Metode Live Memory Acquisition untuk Pencarian Artefak Digital Perangkat Memori Laptop Berdasarkan Simulasi Kasus Kejahatan Siber

by Triawan Cahyanto

Submission date: 13-Feb-2022 04:33AM (UTC+0800)
Submission ID: 1760842874
File name: 28-Article_Text-219-1-10-20211216.pdf (495.02K)
Word count: 3703
Character count: 22795

BIOS : Jurnal Teknologi Informasi dan Rekayasa Komputer
Vol. 2, No. 2, September 2021, hlm. 87 - 94
ISSN: 2722-0850
Laman Jurnal: http://bios.sinergis.org

Metode *Live Memory Acquisition* untuk Pencarian Artefak Digital Perangkat Memori Laptop Berdasarkan Simulasi Kasus Kejahatan Siber

M. Ainul Yaqin[1], Triawan Adi Cahyanto[2], Nur Qadariyah Fitriyah[3]
[1]Program Studi Teknik Informatika, Universitas Muhammadiyah Jember, ainul.yakin009@gmail.com
[2]Program Studi Teknik Informatika, Universitas Muhammadiyah Jember, triawanac@unmuhjember.ac.id
[3]Program Studi Teknik Informatika, Universitas Muhammadiyah Jember, nurfitriyah@unmuhjember.ac.id

Keywords:

Live Memory Acquisition,
Digital Artifact,
Device Memory Analysis,
Social Media Investigation,
Cybercrime,

ABSTRACT

Information technology's hardware and software are constantly evolving. The rise in cybercrime cases is consistent with this trend. While operating systems can be hacked, personal data can be stolen and encrypted, making it impossible for users to access the information. Cybercriminals are using social media data to target personal information currently. Users' usernames, passwords, and other personal information can be stored in a device's memory, as well as browser cookies. Pre-analysis, analysis, and post-analysis are the three stages of the research process. "Live Memory Acquisition" is the proper method for obtaining data from a device's memory. There is digital evidence in the form of an email address, a password, Facebook, and PayPal accounts as well as a link URL discovered in the analysis of the results of the acquisition of artifact one. The results of the artifact 2 acquisition did not reveal any passwords. There was no evidence of email or Facebook passwords in the analysis of artifact 3 acquisition results, but the overall data test results showed that the total number of test results on artifact 1 was 100%, 57.14% on artifact 2, and 71.42% on artifact 3.

Kata Kunci

Akuisisi Langsung Memori,
Artefak Digital,
Analisis Memori Perangkat,
Investigasi Sosial Media,
Pelanggaran Siber,

ABSTRAK

Teknologi informasi selalu berkembang baik dari sisi perangkat keras maupun perangkat lunak. Hal ini selaras pula dengan meningkatnya kasus kejahatan siber. Kejahatan siber saat ini tidak hanya merusak sistem operasi namun juga melakukan pencurian data pribadi dan mengenkripsi data agar terkunci serta tidak dapat diakses oleh pengguna. Data pribadi yang menjadi sasaran kejahatan siber pada saat ini adalah data sosial media. Data tersebut dapat *berupa username, email, password, cookies browser,* dan lain-lain yang umumnya tersimpan pada memori suatu perangkat. Tahapan penelitian dibagi menjadi tiga fase, fase pre-analisis, fase analisis dan post-analisis. Terdapat metode yang tepat untuk melakukan akuisisi data pada memori perangkat yaitu *Live Memory Acquisition*. Analisis pada hasil akuisisi artefak_1, ditemukan bukti digital berupa user_id email, password email, user_id facebook, password facebook, user_id paypal, password paypal dan link url. Analisis pada hasil akuisisi artefak_2 tidak ditemukan bukti password. Sedangkan analisis pada hasil akuisisi artefak_3 tidak ditemukan bukti password email dan password facebook. Hasil pengujian data keseluruhan ditemukan jumlah total keseluruhan dari hasil pengujian pada artefak_1 sebesar 100%, pada artefak_2 sebesar 57,14% dan pada artefak_3 adalah sebesar 71,42%.

Korespondensi Penulis:

Triawan Adi Cahyanto,
Universitas Muhammadiyah Jember,
Jalan Karimata 49 Jember
Telepon: +6282377666660
Email: triawanac@unmuhjember.ac.id

1. PENDAHULUAN

Beberapa jenis dan model teknologi dalam bentuk digital sedang populer dan diminati oleh masyarakat, salah satunya adalah internet. Penggunaan internet melalui berbagai aplikasi dapat dimanfaatkan oleh pengguna komputer. Seiring meluasnya penggunaan komputer maka dimungkinkan terdapat peluang kejahatan yang melibatkan komputer.

