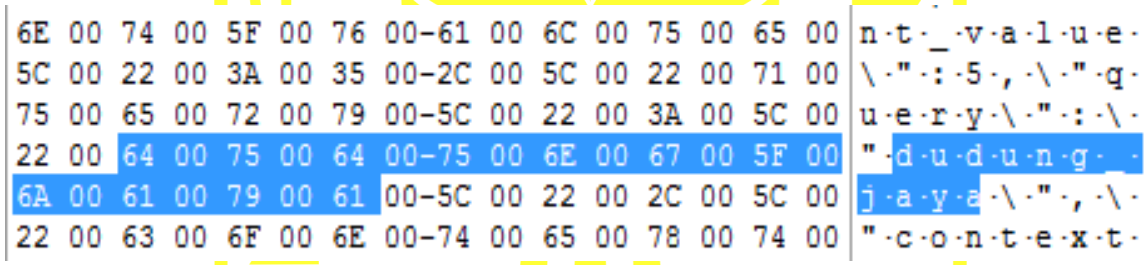
| No | Aktivitas | OS | Alat | Tools | Tanggal | Waktu | Hasil |
|---|---|---|---|---|---|---|---|
| 1 | Pencarian Email | Linux Ubuntu | Laptop | LiME FTK Imager | 30 Januari 2018 | 05.54 PM | Gambar 4.15 |
| 2 | Pencarian Username | Linux Ubuntu | Laptop | LiME FTK Imager | 30 Januari 2018 | 05.54 PM | Gambar 4.16 |
| 3 | Pencarian Link URL | Linux Ubuntu | Laptop | LiME FTK Imager | 30 Januari 2018 | 05.54 PM | Gambar 4.17 |
| 4 | Pencarian Password | Linux Ubuntu | Laptop | LiME FTK Imager | 17 Maret 2018 | 12.53 AM | Gambar 4.18 |
| 5 | Account Internet Banking | Linux Ubuntu | Laptop | LiME FTK Imager | 17 Maret 2018 | 12.53 AM | Gambar 4.19 |
| 6 | Account Paypal | Linux Ubuntu | Laptop | LiME FTK Imager | 17 Maret 2018 | 12.53 AM | Gambar 4.20 |
| 7 | Account Bitcoin | Linux Ubuntu | Laptop | LiME FTK Imager | 17 Maret 2018 | 12.53 AM | Gambar 4.21 |

Bukti pertama yang berhasil didapatkan dari hasil akusisi data pada random access memory laptop linux ubuntu diketahui account email yang biasa diakses yaitu seperti tercantum pada Gambar 4.15




Gambar 4.15 Bukti Email pada Laptop Linux Ubuntu

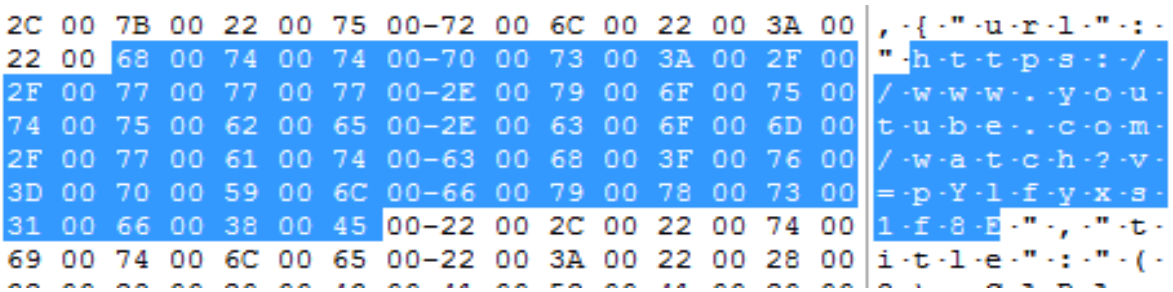
Berdasarkan hasil analisa pada Gambar 4.15 yang merupakan bukti hasil akuisisi random access memory pada perangkat laptop berbasis sistem operasi linux Ubuntu diketahui account email "abdulclp8@gmail.com". Bukti lainnya yang berhasil didapatkan yaitu account dengan username dudung_jaya sesuai dengan Gambar 4.16




