FORENSIK DIGITAL RANDOM ACCESS MEMORY PADA SISTEM OPERASI LINUX MENGGUNAKAN METODE DUMPMEMORY

DIGITAL FORENSIC RANDOM ACCESS MEMORY ON LINUX OPERATING SYSTEM USING DUMPMEMORY METHOD

PROPOSAL PROYEK AKHIR

Disusun Oleh :

Rivan Hikmawan

6702144053

PROGRAM STUDI D3 TEKNIK KOMPUTER

FAKULTAS ILMU TERAPAN

UNIVERSITAS TELKOM

BANDUNG, 2016

Daftar Isi

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi saat ini bisa dimanfaatkan untuk melacak sebuah aktifitas pelaku kejahatan dalam melakukan aksi kejahatan internet, seperti: pencurian, penggelapan, pencucian uangan dan lain sebagainya. Bukti digital dari komputer sulit dibedakan antara asli mupun salinan, karena berdasarkan sifat alaminya, data yang ada dalam komputer sangat mudah dimodifikasi. Seiring berjalannya waktu proses penindak lanjutan kejahatan digital sebagai barang bukti secara sah dalam sebuah pengadilan umum, maka diterbirkan UU ITE untuk mengatur transfer informasi elektronik sesuai dengan etika transaksi informasi elektronik. Sehingga UU No. 11 tahun 2008 diharapkan tidak ada pihak yang merasa dirugikan atas transaksi informasi elektronik. Sebuah proses transaksi elektronik akan disimpan pada media penyimpanan yang digunakan komputer dengan salah satu media penyimpanan pada *Random Access Memory* (RAM).

Random Access Memory (RAM) sebuah komponen sangat penting dalam sebuah sistem komputer dengan berperan sebagai penyimpanan yang bersifat volatile. Kapasitas *main memory* ini sangat berfungsi untuk proses forensik dikarenakan *Random Access Memory* ini menyimpan seluruh aktifitas yang terjadi saat komputer sedang digunakan oleh user.

Forensik memori merupakan sebuah proses investigasi untuk menganalisa data-data *volatile* yang terdapat pada *Random Access Memory* sebuah komputer sebagai bukti digital yang akurat dan dapat dipertanggung jawabkan. Cara kerja digital forensik ialah mengembalikan, mengumpulkan, memeriksa dan menyimpan bukti informasi yang secara magnetis tersimpan pada komputer.

Penangan forensik main memory pada *Random Access Memory* harus sangat berhati-hati dan bersabar karena jika sistem yang sedang berjalan mati maka data yang terdapat di dalam *main memory* akan hilang. Oleh karena itu hasil dari

forensik memori berupa beberapa log aktifitas dan riwayat penyerang dalam sistem operasi yang di retas untuk mengambil data-data kita.

1.2 Rumusan Masalah

Rumusan masalah dalam penulisan proyek akhir ini adalah sebagai berikut:

1. Bagaimana cara kerja forensik memory pada sebuah data *volatile* RAM komputer untuk menjadikan barang bukti dalam sebuah kasus hukum?
2. Bagaimana hasil data forensik yang diperoleh dari main memory dengan menggunakan metode *dumpmemory*?

1.3 Tujuan

Tujuan pengambilan proyek akhir ini adalah sebagai berikut:

1. Mengetahui tahapan forensik memori dalam pengumpulan data-data dari memori *volatile* RAM sebagai bukti yang sah secara digital dengan menggunakan metode *dumpmemroy*.
2. Mendapatkan hasil data forensik RAM diperoleh berupa riwayat maupun log aktifitas yang dilakukan oleh peretas untuk keperluan investigasi.