Untuk menanggulangi peristiwa tersebut, selain dibutuhkan manajemen keamanan yang bertujuan untuk mencegah, diperlukan pula prosedur penanganan apabila suatu risiko terjadi. Salah satu prosedur penanganan yang dilakukan adalah forensik komputer. Forensik komputer adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti digital yang ditemui pada komputer dan media penyimpanan digital, serta menggabungkan keilmuan dibidang hukum dan komputer [1], [2].

Kasus kejahatan siber yang terjadi sekarang ini sudah mengarah terhadap pencurian *username, email dan password* yang merupakan informasi pribadi serta bersifat sensitif bagi sebagian orang [3]. Contohnya adalah seperti pada akun *email, facebook, paypal*, dan lainnya. Akibat dari kejadian pencurian *username, email* dan *password*, bisa saja terjadi pencemaran nama baik yang dilakukan oleh seseorang dengan membuat tulisan tertentu/informasi bohong (*hoax*) pada akun sosial media korban [4]. Sedangkan jika yang dicuri merupakan akun finansial seperti *paypal* maka ada kemungkinan akan terjadi tindak pidana pencurian uang melalui transfer *paypal* dengan cara membebankan biaya kepada si pemilik sah akun.

Informasi akun berupa *username, email* dan *password* selain tersimpan pada *cookies browser*, juga tersimpan di memori perangkat tersebut. Untuk itu diperlukan teknik atau metode yang tepat untuk menganalisis memori pada perangkat laptop. Hal ini dikarenakan data yang ada di memori perangkat bersifat volatil (mudah berubah), maksudnya yaitu data akan hilang jika komputer dimatikan secara prosedural atau mengalami *restart* [5]. Akuisisi data digital yang terdapat di memori perangkat hanya bisa dilakukan ketika sistem dalam kondisi hidup / sedang berjalan. Hal ini berbeda dengan proses akuisisi pada media penyimpanan lain yang bersifat non-volatil. Proses akuisisi data baik dalam kondisi hidup maupun mati tidak menyebabkan data tersebut hilang.

Data volatil menggambarkan seluruh kegiatan yang sedang terjadi / berjalan pada sistem di perangkat yang digunakan. Oleh karena itu, metode *Live Memory Acquisition* adalah metode yang tepat untuk menjamin integritas / legalitas data volatil tanpa menghilangkan data yang berpotensi menjadi barang bukti digital. Jika dibandingkan dengan metode tradisional forensik atau *dead forensic*, metode *Live Memory Acquisition* adalah pilihan yang tepat untuk akuisisi data terhadap media penyimpanan yang bersifat volatil. Kekurangan dari metode tradisional forensik adalah tidak bisa mendapatkan data memori tertentu apabila kondisi sistemnya mati. Contoh kondisi yang dimaksud antara lain aktivitas memori, *network process, swap file, running system process*, dan lain-lain.

2. METODE PENELITIAN

2.1 Studi Literatur

Berikut ini terdapat *literature review* terkait penelitian terdahulu yang menjadi ide dasar untuk penelitian ini adalah sebagai berikut:

Tabel 1. Komparasi Penelitian Terdahulu

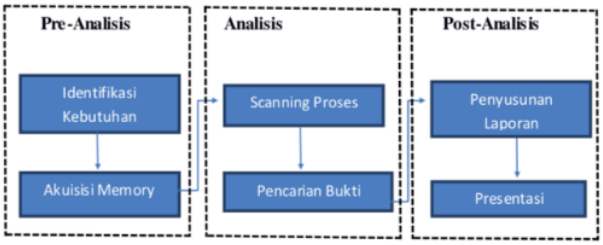
No	Peneliti	Sistem Operasi	Tools yang digunakan	Aspek yang diteliti
1	R. Bintang (2018)	*Windows 10*	*FTK Imager*	Sistem keamanan media sosial (*facebook, instagram, twitter*)
2	D. Yudhistira (2018)	*Windows, Linux*	*LiME, FTK Imager*	*User Id, email, password* dan informasi digital lainnya
3	T. Rochmadi (2017)	*Windows*	*Dumplt FireStag, Volatility dan WinHex*	*History, Timestamp* dan *password*
4	R. Umar (2016	*Windows*	*FTK Imager dan EnCase Microsoft account*	Perbandingan tools yang digunakan dalam metode *live forensics*
5	T. Larasati (2017)	*Windows 10*	*Winhex dan Belkasoft Evidence Center*	Aplikasi *Instant messenger* seperti *facebook, LINE* dan *telegram*
Usulan penelitian		Melakukan akuisisi pada memori perangkat laptop berbasis linux menggunakan metode *live memory acquisition*	Tools yang digunakan dalam penelitian adalah *Linux Memory Extractor (LiME)* untuk mengakuisisi data memori dan *Volatility* untuk menganalisa dan mencari artefak digital	Artefak digital yang dicari adalah *user_id email, password email, user_id facebook, password facebook, user_id paypal, password paypal* dan *link url*

