MENGIDENTIFIKASI ARTEFAK PADA APLIKASI DROPBOX UNTUK MENDUKUNG FORENSIC ANDROID

IDENTIFYING ARTEFACT ON APPLICATION DROPBOX TO SUPPORT ANDROID FORENSICS

Josua Pujion Lasniroha [1], Setia Juli Irzal Ismail S.T.,M.T., [2], Gandeva Bayu Satrya,ST.,MT., Ph.D. [33 1,2,3]Program Studi D3 Teknologi Komputer, Universitas Telkom
[1]pljosua@student.telkomuniversity.ac.id[2] julismail@tass.telkomuniversity.ac.id [3] gandevabs@staff.telkomuniversity.ac.id

Abstrak : Dropbox adalah layanan penyimpanan cloud yang menawarkan penyimpanan gratis 7 GB kepada pengguna. Teknologi ini dapat disalahgunakan untuk tindak kejahatan seperti pornografi atau cybercrime yang diartikan sebagai penelitian terhadap kondisi aplikasi, diantaranya adalah penghapusan data pada aplikasi. Saat ini solusi untuk ini adalah untuk melakukan forensik digital ketika cybercrime telah terjadi. Dalam contoh kasus tersebut penyusun mengerjakan Proyek Akhir ini menggunakan Apllikasi Dropbox dan sebuah Android dalam proses investigasi. Dalam melakukan penyidikan, penyidik membuat model untuk menganalisa hasil forensic pada Android yang terdapat artefak atau yang sering disebut Data Remnant. Data Remnant adalah paket yang dihasilkan dari media penyimpanan yang didapat dari Dropbox setelah melakukan kegiatan forensic digital terhadap bukti digital yang berupa artefak tersebut. Artefak ini dapat digunakan sebagai bukti digital untuk penelitian yang akan dilakukan oleh penyidik forensik dalam meningkatkan pengetahuan tentang praktisi hukum siber. Pada proyek akhir ini penyidik mencari artefak atau data remnant yang dihasilkan dari Dropbox tersebut yang terdapat pada Android saat proses investigasi menggunakan metode crawling data atau sering disebut juga metode pengumpulan data.

Kata Kunci: Dropbox, Forensik Digital, Artefak, Privasi, Investigasi

Abstract : Application Dropbox service that offers up to 7 GB free storages to the User. This technology can be misused for cyber crimes such as : pornography and cybercrime, which is defined as research on application conditions, including deleting data in the application. Current solution for this condition is to do digital forensics when cybercrime has occurred. Due to that case, The Compiler does the final project using application Dropbox and an Android for investigation process. This technology Cloud Storage sometimes can be misused by People. Nowadays the solution for that situation is to do digital forensics when there is a cybercrime. investigator is working on this Final Project using application Dropbox and an Android for investigation process. In conducting an investigation, investigator using a model to analyze the results of artifacts, called by remnant data. It's a package produced from storage media that is obtained from Dropbox after conducting digital forensic activities on digital evidence in form of artifact. Digital forensic Investigators and Researcher also can use this artifact as digital evidence to increase knowledge about cyber legal practitioners. In this final project, investigator is looking for remnant artifacts or data generated from the Dropbox that contained on Android during investigationprocess.

Keywords: Dropbox, Digital Forensic, Artefact, Privacy, Investigation

1. Pendahuluan

Pada umumnya ilmu forensik diartikan dengan penerapan dan pemanfaatan ilmu pengetahuan tertentu untuk kepentingan penegakan hukum dan keadilan. Dalam penyidikan suatu kasus kejahatan, observasi terhadap bukti fisik dan interpretasi dari hasil analisis (pengujian) barang bukti yang merupakan alat utama dalam penyidikan tersebut.

Di era modern seperti sekarang ini, perkembangan teknologi dan informasi khusunya dalam dunia teknologi komputer selain memberikan dampak positif, juga banyak memberikan dampak negatif bagi kehidupan bermasyarakat. Dengan kecanggihan perangkat-perangkat digital saat ini, kejahatan dengan memanfaatkan teknologi digital pun semakin marak terjadi dengan berbagai modus dan model yang belum pernah ada sebelumnya.

Pada tahun 2016 jumlah kasus cybercrime mencapai 4.931 sehingga digital forensik sebagai sebuah ilmu terus berkembang seiring jalan membuat semakin rumitnya modus cybercrime yang terjadi. Menurut data resmi dari Mabes Polri, kuantitas kasus cybercrime di Indonesia meningkat setiap tahun. Melihat dari beragam kasus dan persoalan hukum yang muncul akhir-akhir ini membuat masyarakat sadar akan pentingnya keahlian di bidang Digital Forensik atau yang biasa dikenal dengan komputer forensik dalam mendukung investigasi pada kasus kejahatan khususnya kejahatan pada bidang komputer. Digital forensik merupakan cabang ilmu forensik yang berkaitan dengan bukti hukum yang ditemukan di komputer dan di media penyimpanan digital. Sebagai bagian dari Keamanan Komputer (IT Security) Digital Forensik merupakan kajian yang menarik dengan menerapkan metode metode tertentu dalam menelusuri bukti-bukti secara ilmiah dan dapat dipertanggung jawabkan secara hukum untuk mengungkap sebuah kasus kejahatan/kriminal.

2. Tinjauan Pustaka

Berikut ini adalah teori yang gunakan dalam penyusunan Proyek Akhir ini.

