ANALISIS DIGITAL FORENSIK PADA APLIKASI GOPAY DI ANDROID

Muhammad Farrel Aldian[1], Setia Juli Irzal Ismail[2], Gandeva Bayu Satrya[3]

[1, 2,] Universitas Telkom, Bandung
farrelaldian@student.telkomuniversity.ac.id[1], julismail@tass.telkomuniversity.ac.id[2], gandevabs@staff.telkomuniversity.ac.id[3]

Abstrak

Gopay merupakan salah satu E-Wallet ternama di Indonesia, berdampingan dengan E-wallet lainnya, Gopay dapat digunakan untuk berbagai macam hal transaksi, mulai dari membeli makanan, sampai membayar suatu produk. Teknologi ini dapat disalah gunakan untuk tindak kejahatan seperti tansaksi uang ilegal atau order fiktif yang dapat merugikan pihak penerima order maupun driver penghantar orderan. Dompet digital saat ini termasuk titik celah untuk kejahatan cybercrime. Untuk itu melakukan forensik digital adalah cara yang tepat untuk memecahkan kasus kejahatan cybercrime terhadap dompet digital. Seperti yang akan di kerjakan dalam pengerjaan Proyek Akhir ini pada Aplikasi Gopay dan sebuah Android dalam proses investigasi. Untuk melakukan penyidikan, penyidik membuat model dari metode Forensic untuk menganalisa hasil forensic pada Android yang terdapat artefak atau yang sering disebut Data Remnant. Data Remnant merupakann sebuah represantasi dari data yang sudah ada atu bahkan tetap ada setelah dilakukannya sebuah perubahan data, baik itu di edit, tambahkan, atau bahkan di hapus. Artefak ini dapat digunakan sebagai bukti digital pada aplikasi Gopay untuk penelitian yang akan dilakukan oleh penyidik forensik dalam meningkatkan pengetahuan tentang praktisi hukum siber.

Kata Kunci: GoPay, Forensik Digital, Artefak, Data Remnant, Investigasi

Abstract

Gopay is one of the leading E-Wallets in Indonesia, side by side with other E-wallets, Gopay can be used for various kinds of transactions, from buying food to paying for a product. This technology can be misused for crimes such as illegal money transactions or fictitious orders that can harm the order recipient and the order delivery driver. Today's digital wallets are a loophole for cybercrime. For this reason, digital forensics is the right way to solve cybercrime cases against digital wallets. As will be done in working on this Final Project on the Gopay Application and an Android in the investigation process. To conduct an investigation, investigators create a model from the Forensic method to analyze forensic results on Android that contain artifacts or what is often called Remnant Data. Remnant data is a representation of data that already exists or even remains after a data change is made, whether it is edited, added, or even deleted. These artifacts can be used as digital evidence in the Gopay application for research to be carried out by forensic investigators in increasing knowledge about cyber law practitioners

Keywords: GoPay, Digital Forensic, Artefact, Data Remanant, Investigation

1. Pendahuluan

Gojek merupakan sebuah aplikasi yang digunakan oleh masyarakat secara umum untuk melakukan pemesanan seperti jasa transportasi, pemesanan makanan, pengiriman barang dan lainnya. Seiring berkembangnya zaman maka aplikasi Gojek juga semakin berkembang seperti penyediaan layanan E-Wallet. E-Wallet yang disediakan oleh Gojek ini dapat digunakan untuk melakukan pembayaran secara cepat melalui aplikasi digital. Pembayaran aplikasi melalui aplikasi Gojek ini dinamakan dengan Gopay. Teknologi software belakangan ini banyak digunakan oleh banyak masyarakat namun, teknologi ini rentan terjadinya masalah Cybercrime. Cybercrime yang dimaksud yakni adanya pemalsuan pesanan,seperti saat user melakukan pemesanan pada aplikasi yang telah di Top-Up melalui Mobile Banking yang dimiliki oleh masingmasing pengguna. Setelah pengguna melakukan Top-Up melalui Mobile Banking maka saldo tersebut akan masuk dan menjadi saldo Gopay. Setelah terisinya saldo Gopay pada maka pengguna aplikasi dapat melakukan pemesanan, namun saat pesanan dilakukan dan saldo sudah terpotong pesanan tidak sampai ke tangan pengguna sehingga pengguna mengalami kerugian. Lalu untuk menyelesaikan permasalahan cybercrime seperti penipuan pemesanan dapat di lakukannya digital forensic sebagai solusi di karenakan dalam forensic digital banyak hal yang dapat di dapatkan melalui dari proses persiapan, identifikasi , pengelolaan, analisis, hingga akhir[1]. Dalam pengerjaan pengerjaan proyek akhir ini hal – hal yang dilakukan adalah menggunakan analisis forensic digital dengan metode physical forensic untuk mendapatkan data – data serta informasi detail dari pelaku kejahatan seperti mencari dan mendapatkan foto pelaku, id driver, dan nomor telepon driver serta data – data lain seperti nominal transaksi hingga detail pesanan.

