FORENSIK PADA APLIKASI GOOGLE DRIVE DENGAN METODE FORENSIK NIST

Disusun Oleh:

N a m a	: Syafiq Irfan Isnaindar
NIM	: 18523134

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2022

HALAMAN PENGESAHAN DOSEN PEMBIMBING

FORENSIK PADA APLIKASI GOOGLE DRIVE DENGAN METODE FORENSIK NIST

TUGAS AKHIR

Disusun Oleh:

N a m a : Syafiq Irfan Isnaindar

NIM : 18523134

Yogyakarta, Oktober 2022

Pembimbing,

(Erika Ramadhani, S.T., M.Eng.)

HALAMAN PENGESAHAN DOSEN PENGUJI

FORENSIK PADA APLIKASI GOOGLE DRIVE DENGAN METODE FORENSIK NIST

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika – Program Sarjana di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, Oktober 2022

Tim Penguji

Erika Ramadhani, S.T., M.Eng. _____

Anggota 1

Ahmad Luthfi, S.Kom., M.Kom. _____

Anggota 2

Mukhammad Andri Setiawan, S.T., M.Sc., Ph.D. _____

Mengetahui,

Ketua Program Studi Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia

(Dhomas Hatta Fudholi, S.T., M.Eng, Ph.D)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Syafiq Irfan Isnaindar

NIM : 18523134

Tugas akhir dengan judul:

FORENSIK PADA APLIKASI GOOLE DRIVE DENGAN METODE FORENSIK NIST

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung risiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, Oktober 2022

(Syafiq Irfan Isnaindar)

HALAMAN PERSEMBAHAN

Assalamualaikum Warahmatullahi Wabarakatuh puja dan puji syukur kehadirat pada Allah SWT yang telah memberikan rahmat dan hidayat-Nya sehingga saya bisa menyelesaikan skripsi ini dengan lancar. Terima kasih penulis persembahkan kepada :

1. Orang tua penulis bapak Dwi Taryono, S.Pd dan ibu Tita Rosita, S.Pd yang telah memberikan doa dan semangatnya serta adik saya Rafif Dzaki Muhammad yang memberikan masukan pada saya.
2. Ibu Erika Ramadhani, S.T., M.Eng. dosen pembimbing saya yang telah membantu saya dalam Menyusun skripsi ini sehingga dapat terselesaikan.
3. Rekan saya Riza dan Dany aziz yang membantu saya dalam menyusun dan memberikan dukungan serta informasinya selama menyusun skripsi.
4. Rekan-rekan grup “Hujan Tak Berhenti” yang memberikan informasinya sehingga dapat membantu saya dalam menyusun skripsi dan segala informasi yang diperlukan.

HALAMAN MOTO

"Hatiku tenang karena mengetahui bahwa apa yang melewatkanku tidak akan pernah menjadi takdirku, dan apa yang ditakdirkan untukku tidak akan pernah melewatkanku

-Umar bin Khatab-

KATA PENGANTAR

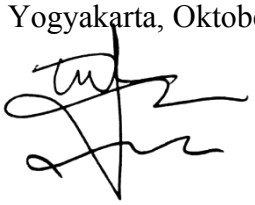
Segala puji dan syukur kehadirat Allah SWT, yang telah melimpahkan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi yang **berjudul "FORENSIK PADA APLIKASI GOOLE DRIVE DENGAN METODE FORENSIK NIST (STUDI KASUS : PEMANFAATAN GOOGLE DRIVE SEBAGAI PENYIMPANAN DOKUMEN KEJAHATAN".**

Terima kasih penulis ucapkan kepada orang tua penulis, adik, dosen pembimbing dan teman-teman penulis yang selalu memberikan semangat dan masukan kepada penulis sehingga dapat menyelesaikan skripsi ini.

Skripsi disusun sebagai syarat untuk memenuhi menyelesaikan Program Studi Sarjana Jurusan Informatika Fakultas Teknologi Industri Universitas Islam Indonesia. Dengan adanya dukungan dari berbagai pihak, penulis berterima kasih sehingga dapat menyelesaikan skripsi ini. Penulis berharap skripsi yang ditulis bisa memberikan manfaat kepada pembaca sekalian terkhusus bagi pembaca yang berminat dengan bidang yang sama dengan penulis susun.

Seperti kata pepatah "Tak ada gading yang tak retak", penulis menyadari skripsi yang ditulis masih jauh dari kata sempurna, sehingga penulis menerima segala bentuk kritik dan saran yang membangun skripsi ini menjadi lebih baik.

Yogyakarta, Oktober 2022



(Syafiq Irfan Isnaindar)

SARI

Seiring dengan perkembangan zaman, media penyimpanan di sekitar kita terus berkembang mengikuti perkembangan teknologi dan tren yang ada di masyarakat. Jika pada zaman dahulu kita memerlukan penyimpanan berwujud fisik seperti harddisk, CD maupun disket, kini penyimpanan melalui media *cloud* menjadi yang populer di masyarakat. Pengguna cukup memerlukan jaringan internet guna mengakses dan menyimpan file mereka pada *cloud* storage. Namun, menyimpan file pada *cloud* storage menimbulkan risiko kejahatan seperti pencurian data mengingat file yang disimpan dalam jaringan *cloud* sehingga perlu dilakukan tindakan digital forensik untuk mencegah kejahatan pada *cloud* storage dan menyusun tindakan pencegahan di masa mendatang. Salah satu metode yang digunakan dalam digital forensik adalah forensik NIST.

Kata kunci: penyimpanan, forensik *cloud*, Google Drive, NIST

GLOSARIUM

Glosarium memuat daftar kata tertentu yang digunakan dalam laporan dan membutuhkan penjelasan, misalnya kata serapan yang belum lazim digunakan. Urutkan sesuai abjad. Contoh penulisannya seperti di bawah ini:

Forensik	ilmu penerapan sains dan pengetahuan dalam penegakan hukum.
Cloud	istilah penyebutan untuk kumpulan server yang digunakan menyimpan data.
Metode	langkah atau jalan kerja untuk mencapai sesuatu
Tools	istilah dari bahasa inggris untuk menyebut alat dalam bidang informasi teknologi.
Pakar	ahli dalam bidang tertentu.
Cybercrime	istilah untuk menyebut tindakan kejahatan dalam dunia digital.
Hacker	seseorang yang menerobos situs atau jaringan computer dan internet
Malware	perangkat lunak yang buat untuk membobol jaringan, server, computer secara illegal.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Media penyimpanan yang dulu memiliki kapasitas terbatas dengan ukuran media besar, kini seiring dengan perkembangan teknologi hadir dengan ukuran media yang kecil dengan kapasitas yang jauh lebih besar. Namun, media penyimpanan kini hadir dengan bentuk non fisik berupa , dimana data milik pengguna disimpan di dalam server. Umumnya pengguna akan menyimpan data atau file mereka pada perangkat penyimpanan seperti CD, Flashdrive, Hardisk maupun pada penyimpanan internal pada komputer atau laptop.

Seiring dengan perkembangan zaman dan kebutuhan para pengguna yang meningkat mendorong para pakar merancang sebuah penyimpanan yang saat ini dikenal sebagai *cloud computing*. Kehadiran penyimpanan *cloud* memberikan alternatif penyimpanan bagi pengguna yang mana akses data dapat dilakukan dimana saja dan kapan saja dengan bermodalkan perangkat untuk mengakes dan jaringan internet tanpa harus membawa perangkat penyimpanan fisik.

Ide mengenai penyimpanan *cloud* sendiri sudah tercetus sejak lama pada tahun 1960 dimana pada saat itu John McCarthy, pakar komputasi dan intelegasi buatan dari MIT mengatakan bahwa kedepannya penyimpanan *cloud* akan menjadi infrastruktur public layaknya listrik dan telepon.

Cloud computing sendiri dikenalkan secara komersil oleh AT&T pada tahun 1994. Pada tahun 2006 Amazon meluncurkan Amazon Web Service S3 yang memulai tren penyimpanan *cloud computing*. *Cloud computing* merupakan model komputasi di mana pemrosesan komputer, penyimpanan, perangkat lunak, dan layanan lainnya disediakan sebagai kumpulan sumber daya virtual melalui jaringan, terutama Internet. "*Cloud*" sumber daya komputasi ini dapat diakses sesuai kebutuhan dari perangkat dan lokasi mana pun yang terhubung(Laudon & Laudon, 2015).

Cloud computing sendiri secara umum terdiri dari beberapa jenis yang mana setiap jenis memiliki layanan dan kegunaan yang berbeda, adapun jenis-jenis *cloud computing* diantaranya adalah :

1. SaaS (Software as a Service)

   Jenis layanan ini memungkinkan data diakses dari perangkat apapun dengan koneksi internet dan browser web dimana pengguna bertanggung jawab atas file dan data miliknya karena ketersediaan maupun reabilitas ditanggung oleh penyedia layanan.
2. PaaS (Platform as a Service)

   Jenis layanan ini memungkinkan pengguna ikut mengembangkan sendiri layanan yang mereka sewa sesuai yang dibutuhkan untuk membangun *cloud computing*.
3. IaaS (Infrastructure as a Service)

   Jenis layanan yang mana penyedia menyediakan resource *cloud* seperti server, storage, jaringan, dll. Pengguna sendiri tidak perlu membeli computer atau perangkat pendukung untuk membangun server maupun pemeliharaan.

Penyimpananan *cloud* sendiri mengubah kebiasan orang-orang yang mana sebelumnya sedikit kesulitan menyimpan file sehingga perlu membawa banyak perangkat penyimpanan macam flashdrive, CD maupun Harddisk sehingga kehadiran *cloud computing* memberikan kemudahan. Beberapa layanan penyimpanan *cloud* yang secara umum banyak digunakan antara lain Dropbox, Oracle, Amazon Web Services, Google Drive, dsb. Berkaitan dengan judul topik yang diambil akan difokuskan pada Google Drive. Google Drive sendiri tersedia dalam bentuk website, desktop serta aplikasi mobile.

Google Drive sendiri diluncurkan oleh Google pada tanggal 24 April 2012 dimana Google Drive memungkinkan penggunanya untuk menyimpan data di server mereka, mensinkronisasi data dengan perangkat lain, dan saling berbagi berkas dengan pengguna lainnya. Pengguna Google Drive sendiri dapat mengedit dokumen yang dimiliki karena platform ini terhubung dengan produk Google lainnya seperti Google docs, Google form, Spreadsheet, dll. Selain itu Google Drive juga menyediakan kapasitas penyimpanan 15 GB untuk versi gratisnya. Tercatat pada Mei 2017 terdapat 2 triliun file yang disimpan dalam layanan tersebut dan 1 miliar pengguna yang memakai layanan ini yang tercatat pada Juli 2018 memperlihatkan bahwa banyak peminat pengguna produk Google tersebut. Namun di balik banyaknya pengguna dan data yang tersimpan tersebut menimbulkan risiko besar mengenai jaminan kemanan data pribadi dan file milik para pengguna tersebut sehingga diperlukan keamanan pada sistem layanan tersebut. Hal ini juga yang mendorong penelitian ini dilakukan

guna mengetahui prosedur dalam melakukan digital forensik pada aplikasi Google Drive mengingat platform tersebut memiliki pengguna dan data yang tersimpan dengan jumlah yang banyak.

Permasalahan pada keamanan tersebut menimbulkan risiko besar seperti kejahatan yang dapat mengintai pengguna nya. Hal ini terjadi karena adanya pengalihan data ke penyedia komputasi awan menimbulkan risiko terhadap integritas sistem informasi karena; ketergantungan pemasok, hilangnya kontrol data, kurangnya enkripsi data dan komunikasi, dan kerentanan yang mengakibatkan pencurian akun dan akses tidak sah (Belbergui , Elkamoun & Hilal, 2017). Perlu adanya tindakan pencegahan guna menghindari tindak kejahatan tersebut melalui digital forensik, dimana digital forensik akan bekerja untuk menelusuri potensi dan tindakan kejahatan dalam dunia digital. Sehingga perlu adanya audit dari pihak ketiga dalam hal ini penyedia layanan *cloud computing* itu sendiri. Audit pihak ketiga di *cloud* digunakan untuk memastikan keamanan dan integritas data pihak ketiga yang dipercaya untuk menyelesaikan konflik antara penyedia layanan *cloud* dan klien (Reddy & Balaraju, 2018).

Salah satu kasus kejahatan yang memanfaatkan Google Drive adalah kasus yang menimpa Sky Lakes Medical Center di Oregon, St. Lawrence Health System di New York, dan Dickingson County Healthcare System di Michigan dan Wisconsin yang terkena serangan Ryuk Ransomware dengan memanfaatkan Google Drive. Atas peristiwa tersebut membuat terganggunya proses pelayanan pasien sehingga memaksa mereka melakukan pelayanan secara manual karena akses terhadap sistem mereka menjadi terganggu. Ryuk Ransomware bekerja dengan melakukan phising melalui email yang berisi link Google Drive dimana apabila setelah dibuka dan diaktifkan maka link tersebut akan mengakses computer korban.

Dalam mencegah tindak kejahatan pada area *cloud computing* perlu dilakukan tindakan digital forensik. Digital forensik perlu dilakukan untuk mengamankan dan menganalisa bukti digital secara legal dari kejahatan dunia maya dalam area *cloud computing*. Selain itu, tindakan ini membantu mendeteksi adanya kemungkinan celah kejahatan lain sehingga bisa diantisipasi oleh para ahli. *Coud computing* sendiri mengingat digunakan sebagai lokasi penyimpanan data oleh pengguna memunculkan risiko yang lebih pada keamanan data para pengguna tersebut, sehingga dalam pengembangan *cloud computing* sendiri para pakar dan ahli melakukan kegiatan digital forensik untuk mencegah tindakan kejahatan digital yang terjadi pada area *cloud computing*. Kegiatan yang dimaksud untuk mengatasi permasalahan ini dikenal sebagai *cloud* forensik dimana kegaiatan tersebut berfokus pada penyelidikan dan pemulihan pada data yang terdapat di *cloud computing*.

Peneliti melihat situasi yang sedang terjadi memang diperlukan sebuah tindakan forensik untuk mencari akar permasalahan di atas dan menyusun tindakan pencegahan kedepannya untuk mencegah kejahatan pada *cloud computing* dapat terulang. Forensik pada sistem siber sendiri perlu dilakukan dengan tujuan untuk mengamankan dan menganalisa barang bukti digital, dan memperoleh temuan dari pelanggaran atau kejahatan dalam lingkup siber yang dapat dijadikan bukti dalam menegakan hukum yang berlaku.

Dalam pelaksanaannya, tindakan digital forensik melalui beberapa tahapan dengan menggunakan metode yang akan digunakan. Penggunaan metode yang sesuai kaidah akan mecatatkan setiap langkah dalam proses forensik sehingga meminimalisir proses atau tahapan yang terlewatkan sekaligus menguji apakah metode tersebut cocok dalam penelitian yang sedang dilakukan. Berbagai metode sendiri telah disusun oleh pakar dimana setiap metode memiliki tahapan yang berbeda satu sama lain. Salah satu metode yang digunakan dalam lingkup digital forensik adalah NIST.

National Institute of Standards and Technology (NIST) sendiri merupakan laboratorium ilmu fisika, dan lembaga non-regulasi pada departemen perdagangan Amerika Serikat (*United States Department of Commerce*) yang bertanggung jawab untuk mengembangkan standar dan pedoman termasuk persyaratan minimum termasuk untuk menyediakan keamanan informasi dan teknologi siber serta metode terbaik seperti cara melindungi data secara aman dan memadai. NIST juga menjadi salah satu metode dan pedoman para pakar dalam melakukan kegiatan digital forensik *cloud*. Metode forensik NIST sendiri menawarkan standar tentang langkah-langkah keamanan apa yang harus dilakukan dan diterapkan untuk memastikan data tetap aman. Melalui standar yang digariskan NIST akan menghasilkan tingkat keseragaman dalam hal pengamanan lingkup siber.

1.2 Tujuan Penelitian

a. Melakukan proses forensik dengan metode forensik NIST pada Google Drive.
b. Menganalisis proses forensik pada aplikasi Google Drive dengan metode forensik NIST.

1.3 Rumusan Masalah

a. Bagaimana cara melakukan forensik aplikasi Google Drive dengan menggunakan metode forensik NIST ?
b. Apakah metode forensik NIST dapat mengumpulkan barang bukti hasil penyelidikan ?

1.4 Batasan Masalah

a. Penelitian menggunakan Operating System Windows 10 Single Home Language.
b. Penelitian menggunakan Google Drive desktop versi 58.0.3.0.
c. Pembahasan langkah forensik dengan metode forensik NIST berkaitan dengan penelitian yang dilakukan.
d. Barang bukti dari hasil forensik berdasarkan 5W+1H.

1.5 Manfaat Penelitian

a. Menjadikan hasil penelitian sebagai referensi penelitian lain di bidang forensika *cloud computing*.
b. Membantu penyidik dalam mengungkap kejahatan *cloud computing*.
c. Menambah wawasan bagi pembaca dalam bidang penanganan kejahatan digital.

BAB II
TEORI DAN TINJAUAN PUSTAKA

2.1 Pengertian dan Peran Forensik

Secara umum forensik berasal dari bahasa Latin *forensis* yang dapat diartikan "debat". Forensik sendiri bertujuan untuk membantu proses penegakan hukum dan keadilan dengan melalui penerapan ilmu sains. Kekuatan forensik sendiri memungkinkan menganalisa dan mendapatkan kembali fakta dari kejadian dan lingkungan sehingga tidak mudah untuk menemukan fakta karena fakta itu sendiri tersembunyi (Sulianta, 2013).

Forensik sendiri mencakup berbagai disiplin ilmu seperti fisika forensik, kimia forensik, kedokteran forensik, computer forensik, psikologi forensik, dll. Forensik sendiri merupakan penerapan dari berbagai ilmu pengetahuan untuk memecahkan permasalahan dalam sebuah hukum yang mana terkait dengan tindak pidana. Ilmu forensik sendiri selalu mengalami pembaharuan mengingat ilmu yang membidanginya selalu mengalami kemajuan, walaupun begitu pembaharuan tersebut memberikan kemajuan bagi ilmu forensik sendiri. Temuan yang didapatkan dalam proses forensik dapat digunakan sebagai bukti pada saat proses persidangan pada perkara tindak kejahatan. Tahapan forensik dilakukan dengan sebagai berikut (Maramis, 2015) :

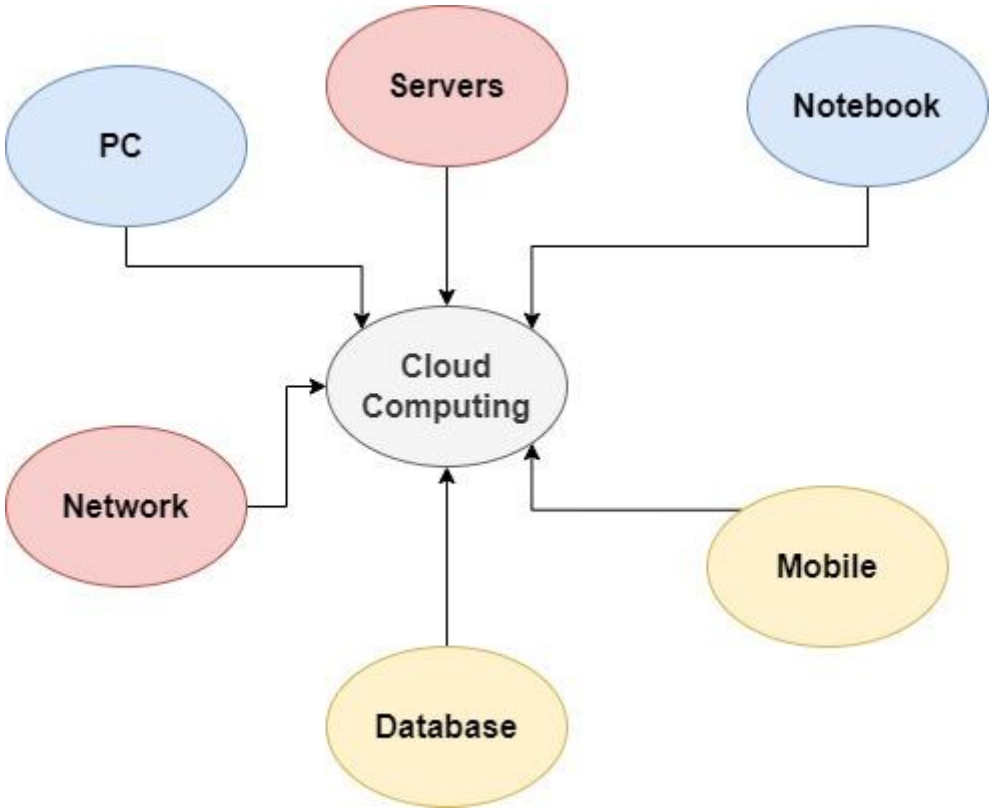
a. Pengumpulan barang bukti.
b. Pemeliharaan barang bukti yang telah didapat.
c. Analisis pada barang bukti yang telah didapat.
d. Presentasi dan penulisan laporan hasil analisis yang didapat.