Gambar 4.16 Bukti Username pada Laptop Linux Ubuntu

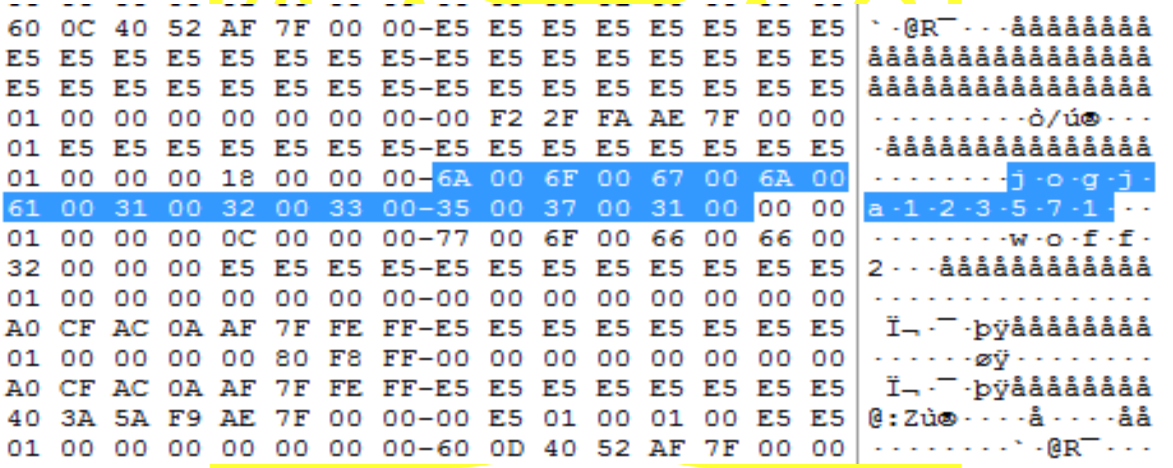
Berdasarkan Gambar 4.16 hasil dari analisa random access memory pada perangkat laptop linux ubuntu diketahui diketahui nilai heksa 64 00 75 00 64 00-75 00 6E 00 67 00 5F 00 6A 00 61 00 79 00 61 yang jika dikonversi menjadi nilai teks menjadi "dudung_jaya". Username ini diduga merupakan username untuk akses media sosial twitter yang digunakan pada laptop berbasis system operasi linux ubuntu.

Bukti lainnya yang juga berasal dari hasil akuisisi random access memory perangkat laptop linux ubuntu yaitu alamat link url yang diakses oleh user menggunakan browser dilaptop. Bukti ini selain tersimpan di cookies browser juga akan tersimpan di random access memory selama laptop tidak dimatikan atau shutdown. Bukti tersebut tercantum pada Gambar 4.17




Gambar 4.17 Bukti Link URL pada Laptop Linux Ubuntu

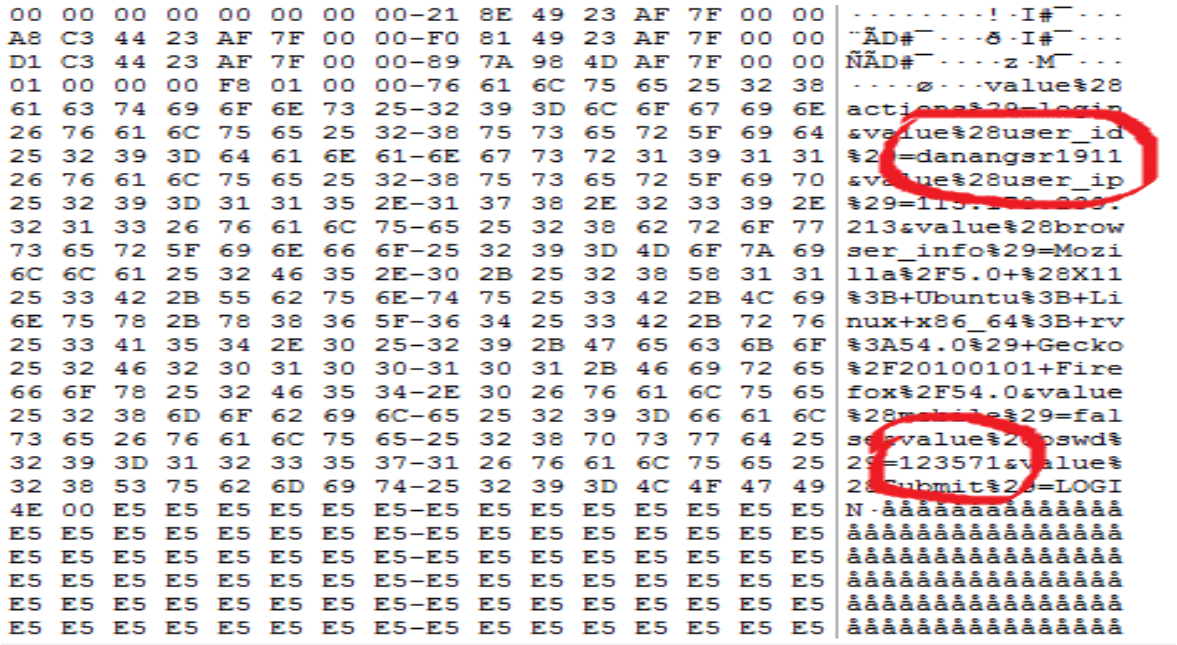
Gambar 4.17 merupakan bukti analisa dari hasil akuisisi random access memory pada laptop berbasis sistem operasi linux ubuntu menggunakan LiME (Linux Memory Extractor). Diketahui hasil konversi dari nilai heksa ke nilai teks terdapat alamat url yang tersimpan pada random access memory yang merupakan alamat url untuk akses channel youtube. Setelah diakses ternyata link youtube tersebut memuat content video cara membuat bom asap. Bukti lainnya yang telah berhasil dianalisa yaitu password. Bukti ini tercantum pada Gambar 4.18