1.4 Batasan Masalah

Batasan masalah yang digunakan dalam pembuatan proyek akhir ini adalah sebagai berikut:

1. Skenario kasus sebagai target dilakukan pada sistem operasi Ubuntu 14.04.4 Desktop yang berjalan pada mesin virtual.
2. Skenario peretas menggunakan sistem operasi Kali Linux 2.0 dan Investigator menggunakan sistem operasi BackBox Linux 4.4.
3. Sistem target yang diserang tidak menggunakan *firewall*, proxy dan sistem keamanan lainnya.
4. Tidak membahas cara kerja *tools* untuk peyerang.
5. Tidak membahas mengenai sistem operasi dan kernel yang digunakan.
6. Tidak membahas tentang cara kerja dari *Random Access Memory*.
7. *Tools* yang digunakan bersifat *opensource*.

8. Menggunakan jaringan *local/hotspot* pribadi.

9. Kecurigaan investigator terhadap barang bukti bersifat tidak alami, karena pihak yang berperan sebagai penyerang dan investigator adalah pengguna yang sama.

1.5 Definisi Operasional

1. Forensik digital adalah penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti informasi yang secara magnetis tersimpan pada komputer atau media penyimpanan digital sebagai alat bukti dalam mengungkap kasus kejahatan yang bisa dipertanggung jawabkan secara hukum.

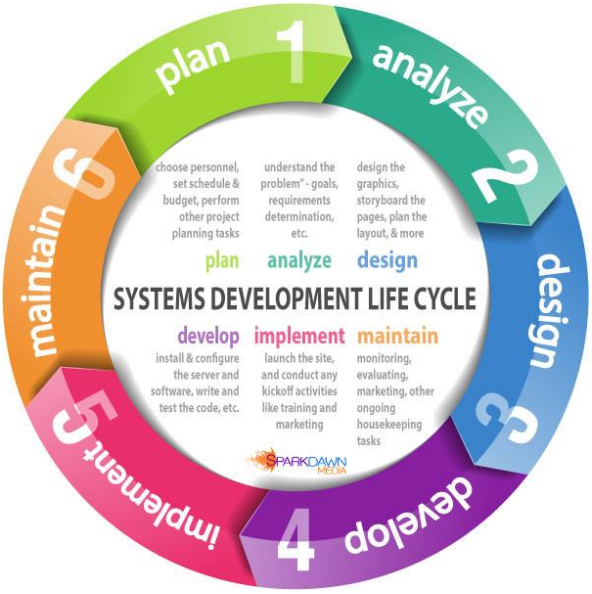
2. *Random Access Memory* adalah memori utama sebuah komputer yang bersifat *volatile* untuk media penyimpanan sementara pada saat komputer dijalankan dan dapat diakses secara acak atau random.

3. Sistem Operasi adalah adalah komponen pengolah peranti lunak dasar tersistem sebagai pengelola sumber daya perangkat keras komputer, dan menyediakan layanan umum untuk aplikasi perangkat lunak.

4. *Dumpmemory* merupakan sebuah metode atau cara untuk mendapatkan berkas digital yang berisikan informasi snapshot (potret) statis sebuah memory *volatile* komputer.

1.6 Metode Pengerjaan

Metode pengerjaan dalam melakukan proyek akhir ini dengan menggunakan metode SDLC (*Systems Development Life Cycle*) yang terdiri dari analisis system, perencanaan sistem, implementasi sistem, operasi dan perawatan sistem. Pada penyusunan Proyek Akhir ini dengan metode SDLC *(Systems Development Life Cycle)* seperti Gambar 1.1.



Gambar 1.1 Metode SDLC (Systems Development Life Cycle)

1. Perencanaan

   Perencana berfungsi untuk melakukan perencanaan jenis aplikasi dan sistem operasi yang dibutuhkan sesuai dengan fungsionalitas dan untuk menunjang penyelesaian Proyek Akhir.

2. Analisis

   Analisis ini melakukan pencarian jeni-jenis aplikasi yang dibutuhkan untuk strategi menyerang target dan investigasi pada pegguna yang telah di serang oleh penyerang.

3. Desain

   Pada tahap ini melakukan sebuah rancangan sistem yang akan di bangun pada sebuah mesin virtual, dengan mendesain topologi jaringan yang digunakan dalam proses pengujian Proyek Akhir.