2.2 Pengertian dan ancaman pada *Cloud computing*

Cloud computing jika diterjemahkan kedalam bahasa Indonesia diartikan sebagai "komputasi awan". Secara umum sendiri *cloud computing* dapat diartikan sebagai kumpulan server yang digunakan menyimpan data. *Cloud computing* atau komputasi awan sendiri dapat didefinisikan sebagai gaya komputasi baru di mana sumber daya yang dapat diskalakan secara dinamis dan seringkali sumber daya tervirtualisasi yang tersedia sebagai layanan melalui internet(Furht & Escalante, 2008).

Melalui *cloud computing* pengguna dapat menggunakan berbagai perangkat untuk mengakses media penyimpanan berbasis *cloud* yang disediakan penyedia layanan seperti

laptop, *smarthphone*, PC, dll sehingga memberikan keuntungan seperti hemat biaya, ketersediaan yang tinggi dan skalabilitas yang mudah (Furht & Escalante, 2008).



Gambar 2. 1 Bagan *Cloud computing*

Sistem dapat dikatakan sebuah *cloud computing* apabila memenuhi lima karakteristik yang diperlukan, sehingga jika belum memenuhi belum bisa dikatakan sebagai *cloud computing*. Adapun berdasarkan NIST sendiri, terdapat lima karakteristik yang diperlukan sistem sehingga sistem tersebut dapat dikatakan sebagi *cloud computing* antara lain (Ivan et al., 2012) :

a) Resource Polling

Penyedia layanan dapat menyediakan sumber daya yang dibutuhkan oleh pelanggan berupa fisik atau virtual seperti *Storage*, CPU, *Network Bandwidth*, dll.

b) Broad Network Access

Kemampuan penyedia layanan untuk memberikan akses di berbagai perangkat milik pelanggan seperti *smarthphone*, laptop, PC, dll.

c) Measured Service

Penyedia layanan dapat menyediakan layanan yang dapat memonitor layanan secara otomatis sehingga dapat melihat berapa sumber daya komputasi yang telah dipakai, seperti: *bandwidth , storage, processing*, dll.

d) Rapid Elasticity

Kemampuan penyedia layanan untuk memberikan kemudahan pelanggan dalam menentukan dengan bebas kapasitas *cloud* sesuai yang dibutuhkan.

e) Self Service

Pelanggan dapat mengkonfigurasikan layanan secara mandiri tanpa perlu interaksi dengan penyedia layanan dan harus tersedia saat itu juga secara otomatis.

Data dari pengguna layanan *cloud computing* sendiri akan disimpan di dalam server sehingga muncul risiko keamanan data tersebut. (T.Chou, 2013) dalam penjelasannya mendefinisikan ancaman keamanan terhadap layanan *cloud computing* berdasarkan 3 pendekatan, yaitu: penyimpangan penggunaan sumber daya dalam konteks *cloud computing*, penyalahgunaan data, dan kejahatan terhadap data di *cloud*.

No	Ancaman
1	Lemahnya otentikasi sistem dapat membuat kerentanan keamanan data pengguna
2	Penggunaan kata sandi yang lemah dapat membuka akses kejahatan dari pihak tidak bertanggung jawab
3	Pencurian akun oleh orang tidak bertanggung jawab berisiko pada pencurian data diri, pelacakan aktivitas,maupun pencurian file pada *cloud computing*
4	*Cloud computing* pada umum nya dapat melakukan berbagi akses dengan pengguna lain, sehingga rentan terhadap akses dari pihak tidak bertanggung jawab

Tabel 2. 1 Ancaman pada *cloud computing*

2.3 Pengertian dan Peran *Cloud* Forensik

Secara umum *Cloud* Forensik sendiri diartikan sebagai cabang ilmu Digital Forensik dilingkungan *Cloud computing*. Kesulitan mendefinisikan forensik awan terletak pada kenyataan bahwa tidak ada definisi *cloud* forensik atau forensik digital yang diterima secara universal (Ruan et al., 2013). Namun berdasarkan NIST *Cloud computing Reference Architecture*, *cloud* forensik adalah aplikasi ilmu forensik digital di lingkungan *cloud* forensik. Secara teknis, ini terdiri dari pendekatan forensik hibrida (misalnya, jarak jauh, virtual, jaringan, langsung, skala besar, klien tipis, klien tebal) menuju generasi bukti digital.

Secara organisasi, ini melibatkan interaksi antara aktor *cloud* (yaitu, penyedia *cloud*, konsumen *cloud*, *broker cloud, operator cloud, auditor cloud*) untuk tujuan memfasilitasi investigasi internal dan eksternal. Secara hukum ini sering menyiratkan situasi multi-yurisdiksi dan multi-penyewa(Liu et al., 2011).

Secara analogi sendiri *cloud* forensik merupakan bagian dari forensik teknologi informasi yang mana menangani kasus kejahatan dunia digital dalam lingkup *cloud computing*. Pekerjaan di lingkup forensik teknologi informasi merupakan pendukung stabilitas dalam berbagai bidang. Berbagai kasus yang terpecahkan memberikan sumbangsih tidak hanya secara implisit kepada pihak yang bersengketa namun juga explicit bagi berbagai pihak lain, sebut saja efek ketakutan bagi penjahat dunia maya (Manuhutu et al., 2021).

Pendapat lain mengenai penjelasan *cloud* forensik adalah model untuk memungkinkan akses jaringan sesuai permintaan yang nyaman ke kumpulan sumber daya yang dapat dikonfigurasi bersama (misalnya, jaringan, server, penyimpanan, aplikasi, dan layanan) yang dapat dengan cepat disediakan dan dirilis dengan upaya manajemen minimal atau penyedia layanan interaksi (Mell & Grace, 2010).

Cloud Forensik secara disiplin ilmu merupakan turunan forensik dalam bidang teknologi informasi memiliki tujuan antara lain (Manuhutu et al., 2021):

a) Menganalisis sistem digital seseorang yang didakwa melakukan tindak pindana tertentu.
b) Mendapatkan fakta yang bersifat objektif pada pelanggaran kemanan sistem informasi.
c) Fakta temuan yang telah diverifikasi akan menjadi bukti dalam proses hukum.
d) Mengamankan serta menganalisis bukti dalam bentuk digital.

Mengingat penyimpanan *cloud* yang mengandalkan koneksi internet untuk akses data serta data pengguna yang disimpan ke dalam server, hal ini menimbulkan ancaman dan serangan pada penyimpanan *cloud* seperti kebocoran data, pencurian data pribadi, kerentanan sistem, hilang dan kerusakan pada data yang tersimpan sehingga menimbulkan tindakan kejahatan dari pihak yang tidak bertanggung jawab. Maka dari itu dibutuhkan *cloud* forensik guna mencegah segala tindakan dan aktivitas yang berisiko mengancam data pengguna yang tersimpan dalam penyimpanan *cloud*. *Cloud* forensik sendiri merupakan komponen terpenting dalam keamanan *cloud computing*. Pakar dan peneliti akan menelusuri bagaimana proses kejahatan tersebut bisa terjadi dan langkah apa yang diperlukan guna mencegah kejahatan *cloud computing* terulang kembali.

2.4 NIST dan Metode Forensik

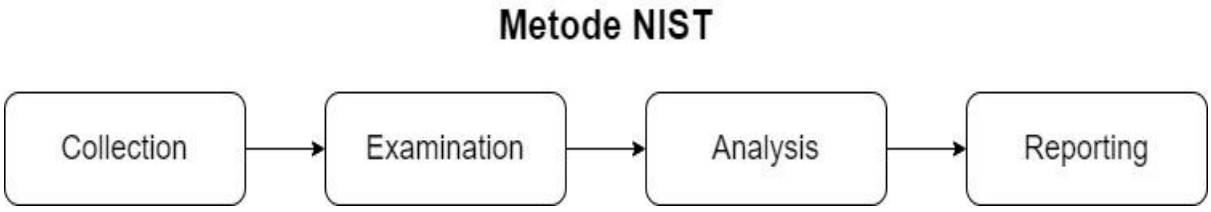
National Institute of Standards and Technology (NIST) atau yang dulunya dikenal sebagai *National Bureau of Standards* (NBS) sendiri didirikan pada 1 Maret 1901 merupakan badan non regulator yang didirikan oleh US Department of Commerce dengan maksud untuk untuk mendorong dan membuat pengukuran, standar, dan teknologi untuk meningkatkan produktivitas, mendukung perdangangan, dan memperbaiki kaualitas hidup semua orang termasuk pada bidang termasuk teknologi IT. NIST sendiri telah melakukan banyak kegiatan penelitian yang berkaitan dengan ilmu forensik. Tujuan dari kegiatan ini adalah untuk meningkatkan akurasi, keandalan, dan validitas ilmiah metode dan praktik ilmu forensik melalui kemajuan dalam pengukuran dan infrastruktur standarnya (NIST, 2020). NIST juga melakukan kegiatan program dalam laboratoriumnya dalam berbagai bidang guna mendorong berbagai inovasi.

NO	Program Laboratorium NIST
1	Sains dan teknologi dalam skala nano
2	Teknik
3	Teknologi informasi
4	Penelitian neutron
5	Pengukuran material
6	Pengukuran fisik

Tabel 2. 2 Informasi program kegiatan laboratorium NIST

Sumber : (Standarku, 2021)

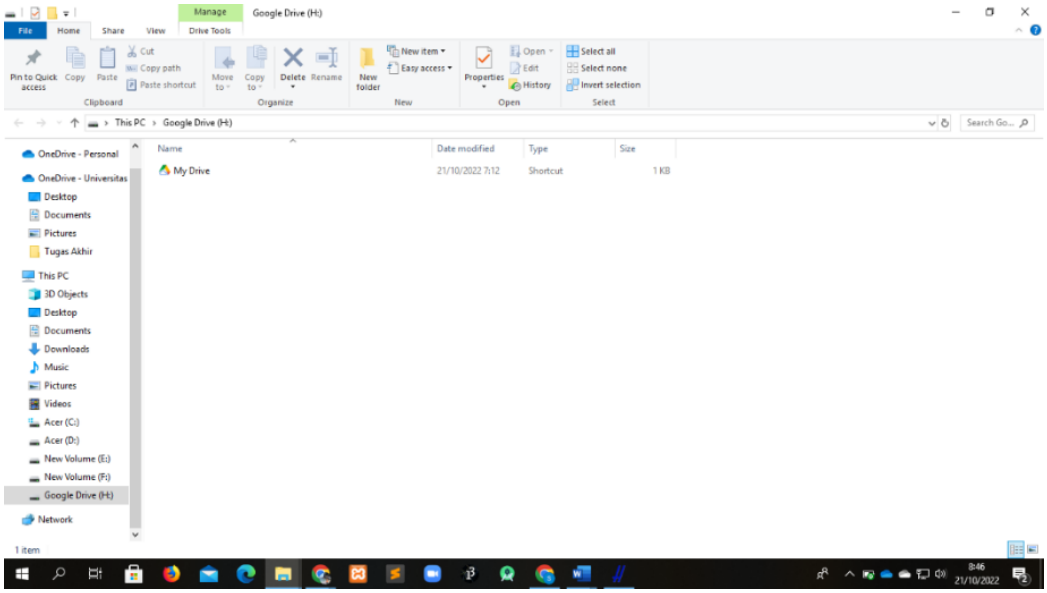
Metode forensik NIST sendiri dalam penerapan digital forensik sendiri secara metode melalui empat tahapan yaitu *Collection, Examination, Analysis dan Reporting*. Masing-masing tahapan sendiri memiliki aktivitas tersendiri dalam proses investigasi digital forensik seperti *Collection* merupakan proses pengumpulan dan dokumentasi barang bukti, *Examination* proses akuisisi data supaya barang bukti tidak berubah, lalu *Analysis* tahapan pemeriksaan barang bukti yang ditemukan, terakhir *Reporting* merupakan tahapan penulisan laporan hasil investigasi.



Gambar 2.2 Bagan alur metode forensik NIST

2.5 Google Drive dan Risiko Keamanan

Google drive merupakan salah satu *cloud* storage yang cukup popular di dunia yang merupakan layanan *cloud* dari Google. Pengguna Google drive dapat menyimpan berbagai file kedalam layanan tersebut seperti foto,dokumen, video, dll. Google Drive sendiri tersedia dalam versi web, mobile phone dan desktop. Google Drive sendiri tersedia dengan kapasitas 15 GB untuk versi gratis, namun apabila pengguna masih merasa kurang dapat menambah kapasitas penyimpanan yang tersedia sebanyak 100 GB, 200 GB hingga 2 TB dengan tarif yang telah disesuaikan.



Gambar 2.3 Tampilan Google Drive Desktop yang telah disinkronkan

Setelah login kedalam Google Drive pengguna dapat langsung menggunakannya. Pengguna Google Drive sendiri dapat berbagi file dengan orang lain tanpa harus mengirimkan file tersebut serta dapat membuat folder yang bisa diakses dengan orang lain. Google Drive juga terhubung dengan layanan Google lainnya seperti, Google docs, Google Sheets, Google Form dan Google Slide. Berkat hal tersebut pengelolaan file dan data dalam Google Drive menjadi lebih efektif. Dibalik keunggulan yang ditawarkan Google Drive memiliki risiko

keamanan bagi penggunanya, menurut makeusof.com berikut alas an mengapa Google Drive memiliki risiko keamanan.

No	Risiko Keamanan
1	Google Drive merupakan target utama para *Hacker* atau peretas
2	Google memiliki riwayat peretasan
3	Google Drive kerap dijadikan media penipuan
4	Perubahan kebijakan privasi tanpa pemberitahuan
5	Google kerap membagikan data dengan pemerintah

Tabel 2. 3 Risiko keamanan pada Google Drive

Sumber : (Baterna, 2022)

Mengingat Google merupakan perusahaan besar, risiko peretasan oleh pihak yang tidak bertanggung jawab menjadi lebih besar. Google sendiri diketahui menyimpan cukup banyak data informasi pribadi pengguna mereka seperti akes email, file, dokumen bahkan pengguna kerap menyimpan informasi dan file rahasia dalam Google Drive sehingga rentan menjadi target peretasan.

Ancaman lain dalam penggunaan *cloud computing* adalah penipuan dengan menggunakan platform tersebut yang mana Google Drive juga memiliki risiko terdampak ancaman tersebut. Secara umum bentuk penipuan tersebut dapat berupa aktivitas berikut :

No	Bentuk Penipuan
1	Memberikan komentar berupa link *phishing*.
2	Menempatkan malware pada Google Drive.
3	Membuat situs Google Drive palsu.

Tabel 2. 4 Bentuk penipuan pada Google Drive

Sumber : (Baterna, 2022)

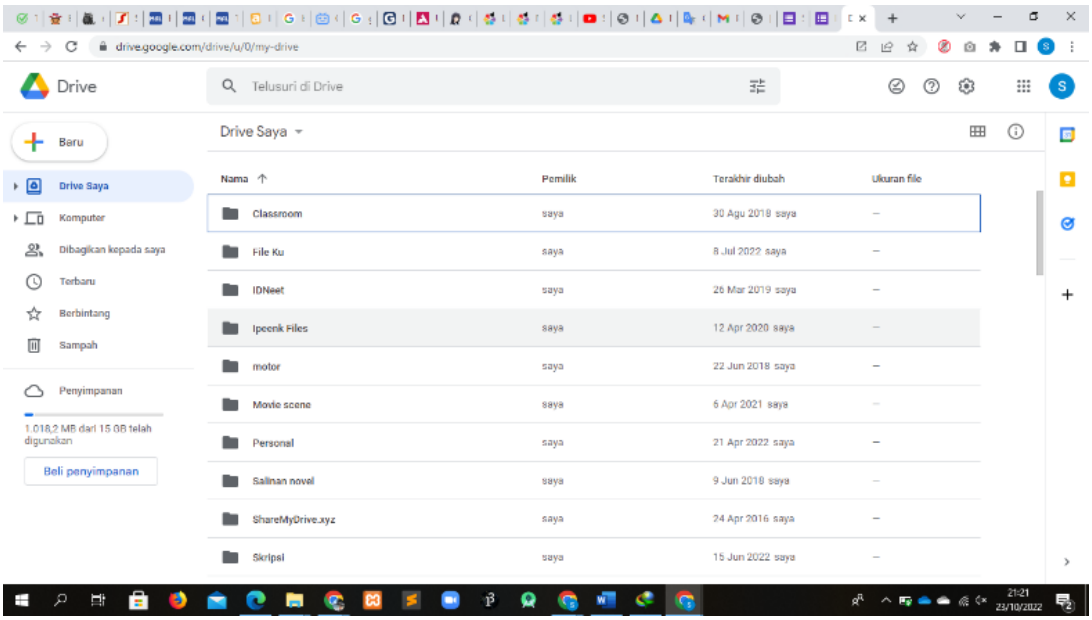
Para penipu dapat memanfaatkan layanan dari Google seperti Google Spreadsheet, Google Docs maupun lainnya yang dapat menggunakan fitur sharing dengan pengguna lainnya sehingga pelaku dapat berpura-pura menjadi orang lain dan melakukan tindak kejahatan dengan meninggalkan link *phishing* pada file tersebut sehingga pengguna lain yang tidak tahu bisa mengklik link tersebut.

Para penipu juga dapat melakukan penipuan dengan membuat situs palsu dengan meniru tampilan dari Google Drive itu sendiri. Pengguna yang tidak sadar dapat mengakses situs palsu tersebut dan kemungkinan mengunggah file mereka ke situs tersebut, sehingga pengguna sendiri juga perlu memerhatikan secara detail situs Google Drive sendiri.

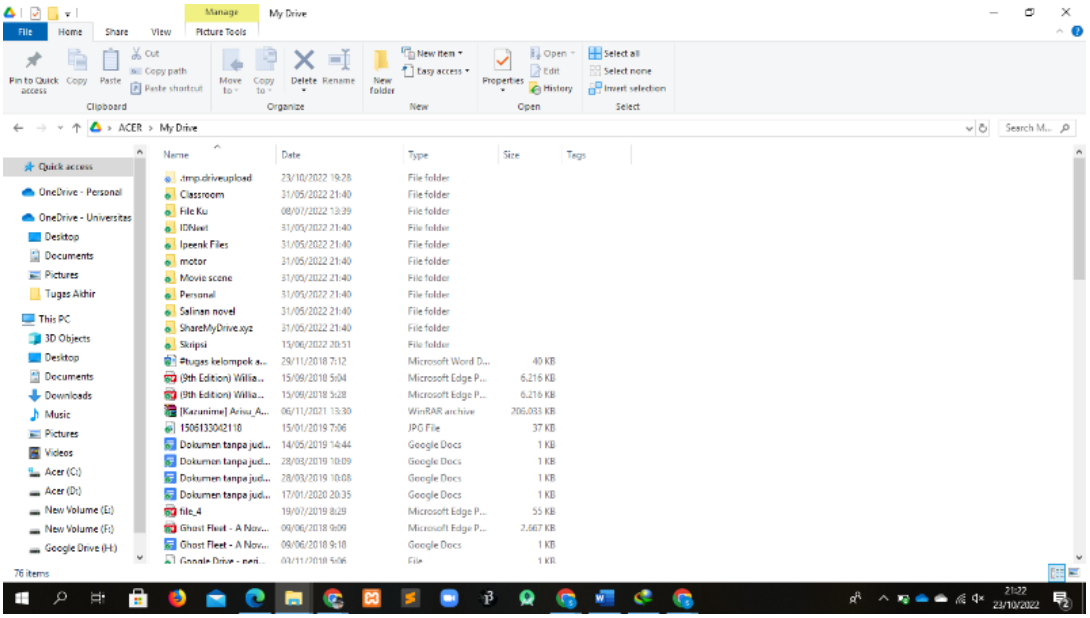
Google Drive sendiri memungkinkan penggunannya untuk mengakses dari berbagai perangkat kapan saja dan dimana saja sehingga dimanfaatkan penipu untuk menanamkan malware dengan memanfaatkan fitur sharing sehingga pengguna yang tidak menaruh curiga dapat mengunduh malware tersebut, meski Google sendiri menyediakan pemindaian virus, namun fitur tersebut terkadang kurang menjangkau file unduhan dengan ukuran besar.