Gambar 4.18 Bukti Password pada Laptop Linux Ubuntu

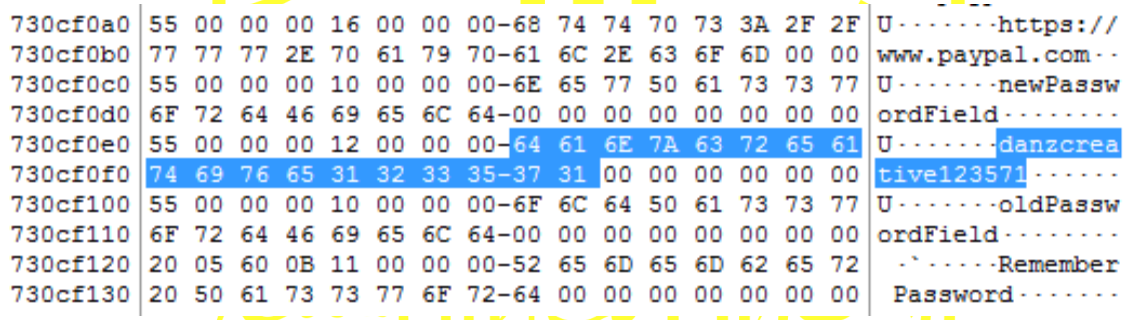
Berdasarkan analisa pada gambar 4.18 diketahui hasil konversi nilai heksa 6A 00 6F 00 67 00 6A 00 61 00 31 00 32 00 33 00-35 00 37 00 31 00 menjadi nilai teks “jogja123571”. Nilai teks ini sesuai dengan hasil akuisisi pada laptop lainnya yaitu terdapat kecocokan seperti pada gambar 4.12 dan 4.4. Nilai teks tersebut merupakan password untuk akses login facebook.

Bukti lain yang diyakini sangat penting yaitu bukti akses login untuk melakukan transaksi internet banking. Bukan hanya user_id saja tetapi password juga berhasil dianalisa dan terbaca dengan baik. Bukti account internet banking tersebut tercantum pada Gambar 4.19



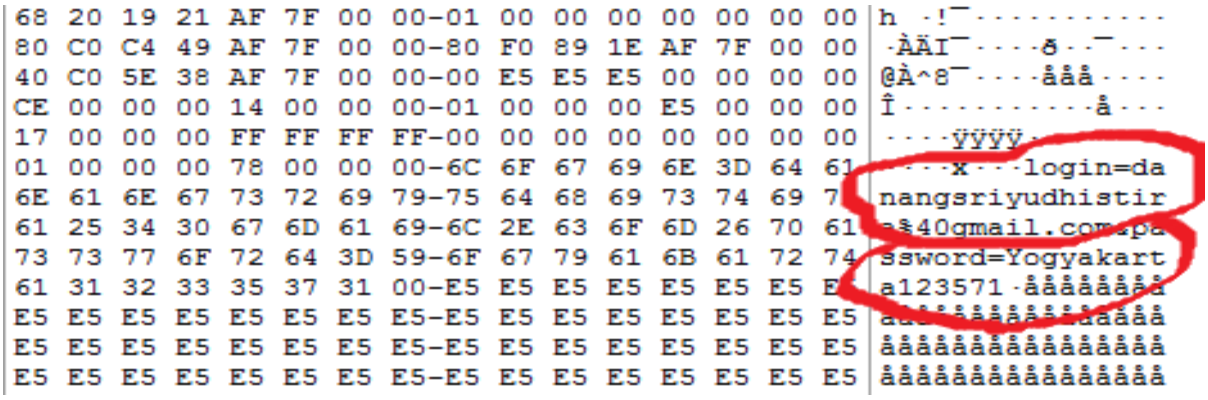
Gambar 4.19 Bukti Internet Banking pada Laptop Linux Ubuntu

Berdasarkan Gambar 4.19 yang merupakan hasil analisa dari random access memory pada laptop linux ubuntu diketahui terdapat user_id “danangsr1911” dan password “123571”. User_id dan password ini merupakan hak akses untuk login ke internet banking Bank BCA. Bukti lain yang berhasil diakusisi yaitu account paypal seperti yang tercantum pada Gambar 4.20