2. Dasar Teori

2.1 Gopay

GoPay merupakan layanan e-money dari salah satu produk atau aplikasi dompet digital yaitu Gojek Indonesia. GoPay digunakan untuk menyimpan Gojek Credit yang mana nantinya bisa dipakai untuk melakukan pembayaran atau transaksi – transaksi 6 yang ada pada semua layanan aplikasi Gojek seperti (GoRide, GoCar, GoSend, GoFood, dan lain sebagainya). GoPay memiliki teknologi keamanan terkini yang menjamin semua data dan transaksi pengguna selalu aman. Aplikasi GO-PAY dapat digunakan sebagai pembayaran pada Layanan di aplikasi Gojek, Toko atau restoran Rekan Usaha GOPAY, Pay Later untuk pelanggan terpilih, dan Transaksi keuangan lainnya seperti transfer saldo GO-PAY ke sesama pengguna dan ke bank bagi pengguna yang sudah melakukan upgrade ke GO-PAY Plus[5].

Gambar 1. (a)
Sumber: App Gojek

2.2 Digital Forensik

Pada umumnya ilmu forensik diartikan dengan suatu ilmu pengetahuan dan keahlian untuk mengidentifikasi, mengoleksi, menganalisa dan menguji bukti– bukti digital pada saat menangani sebuah kasus yang memerlukan penanganan dan identifikasi barang bukti digital. Forensik digital (Digital forensics) atau juga dikenal sebagai ilmu forensik digital adalah salah satu cabang ilmu forensik, terutama untuk penyelidikan dan penemuan konten perangkat digital, dan seringkali dikaitkan dengan kejahatan komputer. Istilah Digital Forensic pada awalnya identik dengan forensik komputer tetapi kini telah diperluas untuk menyelidiki semua perangkat yang dapat menyimpan data digital.[2].

Gambar 2. (b)
Sumber : google.com

2.3 Android Forensik

Android forensik merupakan cabang dari forensik digital yang berkaitan dengan pemulihan bukti digital atau data dari perangkat mobile. Perangkat selular biasanya merujuk ke ponsel, namun juga dapat berhubungan dengan perangkat digital yang memiliki baik memori internal dan komunikasi kemampuan. Proses investigasi biasanya difokuskan pada data yang sederhana seperti data panggilan, dan komunikasi seperti email atau sms, dan juga data yang sudah terhapus dari media penyimpanan mobile device [3].

Gambar 3. (c)
Sumber: google.com

3. Analisis Dan Perancangan

3.1 Gambaran Sistem Saat Ini

Gambar 4. (d)

Maksud dari gambar 3.1 adalah gambaran sistem saat ini, yang menjelaskan mengenai seorang user aplikasi Gojek yang melakukan sebuah laporan mengenai pesanan yang telah dilakukannya, namun akan tetapi selang beberapa waktu setelah pesanan di lakukan, pesanan tersebut belum kunjung sampai, hingga akhirnya pengguna tersebut melakukan laporan yang nantinya bertujuan untuk mendapatkan informasi mengenai pelaku kejahatan melalui analisis serta identifikasi oleh tim forensic dan informasi tersebut dapat di berikan kepada pihak berwajib.