2.1 Drop Box

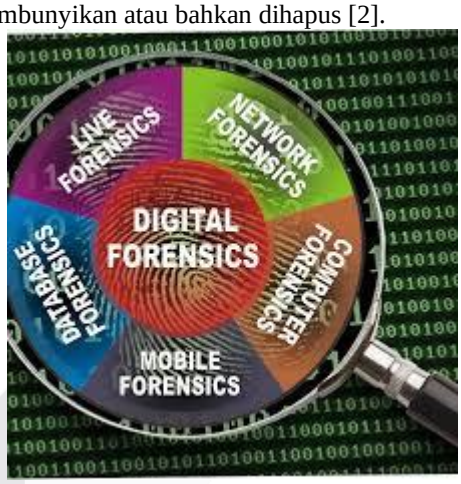
Aplikasi Dropbox sering disebut sebagai media penyimpanan awan yang berfungsi untuk sinkronisasi antar perangkat misalnya komputer dan Smartphone. Aplikasi Dropbox punya manfaat untuk kegiatan sharing data dan file. Aplikasi Dropbox berfungsi juga untuk menjamin data-data agar aman sekalipun perangkat yang dimiliki hilang atau rusak.

Selain fungsi umum aplikasi Dropbox yang telah dijelaskan seperrti diatas Aplikasi Dropbox juga berfungsi dalam bidang Digital Forensik sebagai acuan investigator untuk melakukan investigasi terhadap setiap aktivitas pelaku cybercrime yang dilakukan di Aplikasi Dropbox [1].

Gambar 2.1 DropBox

2.2 Digital Forensik

Aktifitas penyelidikan yang dilakukan untuk menemukan bukti digital yang akan memperkuat atau melemahkan bukti fisik dari kasus yang ditangani merupakan istilah digital forensik. Istilah forensik digital pada awalnya identik dengan forensik komputer. tetapi saat ini berkembang menjadi lebih luas yaitu menganalisa semua perangkat yang dapat menyimpan data digital. Forensik digital sendiri diperlukan karena biasanya data di perangkat digital dikunci, diganti, disembunyikan atau bahkan dihapus [2].



Gambar 2.2 Digital Forensik

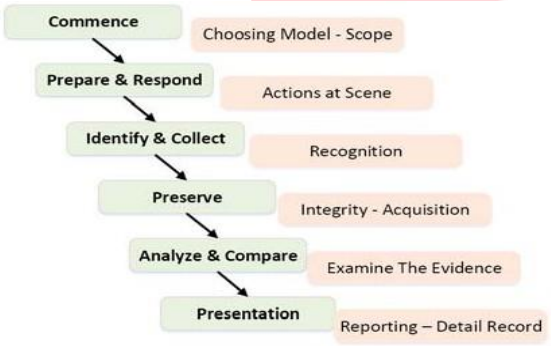
2.3 Android Forensik

Cabang dari forensik digital yang berkaitan dengan pemulihan bukti digital atau data dari perangkat mobile di bawah standart forensic istilah Android Forensik. Perangkat Android biasanya merujuk ke Smartphone , namun juga dapat berhubungan dengan perangkat digital yang memiliki baik memori internal dan komunikasi kemampuan [3].

Gambar 2.3 Android Forensik

3. Analisis dan Perancangan

3.1 Gambaran Sistem Saat Ini



Gambar 3.1 Gambaran Sistem Saat Ini

Pada Gambar 3.1 ini merupakan gambaran sistem saat ini. Sesuai dengan penelitian sebelumnya, beberapa step yang di klasifikasikan beberapa tahap dalam melakukan metode forensik terhadap bukti digital berupa artefak atau data remnant yang artinya adalah representasi sisa dari data digital yang tetap ada bahkan setelah upaya dilakukan untuk mengapus data. Data remnant yang akan di cari dan di temukan dalam Android. Contoh metode forensik yang telah di klasifikasikan antara lain:

Tabel 3. 1 Gambaran Sistem Saat Ini

Commence => Choosing Model – Scope	Pada tahap ini merupakan tahap awal memulai, yang dimaksud tahap awal memulai adalah tahap dimana penyidik membuat sebuah metodologi untuk menyeluruh yang dapat digunakan dalam penyelidikan
Prepare & Respond => Action at Scene	Pada tahap ini merupakan tahap awal kita untuk merespon akibat semakin meningkatnya kejahatan siber pada zaman sekarang. Dan untuk merespon semakin meningkatnya kejahatan siber, kita membutuhkan metodologi seperti model pertama yaitu commence, dan harus memastikan metodologi yang penyidik buat sejalan dengan pendekatan Forensik Digital.
Identify & Collect => Recognition	Pada tahap ini, sebelum akan dilakukan penyelidikan, penyidik harus mengidentifikasi terhadap kasus yang bersangkutan dengan insiden. Misalkan pada kasus dalam penelitian ini melibatkan penyimpanan awan atau sering disebut *Apllikasi* pada Dropbox. Pada tahap ini merupakan tahapan penting bagi penyidik untuk menentukan metode seperti pencarian kata kunci atau memeriksa sistem untuk mendukung proses investigasi.
Preserve => Integrity - Acquisition SHA-1	Pada tahap ini, penyidik harus bisa menjaga integritas dan keaslian bukti pada saat investigasi berlangsung. Sebagai contoh bukti asli tidak boleh dirusak atau di modifikasi seperti apapun, agar saat proses penyalinan barang bukti dapat dijamin tepat keaslian dengan barang bukti yang di dapat
Analyze & Compare => Examine The Evidence	Pada tahap ini penyidik melakukan perbandingan pada tiap tiap database untuk mencari artefak atau data remnant yang cocok saat melakukan tahap investigasi, dikarenakan artefak yang di hasilkan dari tiap tiap proses investigasi berbeda-beda dan menghasilkan beberapa path direktori yang berbeda-beda juga
Presenting => Reporting – Detail Record	Pada tahap ini, adalah tahap akhir dimana penyidik memberikan laporan yang memenuhi prosedur Forensik dan investigasi hukum yang berlaku dalam legislasi siber. Laporan yang di berikan oleh penyidik harus mencakup dari awal sampai akhir proses investigasi

3.2 Analisis Kebutuhan Fungsional dan Non Fungsional

Berdasarkan sistem yang akan dibuat, maka membutuhkan beberapa alat dan bahan berdasarkan fungsionalitas dan non-fungsionalitas, yaitu:

3.2.1 Fungsional

Artefak atau data remnant yang ditemukan sebagai barang bukti digital saat proses investigasi berupa file .db di Android yang dapat berguna sebagai laporan akhir hasil investigasi yang akan dibawa oleh penyidik..