Gambar 4.20 Bukti Account Paypal pada Laptop Linux Ubuntu

Berdasarkan gambar 4.20 yang merupakan hasil analisa hasil akuisisi random access memory pada laptop linux ubuntu diketahui nilai heksa 64 61 6E 7A 63 72 65 61 74 69 76 65 31 32 33 35-37 31 jika dikonversi ke nilai teks menjadi “danzcreative123571”. Nilai teks tersebut merupakan password yang digunakan untuk akses login account paypal. Bukti terakhir yang berhasil diakusisi pada perangkat laptop linux Ubuntu yaitu account bitcoin sesuai yang tercantum pada Gambar 4.21




Gambar 4.21 Bukti Account Bitcoin pada Laptop Linux Ubuntu

Berdasarkan Gambar 4.21 yang merupakan hasil analisa dari random access memory pada perangkat laptop linux ubuntu diketahui terdapat akses login dengan username danangsriyudhistira@gmail.com dan password "Yogyakarta123571". Bukti password pada gambar 4.21 ada kecocokan dengan gambar 4.14 dan 4.8 yang merupakan akses login untuk account bitcoin.

### 4.4.4 Kesimpulan Analisa Random Access Memory Laptop Linux

Berdasarkan analisa terhadap hasil akuisisi random access memory dengan metode live forensics pada 3 perangkat laptop berbasis Linux Santoku, Linux Mint, dan Linux Ubuntu. Maka dapat ditarik kesimpulan bahwa pada distro Linux Santoku telah berhasil ditemukan informasi bukti digital terkait dengan username / user_id, password, accout email dan link url. Hal ini sesuai dengan rumusan masalah di Bab 1 yang sudah diutarakan sebelumnya. Akan tetapi untuk bukti akses account paypal belum bisa diketemukan pada laptop linux santoku.

Pada distro Linux Mint kesimpulan yang didapat berdasarkan analisa hasil penelitian adalah sama dengan hasil analisa di Linux Santoku yaitu berhasil menemukan account email, username / user_id, password, dan link url yang menjadi fokus penelitian ini. Hal ini juga telah sesuai dengan rumusan masalah pada Bab 1. Akan tetapi untuk bukti akses account paypal belum bisa diketemukan pada laptop linux mint.

Berbeda dengan Linux Santoku dan Linux Mint, analisa pada Linux Ubuntu telah berhasil menemukan semua informasi terkait dengan user_id / username, password, account email, dan link url. Berdasarkan analisa dari ketiga barang bukti laptop tersebut, secara garis besar dapat ditarik kesimpulan sesuai dengan Tabel 4.5

Tabel 4.5 Kesimpulan Hasil Akuisisi Random Access Memory Laptop Berbasis Linux

| No | Hasil Akusisi | Laptop Linux Santoku | Laptop Linux Mint | Laptop Linux Ubuntu |
|---|---|---|---|---|
| 1 | User_id / Username | √ | √ | √ |
| 2 | Password | √ | √ | √ |
| 3 | Account Email | √ | √ | √ |
| 4 | Link Url | √ | √ | √ |
| 5 | Account Internet Banking | √ | √ | √ |
| 6 | Account Bitcoin | √ | √ | √ |
| 7 | Account Paypal | - | - | √ |

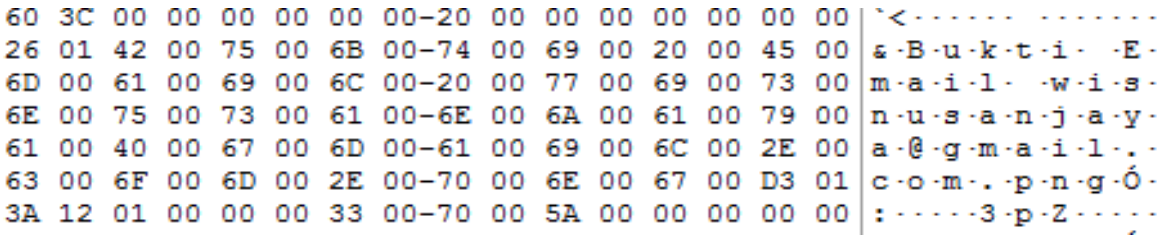
## 4.5 Analisa Random Access Memory Laptop Berbasis Sistem Operasi Windows

Dalam melakukan analisa terhadap random access memory pada laptop berbasis sistem operasi windows, dilakukan beberapa skenario pengujian guna mendapatkan hasil yang diharapkan untuk mampu menjawab rumusan masalah yang sudah diutarakan sebelumnya dibab 1. Hasil pengujian random access memory pada sistem operasi windows seperti yang tercantum pada Tabel 4.6