Tabel 1. (a)

Commence => Choosing Model – Scope	Tahapan ini merupakan tahapan awal dimana keseluruhan rencana telah dibuat, terdiri dari hal apa saja yang kemudian akan dilakukan pada penelitian
Prepare & Respond => Action at Scene	Tahapan ini adalah tahapan untuk melakukan investigasi pada komputer dan smartphone, metode dan alat yang dilakukan tentu berbeda. Tahapan ini dilakukan untuk melakukuan penyelidikan dalam forensik digital secara tepat dan efektif.
Identify & Collect => Recognition	Tahapan ini berisi tentang tahapan dalam menentukan sumber penting dari bukti digital (seperti foto TKP, nama organisasi, log Internet, atau log smartphone). Proses identifikasi ini sangat berkaitan dengan kegiatan analisis barang bukti. Dengan kata lain, jika proses identifikasi dan proses pengumpulan tidak selesai, maka hasil yang didapatkan juga tidak lengkap dan tidak dapat diterima di meja hukum.
Preserve => Integrity - Acquisition	Pada tahap ini adalah tahap untuk penelitian yang mendalam, proses akusisi dan proses (duplikasi sebaiknya dilakukan). Hal tersebut dikarenakan hal terpenting dalam melakukan forensik bergerak adalah memastikan integritas dan keamanan data Ketika proses akuisisi data dilakukan. Dengan keterbatasan

Analyze & Compare => Examine The Evidence	Proses penyimpanan menghasilkan image dari data asli. Image ini akan digunakan untuk melakukan analisis. Penelitian ini menggunakan aplikasi GoPay yang diinstal pada Samsung smartphone, informasi yang diambil dari smartphone Android adalah proses install, signup, upload, download, logout, login, operasi data, topup saldo dan uninstall aplikasi GoPay
Presenting => Reporting – Detail Record	Pada tahap ini, adalah tahap akhir dimana Tahapan selanjutnya adalah menghasilkan laporan yang benar dan dapat diterima berdasarkan hasil analisis yang diperoleh pada tahap sebelumnya untuk diberikan kepada pihak berwenang.

3.2 Identifikasi Kebutuhan Sistem

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

3.2.1 Fungsionalitas

Artefak atau data remnant yang ditemukan sebagai barang bukti digital saat proses investigasi berupa file .db akan di klasifikasikan dan di sortir sesuai aktivitas diatas yang telah dilakukan untuk menemukan satu persatu Artefak yang sesuai pada 12 Android yang dapat berguna sebagai laporan akhir hasil investigasi yang akan dibawa oleh penyidik.

3.2.2 Non Fungsionalitas

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

1. Hardware

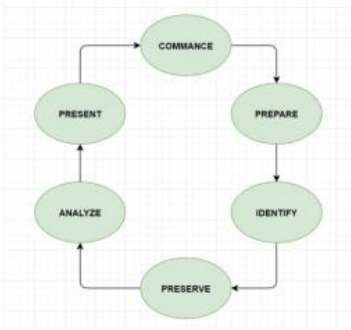
Hardware yang digunakan saat membuat sistem ini adalah satu buah Android yaitu Samsung J5 yang akan di jadikan sebagai barang bukti pertama yang akan di investigasi oleh penyidik saat di temukan pada kejadian pertama kali di lapangan.

2. Software

Software yang digunakan dalam pembuatan Proyek Akhir ini adalah sebagai berikut:

1. Android debug tool v.1.4.2
2. Odin v3.13.1
3. Root Explorer version 4.7.1
4. SQL DB Browser version v3.12.0

3.3 Perancangan Sistem



Gambar 5. (e)

Pada Gambar berikut ini merupakan konsep sistem untuk pengambilan artefak atau data remnant. Terdapat beberapa step by step yang di konsepkan dalam beberapa tahap untuk melakukan metode forensik terhadap bukti digital berupa artefak atau data remnant yang akan di cari.