Kebijakan privasi juga mengancam privasi para penggunannya mengingat Google juga dapat mengontrol akses penggunanya meskipun harus melalui persetujuan pengguna sendiri ditambah Google juga perlu mematuhi aturan yang telah ditetapkan oleh pemerintah menambah keraguan transparasi kemanan layanan (Baterna, 2022).

Google Drive yang digunakan untuk penelitian sendiri merupakan versi desktop dengan versi 58.0.3.0. Dalam versi desktop, pengguna dapat menyinkronkan Google Drive yang terdapat di *cloud* dengan perangkat laptop atau computer pengguna sendiri.



Gambar 2.5 Tampilan Google Drive versi web.



Gambar 2.6 Tampilan Google Drive setelah disinkronkan

2.6 Penelitian Terkait Dengan Metode Forensik NIST

NO	Tahun	Penulis	Bahasan	Metode	Hasil
1	2020	Saad, S., K., Umar, R., & Fadhil, A.	Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIST	NIST (*National Institute of Standards and Technology*)	artefak dari aktivitas pengguna di Dropbox pada *smarthphone* Android Samsung Galaxy Trend dapat dengan mudah ditemukan dengan membandingkan direktori dan database dibuat dari aktivitas-aktivitas tersebut.
2	2020	Nasirudin., Sunardi., Riadi, I.	Analisis Forensik *Smarthphone* Android Menggunakan	NIST (*National Institute of Standards*	Penggunaan *tools* MOBILedit Forensic Express oleh penulis

			Metode NIST dan Tool MOBILedit Forensic Express	*and Technology*)	dianalisa secara manual sehingga hasil yang didapat belum terpenuhi sesuai prosedur.
3	2020	Nofiyan, A., Muslihudin.	Analisis Forensik pada Web *Phishing* Menggunakan Metode National Institute Of Standards And Technology (NIST)	NIST (*National Institute of Standards and Technology*)	Hasil implementasi metode forensik NIST dari proses-proses tersebut antara lain, didapatkan *file capture* barang bukti phising, pemeriksaan nilai Hash MD5, tujuh paket data yang terhubung tindakan phising dari hasil analisis, dan laporan barang bukti berupa URL *phishing*, DNS yang digunakan oleh pelaku, IP address server, IP address destination, identitas penyerang dan email yang menghasilkan informasi tindak kejahatan yang dilakukan phiser.

4	2017	Riadi, I., Firdonsyah, A.	Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method	NIST (*National Institute of Standards and Technology*)	Implementasi metode forensik NIST dengan *tools* Andriller hanya didapatkan bukti digital berupa data percakapan, nama pengirim pesan, PIN pengirim dan penerima pesan beserta tanggal percakapan. Data citra tidak muncul saat proses akuisisi data selesai.

Tabel 2. 5 Penelitian terkait metode forensik NIST.

2.6.1 Pembahasan Penelitian

a) Pada penelitian pertama yang dilakukan oleh Rusydi Umar dan rekan-rekannya, penelitian menggunakan *cloud computing* Dropbox versi mobile dengan perangkat pendukung lainnya seperti *Smarthphone* Samsung Galaxy V Plus, Samsung Galaxy Trend Plus. Dalam jurnal yang ditulis tidak disebutkan Dropbox versi berapa yang digunakan serta *tools* forensik apa yang diapaki. Peneliti melakukan dua tahap utama dalam penelitian yang dilakukan dimana tahap pertama dilakukan analisis artefak menggunakan *smarthphone* Samsung Galaxy V Plus dan Samsung Galaxy Trend Plus. Pada tahap kedua, langkah-langkah yang dilakukan oposisi Samsung Galaxy V Plus diulang pada *smarthphone* Samsung Galaxy Trend untuk memastikan bahwa direktori dibuat selama aktivitas pengguna identik pada keduanya *smarthphone*, hasilnya valid di berbagai OS dan perangkat.

Peneliti melakukan proses dimulai dengan melakukan analisis data instalasi dimana peneliti memeriksa beberapa file yang perlu diperhatikan yang mana jika beberapa file tersebut ada dapat diartikan pengguna telah menginstall Dropbox. Berikutnya peneliti melakukan analisis data pendaftaran untuk menganalisis data informasi pendaftaran dan

data yang berisi file yang disimpan dalam *cloud*, selanjutnya analisis memasukkan data untuk menganalisis file naru yang mencamtukan file pengguna. Langkah berikutnya analisis data keluar untuk menganalisis file yang terbuat saat melakukan aktivitas logout dimana beberapa file juga akan terhapus saat proses logout. Terakhir analisis mengunggah data untuk menganalisis file yang diunggah melalui perubahan basis data.

No.	Aktivittas	Path
1	Install data	data/app/com.Dropbox.android-1.apk
2	Signup Data	data/data/com.Dropbox.android/databases/prefs.db
3	Logout Data	data/data/com.Dropbox.android/databases/prefs.db
4	Login Data	data/data/com.Dropbox.android/databases/prefs.db
5	Uploading Data	data/data/com.Dropbox.android/databases/ID-db.db
6	Downloading Data	data/media/0/Android/data/com.Dropbox.android/files/uID/scratch/
7	Operation File Data (Open)	data/media/0/Android/data/com.Dropbox.android/cache/uID/docpreviews/
8	Operation File Data (New Folder)	ata/data/com.Dropbox.android/databases/ID-db.db
9	Operation File Data (New File)	data/data/com.Dropbox.android/databases/ID-db.db
10	Operation File Data (Move)	data/data/com.Dropbox.android/databases/ID-db.db
11	Operation File Data (Rename)	data/data/com.Dropbox.android/databases/ID-db.db
12	Operation File Data (Share)	data/data/com.Dropbox.android/databases/ID-db.db
13	Operation File Data (Delete)	data/data/com.Dropbox.android/databases/ID-db.db
14	Uninstall Data	data/system/Dropbox

Gambar 2.7 Hasil Penelitian yang dilakukan

Sumber : (Saad et al., 2020)

Hasilnya kesimpulan menurut peneliti artefak dari aktivitas pengguna di Dropbox pada *smarthphone* Android Samsung Galaxy Trend dapat dengan mudah ditemukan dengan membandingkan direktori dan database dibuat dari aktivitas yang dilakukan. Peneliti juga berharap hasil temuannya dapat dijadikan pedoman dalam melakukan investigasi.

b) Penelitian kedua ditulis oleh Nasirudin dan rekan-rekannya, peneliti menggunakan *tools* MOBILedit Forensic Express, *smarthphone* Samsung Galaxy A8, laptop HP Pavilion G series dan kabel USB sebagai penghubung laptop dan *smarthphone*. Peneliti menargetkan dalam proses investigasi ini dapat melakukan pengambilan barang bukti digital seperti profile dari pemilik *smarthphone*, kontak, gambar, SMS, whatssApp dan lain-lain.

Nama Barang	Deskripsi
Laptop	Merk HP Pavilion G series
Kabel USB	Penghubung laptop dan *smartphone*
Smartphone Android	Merk Samsung Galaxy A8
MOBILedit Forensic	*Tool* Forensik

Gambar 2.8 Alat dan bahan yang digunakan peneliti

Sumber : (Nasirudin et al., 2020)

Penelitian menggunakan metode forensik NIST dimulai dengan mengamankan barang bukti berupa *smarthphone* berikut dengan mencatat spesifikasi serta mematikan jaringan data dengan mode terbang dan dilakukan backup data setelah terdeteksi MOBILedit Forensic Express, dimana file akan terlihat. Setelah itu dilakukan pengambilan dan pemeriksaan data yang telah terlihat sebelumnya. Setelah itu peneliti melakukan analisis terhadap barang bukti digital yang telah didapat sebelumnya, dalam proses ini peneliti melakukan secara manual. Terakhir peneliti membuat laporan dari hasil proses investigasi meliputi deskripsi kasus yang terjadi, teknik dan *tools* yang digunakan, ada atau tidaknya tindakan, pedoman, prosedur, perangkat dan aspek lain yang berkaitan dengan penelitian. Kesimpulan penelitian menurut peneliti masih banyak kekurangan dimana menurut peneliti penggunaan *tools* MOBILedit Forensic Express oleh penulis dianalisa secara manual sehingga hasil yang didapat belum terpenuhi sesuai prosedur.

Deskripsi	Total
Contact	1527
Messages	149
Email	278
Call	500
Photos	38
Images File	2038

Gambar 2.9 Laporan temuan yang didapatkan peneliti

Sumber : (Nasirudin et al., 2020)

c) Penelitian ketiga ditulis oleh Nofiyan dan Mushlihudin, peneliti menggunakan dua laptop sebagai proses investigasi dimana satu laptop digunakan sebagai investigator sedangkan laptop lainnya diasumsikan sebagai pelaku.

Hardware	Software	Website
Processor Intel® Celeron® CPU N2840 @ 2.16GHz (2 CPUs), 2.16GHz	Sistem operasi windows 10 Pro 64-bit, x64 based processor	https://centralops.net (pencarian informasi tentang DNS)
Graphics Intel® HD Graphics	Wireshark-win64-3.0	
RAM 2GB	Hashcalc	
Harddisk 1 TB	Mozilla Firefox 71.0(32-bit)	

Gambar 2.10 Tabel perangkat investigator
Sumber : (Mushlihudin & Nofiyan, 2021)

Hardware	Software
Processor Intel® Core™ i7-7700 HQ CPU @ 2.80GHz, 2.80GHz	Sistem operasi windows 10 Pro 64-bit, x64 based processor
Graphics Intel® HD Graphics 630	Sublime Text 3
RAM 8 GB	Xampp versi 3.2.2
	Mozilla Firefox 71.0(64-bit)

Gambar 2.11 Tabel perangkat pelaku
Sumber : (Mushlihudin & Nofiyan, 2021)

Peneliti mengasumsikan dengan skenario telah terjadi *phishing* dimana pelaku mengirimkan email berisi link untuk mencuri *account.* Peneliti kemudian melakukan tindakan forensik sebagai investigator sesuia dengan metode forensik NIST dengan pertama melakukan pengumpulan data menggunaan *tools* Wireshark untuk mengcapture kejadian saat korban mendapatkan dan mengakses email. Setelah proses tersebut dilakukan, penliti melakukan akuisisi data temuaan dengan *tools hashcalc* dengan beberapa data temuan berupa foto berikut dengan nilai hash data MD5.

Peneliti lalu melakukan analisis terhadap data temuan berdasarkan akuisisi pada file barangbuktiphising.pcapng yang telah dilakukan dengan menggunakan beberapa *tools* sehingga didapatkan paket data dengan menggunakan teknik filter yang berisi informasi mengenai *phishing,* seperti informasi mengenai email URL *phishing*, *protocol* DNS, respon *protocol* DNS, *record layer handshake protocol*, IP address, interaksi client dan server. Terakhir peneliti menulis laporan terkait investigasi yang dilakukan dari barang bukti digital yang telah didapat sesuai dengan skenario yang ditetapkan. Hasil implementasi metode forensik NIST dari proses-proses tersebut antara lain, didapatkan *file capture* barang bukti

phising, pemeriksaan nilai Hash MD5, tujuh paket data yang terhubung tindakan phising dari hasil analisis, dan laporan barang bukti berupa URL *phishing*, DNS yang digunakan oleh pelaku, IP address server, IP address destination, identitas penyerang dan email yang menghasilkan informasi tindak kejahatan yang dilakukan phiser.

d) Penelitian keempat dilakukan oleh Riadi dan Firdonsyah, peneliti menggunakan perangkat laptop Asus SonicMaster X450J dengan OS Windows 10 64 bit, *smarthphone* Sony Xperia Z dengan OS Android Lollipop, *tools* forensik Andriller, Aplikasi Blackberry Messenger dan kabel data untuk menghubungkan laptop dan *smarthphone*. Pertama peneliti melakukan pengumpulan barang bukti berupa *smarthphone* Sony Xperia Z yang terinstall didalamnya aplikasi Blackberry Messenger dan mencatat informasi barang bukti tersebut. Lalu menggunakan *tools* Andriller, peneliti memeriksa isi dari barang bukti yang telah didapatkan dengan melakukan akuisisi data. Adapun data yang didapat berupa data pengirim, PIN pengirim, isi pesan, jenis pesan dan waktu pesan. Selanjutnya peneliti melakukan analisis dimana ditemukan isi pesan berupa pemerasan dan file gambar dalam ukuran tertentu namun peneliti tidak bisa mengakses karena keterbasan perangkat forensik.

NO	Material	Deskripsi
1	Laptop	Asus SonicMaster X450J, OS Windows 10 64bit
2	Kabel Data	Kabel data yang bisa digunakan untuk menghubungkan laptop dengan *smarthphone*
3	*Smarthphone*	Sony Xperia Z, OS Android Lollipop
4	Andriller	Berbasis Windows Aplikasi yang dapat digunakan untuk memperoleh bukti digital pada *smarthphone*
5	Blackberry Messenger	Aplikasi pesan instan multiplatform

Tabel 2. 6 Material yang digunakan Riadi dan Firdonsyah

Terakhir peneliti melakukan penulisan laporan dimana menurut penelti, Andriller mampu menghasilkan laporan dan log secara otomatis dalam format HTML dan file teks dengan ekstensi .txt. Laporan yang dibuat berformat HTML dapat diakses melalui browser yang mana berisi data yang diperoleh dari *smarthphone* yang dianalisis, data tersebut berisi: akun email, kata sandi wifi, aplikasi yang diinstal pada *smarthphone*, sms, dan log panggilan.

Kesimpulan peneliti implementasi metode forensik NIST dengan *tools* Andriller hanya didapatkan bukti digital berupa data percakapan, nama pengirim pesan, PIN pengirim dan penerima pesan beserta tanggal percakapan. Data citra tidak muncul saat proses akuisisi data selesai.

BAB III
METODOLOGI PENELITIAN

3.1 Metode Forensik NIST

Peneliti sendiri memiliki berbagai metode saat melakukan proses digital forensik, dimana salah satunya adalah metode forensik NIST. Dalam hal bidang digital forensik sendiri, NIST memiliki metode yang biasa digunakan dalam penanganan kejahatan digital berikut dengan menganalisis proses investigasi atau forensik digital kasus cybercrime dan memunculkan barang bukti digital. Adapun tahapan proses digital forensik dengan metode forensik NIST sebagai berikut :

a) Collection

Tahap pertama dari metode ini adalah Collection, dimana pada tahap ini akan dilakukan pengumpulan data, dokumentasi, pelabelan serta menjaga integritas data yang ditemukan. Tahapan ini sendiri terikat dengan Chain of Custady (CoC) supaya bukti yang didapat terjaga integritasnya dan mencegah terkontaminasi dari luar yang dapat merubah barang bukti tersebut sehingga membuat barang bukti tersebut tidak sah secara hukum.

Adapun berikut prosedur dari Chain of Custady yang harus sesuai kaidah:

1. Menyimpan bukti asli : barang bukti digital asli perlu dibuat salinan sebagai pembanding dengan yang asli guna membuktikan otentikasi barang bukti tanpa adanya modifikasi
2. Ambil bukti foto fisik : foto dari barang bukti akan membuat lebih otentik.
3. Mengambil tangkapan layar dari konten bukti digital : apabila tidak memungkinakn dalam mengambil bukti digital, tangkapan layar menjadi cara efektif penetapan Chain of Custaody.
4. Mencatat tanggal,waktu dan informasi lain yang didapat : memberi label waktu dan tanggal memungkinkan penyelidik membuat garis waktu yang dapat digunakan mengenai informasi barang bukti tersebut sebelum diperoleh.

5. Menyuntikkan klon sedikit demi sedikit dari bukti digital yang didapat ke dalam komputer forensik : untuk memastikan bahwa penyelidik memperoleh duplikat lengkap dari bukti digital yang terkait.
6. Menjalankan analisis uji Hash pada barang bukti untuk mengautentikasi klon yang telah disuntikan : guna memastikan barang bukti dari hasil penyalinan tidak rusak dan terlihat seperti bukti asli yang didapat.

b) Examination.

Tahapan untuk memproses, menilai dan mengekstraksi data menarik yang telah di ambil sebelumnya dengan prosedur yang berlaku baik secara manual maupun secara otomatis untuk memastikan bahwa data yang diambil dari lokasi tidak berubah atau terjaga integritasnya sehingga data yang diperoleh layak untuk dianalisis sekaligus pengujian terhadap bukti ada tidaknya data tertentu.

c) Analysis.

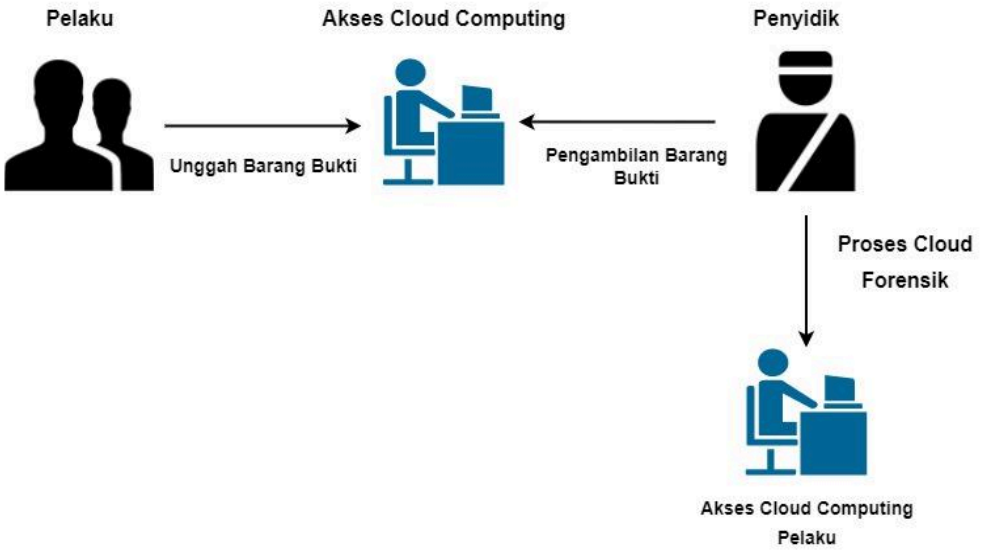
Tahapan yang melibatkan penggunaan metode dan teknik untuk menganalisa bukti digital yang didapat oleh penyidik dengan metode yang sah untuk membuktikan data yang didapat. Hasil dari analisis tersebut harus bisa dibuktikan dan dipertanggung jawabkan secara hukum.

d) Reporting.

Tahapan pelaporan hasil analisa bukti digital yang telah didapat sebelumnya serta melaporkan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai *tools* yang digunakan, metode yang digunakan serta tindakan selanjutnya apabila diperlukan maupun aspek pendukung lainnya saat proses digital forensik saat berlangsung.