4. Pengembangan

   Tahap ini dilakukan untuk mengembangkan teknik penyerangan maupun teknik investigasi dalam pengujian sistem yang sudah dirancang dari setiap aplikasi yang digunakan untuk Proyek Akhir.

5. Implementasi

   Melakukan sebuah pengujian forensik memory dengan menggunakan metode *dumpmemory* dan menganalisa hasil yang diperoleh dari pengujian.

6. Perbaikan

   Tahap ini dilakukan untuk memperbaiki sistem yang tidak jalan maupun memperbaharui aplikasi dengan versi yang terbaru.

1.7 Jadwal Pengerjaan

Tabel 1.1 Jadwal Pengerjaan

Uraian	Tahun 2016 - 2017																			
	September				Oktober				November				Desember				Januari			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Perencanaan																				
Analisis																				
Desain																				
Pengembangan																				
Implementasi																				
Perbaikan																				
Penyusunan Laporan																				

BAB 2

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

i. Forensik Digital

Forensik Digital adalah Penggunaan metode ilmiah yang berasal dan terbukti menuju pelestarian, koleksi, validasi, identifikasi, analisis, interpretasi, dokumentasi dan presentasi bukti digital yang berasal dari sumber-sumber digital untuk tujuan memfasilitasi atau melanjutkan rekonstruksi peristiwa ditemukan pidana, atau membantu untuk mengantisipasi tindakan yang tidak sah terbukti mengganggu operasi yang direncanakan.

ii. Random Access Memory

Random access memory (RAM) adalah sebuah tipe penyimpanan komputer yang isinya dapat diakses dalam waktu yang tetap tidak memperdulikan letak data tersebut dalam memori. Ini berlawanan dengan *alat memori urut*, seperti tape magnetik, disk dan drum, di mana gerakan mekanikal dari media penyimpanan memaksa komputer untuk mengakses data secara berurutan.

Random Access Memory merupakan memori utama pada sebuah komputer yang bersifat volatile dan peletakan data secara acak. RAM digunakan untuk penyimpanan data sementara dan mengeluarkan data yang diminta oleh processor serta alur data yang tersimpan mapun dikeluarkan sangat dinamis.

Dalam memproses sebuah data yang masuk dalam inputan user, beberapa bagian RAM saling membantu proses pengolahan data tersebut. Ini lah bagian utama RAM yang mengelola data dari inputan hinga output:

a) Input storage, digunakan untuk menampung input yang dimasukkan melalui alat input.

b) Penyimpanan program, digunakan untuk menyimpan semua instruksi-instruksi program yang akan diakses.

c) *Working storage*, digunakan untuk menyimpan data yang akan diolah dan hasil pengolahan.

d) *Output storage*, digunakan untuk menampung hasil akhir dari pengolahan data yang akan ditampilkan ke alat *output*.

Berdasarkan proses kerja RAM dalam melakukan penyimpanan data dalam sebuah komputer dari awal penyimpanan hingga pengeluaran data yang akan di tampilkan. Karena hal itu lah yang menjadi alasan mengapa proses forensik digital dapat dilakukan pada sebuah *Random Access Mmeory* dengan hasil yang spesifik dan bisa dipertanggung jawabkan.

Dalam media penyimpanan, *Random Access Memory* memiliki berbagai macam jenis yang digunakan, macam-macam jenis RAM seperti Gambar 2.1.

Gambar 2.1 Jenis *Random Access Memory*

iii. Sistem Operasi

Sistem Operasi (*Operating System* : *OS*) adalah komponen pengolah peranti lunak dasar (*essential component*) tersistem sebagai pengelola sumber daya perangkat keras komputer (hardware), 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:

a. Booting, meletakan karnel kedalam memori
b. Kernel, bagian inti dari sebuah sistem operasi
c. Command Interpreter atau shell, membaca input dari pengguna
d. 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 computer, meskipun kode aplikasi biasanya dieksekusi langsung oleh perangkat keras dan seringkali akan menghubungi system operasi atau terputus oleh itu. Sistem operasi yang ditemukan pada hampir semua perangkat yang berisi computer dari ponsel dan konsol permainan video untuk superkomputer dan server web.

