Investigasi Serangan *Remote Exploit* menggunakan Metode *Live Forensic Investigation*

I Wayan Ardiyasa[1], Ni Luh Gede Pivin Suwirmayanti[2]
Institut Teknologi dan Bisnis STIKOM Bali
e-mail: [1]ardi@stikom-bali.ac.id, [2]pivin@stikom-bali.ac.id

Diajukan: 7 Oktober 2020; Direvisi: 30 September 2021; Diterima: 30 September 2021

Abstrak

Serangan Remote Exploit merupakan eksploitasi jarak jauh yang bekerja melalui media jaringan komputer dan mengeksploitasi vulnerability sistem tanpa akses sebelumnya ke sistem yang rentan. Serangan Remote Exploit ini biasanya menyerang daemon/server yang sedang LISTEN pada port tertentu seperti contoh port 445 dan port 139 pada windows XP. Apabila Sistem operasi komputer pengguna memiliki vulnerability pada port 445 dan port 139 maka serangan Remote Exploit ini akan berhasil dan mampu mencuri data didalam komputer pengguna tersebut, seperti data didalam hard disk, username dan password. Selain itu penyerang (attacker) mampu menanamkan trojan dan backdoor kedalam komputer pengguna dan apabila itu terjadi, maka kapan pun penyerang ingin mengakses komputer target akan secara leluasa bisa dilakukan. Selain sangat berbahaya, serangan ini juga sangat sulit untuk dideteksi menggunakan antivirus karena serangan Remote Exploit memiliki kemampun untuk execute suatu file executable. Hasil dari penelitian ini adalah menghasilkan prosedur dan hasil analisis serangan remote exploit menggunakan metode live forensic investigation. Sehingga mampu mencegah secara dini serangan Remote Exploit dari luar jaringan komputer.

Kata kunci: *Cyber, Exploit, Forensic, Investigasi.*

Abstract

Remote Exploit Attack is a remote attack that works over a network of media computers and exploits system vulnerabilities without prior access to the vulnerable system. Remote Exploit usually attacks daemons / servers that are LISTEN on certain ports such as port 445 and port 139 on windows XP. If the user's computer operating system has a vulnerability on port 445 and port 139, this Remote Exploit attack will succeed and be able to calculate data on the user's computer, such as data on the hard disk, username and password. In addition, the attacker is able to embed trojans and backdoors into the user's computer and that happens, so whenever the attacker wants to freely access the target computer, it can be done. Apart from being very dangerous, this attack is also very dangerous to detect using an antivirus because the Remote Exploit attack has the ability to execute an executable file. To avoid Remote Exploit attacks, it is necessary to use the live forensic method, the results of which are in the form of information and types of attacks.

Keywords*: Cyber, Exploit, Forensic, Investigation.*

1. Pendahuluan

Tingginya pengguna teknologi informasi memicu peningkatan kejahatan komputer atau *cyber crime*. Cyber crime merupakan upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut [1]. Jenis dari kejahatan *cyber* sangat beragam seperti penipuan, *carding*, *malware*, *trojan* dan *hacking*. Menurut data laporan sistem pemantauan trafik internet nasional dari Id-SIRTII/CC (*Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center*) berdasarkan klasifikasi serangan pada tahun 2018 terdapat 10 jenis serangan yang paling banyak antara lain : *trojan-activity* mencapai 37% serangan, *Attemped-user* 19%, *attemped-dos* 14%, *attemped-recon* 12%, *Successful-recon-limited* 9%, *Attemped Administrator Privilage Gain* 5%, *Policy-violation , Denail of Service dan Bad-unknown* mencapai 1% [2].