3.2 Skenario Percobaan

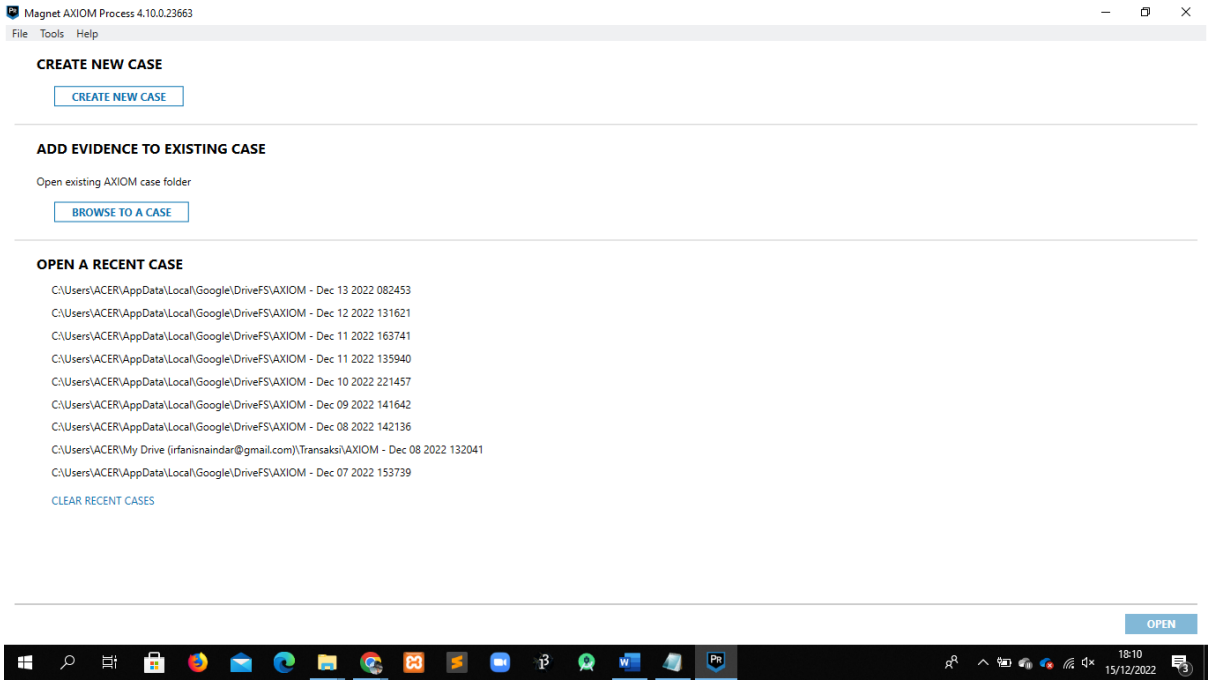
Skenario ini dibuat guna memberikan gambaran tindakan cybercrime pada lingkup *cloud computing* Google Drive dimana pelaku kejahatan memanfaatkan laptop untuk media mengakses *cloud computing* yang digunakan sebagai lokasi penyimpanan data dan file yang digunakan dalam tindak kejahatan dimana pelaku dalam skenario menyimpan beberapa dokumen berkaitan kejahatan dan foto-foto saat melakukan tindakan kejahatan yang dilakukan dengan maksud untuk menghindari penggunaan barang bukti fisik jika pelaku tertangkap. File yang disimpan pelaku didalam Google Drive akhirnya dihapus dimana file yang diunggah berformat PDF, doc, jpg dan txt. Adapun Laptop yang digunakan peneliti akan diskenariokan sebagai barang bukti yang didapatkan serta peneliti sendiri akan berperan sebagai penyidik dalam skenario ini.



Gambar 3.1 Bagan skenario

3.3 Skenario Proses Forensik

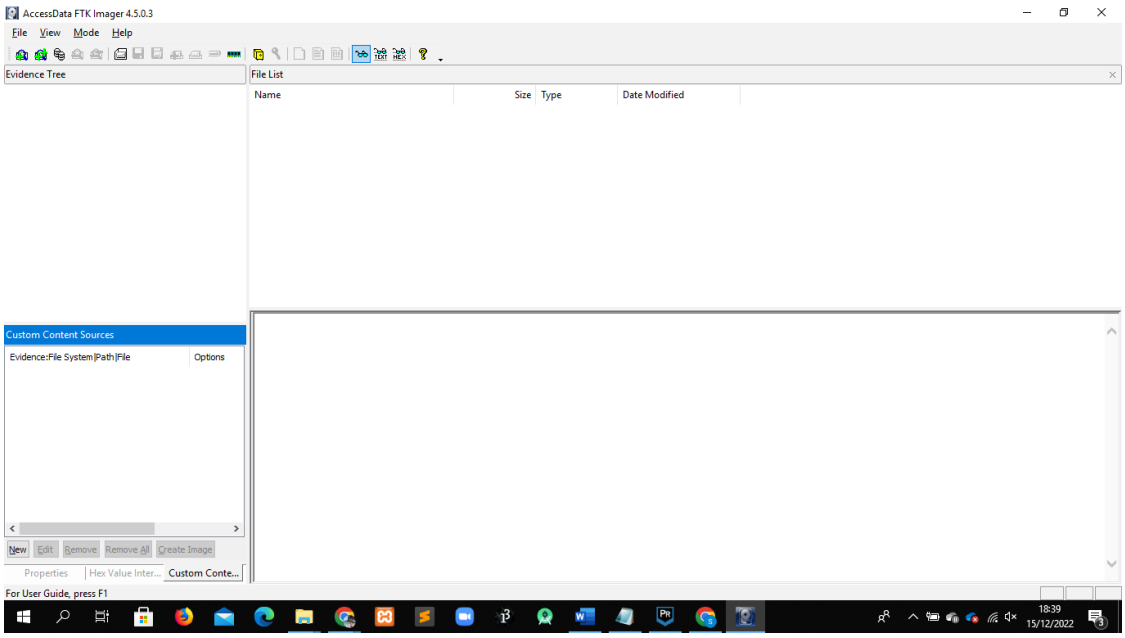
Proses forensik sendiri akan mengikuti kaidah metode forensik NIST sesuai yang dijelaskan diatas. Sebelum itu juga peneliti telah menyiapkan beberapa *tools* untuk mendukung proses forensik meliputi *tools* imaging,akuisisi data dan *tools* untuk mengakses database .



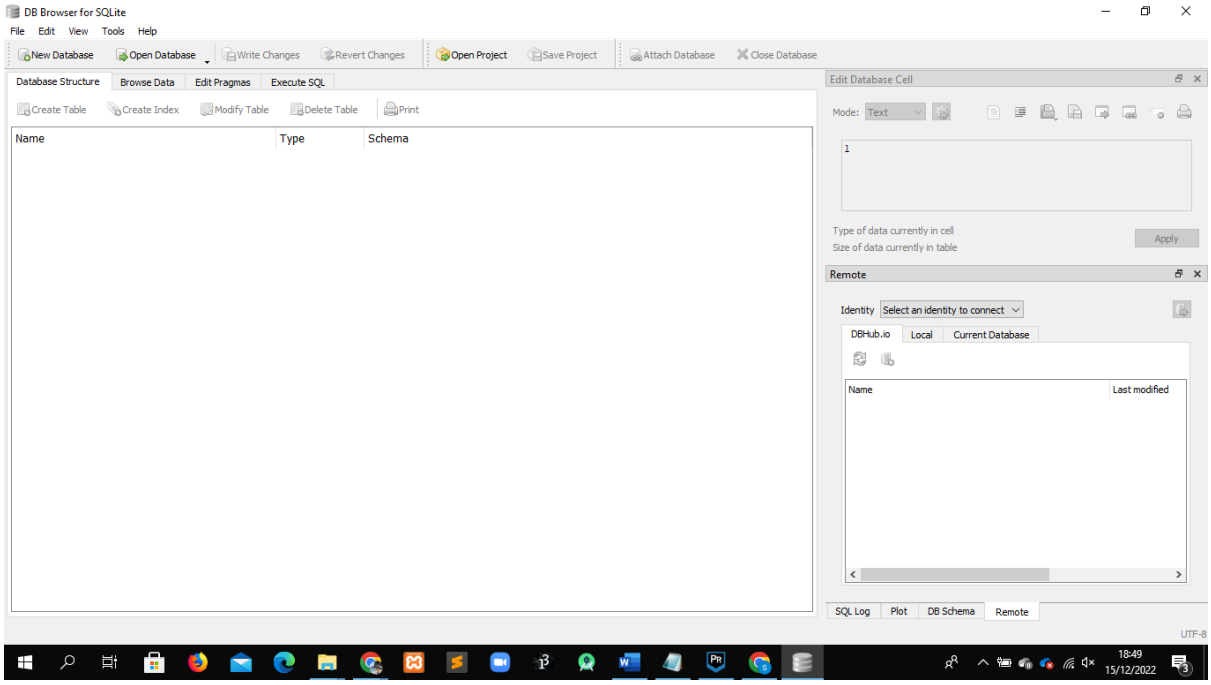
Gambar 3.2 Tampilan *tools* Magnet Axiom

Lebih lanjut pertama dengan diawali melalui proses Collection yang dimana peneliti akan mengakses lokasi folder yang diduga berisi artefak Google Drive pada path C:\Users\ACER\AppData\Local\Google\DriveFS dengan tujuan menemukan artefak utama Google Drive seperti sync_config.db, snapshot.db, dan sync_log.db

Setelah itu peneliti akan melakukan Examination terhadap artefak yang ditemukan pada path yang telah disebutkan dengan melakukan pengambilan Hash value supaya artefak yang ditemukan tetap terjaga integritasnya sehingga tidak berubah kondisinya, proses ini akan dilakukan dengan menggunakan *tools* yang telah disiapkan.



Gambar 3. 3 Tampilan *tools* FTK Imager



Gambar 3. 4 Tampilan *tools* DB Browser for SQLite

Setelah proses Examination dilanjutkan proses Analysis untuk menganalisa hasil temuan yang telah didapatkan sehingga dapat memudahkan saat membuat laporan hasil proses forensik berlangsung. Analisi berdasarkan bukti proses forensik yang telah dilakukan dalam bentuk screenshoot dari *tools* yang telah digunakan, setelah itu akan dianalisa apa yang terlihat.

Terakhir tahapan report untuk membuat laporan mengenai hasil atau temuan yang didapatkan, artefak apa saja yang ditemukan, *tools* yang digunakan. Tahapan ini turut memuat hasil proses analisis pada *tools* berupa screenshoot maupun penjelasan lebih lanjut yang dimuat dalam bentuk tabel.

BAB IV
PEMBAHASAN

4.1 Proses Forensik

Sebelum dilakukan pelaksanaan tahapan pengumpulan data, peneliti melakukan pencatatan software dan perangkat yang digunakan selama melakukan proses digital forensik.

4.1.1 Collection

No	Nama Software/Perangkat	Keterangan
1	Laptop Acer Aspire 5 A514-51G-52M2	Media melakukan digital forensik
2	Google Drive Desktop Version: 66.0.3.0	Media *cloud computing* untuk dilakukan digital forensik
3	Magnet Axiom Process	*Tools* untuk melakukan capturing dan imaging data
4	DB Browser for SQLite Version 3.12.2	*Tools* untuk membuka isi file format database
5	FTK Imager	*Tools* untuk mengakses nilai Hash

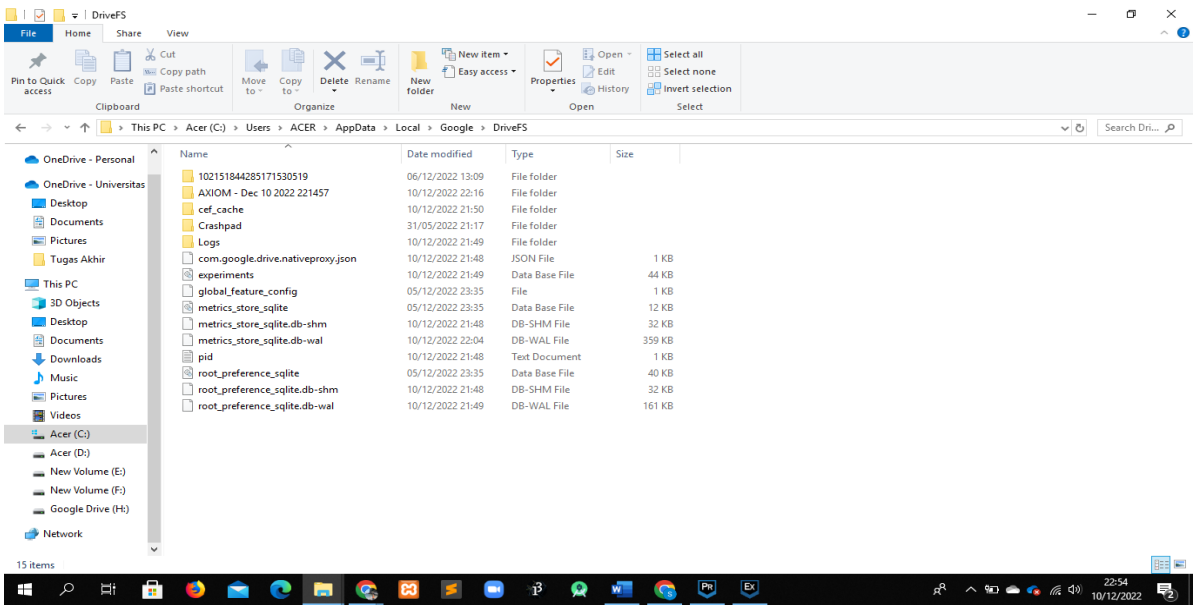
Tabel 4.1 Perangkat/software yang digunakan

Percobaan dilakukan dengan mencoba mengakses lokasi beberapa artefak dari Google Drive sendiri. Peneliti mencoba mencari beberapa artefak seperti sync_config.db, snapshot.db, sync_log.db dengan melakukan akses path folder atau akses lokasi dari C:\Users\ACER\AppData\Local\Google\ DriveFS. Adapun file-file artefak diatas bila diakses berisikan beberapa informasi mengenai akun Google Drive yang tersinkronisasi pada perangkat lebih lanjut berikut penjelasannya. Alasan memilih file dengan format db dibanding file lain karena berharap dari file db tersebut berisikan informasi detail mengenai Google Drive yang digunakan dalam penelitian.

Sebelumnya penelitian dilakukan dengan mengakses langsung ke Google Drive menggunakan *tools* forensik yang ada, Google Drive yang digunakan sendiri merupakan versi File Stream dengan mode Mirror files yang mana file yang diunggah didalam Google Drive itu sendiri bisa diakses secara *offline*. Namun pada saat akan dilakukan akses langsung ke Google Drive, *tools* forensik yang digunakan tidak dapat mendeteksi, sehingga proses forensik dialihkan dengan mengakses path folder yang telah dijelaskan sebelumnya.

File	Keterangan
sync_config.db	file SQLite yang memberi Anda informasi tentang akun Google Drive yang terhubung dan lokasi folder sinkronisasi
snapshot.db	file SQLite yang berisi daftar file yang diketahui Google Drive dan tindakannya sedang dipantau di folder sinkronisasi. Log ini mencakup sedikit info menarik seperti hash file, nama, ID Google, dan stempel waktu
sync_log.db	file teks yang berisi banyak informasi tentang peristiwa yang telah terjadi dalam Google Drive – termasuk peristiwa pembuatan, penghapusan, & modifikasi

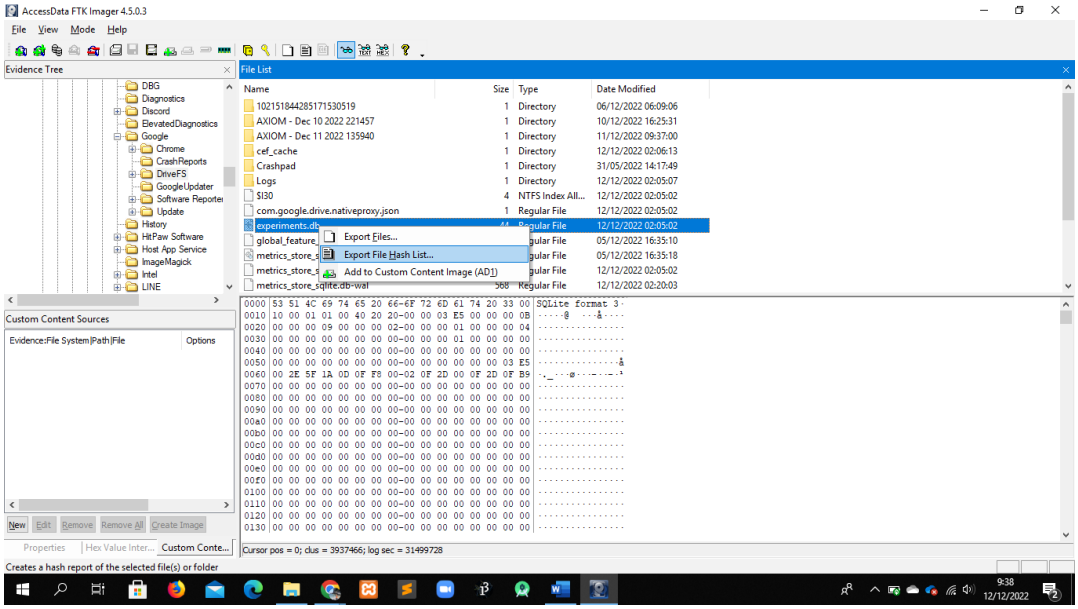
Tabel 4.2 Tabel artefak utama Google Drive



Gambar 4.1 Lokasi folder Google Drive

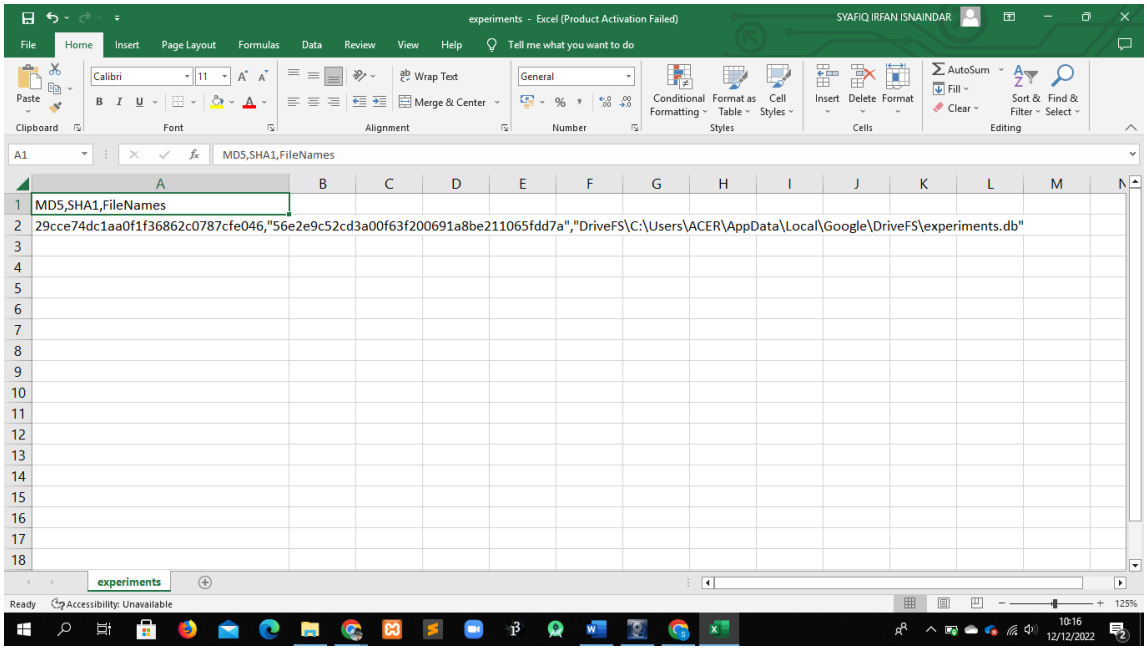
Namun pada saat akses lokasi dilakukan tidak ditemukan beberapa file artefak yang disebutkan diatas. Adapun file database yang ditemukan antara lain experiments.db, metrics_store_sqlite.db dan root_preference_sqlite.db. Karena tidak ditemukan file yang dicari, akhirnya tetap dilanjutkan dengan membuka isi dari file database tersebut dengan *tools* DB Browser terhadap masing-masing file tersebut. Namun, sebelum dibuka isi file tersebut dilakukan pengambilan Hash value terhadap file tersebut untuk mencegah file perubahan pada integritas file tersebut dengan menggunakan FTK Imager.