Penelitian yang dilakukan oleh [6] dengan judul "Perancangan Perbandingan *Live Forensics* Pada Keamanan Media Sosial *Instagram, Facebook* dan *Twitter* di *Windows* 10". Pada penelitian tersebut menjelaskan tentang perbandingan sistem keamanan pada media sosial *instagram, facebook* dan *twitter* dengan menggunakan metode *National Institute of Justice* (NIJ). Metode tersebut diharapkan dapat mengetahui tingkat keamanan dari setiap media sosial tersebut. Penelitian yang dilakukan oleh [7] dengan judul "Metode *Live Forensics* Untuk Analisis *Random*

Access Memory Pada Perangkat Laptop". Pada penelitian tersebut menjelaskan tentang cara kerja metode *live forensics* pada perangkat laptop berbasis *linux* dan *windows*. Penelitian yang dilakukan oleh [8] dengan judul "*Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser*". Menjelaskan tentang keamanan beberapa *web browser* untuk mencegah kegiatan kriminal. Penelitian yang dilakukan oleh [9] dengan Judul "Analisis Kinerja Metode *Live Forensics* Untuk Investigasi *Random Access Memory* Pada Sistem *Proprietary*" yang menjelaskan tentang perbandingan *tools* yang digunakan dalam metode *live forensics*. Perbandingan tersebut mengacu pada penggunaan memori, waktu, jumlah langkah dan akurasi paling baik dalam melakukan *live forensics*. Penelitian yang dilakukan oleh [10] yang berjudul "Analisis *Live Forensics* Untuk Perbandingan Aplikasi *Instant Messenger* Pada Sistem Operasi *Windows* 10". Penelitian tersebut menganalisis aplikasi *instant messenger* seperti *facebook*, *LINE* dan *telegram* untuk mengetahui aplikasi yang mudah dan sulit memperoleh data untuk bukti digital.

2.2 Tahapan Penelitian

Metode dalam penelitian ini merupakan integrasi dari model proses umum respons insiden dan forensik komputer. Model umum investigasi forensik komputer dan metodologi investigasi dilakukan secara bertahap untuk menelusuri proses penggunaan sumber daya komputer. Hal ini diilustrasikan pada gambar berikut:



Gambar 1. Tahapan Penelitian

2.3 Pre-Analisis

Tahap *pre*-analisis terdiri dari dua proses, yaitu:

1. Identifikasi Kebutuhan

   Mengidentifikasi kebutuhan apa saja yang digunakan selama proses analisa dan penelitian, baik *hardware*, *software* maupun bahan-bahan yang berkaitan dengan penelitian.

2. Akuisisi Memori

   Pada tahap ini akan dilakukan akuisisi memori pada perangkat laptop untuk mengumpulkan data-data yang diperlukan dalam melakukan penelitian. Tahap ini dimaksudkan untuk mengumpulkan informasi *live* data yang memberikan informasi penting dari sistem menggunakan *Linux Memory Extractor (LiME)*. Dengan adanya informasi mengenai sistem dalam *live* data, informasi mengenai data yang berhubungan dengan kasus tersebut, penyidik dapat menginvestigasi keberadaan berkas-berkas yang berkaitan dengan kasus.

2.4 Analisis

Tahap analisis merupakan tahap lanjutan dari tahap *pre*-analisis. Tahapannya terdiri dari dua proses, yaitu:

1. *Scanning* Proses

   Melakukan *scanning* proses menggunakan *tool volatility* untuk mengetahui aktivitas yang telah diproses oleh memori perangkat laptop dan mengolah data yang didapatkan dari *scanning* proses tersebut untuk mencari artefak digital.

2. Pencarian Bukti

   Melakukan proses pencarian artefak digital menggunakan *tool volatility* pada memori perangkat laptop. Untuk mencari artefak digital yaitu dengan cara memproses hasil dari *scanning* data pada memori perangkat laptop. Selain itu berkas-berkas bukti diinvestigasi berdasarkan hasil analisis data dan pemahaman kasus secara keseluruhan untuk memperoleh data maupun informasi yang dibutuhkan.