Dalam pemakaian sehari-hari operating sistem berfungsi mengatur jalannya sumber daya perangkat dalam kebutuhan sehari hari. Berikut jenis-jenis sistem operasi yang digunakan seperti Gambar 2.2.

Gambar 2.2 Jenis-Jenis Sistem Operasi

iv. Dumpmemory

Forensik memory merupakan salah satu teknik forensik yang digunakan untuk mendapatkan sebuah data atas inseden penyerangan terhadap suatu pengguna. Dalam digital forensik memiliki dua teknik forensik yang digunakan untuk keperluan investigasi, yaitu: Teknik forensik tradisional dan Teknik live forensik.

Tenik forensik tradisional atau teknik offline merupakan teknik yang sering digunakan untuk investigasi dengan mengharuskan investigator mematikan sistem korban, hal ini bertujuan untuk antisipasi adanya proses berbahaya yang dapat beresiko menghapus data untuk keperluan investigasi.

Teknik live forensik ialah pengembangan dari teknik forensik tradisional yang diharuskan sistem komputer tidak boleh dimatikan untuk proses investigasi, dengan dilakukan teknik live forensik pada sebuah data volatile yang ada dalam sebuah sistem komputer.

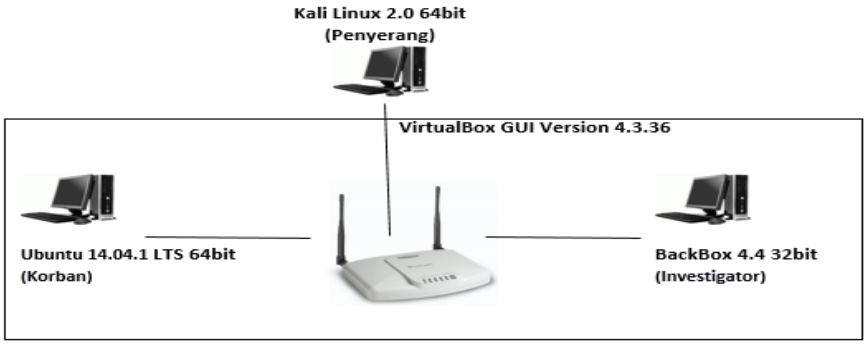
BAB 3

ANALISIS PERANCANGAN SISTEM

3.1 Analisis Kebutuhan Sistem

Proyek Akhir ini melakukan investigasi terhadap sistem yang terindikasi telah diserang oleh pihak tidak bertanggung jawab. Dalam pengujian sistem menggunakan jaringan local atau hotspot pribadi dengan proses investigasi menggunakan metode *dumpmemory* yang merupakan suatu metode forensik digital pada memori fisik. Untuk melakukan metode ini dibutuhkan beberapa perangkat lunak tambahan seperti LiMe, bulk ekstrator, wireshark, dan volatility.

Untuk proses investigasi dibutuhkan sebuah sistem yang sudah terindikasi diserang dan sistem investigasi untuk melakukan analisis dari hasil *dumpmemory*. Sitem operasi korban menggunakan sistem Operasi Ubuntu 14.04.1 LTS yang sudah terinstall paket jaringan seperti DHCP, FTP, SSH sebagai celah keamanan. Tahap pengujian sistem ini digambarkan pada Gambar 3.1 Gambaran Sistem.



Gambar 3.1 Gambaran Sistem

3.1.1 Kebutuhan Perangkat Keras

Spesifik peragkat keras yang digunakan sebagai berikut:

1. Investigator

   Investigator berfungsi sebagai investigasi hasil dari riwayat dan log aktifitas yang dilakukan penyerang (*Hacker*) untuk mengambil data dari pengguna, untuk spesifikasi laptop/kompuer yang digunakan terdapat pada tabel 3.1.