4.1.2 Examination



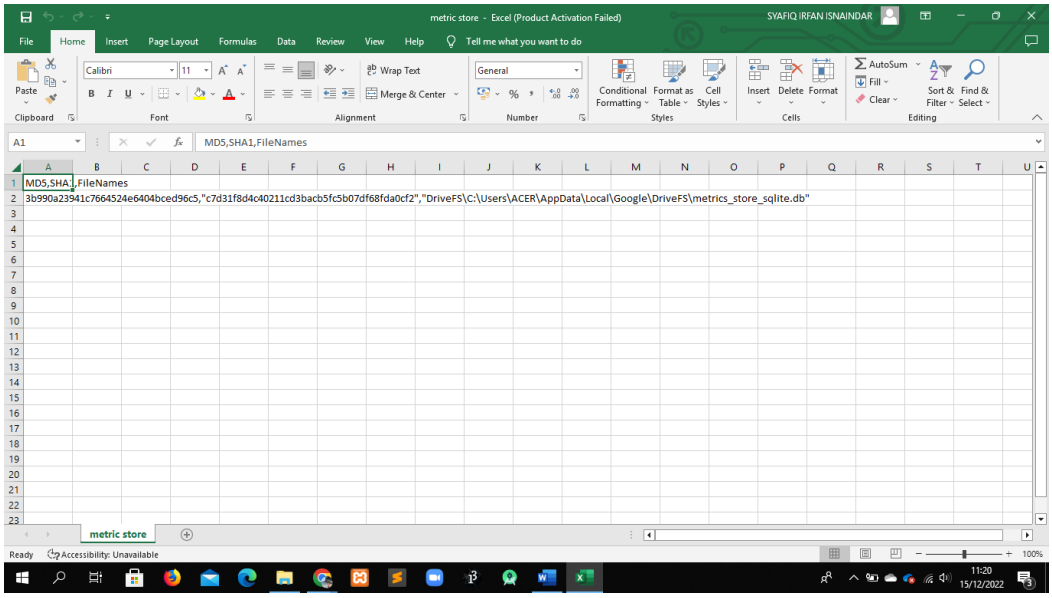
Gambar 4.2 Proses pengambilan Hash value dengan FTK Imager

Setelah dilakukan Collection, langkah berikutnya melakukan proses Examination. Proses ini dilakukan untuk mencegah file artefak yang didapatkan berubah integritasnya, sehingga proses ini dilakukan dengan proses pengambilan Hash value. Pengambilan Hash value sendiri dilakukan dengan menggunakan *tools* FTK Imager dengan cara mengatur evidence tree pada tampilan *tools* tadi ke path folder C:\Users\ACER\AppData\Local\Google\ DriveFS yang kemudian diarahkan ke file db yang ada lalu diklik kanan lalu dipilih Export File Hash List yang mana akan terbentuk file csv yang berisikan Hash value file tersebut dengan tipe MD 5 dan SHA-1. File csv yang didapatkan dibuka menggunakan Microsoft Excel sehingga didapatkan Hash value dan lokasi dari file yang tersebut.



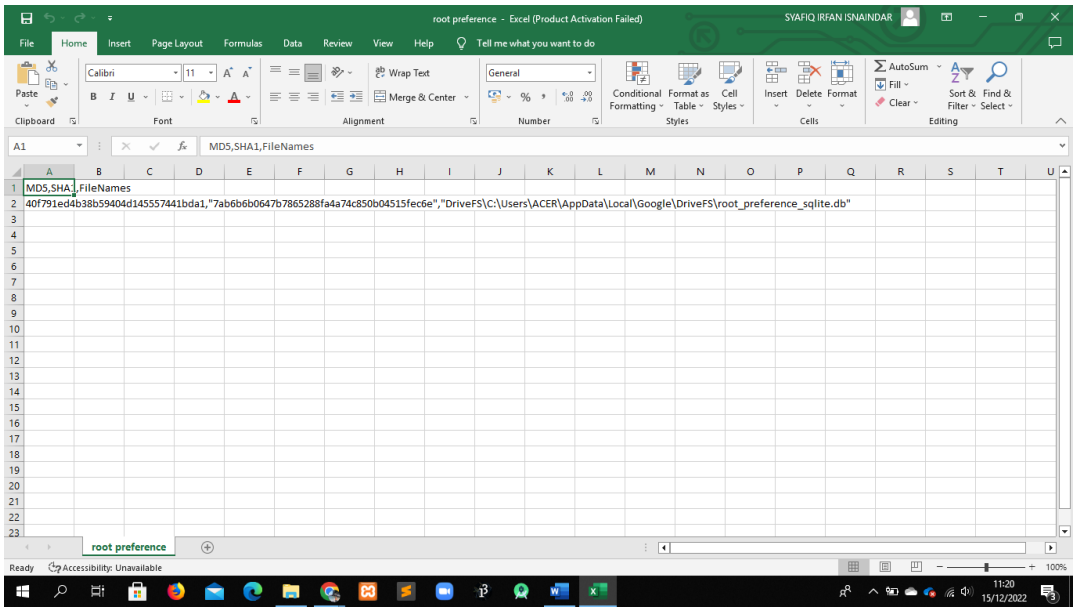
Gambar 4.3 Hash Value file experiments.db diakses dengan Microsoft Excel

File pertama yang dilakukan pengambilan Hash value adalah file experiments.db. File ini sendiri setelah dilakukan pengambilan Hash value dengan *tools* didapatkan value 29cce74dc1aa0f1f36862c0787cfe046 untuk value MD 5 sedangkan value dari SHA-1 adalah 56e2e9c52cd3a00f63f200691a8be211065fdd7a. Hash value ini nantinya akan digunakan sebagai bukti integritas atau keaslian bukti temuan yang didapat.



Gambar 4.4 Hash Value file metric_store_sqlite.db diakses dengan Microsoft Excel

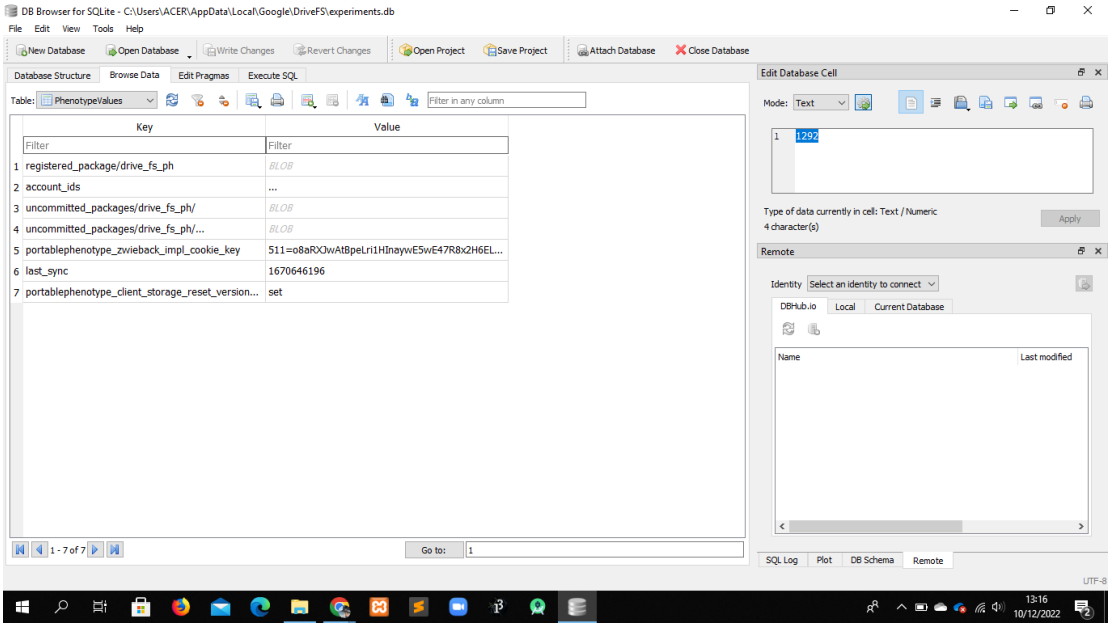
File kedua yang dilakukan proses pengambilan Hash value adalah metric_store_sqlite.db, dimana file ini sendiri setelah dilakukan pengambilan Hash value didapatkan hasil 3b990a23941c7664524e6404bced96c5 untuk value MD 5 sedangkan value dari SHA-1 adalah c7d31f8d4c40211cd3bacb5fc5b07df68fda0cf2



Gambar 4.5 Hash Value file root_preference_sqlite.db diakses dengan Microsoft Excel

File terakhir yang dilakukan pengambilan Hash value adalah root_preference_sqlite.db, sama seperti file-file sebelumnya, setelah dilakukan pengambilan Hash value, file ini mendapatkan hasil 40f791ed4b38b59404d145557441bda1 untuk value MD 5 sedangkan value dari SHA-1 adalah 7ab6b6b0647b7865288fa4a74c850b04515fec6e. Ketiga file tadi menggunakan Microsoft Excel untuk membuka file csv yang berisikan informasi Hash value.

4.1.3 Analysis



Gambar 4.6 artefak experiments.db yang diakses dengan DB Browser

Pada tahap ini penelitian dilakukan dengan mengakses isi dari file yang telah didapat sebelumnya dengan *tools* DB Browser. Proses ini sendiri bertujuan untuk mengakses informasi apa saja yang bisa didapatkan dari file db yang telah ditemukan sebelumnya. File pertama yang diakses adalah experiments.db untuk dilihat isi dari file tersebut, adapun hasilnya dilihat dalam table dibawah ini.

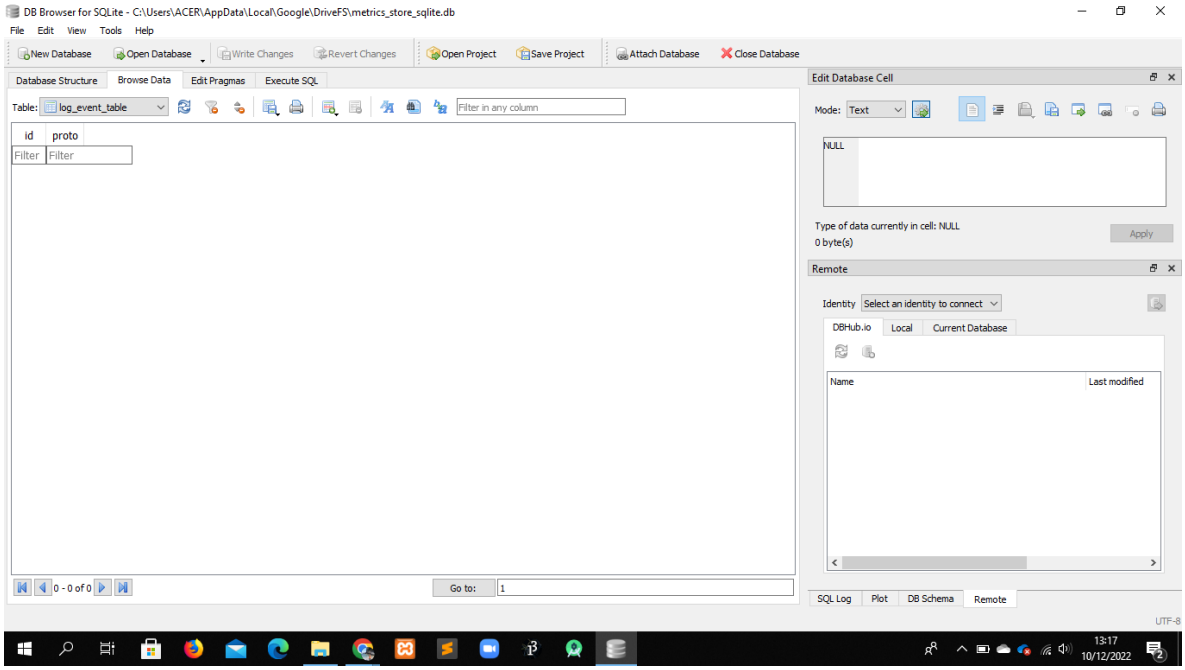
No	Key	Value
1	registered_package/drive_fs_ph	*BLOB*
2	portablephenotype_client_storage_reset_version_key_2	set
3	account_ids	…
4	uncommitted_packages/drive_fs_ph/	*BLOB*
5	uncommitted_packages/drive_fs_ph/102151844285171530519	*BLOB*

6	portablephenotype_zwieback_impl_cookie_key	511=CtCJX4i7tgaeMVl9adJbb70TX8wPAOzWVKUCO_Gxca9GHWFCP9EsBNyfloRrFwtTe2hEcxSqopq5cSlI8iovk2Xp-FmtpZJB2sp4JjcuVzThMpcAPh3dR12N0N1RTm47KfRo2-luPyLdufAan85L45w73gUWVSnW-p-Uk70GK5k
7	last_sync	1670723270

Tabel 4.3 Hasil akses file experiments.db dengan DB Browser

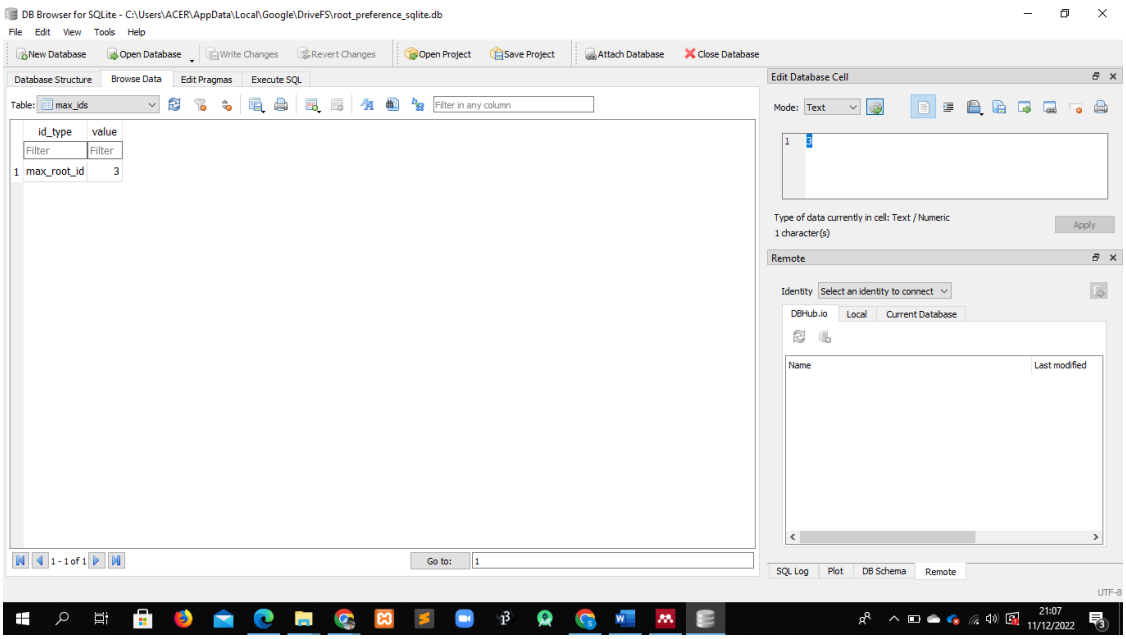
Pada key registered_package/drive_fs_ph dengan value BLOB pada saat diklik value tersebut hanya menampilkan sebuah bilangan binary. Selanjutnya pada key nomor dua yakni portablephenotype_client_storage_reset_version_key_2 hanya menampilkan tulisan set, tanpa ada keterangan lainnya. Key nomor tiga yakni account_ids pada *tools* valuenya menampilkan tanda titik yang mana setelah diklik muncul value NAK102151844285171530519. Selanjutnya pada key nomor empat dan nomor lima yakni uncommitted_packages/drive_fs_ph/ dan uncommitted_packages/drive_fs_ph/102151844285171530519 menampilkan value BLOB yang mana pada saat di klik hanya menampilkan angka binary. Key nomor enam yakni portablephenotype_zwieback_impl_cookie_key menampilkan value semacam kode yang tidak bisa diakses. Terakhir value nomor tujuh last_sync menamilkan sebuah bilangan dengan value 1670723270. Sayangnya file experiments.db sendiri tidak memuat informasi berkaitan seperti informasi akun, email, password, aktivitas akun, maupun informasi lainnya.

Selanjutnya dilakukan akses file berikutnya yakni file metric_store_sqlite.db, file dengan kapasitas 12 KB berada pada path folder yang telah disebutkan sebelumnya yakni pada path C:\Users\ACER\AppData\Local\Google\ DriveFS. Proses akses dilakukan sama dengan menggunakan tools DB Browser, dengan mengklik menu Open Database, lalu diarahkan ke folder lokasi file metric_store_sqlite.db berada, setelah itu klik file tersebut.



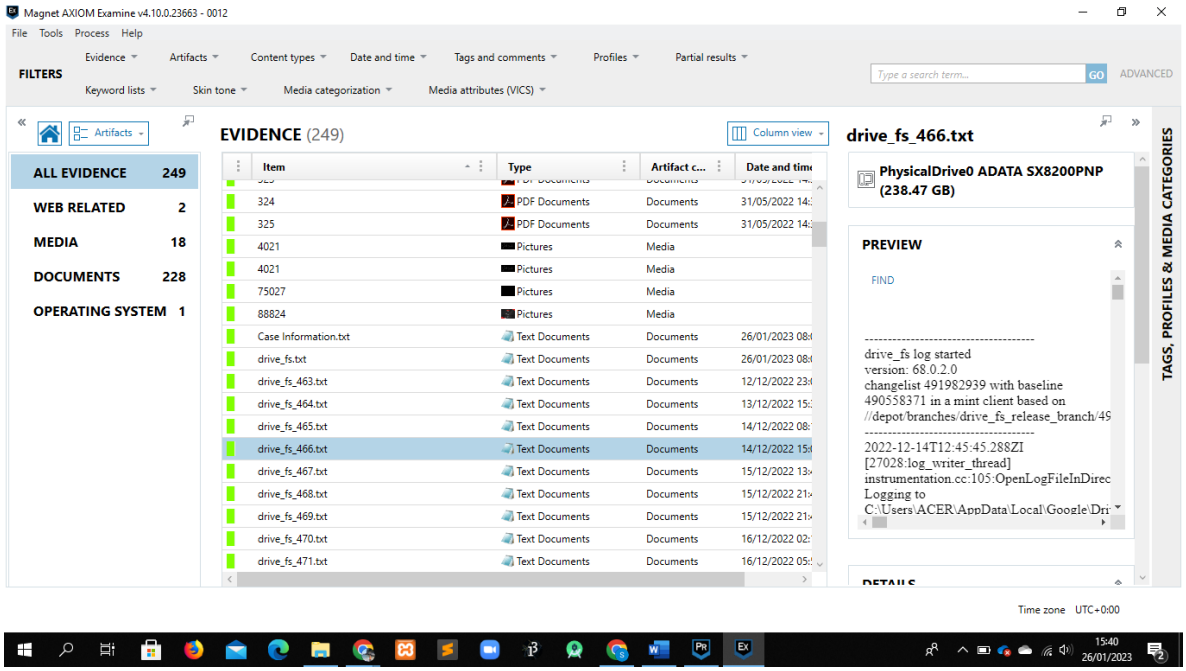
Gambar 4.7 akses file metric_store_sqlite.db dengan DB Browser

Hasilnya pada akses file metric_store_sqlite.db yang dilakukan tidak ditemukan key maupun value dari file tersebut. Hanya tabel kosong tanpa informasi yang spesifik mengenai Google Drive.