2.5 Post-Analisis

Tahap *post*-analisis merupakan tahap akhir yang membahas dan menyimpulkan hasil yang diperoleh selama simulasi dan pengujian. Tahap ini terdiri dari dua proses utama, yaitu:

1. Penyusunan laporan

   Menyajikan hasil temuan dari data akuisisi memori secara rinci berdasarkan dokumentasi dari semua tahapan yang sudah dilakukan.

2. Presentasi

   Menjelaskan mengenai apa saja yang diperoleh selama hasil investigasi dengan menarik kesimpulan dari semua kegiatan penelitian dan menjelaskannya untuk bukti di pengadilan.

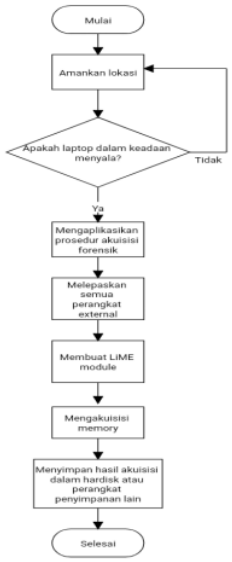
2.6 Simulasi Kasus Kejahatan Siber

Kasus kejahatan siber yang digunakan sebagai objek penelitian merupakan simulasi kasus. Adapun gambaran simulasi kasus dapat dilihat pada berikut ini:

Gambar 2. Skenario Kasus Kejahatan Siber

2.7 Kerangka Akuisisi Data Memori

Proses investigasi pada memori perangkat laptop memerlukan tahapan yang menggambarkan alur proses penanganan barang bukti serta bagaimana cara melakukan akuisisi data untuk mendapatkan barang bukti digital pada memori perangkat.



Gambar 3. Tahapan Akuisisi Memori

Berdasarkan Gambar 3. diketahui bahwa sebelum melakukan akuisisi data terlebih dahulu mengamankan lokasi tempat ditemukan barang bukti. Selanjutnya jika laptop dalam kondisi menyala maka proses forensik akuisisi data dapat dilanjutkan. Untuk melakukan akuisisi data pada memori di perangkat laptop, sebelumnya lepaskan semua perangkat penyimpanan eksternal untuk menghindari virus yang dapat merusak data pada memori serta akuisisi data berjalan dengan baik. Perangkat laptop menggunakan sistem operasi berbasis *Linux*, proses *capture* memori menggunakan *LiME* (*Linux Memory Extractor*). Kemudian membuat modul *LiME* untuk memulai proses akuisisi data pada memori.

3. HASIL DAN ANALISIS

3.1 Akuisisi Memory Pada Perangkat Laptop Menggunakan LiME

Perangkat lunak *Linux Memory Extractor (LiME)* digunakan untuk mengakuisisi memori pada perangkat laptop berbasis linux. Proses akuisisi dilakukan dengan perintah *"sudo insmod lime-4.15.0-43-generic.ko "path=/home/ainul/Documents/artefak.lime format=lime"*. Proses akuisisi memori dilakukan sebanyak tiga kali agar kerelevanan data terjamin sehingga dapat digunakan untuk mencari informasi digital, baik yang tersimpan di *cookies browser*, maupun di memori perangkat. Hasil akuisisi memori adalah sebagai berikut:

```
ainul@X453SA:~/Documents/LiME-master/src$ ls
disk.c  hash.c  lime-4.15.0-43-generic.ko  lime.mod.c  lime.o  main.o    Makefile.sample  Module.symvers  tcp.o
disk.o  hash.o  lime.h                     lime.mod.o  main.c  Makefile  modules.order    tcp.c
ainul@X453SA:~/Documents/LiME-master/src$ sudo insmod lime-4.15.0-43-generic.ko "path=/home/ainul/Documents/artefak_1.lime format=lime"
ainul@X453SA:~/Documents/LiME-master/src$ ls
disk.c  hash.c  lime-4.15.0-43-generic.ko  lime.mod.c  lime.o  main.o    Makefile.sample  Module.symvers  tcp.o
disk.o  hash.o  lime.h                     lime.mod.o  main.c  Makefile  modules.order    tcp.c
ainul@X453SA:~/Documents/LiME-master/src$ sudo insmod lime-4.15.0-43-generic.ko "path=/home/ainul/Documents/artefak_2.lime format=lime"
ainul@X453SA:~/Documents/LiME-master/src$ ls
disk.c  hash.c  lime-4.15.0-43-generic.ko  lime.mod.c  lime.o  main.o    Makefile.sample  Module.symvers  tcp.o
disk.o  hash.o  lime.h                     lime.mod.o  main.c  Makefile  modules.order    tcp.c
ainul@X453SA:~/Documents/LiME-master/src$ sudo insmod lime-4.15.0-43-generic.ko "path=/home/ainul/Documents/artefak_3.lime format=lime"
```