3.2.2. Non Fungsional

Pada bagian ini terdapat dua bagian yaitu hardware dan software adalah sebagai berikut :

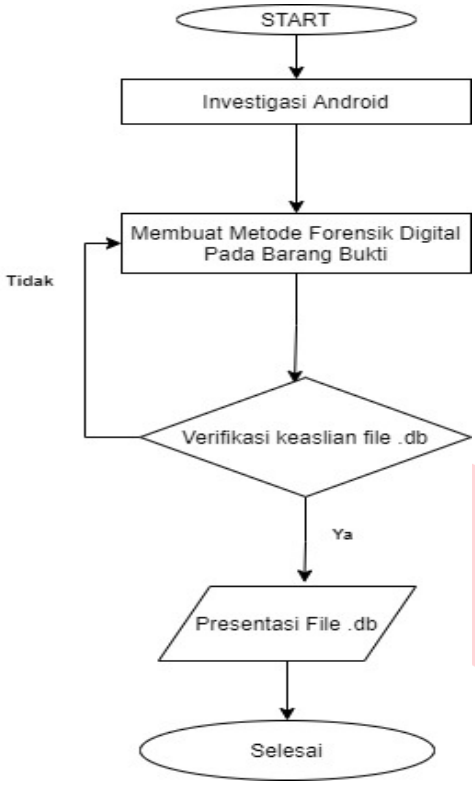
1. Hardware

   Hardware yang digunakan saat membuat sistem ini adalah satu buah (sistem operasi Android 9 Pie) yang akan di jadikan sebagai barang bukti pertama yang akan di investigasi oleh penyidik saat di temukan pada kejadian

2. Software

- Dropbox version 198.2.2
- Ressurection Remix version Pie
- Root Explorer version 4.7.1
- SQL DB Browser version 3.8.0

3.3 Perancangan Sistem



Gambar 3.2 Perancangan Sistem

Saat menemukan Android sebagai barang bukti yang kita dapatkan, Android tersebut akan penyidik investigasi dari tangan pelaku di tempat kejadian pertama kali

1. Setelah mendapatkan Android tersebut, penyidik membuat metode forensik digital yang cocok untuk memecahkan kasus terhadap hasil investagasi terhadap Android yang didapatkan

2. Dari hasil metode forensik digital akan menghasilkan artefak atau data remnant yang dimaksudkan adalah file.db tersebut

3. File .db yang telah didapatkan akan di verifikasikan dahulu terhadap segala aktivitas pelaku yang dia lakukan saat menggunakan Android tersebut

4. Ketika file .db cocok terhadap segala aktifitas yang dilakukan pelaku akan di presentasikan di pengadilan sebagai tahap akhir proses investigasi tersebut

5. Selesai

3.4 Kebutuhan Perangkat Keras Dan Lunak

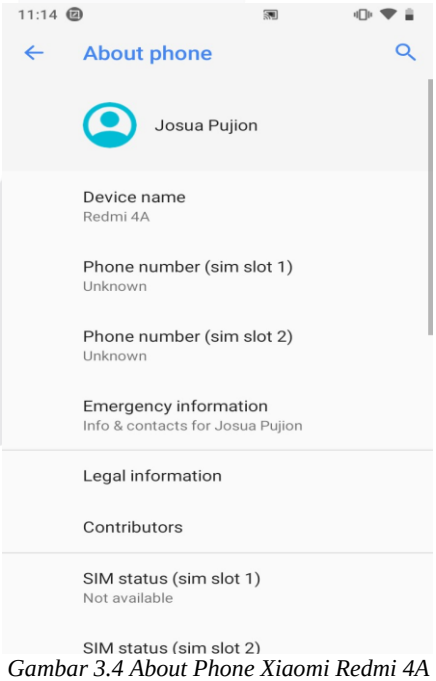
3.4.1 Implementasi Sistem

Implementasi Sistem dalam Proyek Akhir ini terbagi 2, yaitu hardware dan software. Dan tiap-tiap hardware maupun software yang digunakan mempunyai alasan dan fungsi terhadap sistem dalam Proyek Akhir ini, yaitu adalah :

3.4.1.1 Hardware

Hardware yang digunakan adalah sebuah Android yang bertipe Xiaomi redmi 4A (Androi 9 Pie), yang berfungsi sebagai barang bukti yang akan di investigasi untuk di cari file .db dalam Android tersebut. Berikut gambar spesifikasi Smartphone Android yang digunakan :

Gambar 3.3 Android Xiaomi Redmi 4A



Gambar 3.4 About Phone Xiaomi Redmi 4A

Spesifikasi Android bertipe Xiaomi Redmi 4A yang digunakan adalah:

1. Android tersebut mempunyai 2 slot SIM Card

2. Android tersebut bertipe Redmi 4A dengan serial number 1f3194247d04
3. Android tersebut mempunyai IMEI yang berbeda setiap SIM Card, IMEI sim slot 1 adalah 86540231932983. IMEI sim slot 2 adalah 86540231932991
4. Android tersebut adalah versi Android 9 Pie yang pembaharuan lanjutan dari update terbaru dari versi 8.1 oreo dan urutan ke-16 dari sistem operasi Android
5. Android tersebut menggunakan IP Address fe80::4e49:e3ff:feec:44cf 192.168.0.26 dengan Wi-FI MAC Address 4c:4(;e3:ec:44:cf dan Bluetooth address 4c:49:e3:ec:44:ce
6. Android tersebut terdapat build number rr_rolec-userdebug 9 PQ3A. 190705. 003 2354 test-keys yang artinya adalah Android tersebut telah tercantum dengan Customisasi ROM menggunakan Ressurection Remix
7. Android tersebut terdapat SELinux status yang permissive atau telah di izinkan

3.4.1.2 Timeline Saat Melakukan Forensik Digital

1. Install Data
   Timeline pengerjaan forensik digital saat aktivitas Install Data adalah pertama tama siapkan Android yang akan di install aplikasi Dropbox. Langkah selanjutnya cari aplikasi Dropbox tersebut di PlayStore, langkah terakhir mulai proses install aplikasi Dropbox tersebut dan jalankan aplikasi Dropbox tersebut. Setelah melakukan aktivitas Install Data jangan di hapus dahulu Aplikasi Dropbox, karena tahap selanjutnya adalah tahap Sign Up data, jika tahap Sign Up, Sign In, atau Sign Out data sudah di lakukan baru hapus Aplikasi Dropbox untuk menentukan artefak atau data remnant sehingga dapat di bandingkan

2. Sign Up Data
   Timeline pengerjaan forensik digital saat aktivitas Sign Up Data adalah pertama tama buka aplikasi Dropbox yang sudah di install. Langkah selanjutnya adalah registrasi akun Dropbox sehingga membuat akun pribadi yang akan digunakan pada aplikasi Dropbox tersebut. Sign Up data tidak semestinya harus login menggunakan authentikasi ke Aplikasi lainnya, misalnya gmail dll. Pada tahap Sign Up disini lebih baik daftar identitas pribadi pada Aplikasi Dropbox tersebut.

3. Sign In
   Timeline pengerjaan forensik digital saat aktivitas Sign In Data adalah pertama tama adalah buka aplikasi Dropbox yang sudah di install. Langkah selanjutnya adalah login menggunakan akun yang telah dibuat sebelumnya pada Aplikasi Dropbox, bisa juga login menggunakan akun yang di authentikasikan ke Aplikasi lain misalnya gmaiel dll. Tapi yang harus di ketahui pada tahap Sign In jangan sampai prosesnya sama seperti Sign Up, karena akan menghasilkan data remnant atau artefak yang hampir sama

4. Sign Out
   Timeline pengerjaan forensik digital saat aktivitas Sign Out Data adalah pertama tama adalah buka Aplikasi Dropbox yang sudah di install. Langkah selanjutnya adalah login menggunakan akun yang telah dibuat sebelumnya bisa juga dari tahap Sign Up atau Sign In. Langkah terakhir sign out akun yang dibuat sebelumnya dari aplikasi Dropbox tersebut. Pada tahap Sign Out ini lebih baik uninstall Aplikasi Dropbox biar sekalian menentukan hasil data remnant atau artefak dari tahap Uninstall Dropbox

5. Upload Data
   Timeline pengerjaan forensik digital saat aktivitas Upload Data adalah pertama tama buka aplikasi Dropbox yang sudah di install. Langkah selanjutnya adalah login menggunakan akun yang telah dibuat sebelumnya baik itu dari tahap Sign In atau Sign Up. Langkah selanjutnya adalah pilih file dari internal memory yang akan di upload ke Dropbox. Pada tahap ini adalah pelaku cybercrime mengupload sebuah foto dari internal memory ke Aplikasi Dropbox

6. Download Data
   Timeline pengerjaan forensik digital saat aktivitas Download Data adalah pertama tama buka aplikasi Dropbox yang sudah di install. Langkah selanjutnya adalah login menggunakan akun yang telah dibuat sebelumnya baik itu dari tahap Sign In atau Sign Up. Langkah selanjutnya adalah download Microsoft Word di Playstore karena membutuhkan Aplikasi yang lainnya untuk membuat file yang akan di simpan di Aplikasi Dropbox. Langkah terakhir buat file dari appllikasi Microsoft Word yang telah di download sebelumnya dari Playstore

7. Operation File Data
   timeline pengerjaan forensik digital saat aktivitas Operation File Data adalah pertama tama buka aplikasi Dropbox yang sudah di install. Langkah selanjutnya

adalah login menggunakan akun yang telah dibuat sebelumnya baik itu melalui tahap Sign In atau Sign Up data. Langkah selanjutnya adalah buat folder baru di aplikasi Dropbox tersebut yang akan menyimpan file setelah dipindahkan dari halaman home Aplikasi Dropbox tersebut. Langkah terakhir adalah pindahkan file yang dibuat dari Microsoft Word tersebut ke dalam folder yang dibuat sebelumnya

8. Uninstall Data
Timeline pengerjaan forensik digital saat aktivitas Uninstall Data adalah pertama tama buka aplikasi Dropbox yang sudah di install baik melalui tahap Sign In atau Sign Up.. Langkah selanjutnya adalah Sign Out terlebih dahulu dari akun Dropbox tersebut. Langkah terakhir adalah uninstall aplikasi Dropbox. Pada tahap Uninstall Data ini sangat berkesinambungan dengan tahap Sign Out, karena otomatis pada tahap Sign Out selesai, semua aktivitas yang dilakukan sebelumnya sudah berhenti.