Selain serangan tersebut, serangan yang berbahaya dan mampu melakukan akses tanpa diketahui oleh pengguna adalah serangan Remote Exploit. Serangan Remote Exploit merupakan Eksploitasi jarak

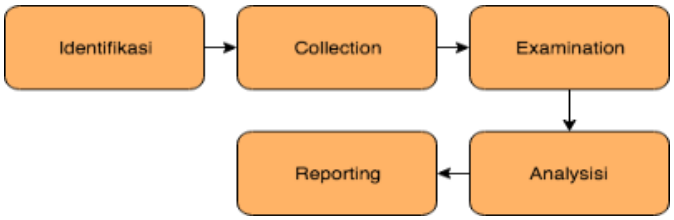
jauh yang bekerja melalui media jaringan komputer dan mengeksploitasi vulnerability sistem tanpa akses sebelumnya ke sistem yang rentan [3]. Serangan *Remote Exploit* ini biasanya menyerang *daemon/server* yang sedang LISTEN pada *port* tertentu seperti contoh *port* 445 dan 139 pada windows XP. Apabila Sistem operasi komputer pengguna memiliki *vulnerability* pada port 445 dan 139 maka serangan *Remote Exploit* ini akan berhasil dan mampu mencuri data didalam komputer pengguna tersebut, seperti data didalam *Hard disk, username* dan *password*. Selain itu penyerang (*attacker*) mampu menanamkan trojan dan *backdoor* kedalam komputer pengguna dan apabila itu terjadi, maka kapan pun penyerang ingin mengakses komputer target akan secara leluasa bisa dilakukan. Selain sangat berbahaya, serangan ini juga sangat sulit untuk dideteksi menggunakan antivirus karena serangan Remote Exploit memiliki kemampun untuk *execute* suatu file executable.

Semakin berkembangnya teknologi, semakin meningkat kejahatan komputer tentu dengan kondisi seperti itu dibarengi juga dengan meningkatnya Sumber Daya Manusia dibidang digital forensic. Digital forensic merupakan ilmu baru yang berkembang terus-menerus sehingga perlu mendalam belajar tentang ilmu ini. Ilmu digital forensic berubah karena perkembangan sistem operasi, smartphone, dan tablet. Live forensic yaitu suatu teknik analisis dimana menyangkut data yang berjalan pada sistem atau data *volatile* yang umumnya tersimpan pada Random Access Memory (RAM) atau transit pada jaringan [4].

Dari hal tersebut, permasalahannya adalah bagaimana cara atau teknik untuk mengetahui serangan Remote Exploit pada komputer sehingga mampu mencegah kehilangan data dan mencari sumber serangan untuk mendapatkan bukti-bukti digital yang valid.

2. Metode Penelitian

Adapun metode penelitian didalam penelitian ini adalah sebagai berikut:



Gambar 1. Metode *Live Forensic*

1) Identifikasi

Identifikasi merupakan tahap melakukan pengecekan terhadap perangkat komputer yang terindikasi terkena serangan *Remote Exploit*.

2) *Collection*

Collection merupakan tahap pengambilan data. Dalam tahap *collection* melakukan teknik akuisisi pada *memory* dengan membuat data imaging dari *memory*.

3) *Examination*

Examination merupakan tahap *recovery* untuk mendapatkan informasi serangan *remote exploit*.

4) *Analysis*

Analysis merupakan tahap penggambaran proses investigasi dan identifikasi sumber serangan menggunakan *tools*.

5) *Reporting*

Reporting merupakan tahap membuat laporan atau dokumentasi terkait dengan tahapan proses yang dilakukan.

Berikut merupakan teknik pengumpulan data:

1) Data Primer

Data primer dari penelitian ini adalah data simulasi serangan *remote exploit* yang dilakukan secara langsung dan melakukan investigasi *live forensic*, sehingga didapatkan data *image* pada *memory*.