Gambar 4. Akuisisi memori perangkat laptop berbasis linux

3.2 Scanning Proses

Proses *scanning* dilakukan untuk melakukan pencarian data yang relevan dengan simulasi kasus yang sudah dibuat pada data hasil akuisisi memori. Dari hasil akuisisi memori pada perangkat berbasis *linux* pada *artefak_1.lime* ditemukan aktivitas *web browser firefox*. Berdasarkan aktivitas *web browser* tersebut nantinya akan dicari artefak digital yang berkaitan dengan simulasi kasus. Selanjutnya hasil akuisisi memori pada perangkat laptop pada *artefak_2.lime* ditemukan *aktivitas web browser chrome*. Kemudian pada akuisisi memori pada perangkat laptop pada *artefak_3.lime* ditemukan aktivitas *web browser opera*.

3.3 Pencarian Bukti Digital

Berdasarkan hasil *scanning* proses ditemukan tiga aktivitas web browser pada perangkat yang diduga digunakan sebagai tindak kejahatan penyalahgunaan account maka tahap berikutnya akan dilakukan pengujian data untuk menemukan artefak digital. *Web browser firefox id pid* 1832 terbukti menyimpan informasi terkait aktivitas pengguna yang terdiri dari aktivitas penggunaan *facebook*, *email* dan *paypal*. Data-data tersebut dapat ditemukan dengan mudah pada *cookies firefox* di hasil akusisi data memori artefak_1. Pengujian hasil akuisisi data *artefak_2* pada aktivitas *web browser chrome* pada memori perlu dilakukan dengan teliti. Terdapat perbedaan penemuan data, dimana data *password* gagal untuk dibaca karena terlindungi oleh proteksi *browser*. Namun pada artefak_2 ini terdapat beberapa *browsing history* yang berhasil ditemukan. Pengujian hasil akuisisi data artefak_3 memperoleh temuan data berupa aktivitas penggunaan *paypal, facebook* dan *link url* "https://www.tokopedia.com". Adapun rincian hasil temuan keseluruhan data artefak dapat dilihat pada tabel berikut ini.

Tabel 2. Hasil temuan data artefak

Data Artefak	Informasi yang ditemukan	Sumber
Email facebook	ainul_yakin94@yahoo.co.id	Artefak_1
Password facebook	a!nuly@qin	Artefak_1
Alamat *Email*	ainul.yakin009@gmail.com	Artefak_1
Password Email	a!nuly@qin	Artefak_1
Username Paypal	ainul.yakin009@gmail.com	Artefak_1
Password Paypal	a!nuly@qin	Artefak_1
Email facebook	ainul_yakin94@yahoo.co.id	Artefak_2
Alamat *Email*	ainul.yakin009@gmail.com	Artefak_2
Username Paypal	ainul.yakin009@gmail.com	Artefak_2
Browsing history	https://indoxxi.bz/ https://www.artikelcara10.com/2018/04/hack-facebook-tanpa-aplikasi	Artefak_2
Username Paypal	ainul.yakin009@gmail.com	Artefak_3
Password Paypal	ainuly@qin009	Artefak_3
Username Facebook	ainul_yakin94@yahoo.co.id	Artefak_3
Browsing history	https://www.tokopedia.com	Artefak_3

3.4 Skenario Pengujian Memori Sebelum Dan Setelah Dilakukan Shutdown

Pengujian bertujuan untuk membuktikan bahwa memori perangkat memang bersifat *volatile* atau sementara, yang artinya memori hanya menyimpan aktivitas yang dilakukan pengguna selama perangkat dalam kondisi menyala. Jika perangkat dalam kondisi mati atau kondisi *restart*, maka aktivitas yang dilakukan pengguna sebelumnya akan hilang atau tidak tersimpan lagi pada memori perangkat.

```
0x000000006dcd1580 gdbus              1035        -          -1         -1         ------------------ -
0x000000006dcd2b00 gmain              1052        -          -1         -1         ------------------ -
0x000000006dcd4080 gmain              1049        -          -1         -1         ------------------ -
0x000000006dcd5600 gnome-shell-cal    1335        -          -1         -1         ------------------ -
0x000000006de98000 gsd-wacom          1056        -          -1         -1         ------------------ -
0x000000006de99580 gsd-sharing        1048        -          -1         -1         ------------------ -
0x000000006de9ab00 gdbus              1047        -          -1         -1         ------------------ -
0x000000006de9c080 gsd-sound          1053        -          -1         -1         ------------------ -
0x000000006de9d600 gsd-smartcard      1051        -          -1         -1         ------------------ -
0x000000006e078000 gmain              1034        -          -1         -1         ------------------ -
0x000000006e079580 gdbus              1021        -          -1         -1         ------------------ -
0x000000006e07ab00 gdbus              1158        -          -1         -1         ------------------ -
0x000000006e07c080 gmain              1086        -          -1         -1         ------------------ -
0x000000006e07d600 packagekitd        1022        -          -1         -1         ------------------ -
0x000000006e0d0000 dconf worker       1330        -          -1         -1         ------------------ -
```