3.4.1.3 Metode Forensik

Metode forensik akuisisi physical adalah metode forensik yang mengacu pada sistem penyimpanan ROM terhadap perangkat yang digunakan. Menggunakan metode forensik akuisisi physical bertujuan untuk mengubah isi penyimpanan ROM seperti mengganti OS dengan custom ROM, duplikasi OS dll. Metode forensik akuisisi physical pada proses investigasi ini digunakan terhadap Android sebagai perangkat utama yang akan di Custom ROM yang akan diberikan akses rooting terhadap Android tersebut. Tahap-tahap metode forensik akuisisi Physical ada beberapa, antara lain :

1. Persiapan
Saat tahap awal persiapan untuk melakukan metode forensik physical ada beberapa hal yang harus di persiapkan, antara lain tools yang digunakan harus sesuai kebutuhan dalam mendukung metode forensic. Tools yang digunakan antara lain: adb, android, laptop, kabel USB. Fungsi tools yang digunakan antara lain:

a) Obyek uji coba yaitu media penyimpanan yang akan di akuisisi yaitu ROM pada Android
b) Adb atau Android Debug Bridge (adb) adalah alat command line serbaguna yang memungkinkan berkomunikasi dengan perangkat. Perintah adb memfasilitasi berbagai tindakan perangkat, seperti menginstal dan men-debug aplikasi, dan memberikan akses ke shell Unix yang dapat digunakan untuk menjalankan berbagai perintah di perangkat
c) Android sebagai barang bukti yang akan di Custom ROM menggunakan Ressurection Remix
d) Laptop sebagai device saat Android akan di konfigurasi untuk di beri akses rooting
e) Kabel USB sebagai penghubung antara Android dengan Laptop agar dapat terhubung satu sama lain

2. Proses Akuisisi Menggunakan Metode Forensik Physical
Langkah pertama yang harus dilakukan yaitu instalasi tools yang akan digunakan yaitu Adb. Karena kegunaan Adb adalah memberikan akses ke shell Unix yang dapat gunakan untuk menjalankan berbagai perintah di perangkat. Ini adalah program klien-server yang meliputi tiga komponen pada Adb:

- Klien, yang mengirimkan perintah. Klien berjalan pada mesin pengembangan. Pengguna dapat memanggil klien dari terminal command line dengan mengeluarkan perintah adb.
- Daemon (adbd), yang menjalankan perintah di perangkat. Daemon berjalan sebagai proses latar belakang di setiap perangkat
.
- Server, yang mengelola komunikasi antara klien dan daemon. Server berjalan sebagai proses latar belakang pada mesin pengembangan Anda

Langkah kedua yang harus dilakukan yaitu mengaktifkan proses debug adb di perangkat Android. Untuk menggunakan adb dengan perangkat yang tersambung melalui USB, harus mengaktifkan proses debug USB dalam setelan sistem perangkat, di bagian Opsi developer. Layar Opsi developer secara default disembunyikan. Agar opsi itu tersedia, buka Setelan > Tentang ponsel lalu ketuk Nomor build tujuh kali. Kembalilah ke layar sebelumnya untuk menemukan Opsi developer di bagian bawah

Langkah ketiga adalah unlock bootloader, fungsi unlock bootloader adalah langkah penting dalam memasang ROM khusus

atau pemulihan kustom. Tanpa unlock bootloader tidak dapat menginstal custom ROM atau Custom recovery. Juga jika ingin me-root ponsel maka harus membuka kunci bootloader. Tanpa unlock bootloader tidak dapat membuat perubahan apa pun pada perangkat lunak Android

Langkah keempat adalah flash recovery image ke twrp, fungsinya untuk melakukan flashing file ROM bentuk .zip maupun .img misalnya file ROM,Root,Mods,Patch, dan lain sebagainya, kemudian juga dapat mencari file yang akan di perlukan dalam bentuk file IMG maupun Zip file, umumnya akan di arahkan ke Dir SdCard atau ke Root Android yang digunakan

Langkah kelima adalah install Custom ROM menggunakan Ressurection Remix. Fungsi Custom ROM antara lain adalah memaksimalkan performa smartphone Android yang artinya dapat mengurangi aplikasi bloatware atau aplikasi yang tidak diperlukan dalam perangkat android, sehingga dapat membuat penyimpanan internal tersedia lebih banyak dan mengosongkan ram. Alhasil, kinerja perangkat android jauh lebih baik untuk bermain game, menjalankan banyak aplikasi atau multitasking. Selain itu dapat melakukan overlocking untuk meningkatkan performa secara derastis

Langkah keenam adalah install supersu via slideload. Sideload sebenarnya memiliki arti yang sama dengan upload atau download. Sideload merupakan proses yang mengacu pada proses transfer data antara Android dengan PC atau laptop. Fungsi Supersu sendiri adalah untuk memberikan hak akses kepada aplikasi-aplikasi yang meminta akses root, di mana Anda bisa mengaturnya sesuai dengan kebutuha

4. IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi

Implementasi adalah penerapan cara kerja sistem berdasarkan hasil analisa dan juga perancangan yang telah dibuat sebelumnya dari sebuah algoritma yang disusun untuk proses investigasi. Implementasi dapat berupa seperti aplikasi, desain, dan sebagainya .Berikut adalah implementasi dari sistem pengerjaan Proyek Akhir ini.