3.4 Kebutuhan Perangkat Keras Dan Perangkat Lunak

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

3.4.1 Perangkat Keras

Hardware yang digunakan adalah sebuah Android yang bertipe Samsung Galaxy J5 (Android 5 Lollipop), 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 6. (f)

Gambar 7. (g)

Spesifikasi Android bertipe Samsung Galaxy J5 yang digunakan adalah:

1. Android tersebut mempunyai 2 slot SIM Card.
2. Android tersebut bertipe Galaxy J5 dengan nomer versi J500GXXU1APG1.
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 5.1.1 Lollipop LMY47D.
5. Android tersebut menggunakan IP Address fe80::4e49:e3ff:feec:44cf 192.168.0.26 dengan Wi-FI MAC Address 4c:49;e3:ec:44:cf dan Bluetooth address 4c:49:e3:ec:44:ce
6. Android tersebut terdapat build number LMY48B.J500GXXU1APG1
7. Android tersebut terdapat SELinux status yang permissive atau telah di izinkan.

3.4.2 Perangkat Lunak

Spesifikasi Android bertipe Samsung Galaxy J5 yang digunakan adalah:

1. Android tersebut mempunyai 2 slot SIM Card.
2. Android tersebut bertipe Galaxy J5 dengan nomer versi J500GXXU1APG1.
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 5.1.1 Lollipop LMY47D.
5. Android tersebut menggunakan IP Address fe80::4e49:e3ff:feec:44cf 192.168.0.26 dengan Wi-FI MAC Address 4c:49;e3:ec:44:cf dan Bluetooth address 4c:49:e3:ec:44:ce
6. Android tersebut terdapat build number LMY48B.J500GXXU1APG1
7. Android tersebut terdapat SELinux status yang permissive atau telah di izinkan.

3.5 Metode Forensik

Metode forensik akuisisi physical adalah metode forensik yang mengacu pada sistem penyimpanan ROM terhadap perangkat yang digunakan. Sedangkan metode crawling data digunakan untuk pemecahan masalah dan akan menentukan kata kunci dalam menghasilkan artefak atau data remnant yang tersedia di direktori Android. 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 diberikan akses rooting terhadap Android tersebut.

3.6 Timeline Saat Melakukan Forensik Digital

1. Install Data

Langkah pertama adalah install aplikasi GoPay melalui Playstore. Langkah selanjutnya di Uninstall lagi terlebih dahulu setelah itu lakukan pengecekan apakah menghasilkan Artefak Install Data yang berupa file .db menggunakan tools

Root Explorer untuk eksplorasi semua file terhadap Android yang sudah di berikan akses rooting

2. Sign Up

Langkah kedua adalah melakukan Sign Up Data yang dimana prosesnya harus terlebih dahulu install lagi aplikasi GoPay pada Playstore. Langkah selanjutnya adalah registrasi akun menggunakan data pribadi client, pada Langkah ini tidak semestinya harus authentikasi ke beberapa aplikasi lain seperti gmail dll untuk registrasi akun.

3. Sign In

Langkah ketiga adalah Sign In, dimana tahap ini adalah tahap login menggunakan akun yang sudah di registrasi sebelumnya. Saat proses Sign Up Data selesai Langkah 19 selanjutnya adalah harus di logout dulu baru di cek menggunakan Root Explorer untuk mendapatkan Artefak Sign In dan membandingkannya dengan tahap aktivitas lainnya.

4. Sign Out

Langkah keempat adalah Sign Out, pada tahap ini saat sudah login menggunakan email dan password yang dibuat Langkah selanjutnya adalah Sign Out atau keluarkan akun yang telah login tadi dan eksplorasi file .db nya menggunakan Root Explorer untuk menemukan Artefak Sign out

5. Explore

Langkah kelima adalah Explore, dimana tahap ini penyidik bebas untuk eksplorasi fitur fitur yang ada aplikasi GoPay tersebut misalnya GoFood, GoRide, dll. Langkah selanjutnya eksplorasi file .db menggunakan Root Explorer untuk mencari Artefak explore tersebut

6. Top Up

Langkah keenam adalah Top Up, dimana pada tahap ini adalah tahap melakukan pengisian saldo GoPay melalui apapun itu misalnya ATM, Mobile Banking, dll. Langkah selanjutnya adalah eksplorasi file .db menggunakan Root Explorer untuk menemukan Artefak dari Top Up tersebut.