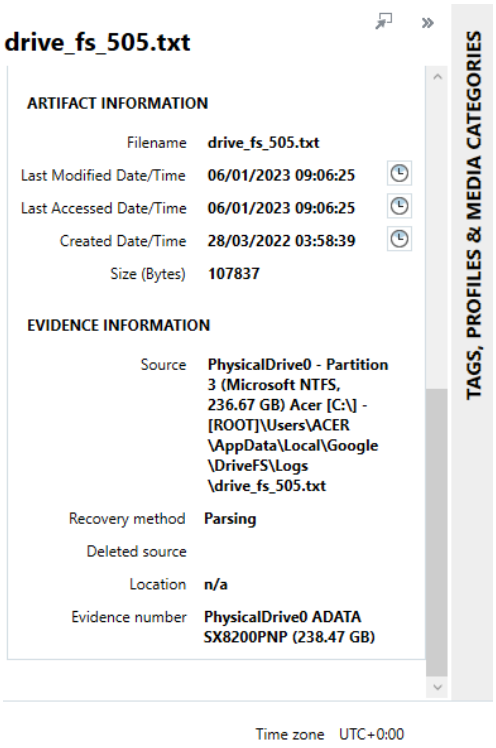
Gambar 4.8 akses file root_preference_sqlite.db dengan DB Browser

Setelah itu dilakukan akses file berikutnya yakni file root_preference_sqlite.db. Dengan melakukan proses dan langkah-langkah yang sama, file tersebut hanya menampilkan informasi berupa id_type berupa max_root_id dengan value 3 tanpa memberikan informasi spesifik mengenai Google Drive itu sendiri.



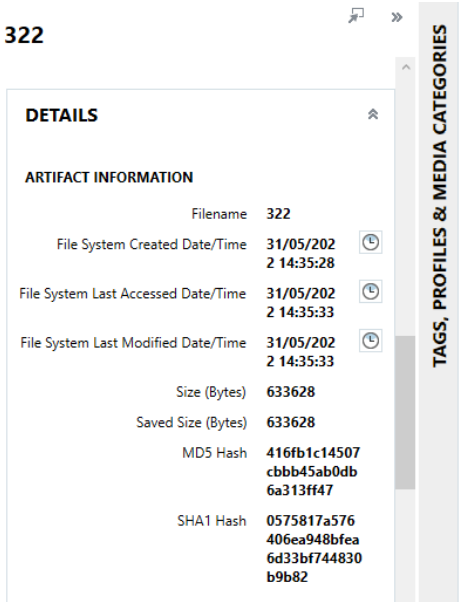
Gambar 4.9 Proses Tagging pada seluruh bukti temuan.

Karena hasil yang didapatkan tadi, penelitian dilanjutkan denggan *tools* lainnya. Peneliti melanjutkan dengan menganalisis bukti digital dengan menggunakan *tools* Magnet Axiom pada folder DriveFS dengan harapan dapat menemukan artefak lain yang terkait dengan informasi Google Drive. Proses dimulai dengan membuat case baru dengan mengklik *create new case* lalu memasukan nomor dan jenis case pada kolom *case number* dan *case type*. Selanjut memastikan file path *location for case files* dan *location for acquired evidence* dan *mengisi scan information* dan klik *Go To Evidence Sources*. Lalu memilih *Evidence Sources*, dalam proses ini dipilih computer lalu memilih *Operating System* yang kita gunakan. Lanjut dengan memilih *Load Evidence*, yang setelah itu akan muncul pilihan jenis *evidence* yang akan diakses, dalam hal ini dipilih *Files & Folders*. Lalu akan muncul tampilan *Add Files & Folders,* pada tampilan bawah akan tampil pilihan *Folder Browser*, lalu di klik dan pilih folder DriveFS dari path folder yang telah disebutkan diawal. Lalu klik *Go To Processing Details*, dilanjutkan mengklik *Go To Artifact Details* lalu akan muncul tombol *Go To Analyze Evidence*, klik tombol tersebut terakhir klik *Analyze Evidence*. Setelah menunggu beberapa saat Magnet Axiom mendeteksi beberapa bukti temuan, dengan lingkup Web Related yang, Media, Documents dan Operating System. Tanda berwarna hijau setelah dilakukan proses Tagging pada bukti hasil temuan dengan *tools* Magnet Axiom.



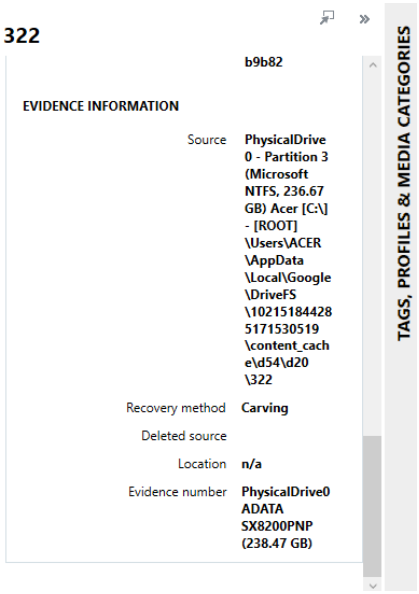
Gambar 4.10 salah satu informasi artefak berformat txt.

Salah satu dari file artefak berformat .txt yang ditemukan menggunakan *tools* Magnet Axiom memuat informasi mengenai nama file, waktu file dimodifikasi, waktu file diakses dan dibuat serta ukuran artefak tersebut. Selain itu informasi bukti lainnya memuat sumber dari file tersebut, metode pemulihan, sumber terhapus, lokasi dan nomor bukti.



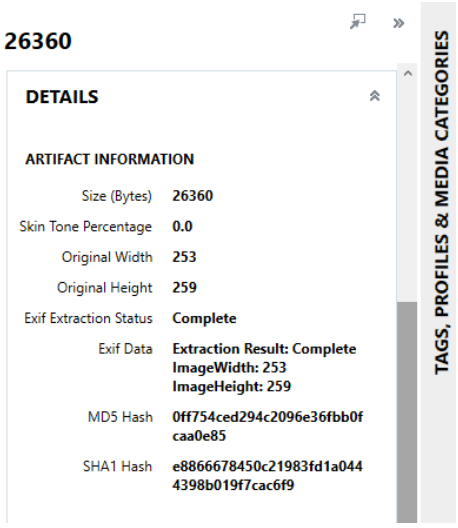
Gambar 4.11 Salah satu artefak dengan format pdf.

File artefak diatas dengan format .pdf adalah file yang ditemukan menggunakan *tools* Magnet Axiom memuat informasi mengenai nama file, waktu file dimodifikasi, waktu file diakses dan dibuat serta ukuran artefak dan ukuran artefak saat tersimpan. Selain itu informasi lainnya memuat nilai Hash berikut dengan format MD 5 dan SHA1.



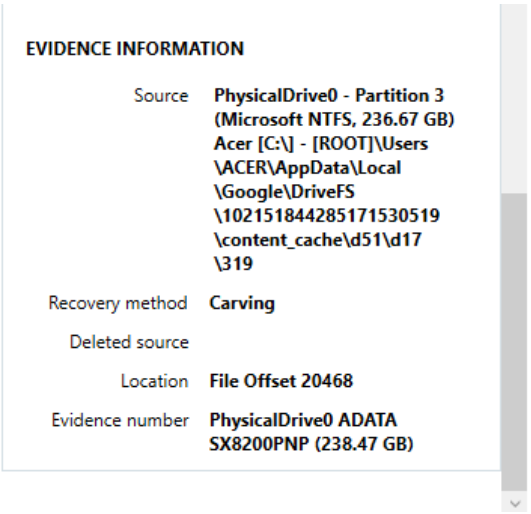
Gambar 4.12 Informasi lain dari artefak berformat pdf

Informasi lain dari file pdf tadi memuat juga informasi lain seperti sumber file, metode pemulihan sumber terhapus, lokasi dan nomor bukti.



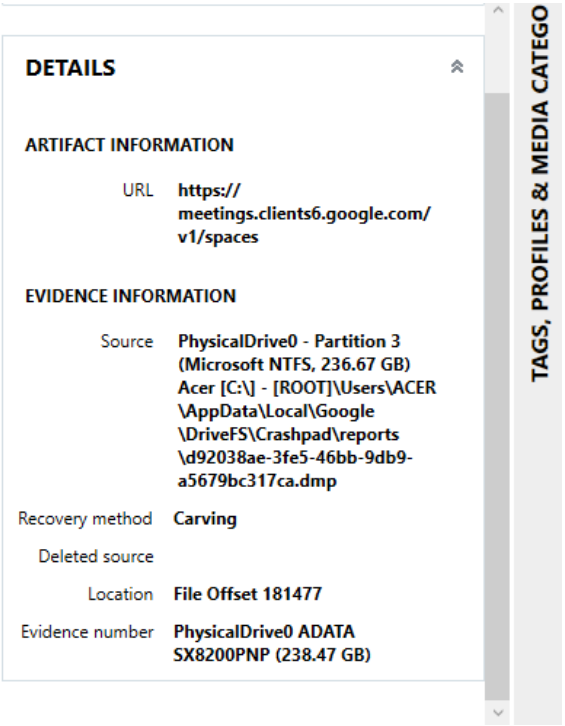
Gambar 4.13 Salah satu artefak berupa gambar.

Informasi diatas berasal dari file artefak berupa gambar yang memuat informasi berupa ukuran file, persentasi warna permukaan, lebar asli, tinggi asli, status ekstraksi exif, data exif serta nilai Hash dengan format MD 5 dan SHA 1.



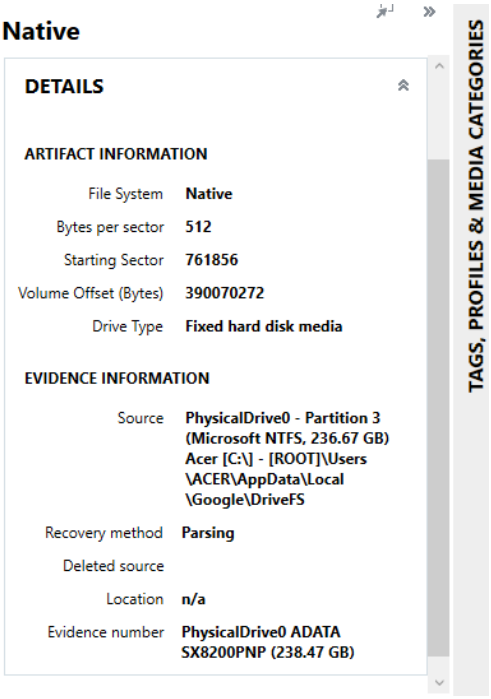
Gambar 4.14 Informasi lain dari artefak berupa gambar.

Informasi lain yang dimuat antara lain sumber file, metode recovery, sumber terhapus, lokasi dan nomor bukti.



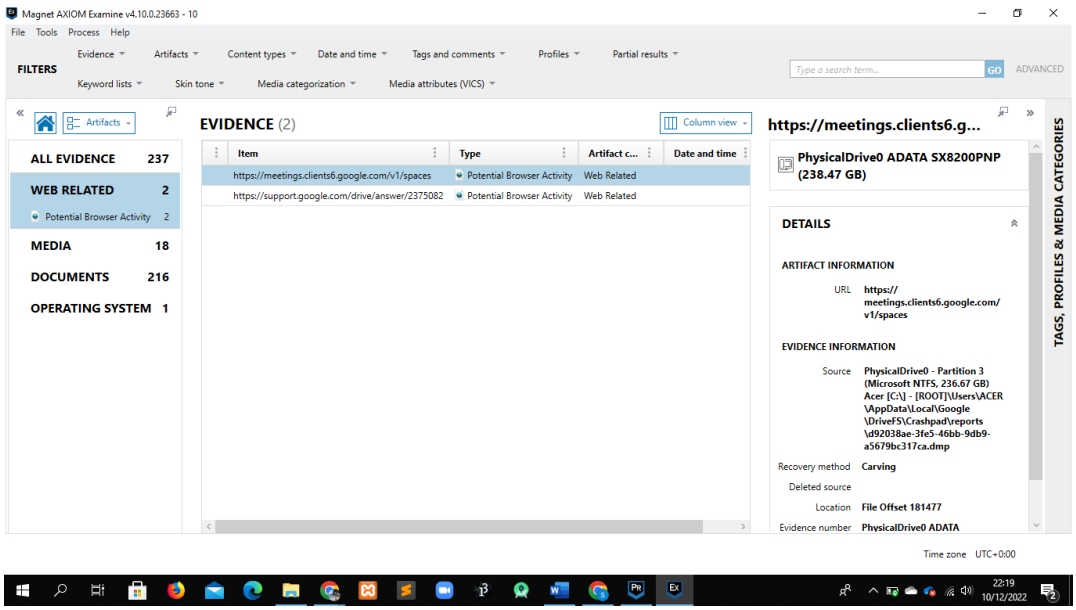
Gambar 4.15 Informasi artefak temuan berupa URL.

Bukti temuan lainnya yang ditemukan dengan *tools* Magnet Axiom berupa URL dengan informasi URL link, sumber, metode recovery, sumber terhapus, lokasi, nomor bukti.



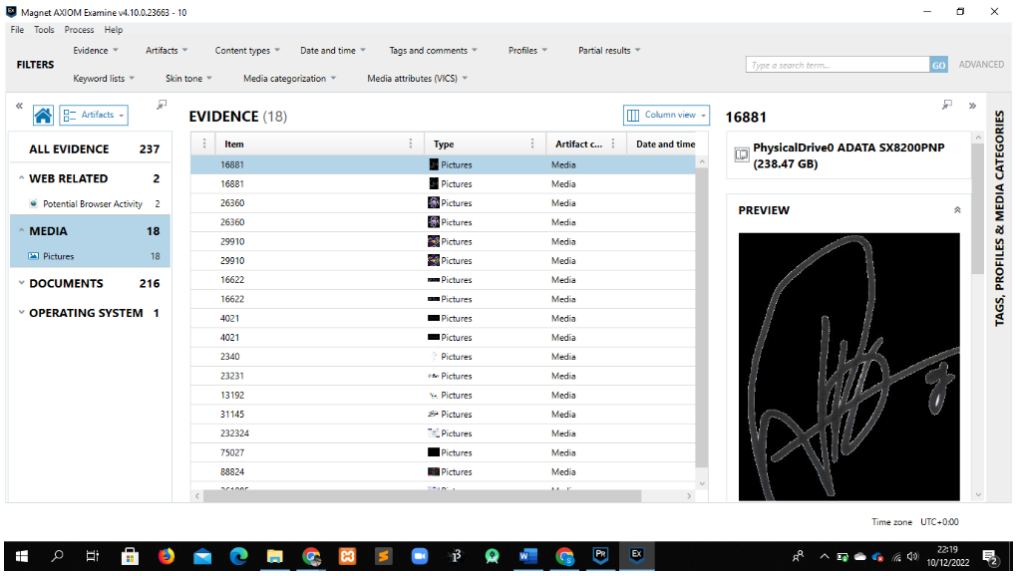
Gambar 4.16 Informasi artefak sistem informasi.

Artefak berikutnya yang ditemukan berupa File System Information dengan informasi jenis file sistem, jumlah bytes per sector, *startic sector, volume offset*, jenis drive. Informasi lain yang dimuat antara lain sumber file, metode *recovery*, sumber terhapus, lokasi, nomor bukti.



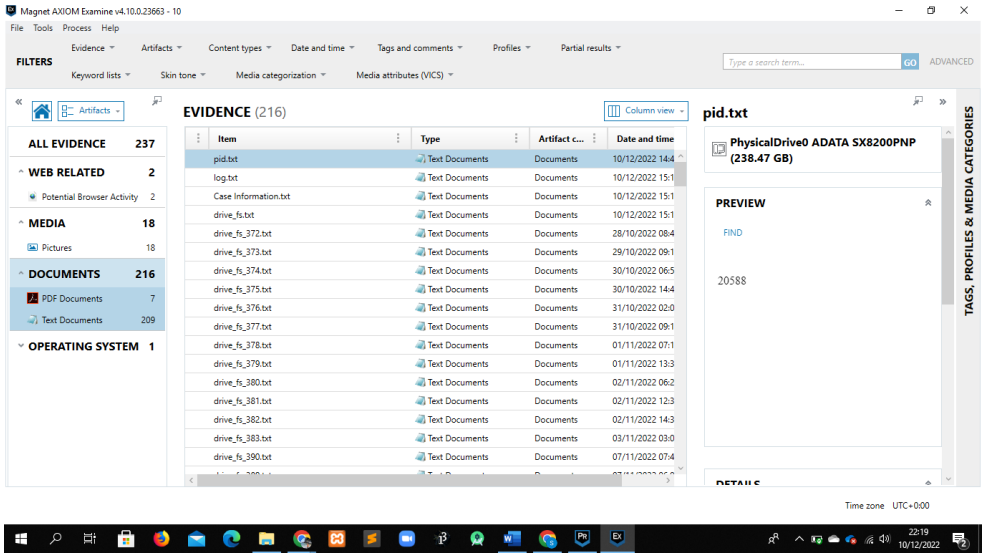
Gambar 4.17 Akses folder DriveFS dengan Magnet Axiom.

Selanjutnya memeriksa masing-masing bukti temuan berdasar jenis bukti tadi. Magnet Axiom mendeteksi 2 bukti berupa yang berkaitan dengan *Web Related* dimana masing-masing memiliki link. Namun hanya satu link yang dapat diakses dimana link tersebut akan membuka akses ke layanan Google Drive help sedangkan bukti link lainnya tidak memiliki akses ke segala web atau sistem manapun.



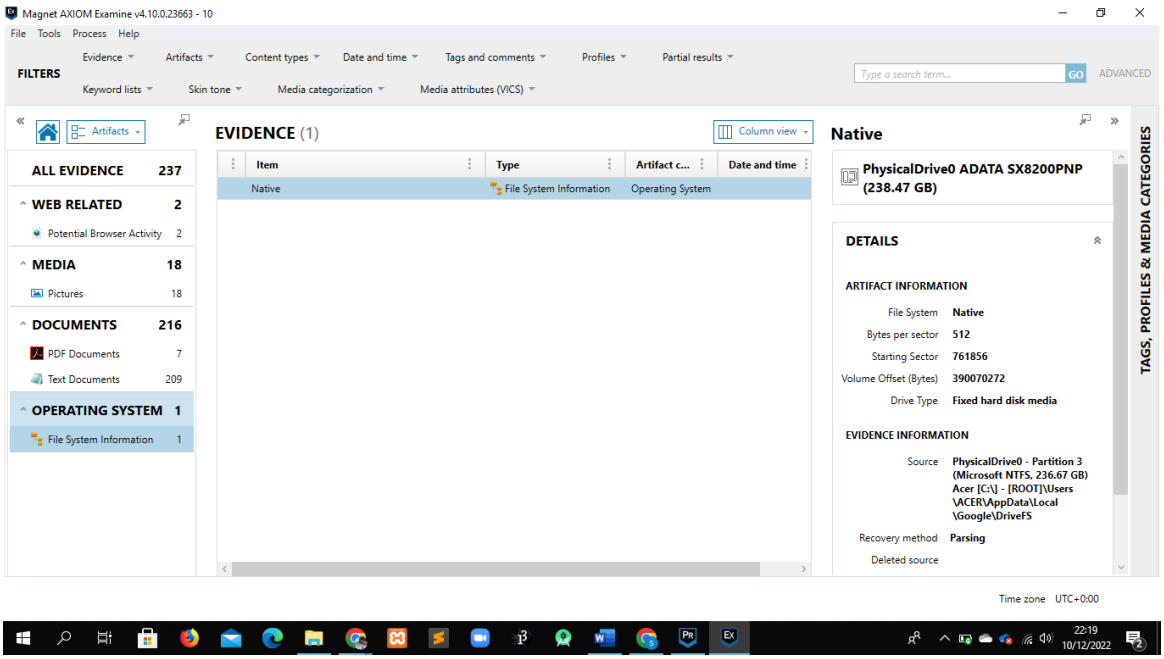
Gambar 4.18 Hasil proses imaging folder DriveFS berupa gambar

Magnet Axiom juga mendeteksi 18 buah artefak berupa gambar dimana hasil analisis juga mendeteksi informasi dari artefak yang ditemukan seperti lokasi, ukuran dan Hash value dari artefak tersebut.