Tabel 4.6 Hasil Analisa Random Access Memory Laptop Berbasis Windows

| Devices | Kondisi | | |
|---|---|---|---|
| | Normal Setelah Booting | Kondisi Setelah Terkoneksi Internet | Setelah Dilakukan Hibernate |
| Random Access Memory Laptop Sistem Operasi Windows | Data yang tersimpan di random access memory merupakan nama nama file yang ada di harddisk dan file yang sedang running. | Kondisi normal ditambah dengan beberapa file yang diakses setelah terkoneksi internet, seperti alamat url, email dan username. | Kondisi terakhir sebelum laptop hibernate dan laptop kembali dinyalakan data yang tersimpan pada random access memory masih sama. |

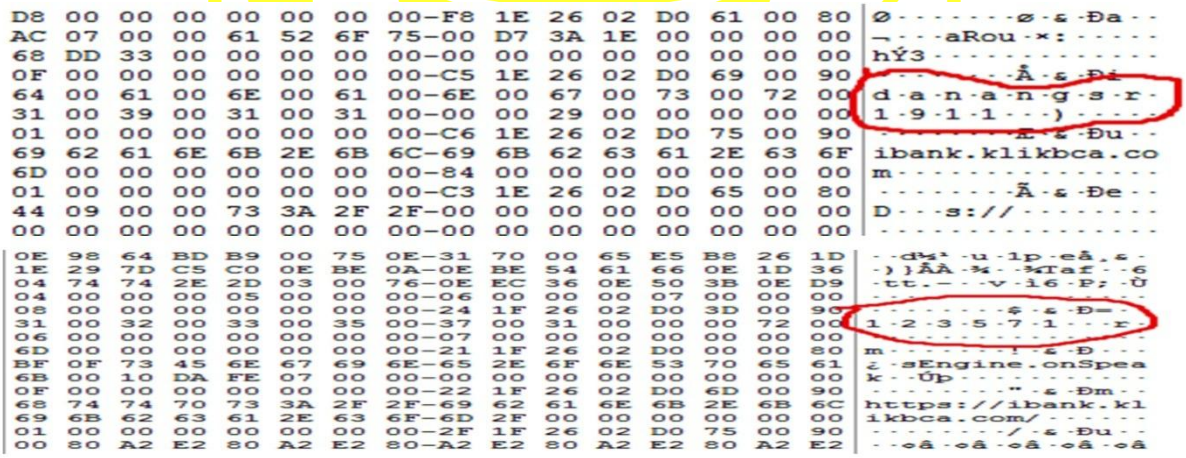
Berdasarkan hasil analisa terhadap hasil akusisi random access memory pada laptop berbasis sistem operasi windows sesuai dengan Tabel 4.6, diketahui bahwa pada kondisi normal setelah booting hanya ditemukan nama nama file seperti yang tersimpan di harddisk, tidak ditemukan file lainnya. Kondisi ini dikarenakan belum digunakannya laptop tersebut untuk melakukan suatu akses ke internet atau kegiatan penggunaan tools yang ada di laptop. Sebagai contoh nama file yang tersimpan di random access memory pada laptop dalam kondisi setelah booting tercantum pada Gambar 4.22.



Gambar 4.22 Hasil Akuisisi Random Access Memory Setelah Booting

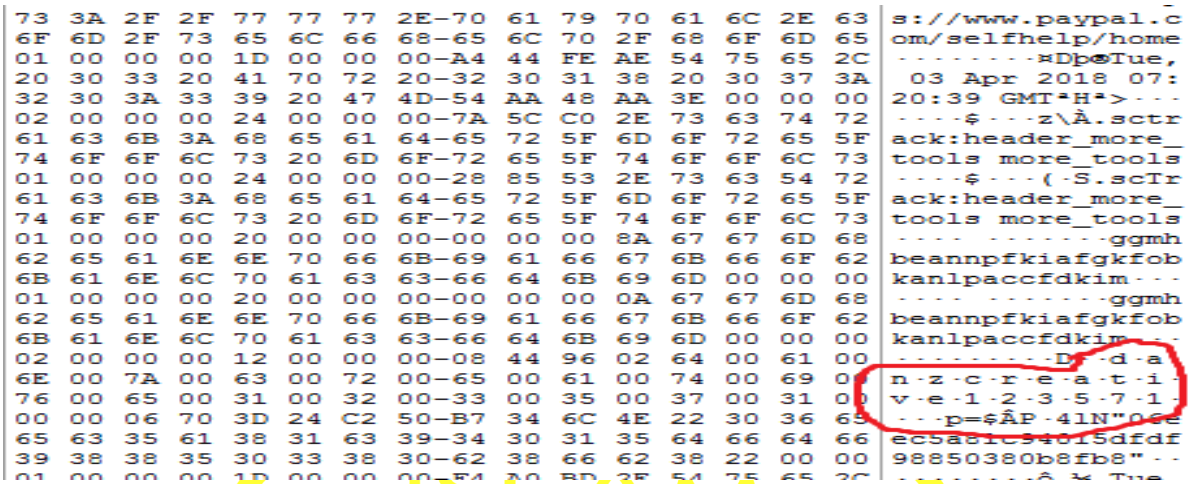
Gambar 4.22 diatas menunjukkan bahwa terdapat file dengan nama "bukti email wisnusanjaya" dengan format ekstensi *.png* yang tersimpan di harddisk dan terbaca oleh random access memory ketika sistem running atau berjalan.