7. Pay

Langkah ketujuh adalah Pay, dimana pada tahap ini saat dimana melakukan order melalui aplikasi GoPay seperti GoFood, GoRide dll dan membayarnya menggunakan GoPay. Langkah selanjutnya adalah mengeksplorasi file .db menggunakan Root Explorer untuk mencari Artefak dari Pay tersebut

8. Uninstall Data

Langkah terakhir adalah Langkah Uninstall Data, dimana pada tahap ini tahap akhir setelah semua tahap aktivitas diatas telah dilakukan. Langkah selanjutnya eksplorasi file .db menggunakan Root Explorer untuk mencari Artefak Uninstall Data dan membandingkan dengan Artefak setiap aktivitas yang dilakukan

4. Implementasi Dan Pengujian

Implementasi adalah suatu tindakan atau pelaksanaan dari sebuah rencana yang sudah disusun secara matang dan terperinci. Implementasi physical forensic biasanya dilakukan setelah perencanaaan sudah dianggap sempurna[8]. atau di desain untuk kemudian dijalankan sepenuhnya. Maka, implementasi juga dituntut untuk melaksanakan sepenuhnya apa yang telah direncanakan dalam pengerjaan Proyek Akhir.

4.1 Perangkat Lunak Pembangunan

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

1. GoPay, Aplikasi yang berupa dompet digital (E-wallet) yang digunakan sebagai pusat untuk melakukan setiap aktivitas yang dilakukan oleh pelaku cybercrime sesuai kebutuhan sistem yang diperlukan
2. Rooting Android, untuk memberikan akses rooting terhadap Smartphone Android

4.2 Tampilan Android Menggunakan Odin (Stock ROM)

Hasil tampilan Android menggunakan Odin (Stock ROM) adalah sebagai berikut :

Gambar 8. (h)

Pada Gambar 8 ini merupakan Android menggunakan Stock ROM, karena untuk Android Samsung apapun itu tidak perlu Custom ROM untuk di root seperti beberapa Android yang lain.

Langkah rooting terhadap Android tersebut adalah:

1. Pada perangkat Android mode USB harus sudah di Debuggin.
2. Siapkan software Odin v3.13.1, ADB Fastboot Tools v1.4.2, dan CF Auto Root
3. Buka aplikasi Odin v3.13.1
4. Pada perangkat Android harus masuk ke dalam Download Mode lalu sambungkan ke laptop / PC.
5. Klik AP pada aplikasi Odin v3.13.1, masukkan file CF Auto Root dan klik start
6. Tunggu proses sampai notif reset dan tunggu hingga bertulisan Pass maka Android dapat di putuskan dari laptop dan Android sudah di beri akses rooting.
7. Gunakan aplikasi Root Checker untuk menguji apakah Android sudah verifikasi root atau belum sebelum di gunakan.

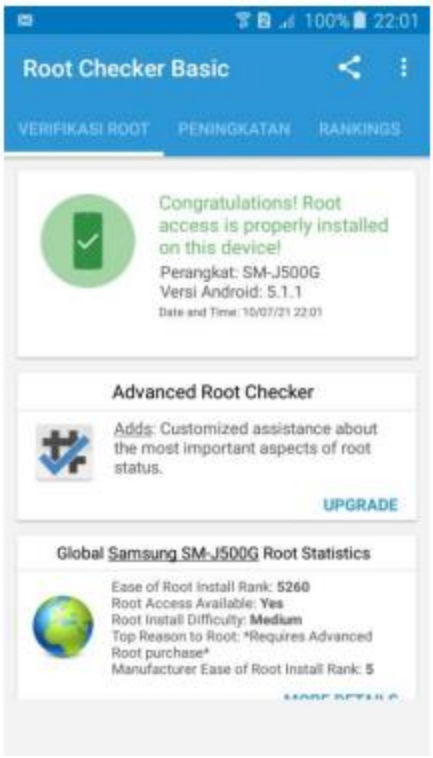
4.3 Perangkat Keras Pembangunan

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 jenis Samsung J5, sebagai barang bukti pertama yang diamankan dari terjadinya di tempat dari pelaku cybercrime untuk memecahkan proses investigasi. Smartphone Android disini sebelumnya harus sudah di beri akses rooting