Tabel 3.1 Spesifikasi Komputer Investigator

Processor	Intel® Core™ i3-4030U, 1,9GHz
Chipset	Intel® Core™ i3 Chipset
Memory	6GB DDR3 1600MHz
Graphic	Intel® HD Graphics
Baterai	Built-in Battery 2 Cells-Polymer
Drive Optic	DVD +/- RW
Storage	2,5” ATA 500GB
Networking and Interface	• Bluetooth V 4.0 • 10/100/1000 Base T • 1xRJ45 LAN jack for LAN insert • 1xHDMI • 1xUSB 3.0 port • 2xUSB 2.0 port

2. Penyerang/Attacker

Penyerang/Attacker berfungsi sebagai penyerang untuk menyerang komputer sistem user, untuk spesifikasi laptop/komputer yang digunakan terdapat pada tabel 3.2.

Tabel 3.2 Spesifikasi Komputer Penyerang

Processor	Intel® Core™ i3-3110M, 1.5GHz
Chipset	Intel® Core™ i3 Chipset

Memory	8GB DDR3 PC-12800
Graphic	Intel® HD Graphics 4000
Baterai	6-Cell 48Wh (40W/60W Ac Adaper)
Drive Optic	DVD +/- RW
Storage	2,5” ATA 500GB
Networking and Interface	• Bluetooth V 4.0 • 1xRJ45 LAN jack for LAN insert • 1xHDMI • 1xUSB 3.0 port • 2xUSB 2.0 port

3.1.2 Kebutuhan Perangkat Lunak

Spesifik perangkat lunak yang digunakan sebagai berikut:

Adapun spesifikasi perangkat lunak yang digunakan untuk menunjang dalam penyelesaian Proyek Akhir tersebut, jenis jenis perangkat lunak yang digunakan terdapat pada Table 3.3.

Tabel 3.3 Kebutuhan Perangkat Lunak

No	Software	Fungsionalitas
1	BackBox Linux 4.4	Sistem Operasi Laptop(host) dan Sitem Operasi Investigator
2	Kali Linux 2.0	Sistem Operasi Penyerang
3	Ubuntu 14.04.1 LTS	Sistem Operasi Korban
4	Vollatillity	Perangkat lunak untuk menganalisa hasil dari

		dumpmemory
5	Wireshark	Perangkat lunak untuk menganalisa jaringan data hasil dari dumpmemory
6	LiME	Perangkat lunak dumpmemory pada sistem operasi linux
7	Bulk Extractor	Perangkat lunak yang digunakan untuk menganalisa hasil dari dumpmemory
8	Tempar Data	Perangkat lunak tambahan pada browser yang berfungsi sebagai pengubah SSID Cookie
9	Oracle VM VirtualBox GUI Version 5.1.6	Perangkat lunak untuk menjalankan sistem virtualisasi pada sistem operasi korban

3.2 Perancangan Sistem

Kali Linux 2.0 pada sistem perancangan ini berfungsi sebagai sistem operasi penyerang yang digunakan untuk menyerang target. BackBox 4.4 berfungsi sebagai sistem operasi komputer untuk menjalankan virtual machine. Virtual machine digunakan sebagai penyimpanan sistem operasi target yang menggunakan Ubuntu 14.04.1 LTS.

Skenario pengujian menggunakan beberapa teknik *cyber-attack*.

I. Skenario 1: *Session Hijacking*

Skenario pertama ini merupakan proses pengambilan kendali *session* milik korban dengan sebelumnya penyerang mendapatkan autentikasi ID *session* yang tersimpan dalam *cookie*.

Untuk menentukan akurasi skenario ini maka investigator harus mengidentifikasi:

a) *IP Address* penyerang

b) Jenis *script* yang di gunakan penyerang

c) Waktu proses penyerangan korban

II. Skenario 2: *FTP Attack*

Skenario kedua ini merupakan proses pengambilan kendali sistem korban dengan memanfaatkan celan keamanan pada *File Transfer Protocol* (FTP). Penyerangan dilakukan dengan teknik brute force pada FTP dengan mengambil alih kendali sistem korban.