Gambar 5. Kondisi sebelum reboot pada memory perangkat laptop

Pengujian aktivitas dilakukan dengan cara akses ke *internet* menggunakan *web browser firefox*. Proses analisis dilakukan dengan bantuan *tools volatility*. Berdasarkan analisis, ditemukan aktivitas *web browser firefox* dengan *id pid* 2724 dan 2715. Selanjutnya dilakukan analisis memori perangkat laptop setelah perangkat laptop mengalami *restart*. Berikut adalah hasil dari analisa setelah perangkat laptop *restart* seperti gambar berikut ini

```
0x0000000079045600 avahi-daemon       683         -          -1         -1         ------------------ -
0x0000000079148000 FS Broker 2717     2724        -          0          0          0x0000000000000000 -
0x0000000079149580 firefox            2716        -          0          0          0x0000000000000000 -
0x000000007914ab00 ImageBr~geChild    2744        -          0          0          0x0000000000000000 -
0x000000007914c080 firefox            2715        -          0          0          0x0000000000000000 -
0x000000007914d600 ImageBr~geChild    2723        -          0          0          0x0000000000000000 -
0x0000000079158000 ImageIO            2829        -          0          0          0x0000000000000000 -
```

Gambar 6. Kondisi setelah reboot pada memory perangkat laptop

Gambar tersebut menunjukkan aktivitas dari sistem operasi *linux ubuntu* ketika perangkat menyala dan tidak ada aktivitas sebelumnya ketika sebelum perangkat di *restart*. Maka dari itu membuktikan bahwa data pada memori perangkat bersifat *volatile* atau sementara sehingga data-data yang sebelumnya dapat diperoleh menjadi hilang ketika dilakukan *restart* sistem.

3.5 Hasil Analisis

Setelah melakukan beberapa tahapan analisis, hasil analisis dalam penelitian ini dapat dilihat sebagai berikut :

Tabel 3. Hasil analisis artefak_1

No	PID	User Email	Pass Email	User Paypal	Pass Paypal	User Facebook	Pass Facebook	Link URL	Tidak Terdeteksi
1	1918	-	-	-	-	-	-	-	√
2	1832	√	√	√	√	√	√	√	-
3	1919	-	-	-	-	-	-	-	√

Berdasarkan tabel hasil analisis *artefak_1*, informasi yang didapat adalah pada *id pid* 1918 dan 1919 tidak dapat terdeteksi oleh *volatility*. Selanjutnya pada *id pid* 1832 berhasil menemukan artefak digital yang berkaitan dengan simulasi kasus. Untuk hasil analisis akuisisi data pada *artefak_2* pada aktivitas *web browser chrome* dapat dilihat pada tabel berikut

Tabel 4. Hasil analisis artefak_2

No	PID	User Email	Pass Email	User Paypal	Pass Paypal	User Facebook	Pass Facebook	Link URL	Tidak Terdeteksi
1	2491	-	-	-	-	-	-	-	-
2	2122	√	-	-	-	√	-	-	-
3	2310	√	-	-	-	-	-	-	-
4	2428	-	-	√	-	-	-	-	-
5	1735	-	-	-	-	-	-	-	√
6	1760	√	-	-	-	-	-	-	-
7	1720	√	-	-	-	√	-	√	-
8	1734	-	-	-	-	-	-	-	-
9	1814	-	-	-	-	-	-	-	-
10	1730	-	-	-	-	-	-	-	-
11	2367	√	-	-	-	-	-	-	-
12	3494	-	-	-	-	-	-	-	-
13	3546	-	-	-	-	-	-	-	√
14	2549	-	-	-	-	-	-	-	-
15	3556	-	-	-	-	-	-	-	-

Berdasarkan tabel hasil analisis *artefak_2,* informasi yang didapat yaitu ada 2 id pid yang tidak bisa diproses oleh *volatility* atau tidak bisa terdeteksi oleh *volatility* yaitu *id pid* 1735 dan 3546. Artefak digital yang ditemukan dari aktivitas *web browser chrome* berada pada *id pid* 2122, 2310, 2428, 1760, 1720 dan 2367 yaitu *username email, username facebook, username paypal* dan *link url* yang berkaitan dengan simulasi kasus. Untuk *id pid* 2491, 1734, 1814, 1730, 3494, 2549 dan 3556 tidak ditemukan artefak digital yang berkaitan dengan simulasi kasus.