4.4 Tampilan Verifikasi Android Telah Diberi Akses Rooting

Hasil verifikasi Android yang telah diberi akses rooting adalah sebagai berikut :



Gambar 9. (i)

4.5 Tabel Aktivitas User Untuk Mendapatkan Artefak Atau Data Remnant Pada Android

Tabel 2. (b)

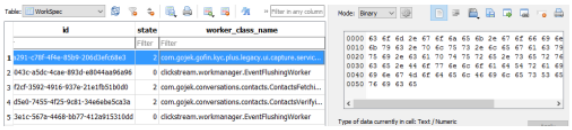
Install data	InstallPay.db
Sign up data	SignuPay.db
Sign in data	SigninPay.db
Sign out data	SignoutPay.db
Explore	ExplorePay.db
Top Up	TopupPay.db
Pay	PayPay.db
Uninstall data	UninstallPay.db

4.6 Pengujian

Pengujian yang dilakukan adalah hasil dari beberapa analisa yang disusun dalam setiap proses investigasi untuk memecahkan setiap Artefak pada bukti digital yang terdapat pada Android. Pada pengujian ini di buat tabel untuk menentukan path direktori yang sesuai dari setiap aktivitas yang telah dilakukan pelaku cybercrime pada Aplikasi GoPay tersebut. Berikut tabel path direktori hasil pengujian dari setiap aktivitas yang dilakukan pelaku cybercrime pada Aplikasi GoPay tersebut

4.7 Pengujian Hasil Analisa Menggunakan SQL DB Browser

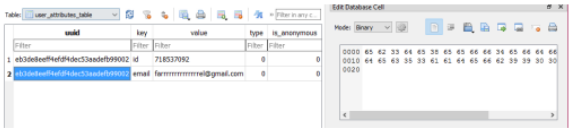
Analisa hasil pengujian terhadap aktivitas Install Data pada Aplikasi Gopay adalah sebagai berikut :



Gambar 10. (j)

Langkah pertama adalah membuka SQL DB Browser yang sudah di download melalui laptop. Langkah selanjutnya copy file.db hasil aktivitas Install Data pada GoPay ke SQL DB Browser dan di Analisa melalui mode yang ada pada aplikasi SQL DB Browser, lalu bila ingin mengganti table click table lalu nanti akan muncul banyak database yang dapat di tampilkan, seperti Dependency, Preference, SystemIdInfo, WorkName, WorkProgress, WorkSpec, WorkTag, android_metadata, dan room_master_table.

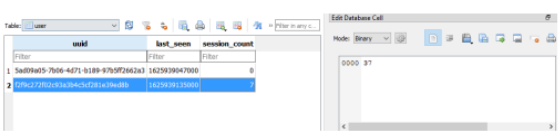
Analisa hasil pengujian terhadap aktivitas Sign Up Data pada Aplikasi Gopay adalah sebagai berikut :



Gambar 11. (k)

Langkah pertama adalah membuka SQL DB Browser yang sudah di download melalui laptop. Langkah selanjutnya copy file.db hasil aktivitas Sign Up Data pada GoPay ke SQL DB Browser dan di Analisa melalui mode yang ada pada aplikasi SQL DB Browser untuk artefak pada Sign Up pada bagian table akan menampilkan banyak database dan database yang menampilkan artefaknya adalah database user_attribute_table.

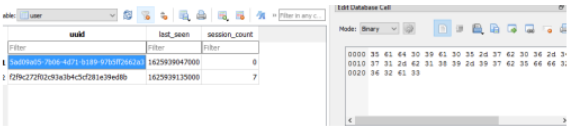
Analisa hasil pengujian terhadap aktivitas Sign In Data pada Aplikasi Gopay adalah sebagai berikut :



Gambar 12. (l)

Langkah pertama adalah membuka SQL DB Browser yang sudah di download melalui laptop. Langkah selanjutnya copy file.db hasil aktivitas Sign In Data pada GoPay ke SQL DB Browser dan di Analisa melalui mode yang ada pada aplikasi SQL DB Browser pada bagian Sign In artefak dapat dilihat pada bagian User dan disana akan terlhat data – data artefaknya.