Berbeda ketika laptop sudah terkoneksi dengan internet dan sudah dilakukan beberapa aktifitas untuk berselancar didunia maya dengan menggunakan browser. Ada beberapa data dan aktifitas yang ikut tersimpan di random access memory selain tersimpan dihistory cookies browser diantaranya ketika user melakukan akses untuk login ke internet banking dan paypal guna melakukan transaksi, maka secara otomatis user_id dan password juga akan tersimpan kedalam random access memory. Sebagai buktinya seperti yang tercantum pada Gambar 4.23.



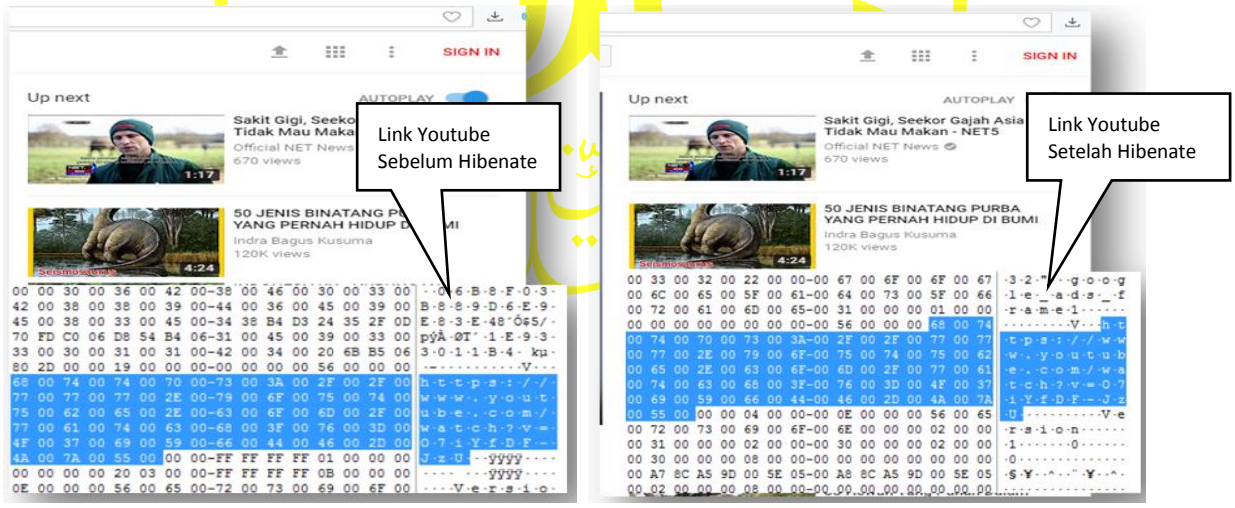
Gambar 4.23 Bukti Akses Internet Banking Sebelum Dilakukan Hibernate

Berdasarkan Gambar 4.23 diketahui bahwa user_id dan password untuk akses login ke aplikasi internet banking melalui browser laptop menggunakan user_id "danangsri19111" dan password "123571". Account tersebut tersimpan di random access memory. Hal ini juga sama ketika user melakukan akses untuk login paypal, password secara otomatis tersimpan dirandom access memory. Sebagai buktinya seperti pada gambar 4.24



Gambar 4.24 Bukti Akses Login Paypal Sebelum Dilakukan Hibernate

Gambar 4.24 membuktikan bahwa setiap kita melakukan akses login, user_id dan password yang kita inputkan akan tersimpan di random access memory. Hasil pengujian terakhir dilakukan pada random access memory perangkat laptop saat kondisi hibernate dengan uji coba durasi waktu 20 menit, setelah laptop diaktifkan kembali ke kondisi normal, keadaan isi random access memory tetap sama seperti kondisi sebelum dilakukan hibernate, file ataupun akses link url yang kita buka tetap dalam kondisi aktif. Hal ini dibuktikan dengan membandingkan isi random access memory pada saat sebelum dilakukan hibernate dan setelah keadaan normal diaktifkan kembali. Hasil perbandingan tersebut menunjukkan kesamaan isi random access memory, hal ini mengambil contoh pada bukti akses link channel youtube.