4.1.1 Perangkat Lunak Pembangun

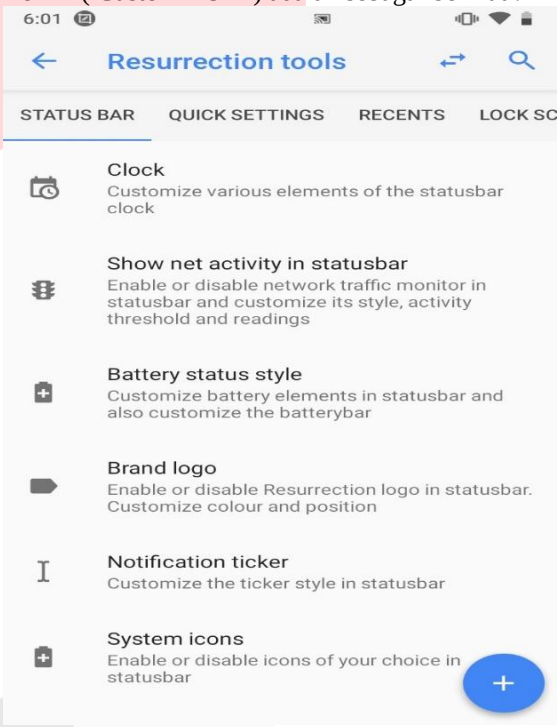
Perangkat lunak pembangun merupakan software atau Aplikasi yang digunakan untuk mendukung pembangunan kebutuhan aplikasi terhadap sistem yang dibuat, software atau Aplikasi yang digunakan sebagai berikut.

1. Dropbox, Aplikasi yang digunakan sebagai pusat untuk melakukan setiap aktivitas yang dilakukan oleh pelaku cybercrime sesuai kebutuhan sistem yang diperlukan

2. Custom ROM, untuk memberikan akses rooting terhadap Smartphone Android

4.1.2 Tampilan Android Menggunakan Ressurection ROM (Custom ROM)

Hasil tampilan Android menggunakan Ressurection Remix (Custom ROM) adalah sebagai berikut :



Gambar 4.1 Tampilan Custom Rom di Android

Pada gambar 4.3 ini merupakan Android menggunakan Ressurection ROM (Custom ROM) agar bisa di beri aksess rooting pada Android tersebut. Alasan melakukan Custom ROM menggunakan Ressurection Remix adalah untuk mengubah atau memodifikasi sistem media penyimpanan ROM terhadap Android tersebut agar dapat diberi akses rooting setelah sebelumnya terjadinya bootlop terhadap Android tersebut
Langkah rooting terhadap Android tersebut adalah:

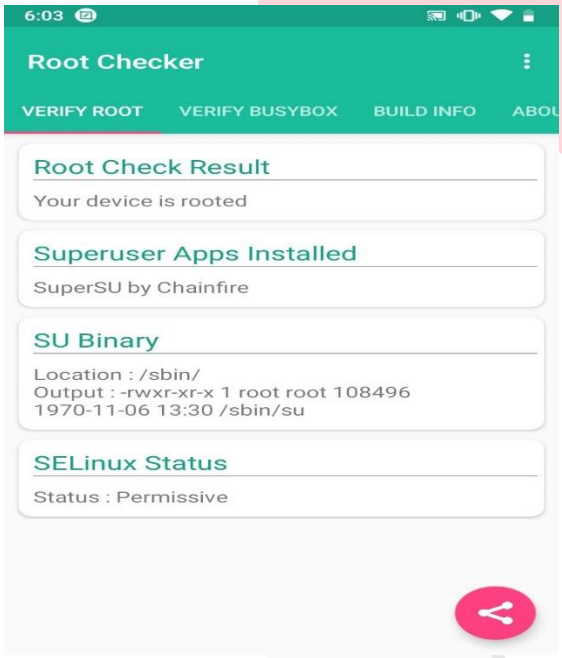
1. Unlock bootloader pada Android tersebut
2. Flash recovery image ke twrp
3. Install Custom ROM menggunakan Ressurection Remix
4. Install super su via slideload
5. Restart

4.1.3 Perangkat Keras Pembangun

Perangkat keras pembangun merupakan penjelasan dari perangkat keras yang digunakan untuk mendukung proses investigasi, alat yang digunakan pada sistem ini sebagai berikut.

1. Smartphone Android, sebagai barang bukti pertama yang diamankan dari pelaku cybercrime untuk memecahkan proses investigasi. Smartphone Android disini sebelumnya harus sudah di beri akses rooting

4.1.4 Tampilan Verifikasi Android Telah Di Beri Akses Rooting



Gambar 4.2 Verifikasi Android Yang Telah Di Rooting

4.2 Pengujian

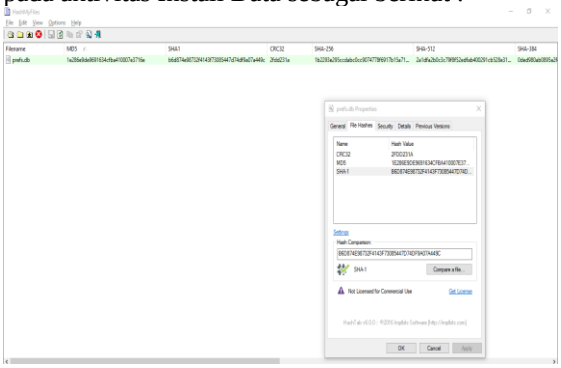
Tahap pengujian merupakan untuk memvalidasi sistem yang dibuat telah berjalan sesuai dengan fungsinya. Dalam tahap ini terdapat berbagai masalah yang berkaitan dengan fingsionalitas sistem.