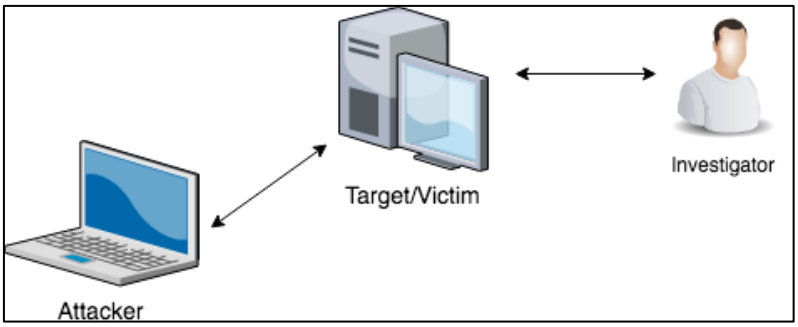
2) Studi Pustaka

Didalam tahap ini, peneliti menggali data dan informasi melalui buku-buku, internet, jurnal, *ebook* yang ada kaitannya dengan penelitian yang dilakukan.

3. Hasil dan Pembahasan

3.1. Skema Jaringan

Pada penelitian ini menggunakan skema jaringan untuk melakukan simulasi serangan *remote exploit* terhadap perangkat komputer yang dijadikan target serangan. Skema jaringan yang digunakan yaitu topologi *peer-to-peer*.



Gambar 2. Skema Jaringan

Pada Gambar 2 merupakan skema jaringan tersebut, terdapat *attacker* yang terhubung dengan komputer target. Pada komputer *attacker* menggunakan IP *Address* 192.168.64.137 dan pada komputer target menggunakan IP *Address* 192.168.64.138 dengan sistem operasi Windows XP SP 1. Penggunaan OS Windows XP SP 1 dikarenakan untuk dapat mengetahui bagaimana serangan *remote exploit* bisa digunakan untuk melakukan serangan kedalam perangkat komputer. Pada skema tersebut *attacker* melakukan simulasi serangan *remote exploit* pada komputer target. Setelah melakukan serangan, investigator *digital forensic* melakukan investigasi untuk melakukan analisis secara *live* pada komputer dalam kondisi *running*.

3.2. Perangkat Pendukung

Perangkat pendukung yang digunakan pada penelitian ini didalam melakukan simulasi serangan *remote exploit* dan investigasi *digital forensic* serangan *remote exploit* dengan metode *live forensic* adalah sebagai berikut:

Tabel 1. Tabel Perangkat Keras

No.	Nama Perangkat Keras	Jumlah
1.	*Laptop*	2 Unit
2.	*Pendrive*	1 Pcs

Tabel 2. Tabel Perangkat Lunak

No.	Nama Perangkat Lunak	Keterangan
1.	Windows XP SP 1	Sistem operasi pada komputer target.
2.	Kali Linux 2.0	Sistem operasi berbasis linux yang digunakan untuk melakukan pentesting.
3.	FTK Imager Lite	Aplikasi untuk melakukan akuisisi data atau data imaging.
4.	*Volatility*	Aplikasi yang digunakan untuk melakukan analisis data image memory.
5.	Metasploit	Aplikasi yang digunakan untuk melakukan serangan *remote exploit* kedalam mesin target.

3.3. Hasil Pembahasan

Didalam melakukan investigasi serangan *remote exploit* secara *live digital forensic*, dilakukan simulasi serangan terhadap komputer yang dijadikan target serangan. Setelah dilakukan simulasi, baru dilakukan analisis serangan terhadap komputer target secara *live.*

3.3.1. *Remote Exploit*

Serangan *remote exploit* pada komputer target yang menggunakan OS Windows XP SP 1 yang memiliki *vulnerability* pada port 445 yaitu Protokol *Server Message* Protokol (SMB) yang memungkinkan *sharing file* antar *client* pada jaringan komputer. Dengan menggunakan *exploit* "ms08_067_netapi" pada aplikasi Metasploit, memungkinkan *attacker* untuk mendapatkan akses *privilege* pada sebuah system. Berikut langkah-langkah didalam melakukan serangan *remote exploit*:

```
msf5 > use exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.64.138
RHOSTS => 192.168.64.138
msf5 exploit(windows/smb/ms08_067_netapi)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.64.137
LHOST => 192.168.64.137
msf5 exploit(windows/smb/ms08_067_netapi) > show options
[*] Started reverse TCP handler on 192.168.64.137:4444
[*] 192.168.64.138:445 - Automatically detecting the target...
[*] 192.168.64.138:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.64.138:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.64.138:445 - Attempting to trigger the vulnerability...
[*] Sending stage (180291 bytes) to 192.168.64.138
[*] Meterpreter session 1 opened (192.168.64.137:4444 -> 192.168.64.138:1037) at 2020-09-29 12:06:46 -0400
meterpreter >
```