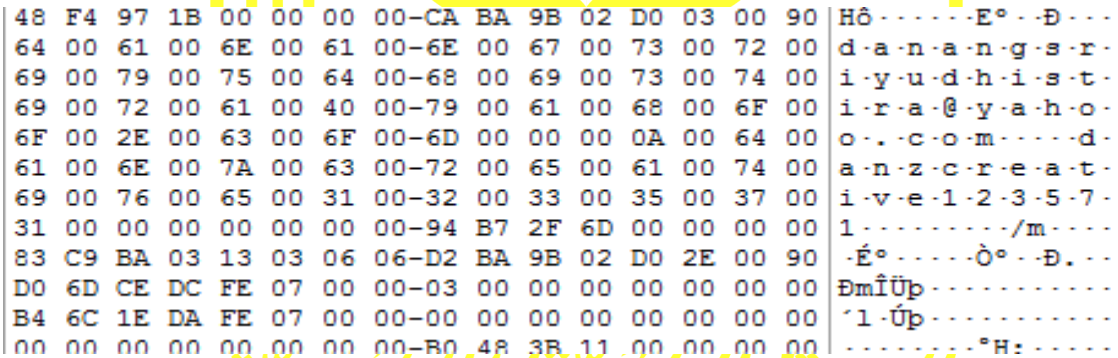

Dari hasil analisa terhadap kedua gambar diatas maka ditemukan fakta bahwa tidak ada perbedaan nilai teks, jika dikonversi menghasilkan link youtube yang sama. Ini

membuktikan bahwa kondisi random access memory sebelum hibernate dengan kondisi random access memory setelah hibernate tidak ada perubahan kecuali pada headernya saja.

## 4.6 Analisa Hasil

Berdasarkan latar belakang masalah yang terjadi mengenai kasus cybercrime tentang penyalahgunaan account secara illegal. Dalam hal ini adalah pencurian user_id dan juga password maka tindakan ini dapat berakibat kerugian bagi si pemilik sah account tersebut dikarenakan account miliknya digunakan secara illegal oleh orang yang tak bertanggung jawab.

Informasi sensitif atau bersifat private terkait user_id dan password tersebut tersimpan di dalam random access memory pada perangkat komputer ketika kita melakukan akses login ke sebuah laman internet (Divyang Rahevar, 2013). Yang memiliki hak akses tersebut seharusnya hanyalah si pemilik sah account. Akan tetapi kenapa bisa terjadi penggunaan account secara illegal ? Dalam hal ini dimungkinkan telah terjadi pengambilan secara illegal terhadap account tersebut melalui akuisisi data yang ada di random access memory. Sebagai contoh terdapat account paypal yang tersimpan di random access memory seperti tercantum pada Gambar 4.25.




Gambar 4.25 Bukti Akses Login Account Paypal

Berdasarkan hasil analisa random access memory pada perangkat laptop seperti tercantum pada Gambar 4.25 diketahui bahwa akses login account paypal menggunakan user_id berupa email “danangsriyudhistira@yahoo.com” dan password “danzcreative123571”. Bukti akses login tersebut akan tersimpan dirandom access memory selain di cookies browser laptop yang kita gunakan untuk akses website paypal.

Penelitian ini memberikan gambaran bagaimana kita bisa melakukan akuisisi data yang ada di random access memory pada perangkat laptop untuk mendapatkan informasi bukti digital terkait user_id dan password serta informasi digital lain yang tersimpan di

random access memory seperti link url. Dari hasil penelitian dan kajian berdasarkan studi literature diketahui bahwa informasi yang kita akses akan tetap tersimpan di random access memory selama perangkat laptop tidak kita matikan. Walaupun kita sudah melakukan proses logout pada pada laman aplikasi browser yang mengharuskan kita untuk menginputkan user_id dan password, informasi digital terkait account tersebut akan tetap tersimpan di random access memory.

Solusi dari penanganan terkait data informasi yang ada di random access memory agar tidak disalahgunakan oleh orang lain yaitu apa bila kita telah selesai menggunakan komputer atau laptop maka ada baiknya segera dilakukan shutdown pada perangkat yang kita gunakan, agar jejak jejak digital yang kita akses dalam laptop dan komputer tersebut akan segera hilang.