4.2.1 Pengujian Integrity File.db

Tujuan integrity file adalah memastikan akurasi dan konsistensi semua sistem yang menyimpan, memproses, atau pengambilan data. Berikut adalah hasil cek integrity melalui checksum SHA-1 terhadap setiap file.db hasil dari aktivitas yang dilakukan pada Aplikasi Dropbox tersebut

4.2.2 Install Data

Hasil integrity data menggunakan checksum SHA-1 pada aktivitas Install Data sebagai berikut :

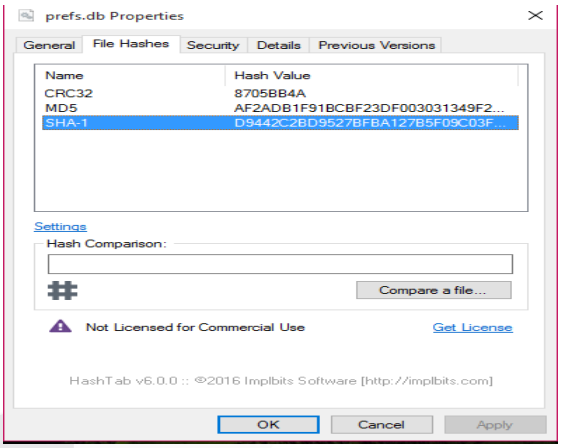


Gambar 4.3 Hasil Checksum SHA-1 file.db Terhadap Aktivitas Install Data

Pada proses checksum file.db tahap aktivitas Install Data menggunakan tools HashMyFiles menghasilkan SHA-1 dari tahap aktivitas tersebut yaitu B6D874E98732F4143F73085447D74DF9A07A449C

4.2.3 Sign Up

Hasil integrity data menggunakan checksum SHA-1 pada aktivitas Sign Up Data sebagai berikut :

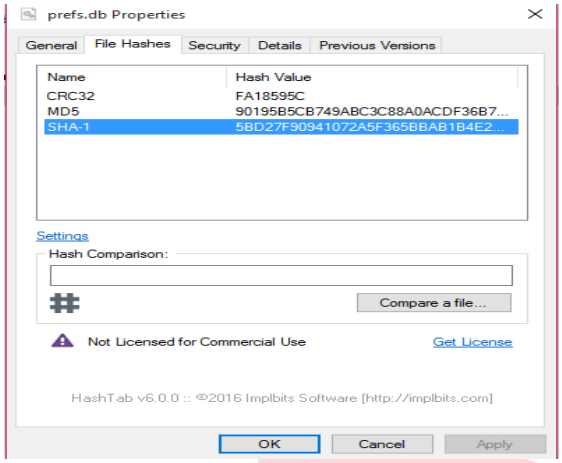


Gambar 4.4 Uji Integrity File.db

Pada proses checksum file.db tahap aktivitas Sign Up Data menggunakan tools HashMyFiles menghasilkan SHA1 dari tahap aktivitas tersebut yaitu D9442C2BD9527BFBA127B5F09C03F51C1ED0E5A1

4.2.4 Sign In

Hasil integrity data menggunakan checksum SHA-1 pada aktivitas Sign In Data sebagai berikut :

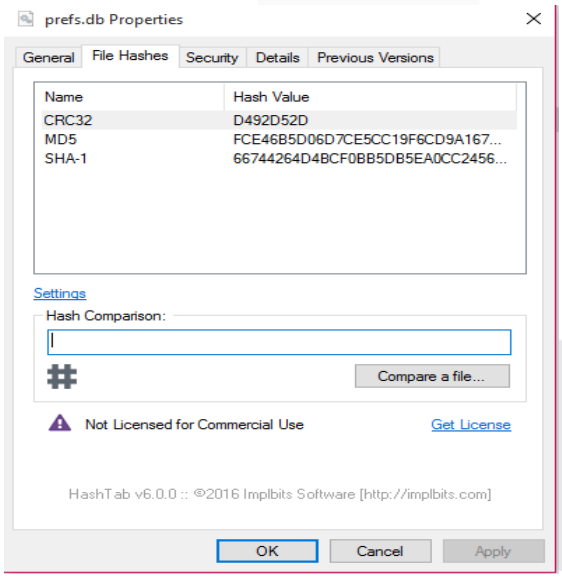


Gambar 4.5 Uji Integrity File.db aktivitas sign in data

Pada proses checksum file.db tahap aktivitas Sign In Data menggunakan tools HashMyFiles menghasilkan SHA1 dari tahap aktivitas tersebut yaitu 5BD27F90941072A5F365BBAB1B4E25CB5D4A757C

4.2.5 Sign Out

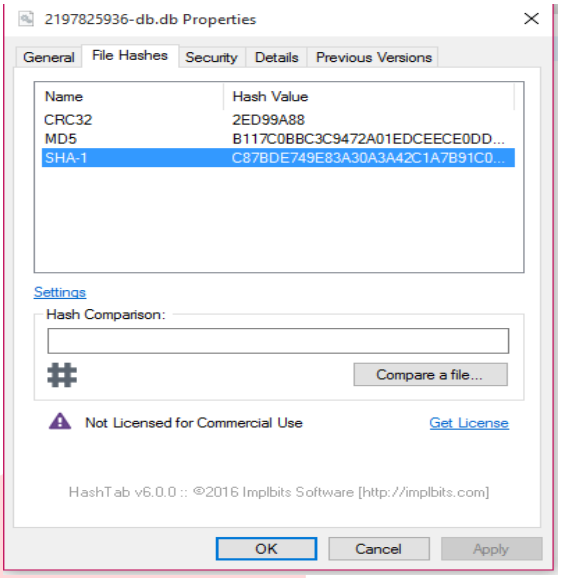
Hasil integrity data menggunakan checksum SHA-1 pada aktivitas Sign Out Data sebagai berikut :



Gambar 4.6 Uji Integrity File db Aktivitas Sign Out Data

4.2.6 Upload Data

Hasil integrity data menggunakan checksum SHA-1 pada aktivitas Upload Data sebagai berikut :