Gambar 3. *Exploit* Mesin Target

3.3.2. Hasil Investigasi Metode *Live Forensic*

Investigasi dengan metode *live forensic* merupakan metode investigasi yang dilakukan oleh investigator *digital forensic* untuk mendapatkan informasi dari barang bukti berupa perangkat komputer, dengan kondisi perangkat komputer tersebut dalam keadaan *running*. Setelah dilakukan simulasi serangan *remote exploit* terhadap komputer target yang menggunakan Sistem Operasi Windows XP SP 1 dengan memanfaatkan kelemahan pada protocol Service Message Block (SMB) yang berfungsi sebagai protocol *file sharing* antar *client* didalam jaringan komputer yang menggunakan *port* 445. Langkah yang dilakukan untuk mendapatkan informasi dari barang bukti dengan menerapkan metode *Live Forensic Investigation* adalah sebagai berikut:

1) Identifikasi

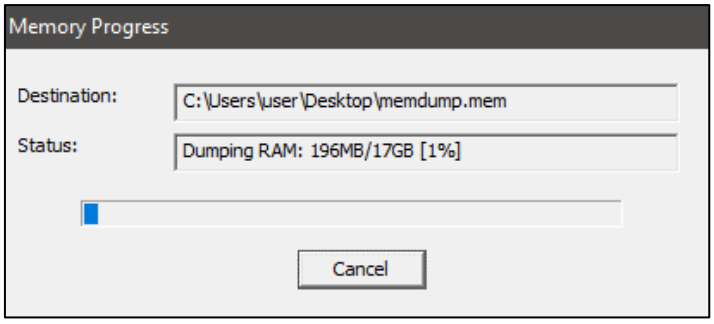
Identifikasi yaitu tahap melakukan pengecekan terhadap barang bukti perangkat komputer yang terindikasi terkena serangan *remote exploit.* Tahap identifikasi sebagai tahap awal untuk mendeteksi serangan *remote exploit* dengan menggunakan perintah netstat. Netstat atau *network statistic* merupakan aplikasi yang bisa digunakan untuk *monitoring* komunikasi antar *client* didalam jaringan komputer. Berikut hasil dari tahap identifikasi:

```
C:\Documents and Settings\Administrator>netstat -na
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1029         0.0.0.0:0              LISTENING
  TCP    192.168.64.138:139     0.0.0.0:0              LISTENING
  TCP    192.168.64.138:1037    192.168.64.137:4444    ESTABLISHED
  UDP    0.0.0.0:445            *:*
```

Gambar 4. *Exploit* Mesin Target

2) *Collection*

Collection merupakan tahap pengambilan data. Pada tahap *collection investigator* melakukan akuisisi data untuk mengamankan barang bukti. Akuisisi data yang dilakukan yaitu untuk menghasilkan data *image* dari *memory* (RAM) komputer.



Gambar 5. *Progrees Data Image* pada *Memory*

3) *Examination*

Examination merupakan tahap *recovery* untuk mendapatkan informasi serangan *remote exploit*. Pada tahap *examination*, akan dilakukan *recovery* dengan membaca hasil *data image memory* dengan menggunakan aplikasi *volatility*. Berikut proses didalam examination file image *memory*:

```
sh-3.2# ./volatility -f /Users/owner/Documents/PENELITIAN\ 2020/PENELITIAN\ 2020/image\ RAM/memdump02.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/Users/owner/Documents/PENELITIAN 2020/PENELITIAN 2020/image
RAM/memdump02.mem)
                      PAE type : PAE
                           DTB : 0x31c000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2020-09-29 16:33:27 UTC+0000
                                 Image local date and time : 2020-09-29 23:33:27 +0700
```