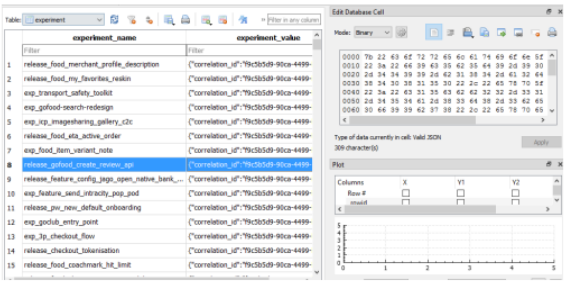
Analisa hasil pengujian terhadap aktivitas Sign Out Data pada Aplikasi Gopay adalah sebagai berikut :



Gambar 13. (m)

Langkah pertama adalah membuka SQL DB Browser yang sudah di download melalui laptop. Langkah selanjutnya copy file.db hasil aktivitas Sign Out Data pada GoPay ke SQL DB Browser dan di Analisa melalui mode yang ada pada aplikasi SQL DB Browser sama seperti bagian Sign In pada bagian Sign Out artefak berada di bagian database User.

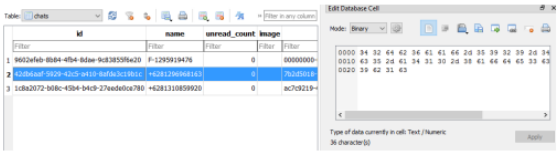
Analisa hasil pengujian terhadap aktivitas Explore Data pada Aplikasi Gopay adalah sebagai berikut :



Gambar 14. (n)

Langkah pertama adalah membuka SQL DB Browser yang sudah di download melalui laptop. Langkah selanjutnya copy file.db hasil aktivitas Explore pada GoPay ke SQL DB Browser dan di Analisa melalui mode yang ada pada aplikasi SQL DB Browser 31 untuk bagian Explore data artefak dapat di temukan pada database Experiment dan pada database tersebut dapat di temukan banyak data yang berupa artefak tersebut.

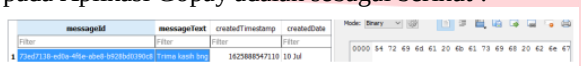
Analisa hasil pengujian terhadap aktivitas Top Up pada Aplikasi Gopay adalah sebagai berikut :



Gambar 15. (o)

Langkah pertama adalah membuka SQL DB Browser yang sudah di download melalui laptop. Langkah selanjutnya copy file.db hasil aktivitas Top Up pada GoPay ke SQL DB Browser dan di Analisa melalui mode yang ada pada aplikasi SQL DB Browser tersebut pada bagian Top Up artedfak dapat dilihat pada bagian chats, yang dimana disana dapat dlihat pembicaraan antara pengguna dan driver.

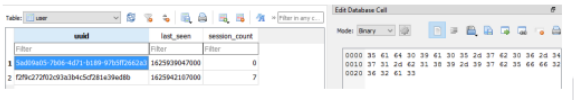
Analisa hasil pengujian terhadap aktivitas Pay pada Aplikasi Gopay adalah sebagai berikut :



Gambar 16. (p)

Langkah pertama adalah membuka SQL DB Browser yang sudah di download melalui laptop. Langkah selanjutnya copy file.db hasil aktivitas Pay pada GoPay ke SQL DB Browser dan di Analisa melalui mode yang ada pada aplikasi SQL DB Browser sama seperti bagian Top Up pada bagian Pay data artefaknya dapat dilihat pada bagian kanan di tabel MessageData.

Analisa hasil pengujian terhadap aktivitas Uninstall Data pada Aplikasi Gopay adalah sebagai berikut :



Gambar 17. (q)

Langkah pertama adalah membuka SQL DB Browser yang sudah di download melalui laptop. Langkah selanjutnya copy file.db hasil aktivitas Uninstall Data pada GoPay ke SQL DB Browser dan di Analisa melalui mode yang ada pada aplikasi SQL DB Browser pada bagian Uninstall Data artefak dapat dilihat pada bagian database user

4.8 Pengujian Integrity File.db

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

Gambar 18. (r)

Pada proses checksum SHA-1 menggunakan HashMyFiles untuk menguji integritas Artefak yang digunakan terhadap aktivitas Install Data.