Untuk menentukan akurasi skenario ini maka investigator harus mengidentifikasi:

a) *IP Address* penyerang

b) Jenis Celah Keamanan yang digunakan korban

c) Aktifitas yang dilakukan oleh penyerang

d) Waktu proses penyerangan korban

III. Skenario 3*: Illegal Access*

Skenario ketiga ini merupakan proses penyerang melakuakan akses kedalam sistem korban dari jaringan local yang tersedia, melakukan eksploitasi pada celah keamanan yang ada pada korban dengan masuk celah keamanan yang ditemukan. Setelah masuk pada sistem korban, penyerang akan melakukan perubahan dan pengunduhan file lalu mengunggah *playload* pada sistem.

Untuk menentukan akurasi skenario ini maka investigator harus mengidentifikasi:

a) *IP Address* penyerang

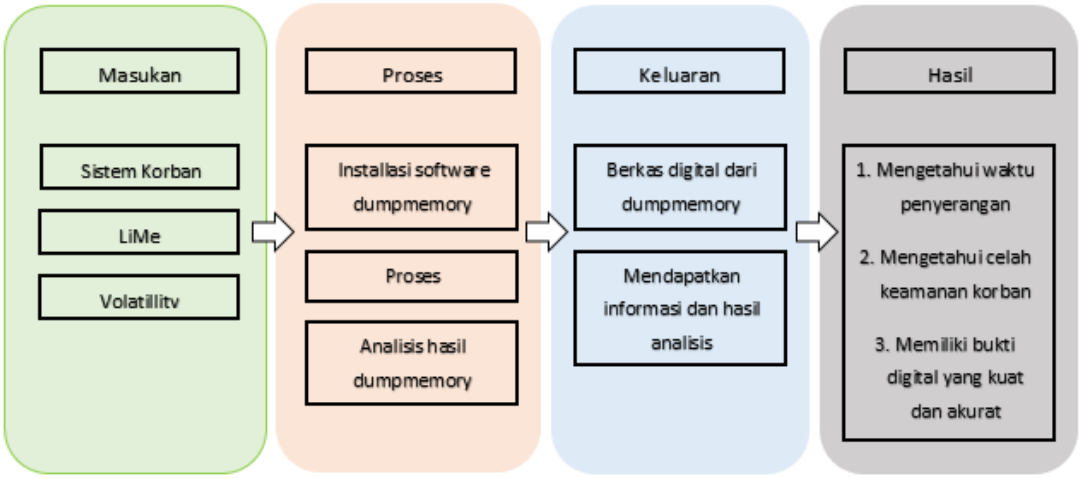
b) Jenis Celah Keamanan yang digunakan korban

c) Jenis perubahan dan file yang diunduh oleh penyerang

d) Menemukan Playload

e) Waktu proses penyerangan korban

Pada tahap pengujian sistem yang terindikasi diserang, berikut gambaran besar logika pengujian sistem pada Gambar 3.2 Bagan Logika Pengujian.