Gambar 6. Proses Mencari Profil *Data Image*

Pada Gambar 6 merupakan proses mencari profil *data image* yang berhasil dibaca oleh aplikasi *volatility*. Dari hasil profil tersebut, didapatkan bahwa komputer target menggunakan Sistem Operasi Windows XP SP2 dan profil ini penting untuk diketahui didalam proses investigasi lanjutan guna mendapatkan informasi tambahan terkait serangan *remote exploit*.

```
sh-3.2# ./volatility -f /Users/owner/Documents/PENELITIAN\ 2020/PENELITIAN\ 2020/image\ RAM/memdump02.mem --
profile=WinXPSP2x86 connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x863ee398 192.168.64.138:1041      192.168.64.137:4545      424
0x86276b28 192.168.64.138:1042      192.168.64.137:4545      1624
0x860828c0 192.168.64.138:1037      192.168.64.137:4444      1008
0x861544f8 192.168.64.138:1040      192.168.64.137:4545      432
```

Gambar 7. Mencari Informasi Jaringan Komputer

Pada Gambar 7 proses untuk mengetahui koneksi TCP/IP yang aktif pada saat melakukan akuisisi data *image memory*. Dari proses tersebut, didapatkan informasi terkait status informasi TCP/IP dimana IP *Address* yang melakukan serangan *remote* menuju komputer target adalah 192.169.64.137 dengan membuka *port* 4444. Selain informasi koneksi TCP/IP, informasi PID menampilkan PID 1008 yang artinya ada proses yang berjalan pada saat serangan *remote exploit* itu terjadi dengan Proses ID 1008.

```
sh-3.2# ./volatility -f /Users/owner/Documents/PENELITIAN\ 2020/PENELITIAN\ 2020/image\ RAM/memdump02.mem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x865c6830 System                    4      0     57      260 ------      0
0x86255da0 smss.exe                372      4      3       21 ------      0 2020-09-29 15:48:01 UTC+0000
0x86436810 csrss.exe               600    372     11      382      0      0 2020-09-29 15:48:02 UTC+0000
0x864b9020 winlogon.exe            624    372     18      507      0      0 2020-09-29 15:48:03 UTC+0000
0x864b3a08 services.exe            668    624     16      280      0      0 2020-09-29 15:48:03 UTC+0000
0x86012658 lsass.exe               680    624     22      355      0      0 2020-09-29 15:48:03 UTC+0000
0x860a4990 vmacthlp.exe            836    668      1       24      0      0 2020-09-29 15:48:04 UTC+0000
0x8618c7f8 svchost.exe             852    668     16      192      0      0 2020-09-29 15:48:04 UTC+0000
0x86481598 svchost.exe             916    668     10      267      0      0 2020-09-29 15:48:04 UTC+0000
0x861cfda0 svchost.exe            1008    668     65     1258      0      0 2020-09-29 15:48:04 UTC+0000
0x864b4300 svchost.exe            1052    668      4       61      0      0 2020-09-29 15:48:04 UTC+0000
0x860a5da0 svchost.exe            1100    668     14      206      0      0 2020-09-29 15:48:05 UTC+0000
0x861e2da0 spoolsv.exe            1380    668     10      129      0      0 2020-09-29 15:48:06 UTC+0000
```