Tabel 5. Hasil analisis artefak_3

No	PID	User Email	Pass Email	User Paypal	Pass Paypal	User Facebook	Pass Facebook	Link URL	Tidak Terdeteksi
1	2221	-	-	-	-	-	-	-	√
2	1955	-	-	-	-	-	-	-	-
3	1919	-	-	-	-	-	-	-	-
4	2247	-	-	√	√	-	-	-	-
5	2285	-	-	-	-	-	-	-	-
6	2247	-	-	-	-	-	-	-	-
7	1727	-	-	-	-	-	-	-	-
8	2479	-	-	-	-	-	-	-	√
9	1721	-	-	√	√	√	-	√	-
10	1785	-	-	-	-	-	-	-	-
11	1728	-	-	-	-	-	-	-	√
12	1799	√	-	-	-	-	-	-	-
13	1725	-	-	-	-	-	-	-	-
14	1773	-	-	-	-	-	-	-	-
15	1876	-	-	-	-	-	-	-	-
16	2324	-	-	-	-	-	-	-	-
17	2311	-	-	-	-	-	-	-	-

Tabel tersebut merupakan data hasil analisis artefak_3 dari aktivitas *web browser opera*. Artefak digital yang ditemukan ada pada *id pid* 2247, 1721 dan 1799 pada aktivitas *web browser opera* yaitu *username email, username paypal, password paypal, username facebook* dan *link url* yang berkaitan dengan simulasi kasus. Untuk *id pid* 2221, 2479 dan 1728 pada aktivitas *web browser opera* tidak dapat diproses atau tidak dapat terdeteksi oleh *volatility*. Untuk *id pid* 1955, 2285, 2247, 1727, 1785, 1725, 1773, 1876, 2324 dan 2311 tidak ditemukan artefak digital yang berkaitan dengan simulasi kasus.

Berdasarkan analisis pada hasil akuisisi memori pada perangkat berbasis *linux* dengan menggunakan metode *live forensics*, bahwa setiap aktivitas *web browser* dari ketiga akuisisi data terdapat artefak digital pada *id pid* yang berbeda-beda. Pada akuisisi pertama terdapat aktivitas *web browser firefox* dan menemukan artefak digital berupa *username / user_id, password* dari *account email, facebook* dan *paypal,* serta *link url* pada *id pid* yang berbeda dari *web browser firefox*. Pada akuisisi kedua terdapat aktivitas *web browser chrome* dan menemukan artefak digital berupa *username* dari *account email, account facebook* dan *paypal,* serta *link url* pada *id pid* yang berbeda dari *web browser chrome*. Pada akuisisi ketiga terdapat aktivitas *web browser opera* dan menemukan artefak digital berupa *username* dari *account email, account facebook* dan menemukan *username* beserta *password* dari *account paypal,* serta *link url* pada *id pid* yang berbeda dari *web browser opera*. Ini membuktikan bahwa memori perangkat menyimpan aktivitas internet pengguna.

Tabel 6. Kesimpulan hasil analisis memori pada perangkat laptop

No	Artefak digital	Artefak_1 Firefox	Artefak_2 Chrome	Artefak_3 Opera
1	*User_ID Email*	√	√	√
2	*Password Email*	√	-	-
3	*User_ID Facebook*	√	√	√
4	*Password Facebook*	√	-	-
5	*User_ID Paypal*	√	√	√
6	*Password Paypal*	√	-	√
7	*Link URL*	√	√	√
8	*Start Time*	2019-01-14 12:08:20	2019-01-24 18:25:59	2019-01-25 04:37:34
9	Jumlah Total Artefak	100%	57,14%	71,42%

4. KESIMPULAN

Berdasarkan hasil analisa yang sudah dikerjakan, maka dapat disimpulkan sebagai berikut:

1. Analisis pada hasil akuisisi artefak_1, ditemukan bukti digital berupa *user_id email, password email, user_id facebook, password facebook, user_id paypal, password paypal* dan *link url*. Analisis pada hasil akuisisi artefak_2 ditemukan bukti digital berupa *user_id email, user_id facebook, user_id paypal* dan *link url*. Sedangkan analisis pada hasil akuisisi artefak_3 ditemukan bukti digital berupa *user_id email, user_id facebook, user_id paypal, password paypal* dan *link url*.
2. Hasil pengujian data keseluruhan ditemukan jumlah total keseluruhan dari hasil pengujian pada artefak_1 sebesar 100%, pada artefak_2 sebesar 57,14% dan pada artefak_3 adalah sebesar 71,42%.