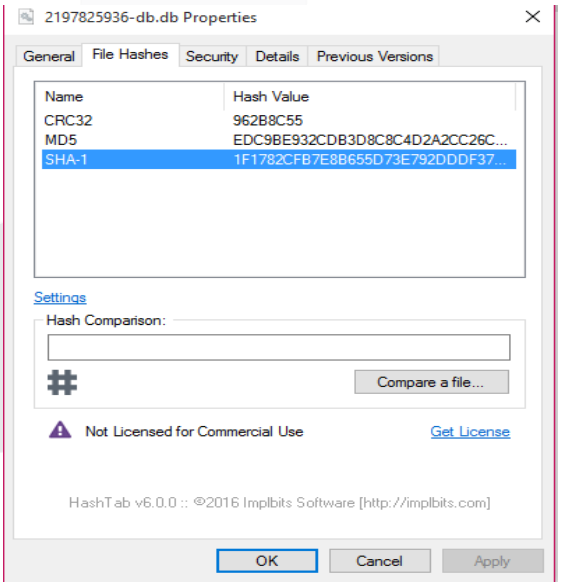


Gambar 4.7 Uji Integrity File db aktivitas Upload Data

Pada proses checksum file.db tahap aktivitas Upload Data menggunakan tools HashMyFiles menghasilkan SHA1 dari tahap aktivitas tersebut yaitu C87BDE749E83A30A3A42C1A7B91C0B32CA12F4D6

4.2.6 Download Data

Hasil integrity data menggunakan checksum SHA-1 pada aktivitas Download Data sebagai berikut :

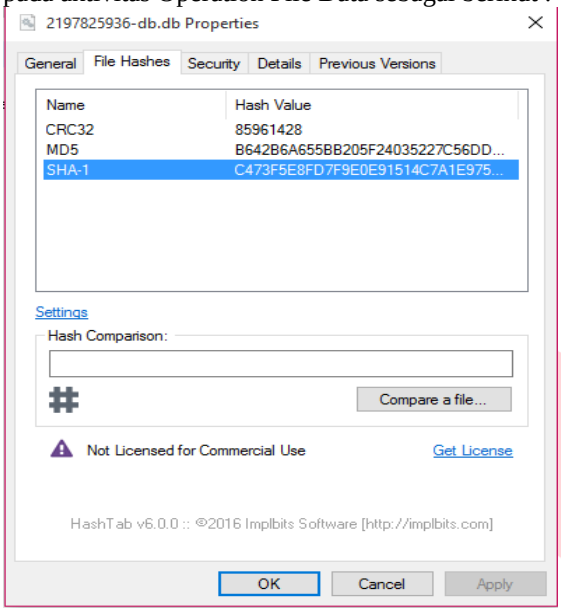


Gambar 4.8 Uji Integrity File db Aktivitas Download Data

Pada proses checksum file.db tahap aktivitas Download Data menggunakan tools HashMyFiles menghasilkan SHA1 dari tahap aktivitas tersebut yaitu 1F1782CFB7E8B655D73E792DDDF37AE4C5A0459A

4.2.6 Operation File Data

Hasil integrity data menggunakan checksum SHA-1 pada aktivitas Operation File Data sebagai berikut :



Gambar 4.9 *Uji Integrity File db Aktivitas Operation File Data*

Pada proses checksum file.db tahap aktivitas Operation File Data menggunakan tools HashMyFiles menghasilkan SHA1 dari tahap aktivitas tersebut yaitu C473F5E8FD7F9E0E91514C7A1E975DBF56D2D71B

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil pengerjaan Proyek Akhir ini, dapat disimpulkan bahwa

1. Untuk membuktikan hasil penemuan artefak dari setiap aktivitas yang dilakukan di Dropbox Setiap harus di cek integrity file .db tersebut agar memastikan akurasi dan konsistensi yang terbukti terhadap file.db dari setiap aktivitas yang dilakukan
2. Untuk membuktikan akurasi dan konsistensi saat manual investigasi bisa menggunakan metode forensik sesuai standart dunia forensik. Metode forensic untuk manual investigasi paling cocok adalah metode forensic physical yang titik utamanya terletak pada media penyimpanan ROM

5.2 Saran

Saran untuk penelitian lanjutan adalah :

1. Harus menggunakan metode forensik yang berbeda, contohnya adalah metode forensik logical, dll
2. Harus menggunakan media penyimpanan awan yang berbeda, contohnya adalah box,

REFERENSI

[1] Bakti Kominfo, " Dropbox : Pengertian, fungsi, dan manfaatnya, unduh sekarang, juga demi keamanan data anda" 2019. [Online].

Available: https://www.baktikominfo.id/en/informasi/pengetahuan/dropbox_pengertian_fungsi_dan_manfaatnya_unduh_sekarang_juga_demi_keamanan_data_anda-955 .[Accessed 29 Agusus 2020].

[2] Aliyhafiz.com, " Digital Forensik : Pengertian, metode, dan software yang digunakan" 2020. [Online].

Available: https://aliyhafiz.com/digital-forensik-pengertian-metode-dan-software-yang-digunakan/.[Accessed 29 Agusus 2020].

[3] Abdallah, A., Alamin, M., Babiker, A., & Mustafa, N. (2015). A Survey on Mobile Forensic for Android Smartphones. IOSR Journal of Computer Engineering, 17(1), 2278–661. http://doi.org/10.9790/0661-17211519

[4] Gandeva Bayu Satrya, Ahmad Nasrullah, Soo Young Shin (2017). Identifying artefact on Microsoft OneDrive client to support Android forensics. International Journal Of Security and Digital Forensics Electronic Security IOSR.085192 https://doi.org/10.1504/IJESDF.2017.085192