Gambar 8. Menampilkan Informasi *Service* Aktif

4) *Analysis*

Pada tahap Analysis merupakan tahap penggambaran proses investigasi dan identifikasi sumber serangan. Dari investigasi yang sudah dilakukan menggunakan *volatility* didapatkan informasi sumber serangan yang berasal dari IP Address 192.168.64.137 *port* 4444 yang terbukti melakukan komunikasi ke *client* dengan IP *Address* 192.168.64.138. Itu dibuktikan dengan informasi yang didapatkan pada Gambar 7. Informasi jaringan komputer dengan melihat koneksi TCP/IP. Selain itu, untuk memastikan bahwa memang benar adanya serangan *remote exploit* pada komputer target, dilakukan pengecekan *signature file* pada *file data image* dari *memory* dengan menggunakan perintah *yarascan*, seperti dibawah ini:

```
sh-3.2# ./volatility -f /Users/owner/Documents/PENELITIAN\ 2020/PENELITIAN\ 2020/image\ RAM/memdump02.mem --profile=WinXPSP2x86 yarascan
-Y "192.168.64.137"
Owner: Process vmtoolsd.exe Pid 1648
0x019bbd47  31 39 32 2e 31 36 38 2e 36 34 2e 31 33 37 0a 6d   192.168.64.137.m
0x019bbd57  73 66 35 20 65 78 70 6c 6f 69 74 28 77 69 6e 64   sf5.exploit(wind
0x019bbd67  6f 77 73 2f 73 6d 62 2f 6d 73 30 38 5f 30 36 37   ows/smb/ms08_067
0x019bbd77  5f 6e 65 74 61 70 69 29 20 3e 20 73 68 6f 77 20   _netapi).>.show.
0x019bbd87  6f 70 74 69 6f 6e 73 20 0a 0a 4d 6f 64 75 6c 65   options...Module
0x019bbd97  20 6f 70 74 69 6f 6e 73 20 28 65 78 70 6c 6f 69   .options.(exploi
0x019bbda7  74 2f 77 69 6e 64 6f 77 73 2f 73 6d 62 2f 6d 73   t/windows/smb/ms
0x019bbdb7  30 38 5f 30 36 37 5f 6e 65 74 61 70 69 29 3a 0a   08_067_netapi):.
0x019bbdc7  0a 20 20 20 4e 61 6d 65 20 20 20 20 20 43 75 72   ....Name.....Cur
0x019bbdd7  72 65 6e 74 20 53 65 74 74 69 6e 67 20 20 52 65   rent.Setting..Re
0x019bbde7  71 75 69 72 65 64 20 20 44 65 73 63 72 69 70 74   quired..Descript
0x019bbdf7  69 6f 6e 0a 20 20 20 2d 2d 2d 2d 20 20 20 20 20   ion....----.....
0x019bbe07  2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20   ---------------.
0x019bbe17  20 2d 2d 2d 2d 2d 2d 2d 2d 20 20 2d 2d 2d 2d 2d   .---------..-----
0x019bbe27  2d 2d 2d 2d 2d 2d 0a 20 20 20 52 48 4f 53 54 53   ------....RHOSTS
0x019bbe37  20 20 20 31 39 32 2e 31 36 38 2e 36 34 2e 31 33   ...192.168.64.13
```

Gambar 9. Pengecekan *Signature File*

4. Kesimpulan

Adapun kesimpulan dari penelitian ini adalah sebagai berikut:

1. Telah dilakukannya investigasi dengan metode *live digital forensic* pada perangkat komputer dan mendapatkan informasi serangan *remote exploit* pada komputer target.
2. FTK Imager Lite mampu melakukan akuisisi data pada *memory* dan menghasilkan *data image*.
3. Menggunakan aplikasi *volatility* untuk mendapatkan informasi serangan *remote exploit* dengan metode *live forensic*.

Daftar Pustaka

[1] M. M. Arief Mansur, Dikdik Drs., SH. and M. Gultom, Elisatris, SH., *Cyberlaw Aspek Hukum Teknologi Informasi*. 2009.

[2] ID-SIRTII, "Top 10 Serangan Berdasarkan Klasifikasi Tahun 2018,", 2018.

[3] K. Graves, *CEH: Official Certified Ethical Hacker Review Guide*, vol. 1, no. 11. 2007.

[4] M. N. Faiz, R. Umar, and A. Yudhana, "Implementasi *Live Forensics* untuk Perbandingan *Browser* pada Keamanan *Email*," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 1, no. 3, p. 108, 2017.