Pada penelitian ini telah berhasil menemukan artefak digital pada memori berbasis sistem operasi *linux ubuntu*. Untuk pengembangan penelitian selanjutnya diharapkan dapat menemukan data bukti digital lainnya yang tidak terdeteksi dengan bantuan *tools volatility*. Tentunya ada banyak *tools* alternatif lainnya yang dapat digunakan untuk proses analisa data di memori perangkat.

UCAPAN TERIMA KASIH

Terima kasih diucapkan kepada LPPM dan Program Studi Teknik Informatika UM Jember serta pihak-pihak lain yang tidak bisa disebutkan satu persatu, atas masukkan, dukungan dan semangatnya sehingga luaran dari penelitian yang berbentuk artikel ini, dapat selesai disusun dengan tepat waktu.

REFERENSI

[1] N. Al Mutawa, J. Bryce, V. N. L. Franqueira, and A. Marrington, "Forensic investigation of cyberstalking cases using behavioural evidence analysis," *DFRWS 2016 EU - Proc. 3rd Annu. DFRWS Eur.*, vol. 16, pp. S96–S103, 2016, doi: 10.1016/j.diin.2016.01.012.

[2] T. A. Cahyanto and Y. Prayudi, "Investigasi Forensika Pada Log Web Server untuk Menemukan Bukti Digital Terkait dengan Serangan Menggunakan Metode Hidden Markov Models," *Snati*, pp. 15–19, 2014.

[3] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis," *Justindo, J. Sist. Teknol. Inf. Indones.*, vol. 2, no. 1, pp. 19–30, 2017, Accessed: Jan. 30, 2018. [Online]. Available: http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/1037.

[4] E. Chintia, R. Nadiah, H. N. Ramadhani, Z. F. Haedar, A. Febriansyah, and N. A. Rakhmawati S.Kom., M.Sc.Eng, "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya," *J. Inf. Eng. Educ. Technol.*, vol. 2, no. 2, p. 65, 2019, doi: 10.26740/jieet.v2n2.p65-69.

[5] "Digital Forensics, Part 2: Live Memory Acquisition and Analysis." https://www.hackers-arise.com/post/2016/09/27/digital-forensics-part-2-live-memory-acquisition-and-analysis (accessed Jan. 31, 2020).

[6] R. A. K. N. Bintang, R. Umar, and U. Yudhana, "Perancangan perbandingan live forensics pada keamanan media sosial Instagram, Facebook dan Twitter di Windows 10," *Pros. SNST ke-9 Tahun 2018 Fak. Tek. Univ. Wahid Hasyim*, pp. 125–128, 2018.

[7] D. S. Yudhistira, "Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop," 2018.

[8] T. Rochmadi, I. Riadi, and Y. Prayudi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," *Int. J. Comput. Appl.*, vol. 164, no. 8, pp. 31–37, 2017, doi: 10.5120/ijca2017913717.

[9] R. Umar, A. Yudhana, and M. Nur Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," *Pros. Konf. Nas. Ke- 4 Asos. Progr. Pascasarj. Perguru. Tinggi Muhammadiyah*, pp. 207–211, 2016.

[10] T. D. Larasati and B. C. Hidayanto, "Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10," 2017.

Metode Live Memory Acquisition untuk Pencarian Artefak Digital Perangkat Memori Laptop Berdasarkan Simulasi Kasus Kejahatan Siber

ORIGINALITY REPORT

7%	6%	1%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.scilit.net Internet Source	1%
2	repository.its.ac.id Internet Source	1%
3	eprints.ums.ac.id Internet Source	1%
4	core.ac.uk Internet Source	1%
5	Wilonotomo Wilonotomo, Bagas Hidayat Putra, Ridwan Arifin. "Rancangan Sistem Pendeteksian Paspor Palsu: Solusi Pemeriksaan Keimigrasian di Indonesia", Jurnal Sistem dan Teknologi Informasi (Justin), 2020 Publication	1%
6	doku.pub Internet Source	1%
	conference.upnvj.ac.id	

7	Internet Source	1%
8	heruiw86.blogspot.com Internet Source	1%

Exclude quotes	On	Exclude matches	< 20 words
Exclude bibliography	On		