Gambar 4.19 Hasil proses imaging folder DriveFS berupa dokumen.

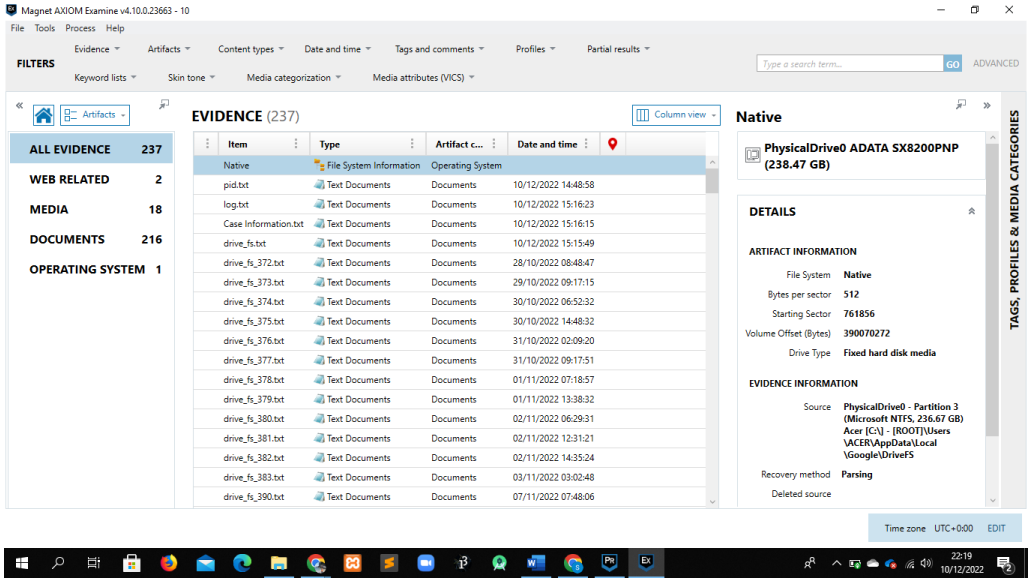
Artefak lain yang terdeteksi berupa dokumen dengan format PDF dan txt, yang mana dokumen PDF terdeteksi berjumlah 7 sedangkan txt 209. Artefak yang ditemukan juga memuat informasi mengenai kapan file tersebut terakhir dibuat, diakses dan dimodifikasi berikut lokasi file tersebut dan Hash value. Selain itu nomor bukti dan metode recovery juga dapat ditampilkan.



Gambar 4.20 Hasil proses imaging folder DriveFS berupa Operating System.

Terakhir pada artefak operating system hanya menampilkan item *Native* berikut informasi seperti lokasi file tersebut tanpa menampilkan informasi berkaitan dengan Google Drive sendiri. Google Drive yang digunakan peneliti merupakan versi terbaru yakni Google Drive File Stream sedangkan versi terdahulunya Google Backup and Sync, belum ada penelitian atau penjelasan terkait mengapa bisa file artefak terkait informasi Google Drive pada versi sebelumnya tidak ditemukan pada lokasi folder DriveFS.

4.1.4 Report



Gambar 4.21 Hasil proses imaging folder DriveFS secara keseluruhan.

Laporan yang didapat dengan *tools* Magnet Axiom setelah dilakukan proses analisis pada folder DriveFS dimana total terdapat 237 bukti yang didapat menggunakan *tools* tersebut.

Bukti temuan	**Keterangan**	**Jumlah**
Web Related	Satu dari dua bukti menampilkan berupa link yang mengakses layanan bantuan Google Drive, sedangkan link satunya tidak bisa diakses	2
Media	Artefak yang ditemukan berupa gambar berikut dengan informasi lain seperti ukuran, lokasi, Hash value, dll.	18
Documents	Artefak yang ditemukan dalam format PDF dan txt dimana memuat informasi seperti kapan file tersebut terakhir dibuat, diakses dan dimodifikasi berikut lokasi file, Hash value, Nomor bukti, metode recovery,dll.	216
Operating System	Hanya menampilkan item Native berikut informasi seperti lokasi file tersebut tanpa menampilkan informasi berkaitan dengan Google Drive sendiri	1

Tabel 4.4 laporan hasil imaging dengan Magnet Axiom

Artefak	Keterangan
experiments.db	Setelah diakses menampilkan tujuh key dengan masing-masing key memiliki value yang berbeda.
metric_store_sqlite.db	Setelah diakses kosong tidak ada informasi yang didapat
root_preference_sqlite.db	Hanya menampilkan dua item berupa id_type dan value

Tabel 4.5 Laporan analisis dengan DB Browser

Artefak diatas merupakan artefak database yang mana pada saat penelitian, peneliti mengira artefak tersebut akan berisi informasi mengenai akun Google Drive tetapi setelah diakses dengan DB Browser ternyata informasi yang terlihat tidak berkaitan dengan akun Google Drive sama sekali bahkan satu artefak tidak terdapat informasi sama sekali.

Untuk menjawab rumusan masalah poin b dilakukan dengan menggunakan 5W+1H dengan rincian Who (siapa), What (apa), when (kapan), where (dimana), Why (kenapa), How (bagaimana) dijelaskan dalam tabel berikut :

Cakupan	Pertanyaan	Keterangan
Who	Siapa yang terlibat?	Seorang pelaku dengan barang bukti laptop dan peneliti berperan sebagai penyelidik berdasarkan skenario.
What	Apa yang dilakukan pelaku? Apa yang didapatkan?	Pelaku mengunggah beberapa dokumen untuk melakukan kejahatan pada Google Drive, penyidik menemukan beberapa dokumen dari penyelidikan dengan *tools* Magnet Axiom berupa gambar, file PDF dan txt.
When	Kapan pelaku melakukan aksi?	Berdasarkan hasil temuan penyidik dengan *tools* menunjukan waktu yang berbeda-beda. Namun akses

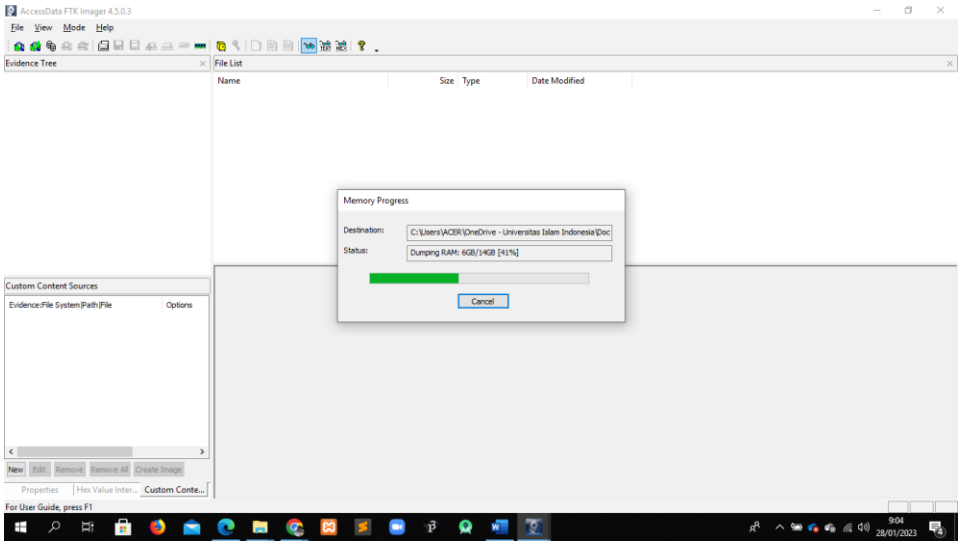
		pelaku menggunakan Google Drive terjadi pada rentang bulan Maret 2022 hingga Desember 2022
Where	Dimana peristiwa berlangsung?	Dalam penyelidikan dengan *tools* tidak ditemukan lokasi
Why	Mengapa pelaku melakukan hal tersebut?	Pelaku memanfaatkan Google Drive untuk menghindari temuan bukti fisik jika tertangkap
How	Bagaimana penyidik melakukan proses forensik?	Penyidik menggunakan metode forensik NIST sesuai dengan kaidah dan langkah-langkahnya serta menggunakan *tools* pendukung seperti DB browser, FTK Imager, Magnet Axiom.

Tabel 4.6 5W + 1H mengenai hasil proses forensik.

Sayangnya peneliti tidak menemukan dokumen yang terkait langsung dengan skenario yang peneliti buat. Banyak file-file kosong maupun file yang sebenarnya bukan bagian dari skenario yang dirancang ikut terproses saat dilakukan analisis dan imaging. File gambar beberapa juga tidak terproses 100% hanya sebagian dari gambar yang terproses, selain itu file txt yang terlihat dengan *tools* Magnet Axiom juga bukan bagian dari file skenario justru berisi informasi semacam kode acak. File PDF yang terproses juga bukan bagian dari file skenario yang dipersiapkan untuk proses forensik sendiri. Kebanyakan file yang terproses imaging sendiri berasal dari luar folder yang peneliti siapkan untuk menjalankan skenario sehingga ikut kedalam proses analisis.

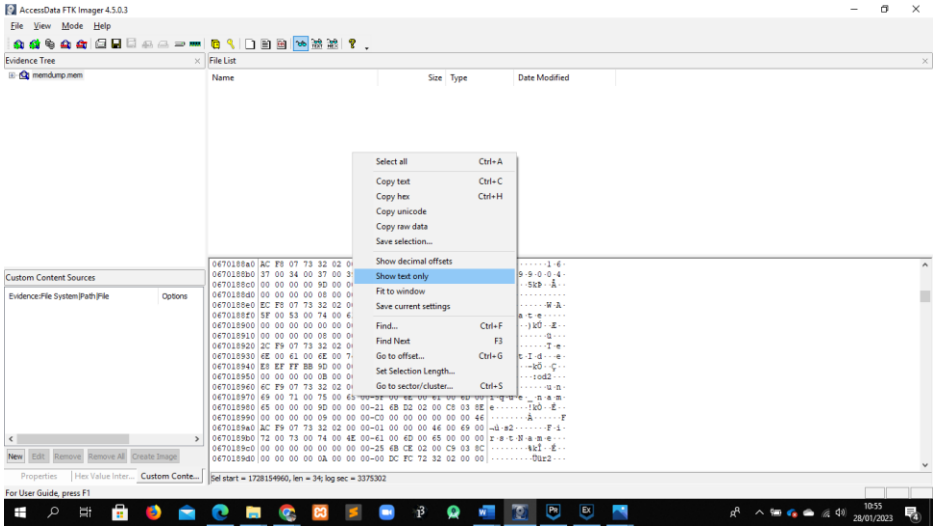
Dalam penelitian sempat dilakukan pengulangan proses yang dilakukan dengan *tools* Magnet Axiom namun tetap hanya menemukan dokumen file pdf, txt dan gambar yang bukan bagian dari skenario. File file tersebut merupakan hasil analisis dan imaging dengan *tools* Magnet Axiom tetapi file tersebut bukanlah file bagian dari proses skenario penelitian.

Melihat hasil yang didapat maka dilakukan live forensics untuk membuktikan metode forensik NIST apakah cocok untuk melakukan digital forensik pada Google Drive. Proses dilakukan dengan mengacapture RAM, pada proses ini Google drive versi desktop yang digunakan dalam keadaan sedang login dan posisi mode mirror files yang mana file dalam google drive dapat diakses secara offline.



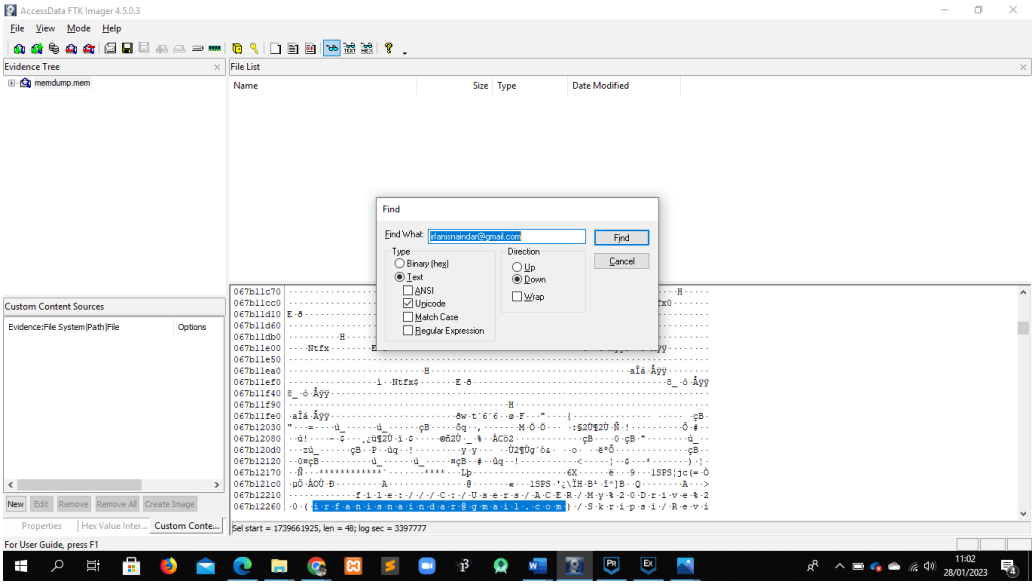
Gambar 4.22 Proses live forensic dengan *tools* FTK Imager.

Proses capture RAM sendiri dilakukan dengan *tools* FTK Imager dengan mengklik tombol capture memory yang ada pada *tools*.



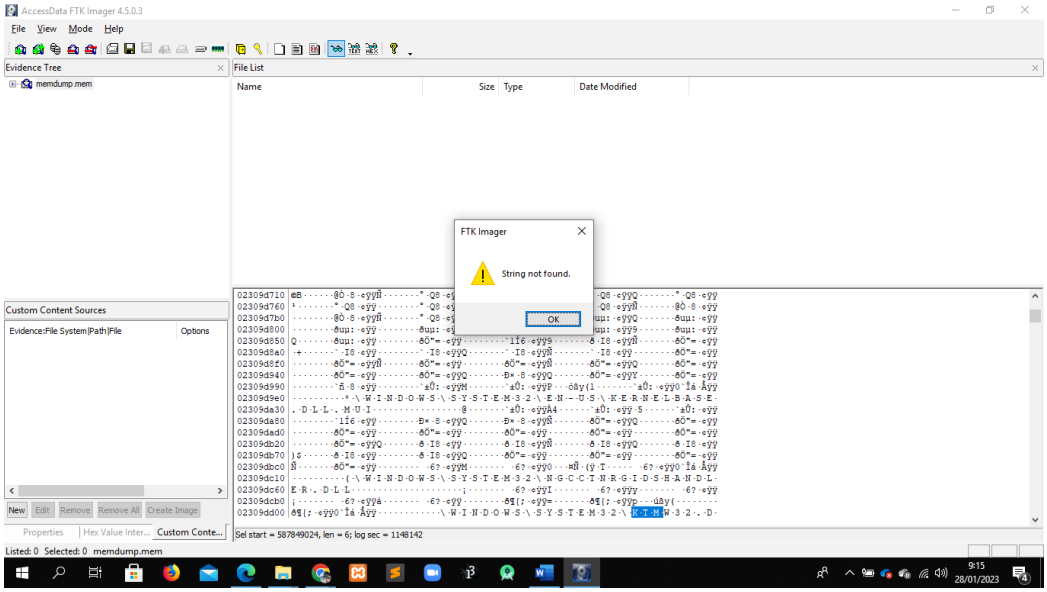
Gambar 4.23 Merubah tampilan hasil capture memory menjadi show text only.

Setelah berhasil, berikut tampilan dari proses capture memory, untuk melacak informasi Google drive, dirubah tampilannya dengan show text only.



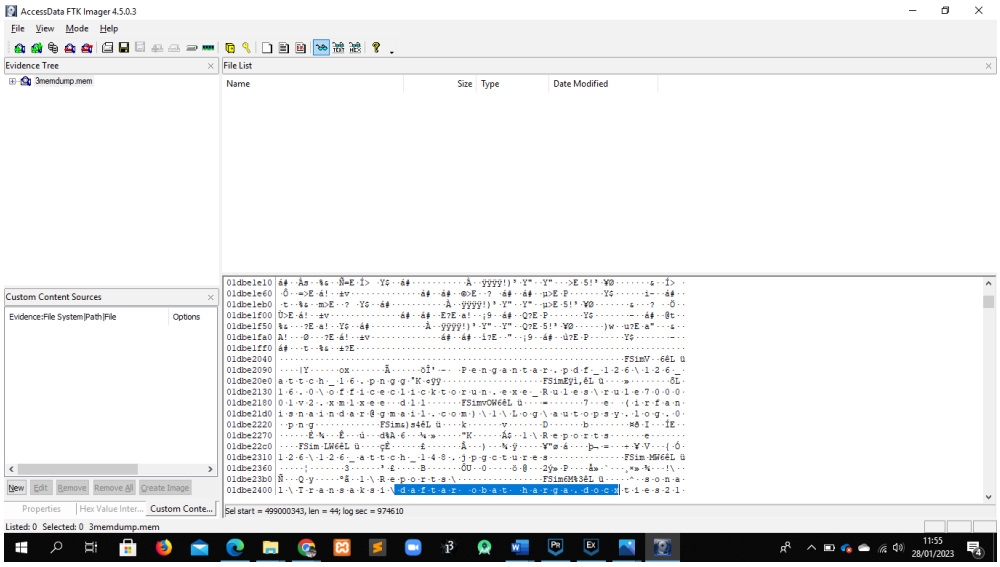
Gambar 4.24 Proses mencari alamat email dengan FTK Imager.

Berikut tampilan dari hasil capture memory setelah dirubah tampilannya ke show text only, lalu dilakukan pencarian dengan menekan ctrl+F dan mengetikan alamat email yang digunakan pada akun Google Drive, hasilnya alamat email dapat ditemukan.

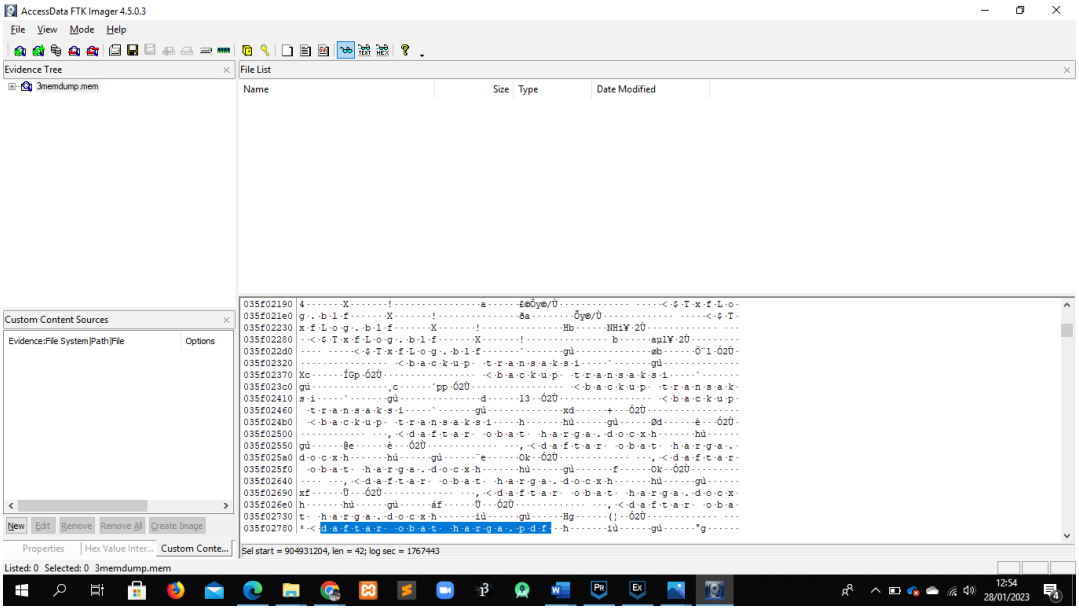


Gambar 4.25 Proses mencari password akun Google Drive.