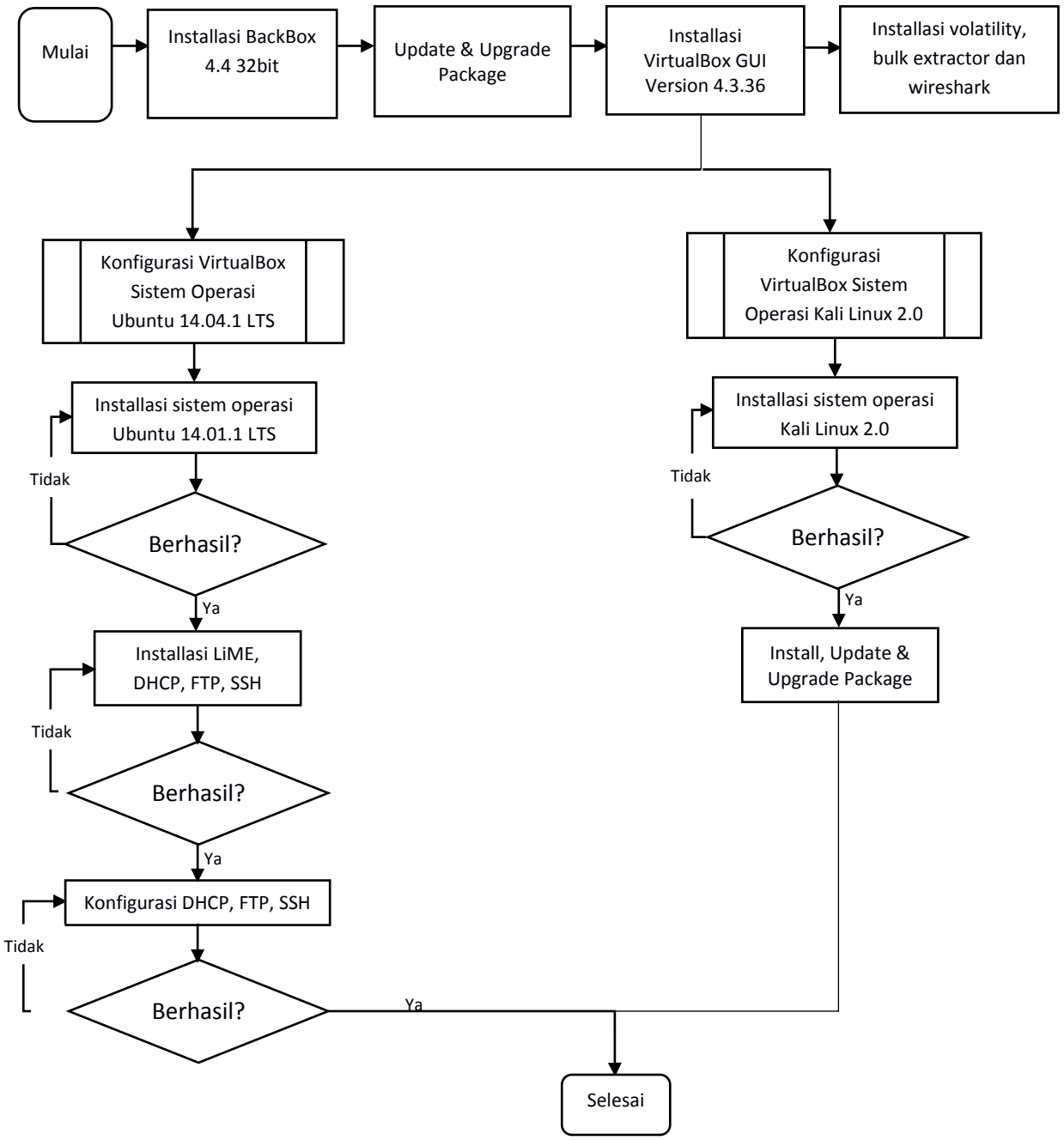
Gambar 3.2 Bagan Logika Pengujian

DAFTAR PUSTAKA

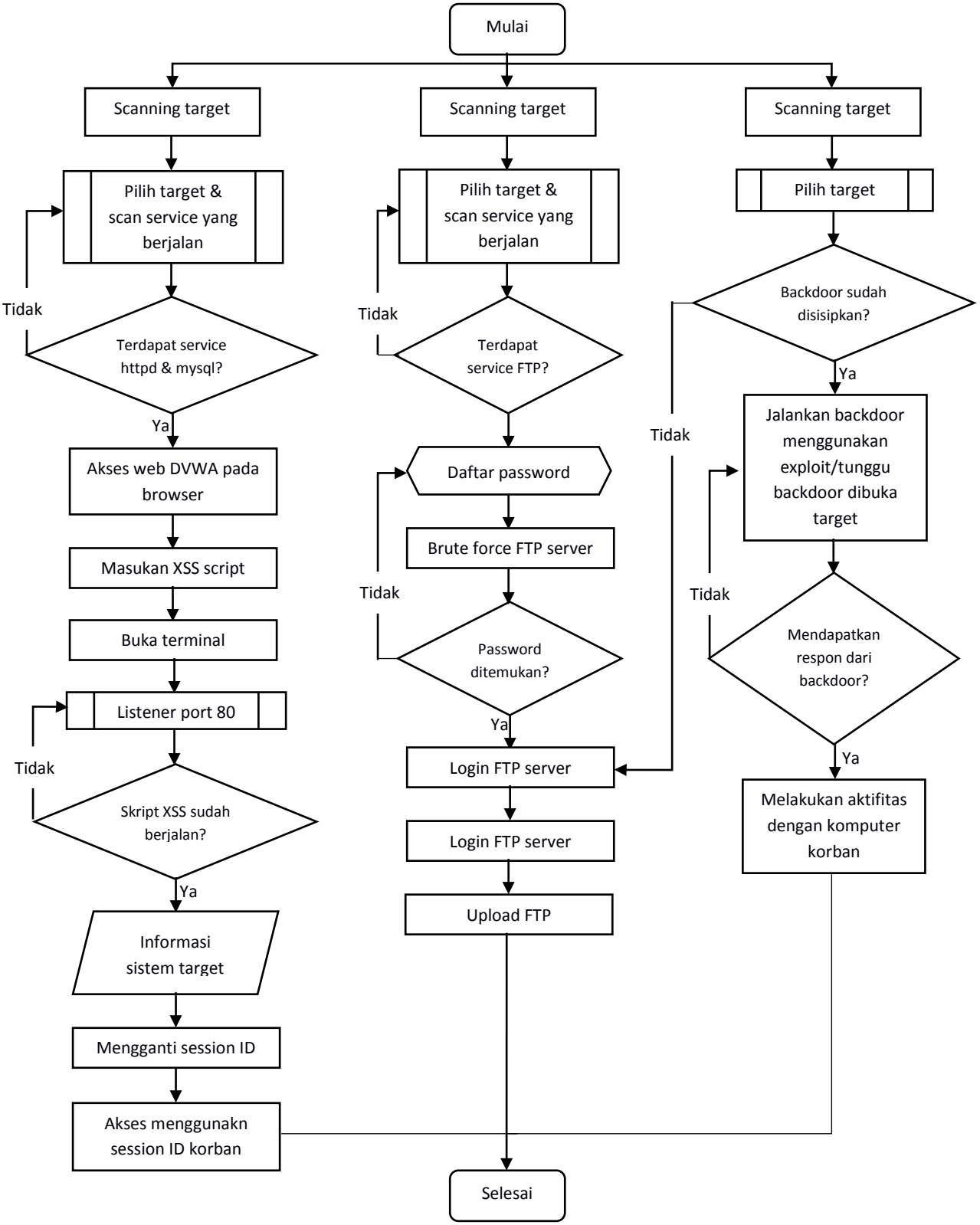
[1]	Wijaya, Roni. Forensik Digital Random Access Memory Pada Sistem Operasi Komputer Menggunakan Metode Dumpmemory. Bandung: Telkom University, 2016.
[2]	Cory, Altheide and Carvey, Harlen. Digital Forensics With Open Source Tools. USA: Syngress, 2011.
[3]	Al-Azhar, Muhammad Nuh. Digital Forensic – Panduan Praktis Investigasi Komputer. Depok: Salemba Infotek, 2012.
[4]	Sudyana, Didik. Belajar Mengenali Forensika Digital. Yogyakarta: Diandra, 2015.
[5]	E. V. Haryanto and U. P. Utama, Sistem Operasi Konsep dan Teori, Yogyakarta: Penerbit Andi, 2012.

LAMPIRAN

Lampiran 1
Diagram Alur Implementasi Sistem



Lampiran 2
Diagram Alur Pengujian



Lampiran 3
Diagram Alur Investigasi