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

Gambar 19. (s)

Pada proses checksum SHA-1 menggunakan HashMyFiles untuk menguji integritas Artefak yang digunakan terhadap aktivitas Sign Up Data.

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

Gambar 20. (t)

Pada proses checksum SHA-1 menggunakan HashMyFiles untuk menguji integritas Artefak yang digunakan terhadap aktivitas Sign In Data

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

Gambar 21. (u)

Pada proses checksum SHA-1 menggunakan HashMyFiles untuk menguji integritas Artefak yang digunakan terhadap aktivitas Sign Out Data

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

Gambar 22. (v)

Pada proses checksum SHA-1 menggunakan HashMyFiles untuk menguji integritas Artefak yang digunakan terhadap aktivitas Explore

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

Gambar 23. (w)

Pada proses checksum SHA-1 menggunakan HashMyFiles untuk menguji integritas

Artefak yang digunakan terhadap aktivitas Top Up Data.

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

Gambar 24. (x)

Pada proses checksum SHA-1 menggunakan HashMyFiles untuk menguji integritas Artefak yang digunakan terhadap aktivitas Pay.

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

Gambar 25. (y)

Pada proses checksum file.db tahap aktivitas Uninstall Data menggunakan tools HashMyFiles menghasilkan SHA-1 dan type Hash lainnya.

5. Kesimpulan Dan Saran

Kesimpulan dari hasil pengerjaan Proyek Akhir ini, dapat disimpulkan bahwa:

1. Untuk menguji Artefak pada aplikasi Gopay dengan metode forensik Physical.
2. Untuk membandingkan hasil Artefak dari aplikasi Gopay yang menghasilkan file .db dan untuk menguji Integrity dan akurasi.

Saran untuk penelitian lanjutan adalah :

1. Harus dapat menggunakan Aplikasi yang berbeda khususnya dompet digital lainnya, misalnya OVO, Dana, dan Shopeepay.
2. Harus lebih memperdalam dalam melakukan proses pencarian artefak, seperti dapat melihat alamat user, dan saldo user

Referensi

[1] G. B. Satrya, A. A. Nasrullah, and S. Y. Shin, “Identifying artefact on Microsoft OneDrive client to support Android forensics,” Int. J. Electron. Secur. Digit. Forensics, vol. 9, no. 3, pp. 269–291, 2017, doi: 10.1504/IJESDF.2017.085192.

[2] J. P. Lasniroha, S. Juli, I. Ismail, G. B. Satrya, U. Telkom, and F. Digital, “Mengidentifikasi Artefak Pada Aplikasi Dropbox Untuk Mendukung Forensic Android Identifying Artefact on Application Dropbox To Support Android,” vol. 6, no. 2, pp. 3293–3304, 2020.

[3] S. K. Saad, R. Umar, and A. Fadlil, “Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIST,” Semin. Nas. Din. Inform., pp. 119– 123, 2020.

[4] O. Riandy et al., “Analisis Forensik Recovery Dengan Keamanan,” no. 12.

[5] A. Hutagalung, “**済無**No Title No Title No Title,” Angew. Chemie Int. Ed. 6(11), 951–952., pp. 5–24, 1967.

[6] W. N. Hamzah, F. Yudha, S. Kom, and M. Kom, “5 Yogyakarta 55501- Indonesia Telp. (0274) 895287 ext. 122, Faks.” [Online]. Available: https://twrp.me/Devices/.

[7] M. S. Asyaky, “Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android,” J. Penelit. Tek. Inform., vol. Vol. 3 No, no. 1, pp. 220–231, 2019.

[8] 13523267 Waldy Nur Hamzah, “ANALISIS DAN PERANCANGAN APLIKASI FORENSIC IMAGING PADA PONSEL ANDROID DENGAN MEMANFAATKAN CUSTOM RECOVERY,” Jalan Kaliurang Km, vol. 14, no. 0274, pp. 895007– 148, Oct. 2018, Accessed: Aug. 12, 2021. [Online]. Available: https://dspace.uii.ac.id/handle/123456789/13348.