# BAB 5
# Kesimpulan dan Saran

## 5.1 Kesimpulan

Setelah dilakukan serangkaian penelitian dan analisa terhadap random access memory pada sistem operasi linux dan windows dapat diambil kesimpulan bahwa random access memory mampu menyimpan informasi terkait segala aktifitas yang dilakukan oleh user atau pengguna. Dalam penelitian ini telah berhasil dilakukan akusisi pada random access memory untuk menemukan account email, user_id / username, password, dan link url. Cara untuk mendapatkan data informasi digital tersebut dengan melakukan akusisi random access memory menggunakan tools linux memory extractor (LiME) pada laptop berbasis system operasi linux dan menggunakan tools FTK imager digunakan untuk laptop berbasis system operasi windows

Tools linux memory extractor (LiME) dan FTK Imager mampu melakukan capture memori secara menyeluruh sehingga informasi yang didapatkan dari random access memory bisa lengkap dan bisa digunakan untuk barang bukti digital dalam suatu penanganan kasus kejahatan yang melibatkan barang bukti laptop berbasis sistem operasi linux dan windows.

## 5.2 Saran

Pada penelitian ini telah berhasil menemukan akses login account social media, internet banking dan paypal yang tersimpan di random access memory pada perangkat laptop baik berupa user_id atau username dan password, untuk pengembangan penelitian selanjutnya diharapkan mampu menemukan account kartu kredit yang diinputkan ketika melakukan transaksi E-Commerce untuk berbelanja secara online dengan menggunakan fasilitas browser dilaptop. Account kartu kredit tersebut selain tersimpan di cookies browser juga akan tersimpan dalam random access memory pada perangkat yang digunakan dalam hal ini laptop.

# Daftar Pustaka


Anand, V. N. (2016). Acquisition Of Volatile Data From Linux System. *International Journal of Advanced Research Trends in Engineering and Technology*, *3*(5), 95–97.

Bharath, B., & R, N. M. A. (2015). Automated Live Forensics Analysis for Volatile Data Acquisition. *Int. Journal of Engineering Research and Applications*, *5*(3), 81–84.

Dave, R., Mistry, N. R., & Dahiya, M. S. (2014). Volatile Memory Based Forensic Artifacts & Analysis. International Journal For Research In Applied Science And Engineering Technology, *2*(I), 120–124.

Divyang Rahevar. (2013). Study on Live analysis of Windows Physical Memory. *IOSR Journal of Computer Engineering (IOSR-JCE)* , *15*(4), 76–80. Retrieved from http://www.iosrjournals.org/iosr-jce/papers/Vol15-issue4/M01547680.pdf?id=7557

Faiz, M. (2017). Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary. *Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM)*, *4*(April), 207–211.

Gruhn, M., & Freiling, F. C. (2016). Evaluating atomicity, and integrity of correct memory acquisition methods. *Www.elsevier.com/locate/diin DFRWS*, *16*, S1–S10. https://doi.org/10.1016/j.diin.2016.01.003

Gupta, M. P. (2013). Capturing Ephemeral Evidence Using Live Forensics. *IOSR Journal of Electronics and Communication Engineering*, 109–113.

Karayianni, S., & Katos, V. (2012a). Practical password harvesting from volatile memory. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, *99 LNICST*(May 2014), 17–22. https://doi.org/10.1007/978-3-642-33448-1_3

Karayianni, S., & Katos, V. (2012b). Practical password harvesting from volatile memory. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, *99 LNICST*(August), 17–22. https://doi.org/10.1007/978-3-642-33448-1_3

Nisbet, A. (2016). Memory forensic data recovery utilising RAM cooling methods, (December), 11–16. https://doi.org/10.4225/75/58a54cc3c64a2

Panchal, E. P. (2013). Extraction of Persistence and Volatile Forensics Evidences from Computer System. *International Journal of Research in Computer Engineering and Information Technology*, *1*(1), 1–5.

Richard Carbone. (2012). The definitive guide to Linux-based live memory acquisition

tools. *DRDC Valcartier TM 2012-319*, (September). Retrieved from http://cradpdf.drdc-rddc.gc.ca/PDFS/unc160/p800486_A1b.pdf

Robert H. Blissmer 1985-1986, "Computer Annual, An Introduction to Information System (2nd Edition)", John Wiley & Sons.

Socała, A., & Cohen, M. (2016). Automatic profile generation for live Linux Memory analysis. *Proceedings of the Third Annual DFRWS Europe Automatic*, *16*, S11–S24. https://doi.org/10.1016/j.diin.2016.01.004

Stüttgen, J., Vömel, S., & Denzel, M. (2015). Acquisition and analysis of compromised firmware using memory forensics. *DFRWS 2015 Europe*, *12*(S1), S50–S60. https://doi.org/10.1016/j.diin.2015.01.010

V.Carl Hamacher, Zvonko G. Vranesic, Safwat G. Zaky, (2001). "Computer Organization (5th Edition)", McGraw-Hill.

Vömel, S. (2013). Forensic Acquisition and Analysis of Volatile Data in Memory.