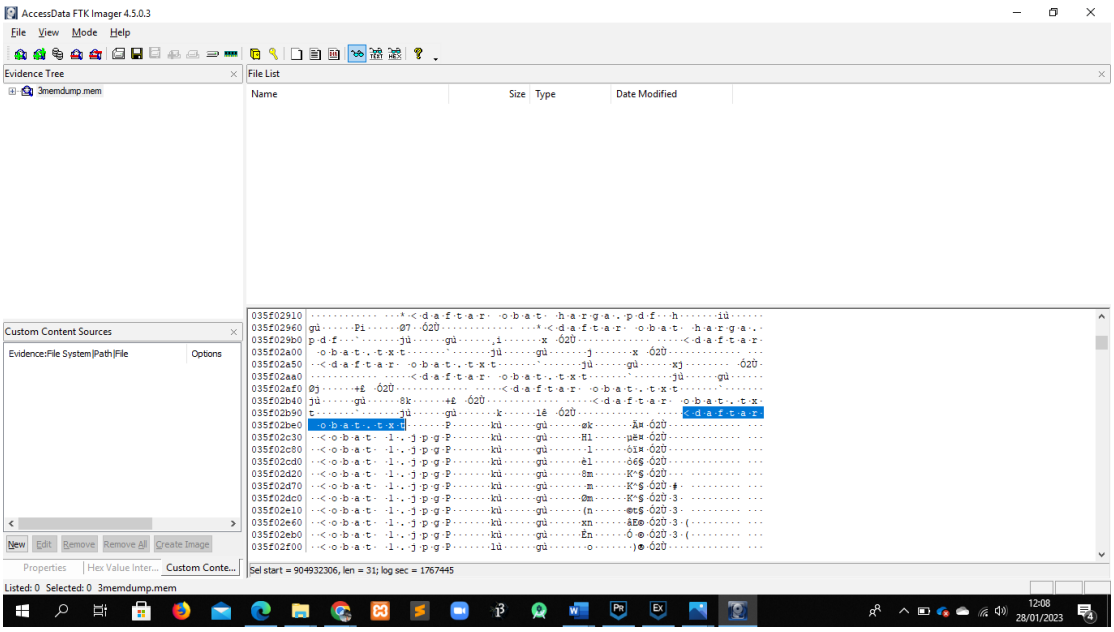
Namun, saat dilakukan pencarian pada password sayangnya tidak dapat ditemukan. Akhirnya dicoba melakukan pencarian pada file percobaan, seperti file daftar obat harga.docx, daftar obat harga.pdf, daftar obat.txt, obat 1.jpg berdasarkan skenario. Hasilnya dapat ditemukan, meskipun sebenarnya file tersebut telah dihapus sebelumnya.



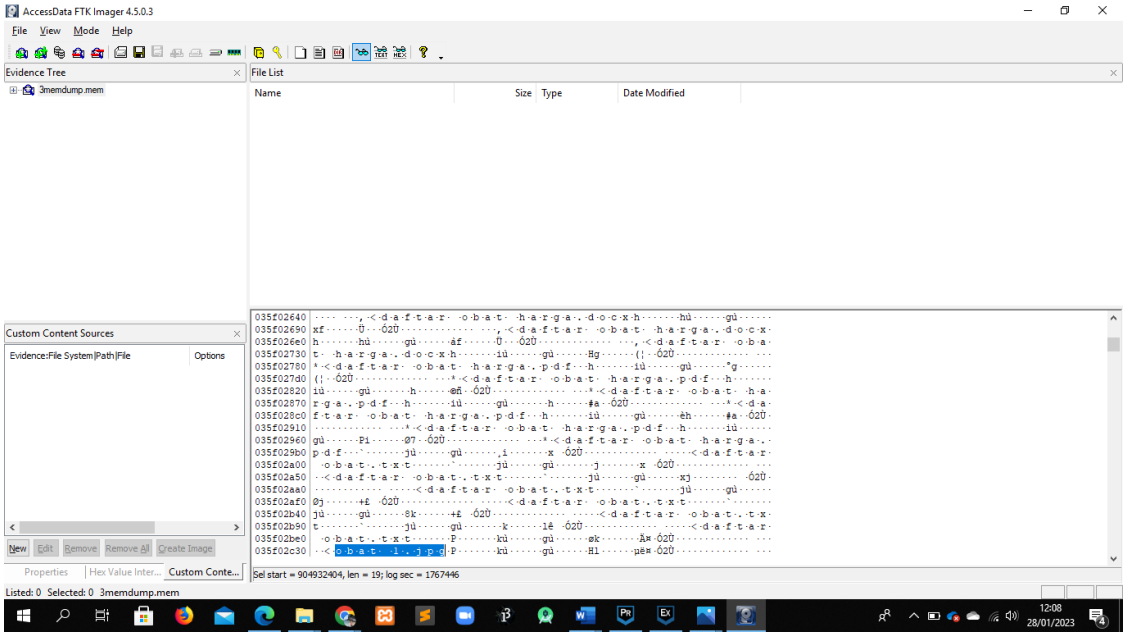
Gambar 4.26 File daftar obat harga.docx



Gambar 4.27 File daftar obat harga.pdf



Gambar 4.28 File daftar obat.txt



Gambar 4.29 File obat 1.jpg

Dari hasil live forensic diatas dengan menggunakan *tools* FTK Imager dilakukan capture memory ditemukan alamat email yang digunakan pada akun Google Drive, namun sayangnya password sendiri tidak dapat ditemukan. Sedangkan untuk file yang digunakan sebagai skenario percobaan forensic dapat ditemukan semuanya dari hasil live forensics dengan *tools* FTK Imager.

4.1.5 Perbandingan *Tools* Forensik

Tools yang digunakan untuk perbandingan adalah Magnet Axiom dan FTK Imager. Hasil yang didapatkan dari masing-masing *tools* melalui proses yang berbeda, Magnet Axiom dengan mengakuisisi folder Google Drive sendiri sedangkan FTK Imager dengan mengcapture memory pada laptop sendiri. Baik Magnet Axiom maupun FTK Imager sama-sama belum bisa menemukan file yang digunakan dalam proses skenario forensic yang telah dibuat. Magnet Axiom justru mengakuisisi file dan data yang tidak digunakan dalam proses skenario forensik yang telah dibuat, sedangkan FTK Imager sendiri juga tidak menemukan file maupun data yang terlibat untuk proses skenario forensic, namun FTK Imager sempat mengcapture file yang digunakan dalam proses forensik, meskipun hanya sebatas mengcapture nama file dan tidak mengakuisisi file tersebut. Selain itu FTK Imager juga menemukan email yang digunakan pada akun Google Drive.

BAB V
KESIMPULAN

Penelitian diatas dilakukan berdasarkan metode forensik NIST yang mana setiap langkah diberi penjelasan sesuai prosedur dan skenario yang dibuat. Adapun dari hasil penelitian yang telah dilakukan penulis tidak menemukan artefak-artefak yang sebagiamana mesti terdapat pada lokasi folder Google Drive. Artefak yang peneliti temukan beberapa diantaranya justru kosong tidak ada informasi yang bisa didapatkan setelah diakses dengan *tools* DB Browser. Lebih lanjut peneliti melakukan imaging dengan *tools* Magnet Axiom dengan harapan menemukan file yang terkait langsung dengan Google Drive. Tetapi *tools* Magnet Axiom menganalisis file artefak berupa gambar, dokumen PDF dan txt yang mana bukan merupakan file yang terkait dengan proses penelitian degan skenario yang berlangsung tanpa menemukan file penting lainnya. Menurut peneliti, berdasalkan hasil yang didapatkan, metode forensik NIST kurang cocok untuk melakukan proses digital forensik pada Google Drive. Peneliti berargumen Google Drive yang digunakan peneliti merupakan versi terbaru yakni Google Drive File Stream mempengaruhi file artefak yang ditemukan, mengingat file yang didapatkan tidak terkait dengan penelitian. Saran kepada penelitian berikutnya untuk dapat menganalisis lebih lanjut mengapa file artefak yang sebagaimana seharusnya ada menjadi tidak ada. Selain itu diharapkan juga dapat menggunakan *tools* forensik yang berbeda dengan harapan dengan *tools* yang berbeda dapat menemukan artefak maupun informasi lainnya selama melakukan proses digital forensik.

DAFTAR PUSTAKA

Baterna, Q. (2022). *5 Reasons Why Google Drive Is a Security Risk*. Makeuseof.Com. https://www.makeuseof.com/why-google-drive-is-a-security-risk/

Furht, B., & Escalante, A. (2008). Handbook Of *Cloud computing*. In *Cal. App. 4th* (Vol. 165, Issue No. B203726). http://scholar.google.com/scholar?as_q=internet&num=100&as_epq=identity+theft&as_oq=&as_eq=&as_occt=any&as_sauthors=&as_publication=&as_ylo=1994&as_yhi=2010&as_sdt=4&as_sdts=5&btnG=Search+Scholar&hl=en&num=100#12

Ivan, E., Mulkan, L., & Syaifudin, Z. (2012). *2012 Pengantar Cloud computing Pengantar Cloud computing*.

Manuhutu, M. A., Muttaqin, M., Irmayani, D., Tamara, T., Gustiana, Z., Hazriani, H., Manullang, S. O., Jamaludin, J., Iskandar, A., Negara, E. S., & others. (2021). *Pengantar Forensik Teknologi Informasi*. Yayasan Kita Menulis. https://books.google.co.id/books?id=urclEAAAQBAJ

Maramis, M. R. (2015). Peran Ilmu Forensik dalam Penyelesaian Kasus Kejahatan Seksual dalam Dunia Maya (Internet). *Jurnal Ilmu Hukum*, *2*(7), 42–53.

Mushlihudin, M., & Nofiyan, A. (2021). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology. *Cybernetics*, *4*(02), 11–23. https://doi.org/10.29406/cbn.v4i02.2287

Nasirudin, N., Sunardi, S., & Riadi, I. (2020). Analisis Forensik *Smarthphone* Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, *5*(1), 89. https://doi.org/10.32493/informatika.v5i1.4578

NIST. (2020). NIST - NISTIR 8006 - NIST *Cloud computing* Forensic Science Challenges. *National Institute of Standards and Technology Interagency or Internal Report*. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf

Standarku, A. (2021). *Mengenal Organisasi Standar NIST*. Standarku.Com. https://standarku.com/mengenal-organisasi-standar-nist/#:~:text=Didirikan pada 1 Maret 1901,(Departemen Perdagangan Amerika Serikat).

Sulianta, F. (2013). *Komputer Forensik*. Elex Media Komputindo. https://books.google.co.id/books?id=Z01bDwAAQBAJ

Baterna, Q. (2022). *5 Reasons Why Google Drive Is a Security Risk*. Makeuseof.Com. https://www.makeuseof.com/why-google-drive-is-a-security-risk/

Furht, B., & Escalante, A. (2008). Handbook Of *Cloud computing*. In *Cal. App. 4th* (Vol. 165, Issue No. B203726). http://scholar.google.com/scholar?as_q=internet&num=100&as_epq=identity+theft&as_oq=&as_eq=&as_occt=any&as_sauthors=&as_publication=&as_ylo=1994&as_yhi=2010&as_sdt=4&as_sdts=5&btnG=Search+Scholar&hl=en&num=100#12

Ivan, E., Mulkan, L., & Syaifudin, Z. (2012). *2012 Pengantar Cloud computing Pengantar Cloud computing*.

Budidarma, J. M. I. (2019). *Jurnal MIB Volume 3 No 3 Juli 2019*. Green Press. https://books.google.co.id/books?id=jDunDwAAQBAJ

Manuhutu, M. A., Muttaqin, M., Irmayani, D., Tamara, T., Gustiana, Z., Hazriani, H., Manullang, S. O., Jamaludin, J., Iskandar, A., Negara, E. S., & others. (2021). *Pengantar Forensik Teknologi Informasi*. Yayasan Kita Menulis. https://books.google.co.id/books?id=urclEAAAQBAJ

Maramis, M. R. (2015). Peran Ilmu Forensik dalam Penyelesaian Kasus Kejahatan Seksual dalam Dunia Maya (Internet). *Jurnal Ilmu Hukum*, *2*(7), 42–53.

Mushlihudin, M., & Nofiyan, A. (2021). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology. *Cybernetics*, *4*(02), 11–23. https://doi.org/10.29406/cbn.v4i02.2287

Nasirudin, N., Sunardi, S., & Riadi, I. (2020). Analisis Forensik *Smarthphone* Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, *5*(1), 89. https://doi.org/10.32493/informatika.v5i1.4578

NIST. (2020). NIST - NISTIR 8006 - NIST *Cloud computing* Forensic Science Challenges. *National Institute of Standards and Technology Interagency or Internal Report*. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf

Saad, S. K., Umar, R., & Fadlil, A. (2020). Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIST. *SEMINAR NASIONAL Dinamika Informatika 2020 Universitas PGRI Yogyakarta*, 119–123.

Standarku, A. (2021). *Mengenal Organisasi Standar NIST*. Standarku.Com. https://standarku.com/mengenal-organisasi-standar-nist/#:~:text=Didirikan pada 1 Maret 1901,(Departemen Perdagangan Amerika Serikat).

Sulianta, F. (2013). *Komputer Forensik*. Elex Media Komputindo. https://books.google.co.id/books?id=Z01bDwAAQBAJ

Obbayi, L. (2019). *Computer forensics: Chain of custody [updated 2019]*. Https://Resources.Infosecinstitute.Com/. https://resources.infosecinstitute.com/topic/computer-forensics-chain-custody/#:~:text=What is the chain of,control%2C transfer%2C and analysis.

Manuhutu, M. A., Muttaqin, M., Irmayani, D., Tamara, T., Gustiana, Z., Hazriani, H., Manullang, S. O., Jamaludin, J., Iskandar, A., Negara, E. S., & others. (2021). *Pengantar Forensik Teknologi Informasi*. Yayasan Kita Menulis. https://books.google.co.id/books?id=urclEAAAQBAJ

Giap, Y. C., Riki, R., Kurnaedi, D., Nursanty, E., Nugroho, M. A., Simarmata, J., Ardilla, Y., & Limbong, T. (2020). *Cloud computing: Teori dan Implementasi*. Yayasan Kita Menulis. https://books.google.co.id/books?id=7g3uDwAAQBAJ

Sulianta, F. (2013). *Komputer Forensik*. Elex Media Komputindo. https://books.google.co.id/books?id=Z01bDwAAQBAJ

Wolff, J. (2020). *Criminals Are Using Google Drive to Infect Hospitals With Ransomware*. Https://Slate.Com/. https://slate.com/technology/2020/11/ryuk-trickbot-hospital-ransomware-google-drive.html

Sejarah Perkembangan Penyimpanan Komputer (Storage). (2022). Jalansenja.Com. https://jalansenja.com/sejarah-perkembangan-penyimpanan-komputer-storage/

Baterna, Q. (2022). *5 Reasons Why Google Drive Is a Security Risk*. Makeuseof.Com. https://www.makeuseof.com/why-google-drive-is-a-security-risk/

Furht, B., & Escalante, A. (2008). Handbook Of *Cloud computing*. In *Cal. App. 4th* (Vol. 165, Issue No. B203726). http://scholar.google.com/scholar?as_q=internet&num=100&as_epq=identity+theft&as_oq=&as_eq=&as_occt=any&as_sauthors=&as_publication=&as_ylo=1994&as_yhi=2010&as_sdt=4&as_sdts=5&btnG=Search+Scholar&hl=en&num=100#12

Ivan, E., Mulkan, L., & Syaifudin, Z. (2012). *2012 Pengantar Cloud computing Pengantar Cloud computing*.

Manuhutu, M. A., Muttaqin, M., Irmayani, D., Tamara, T., Gustiana, Z., Hazriani, H., Manullang, S. O., Jamaludin, J., Iskandar, A., Negara, E. S., & others. (2021). *Pengantar Forensik Teknologi Informasi*. Yayasan Kita Menulis. https://books.google.co.id/books?id=urclEAAAQBAJ

Maramis, M. R. (2015). Peran Ilmu Forensik dalam Penyelesaian Kasus Kejahatan Seksual dalam Dunia Maya (Internet). *Jurnal Ilmu Hukum*, *2*(7), 42–53.

Mushlihudin, M., & Nofiyan, A. (2021). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology. *Cybernetics*, *4*(02), 11–23. https://doi.org/10.29406/cbn.v4i02.2287

Nasirudin, N., Sunardi, S., & Riadi, I. (2020). Analisis Forensik *Smarthphone* Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, *5*(1), 89. https://doi.org/10.32493/informatika.v5i1.4578

NIST. (2020). NIST - NISTIR 8006 - NIST *Cloud computing* Forensic Science Challenges. *National Institute of Standards and Technology Interagency or Internal Report*. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf

Saad, S. K., Umar, R., & Fadlil, A. (2020). Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIST. *SEMINAR NASIONAL Dinamika Informatika 2020 Universitas PGRI Yogyakarta*, 119–123.

Standarku, A. (2021). *Mengenal Organisasi Standar NIST*. Standarku.Com. https://standarku.com/mengenal-organisasi-standar-nist/#:~:text=Didirikan pada 1 Maret 1901,(Departemen Perdagangan Amerika Serikat).

Sulianta, F. (2013). *Komputer Forensik*. Elex Media Komputindo. https://books.google.co.id/books?id=Z01bDwAAQBAJ

Baterna, Q. (2022). *5 Reasons Why Google Drive Is a Security Risk*. Makeuseof.Com. https://www.makeuseof.com/why-google-drive-is-a-security-risk/

Furht, B., & Escalante, A. (2008). Handbook Of *Cloud computing*. In *Cal. App. 4th* (Vol. 165, Issue No. B203726). http://scholar.google.com/scholar?as_q=internet&num=100&as_epq=identity+theft&as_oq=&as_eq=&as_occt=any&as_sauthors=&as_publication=&as_ylo=1994&as_yhi=2010&as_sdt=4&as_sdts=5&btnG=Search+Scholar&hl=en&num=100#12

Ivan, E., Mulkan, L., & Syaifudin, Z. (2012). *2012 Pengantar Cloud computing Pengantar Cloud computing*.

Laudon, K. C., & Laudon, J. P. (n.d.). *Management Information Systems THIRTEENTH EDITION GLOBAL EDITION*.

Manuhutu, M. A., Muttaqin, M., Irmayani, D., Tamara, T., Gustiana, Z., Hazriani, H., Manullang, S. O., Jamaludin, J., Iskandar, A., Negara, E. S., & others. (2021). *Pengantar Forensik Teknologi Informasi*. Yayasan Kita Menulis. https://books.google.co.id/books?id=urclEAAAQBAJ

Maramis, M. R. (2015). Peran Ilmu Forensik dalam Penyelesaian Kasus Kejahatan Seksual dalam Dunia Maya (Internet). *Jurnal Ilmu Hukum*, *2*(7), 42–53.

Mushlihudin, M., & Nofiyan, A. (2021). Analisis Forensik pada Web Phishing Menggunakan

Metode National Institute of Standards and Technology. *Cybernetics*, *4*(02), 11–23. https://doi.org/10.29406/cbn.v4i02.2287

Nasirudin, N., Sunardi, S., & Riadi, I. (2020). Analisis Forensik *Smarthphone* Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, *5*(1), 89. https://doi.org/10.32493/informatika.v5i1.4578

NIST. (2020). NIST - NISTIR 8006 - NIST *Cloud computing* Forensic Science Challenges. *National Institute of Standards and Technology Interagency or Internal Report*. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf

Saad, S. K., Umar, R., & Fadlil, A. (2020). Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIST. *SEMINAR NASIONAL Dinamika Informatika 2020 Universitas PGRI Yogyakarta*, 119–123.

Standarku, A. (2021). *Mengenal Organisasi Standar NIST*. Standarku.Com. https://standarku.com/mengenal-organisasi-standar-nist/#:~:text=Didirikan pada 1 Maret 1901,(Departemen Perdagangan Amerika Serikat).

Sulianta, F. (2013). *Komputer Forensik*. Elex Media Komputindo. https://books.google.co.id/books?id=Z01bDwAAQBAJ