JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 2 Bulan September - Page: 390-399

Penerapan Digital Forensics Research Workshop Dalam Akuisisi Evidence Forensik Aplikasi Snack Video

Ilham Faisal, Arief Budiman, Elsya Indah Fitiria

[1] Fakultas Teknik, Teknik Informatika, Universitas Harapan, Medan, Indonesia
[2] Fakultas, Teknik Informatika, Universitas Harapan, Medan, Indonesia
Email: elsaindah304@email.com

Abstrak

Tersedia media penyebaran informasi yang berkembang saat ini salah satunya ditandai dengan hadirnya media sosial yang sering diakses masyarakat. Layanan media sosial yang sering diakses masyarakat diantaranya adalah *Snack Video*. Efek positif yang ditimbulkan dari penggunaan media sosial dapat saling berinteraksi dengan pengguna lain serta memberikan video konten *random*. Penggunaan media sosial tidak hanya berdampak positif, tetapi juga dapat disalahgunakan sebagai sarana untuk melakukan hal hal yang merugikan. Salah satu hal merugikan yang sering terjadi adalah *cyberchrime* seperti menyebarkan fitnah, *drug tafficking, selfharm* sampai penyebaran video asusila. Fitur membuat video pendek menjadi fitur yang digunakan pelaku kejahatan untuk mengirimkan informasi kejahatan kepada pengguna lain. Pelaku mencoba meng*upload* video mengatasnamakan korban lalu menghapus video tersebut. Oleh karena itu, diperlukan penerapan metode forensik digital untuk membantu pihak berwajib mengungkap bukti kejahatan yang coba disingkirkan oleh pelaku. Dengan kerangka kerja *Digital Forensics Research Workshop* dimana tahap forensik *identification, preservation, collection, examination, analysis,* dan *presentation* dalam menemukan bukti kejahatan digital. Menggunakan 2 alat forensik yaitu *Oxygen Forensic* dan *Magnet Axiom* untuk mengumpulkan bukti, hasil yang di dapat disajikan dalam bentuk *report* dan bukti menghasilkan *file text chat,* video kontex, *image, caption, usertag* dan *hastag*. Perbandingan kemampuan *tools* forensik memiliki keakuratan serta tingkat persentase berbeda *Oxygen Forensic* yakni 100 % dan *Magnet Axiom* yakni 83,3% dalam memperoleh bukti. Barang bukti digital dapat digunakan sebagai alat bukti yang menguatkan dalam suatu gugatan.

Kata Kunci: Media Sosial, Cybercrime, Digital Forensik, DFRWS

Abstract

There are media for disseminating information that is developing today, one of which is marked by the presence of social media that is often accessed by the public. Social media services that are often accessed by the public include video snacks. The positive effects caused by the use of social media can interact with other users and provide random content videos. The use of social media is not only good, but can also be misused as a means to do harm. One of the detrimental things that often happens is cyberchrime such as spreading slander, drug tafficking, selfharm to the spread of immoral videos. The feature of making short videos is one of the features used by criminals to send crime information to other users. The perpetrator tries to upload a video on behalf of the victim and then deletes the video. Therefore, it is necessary to apply digital forensic methods to help the authorities uncover evidence of crimes that are tried to be removed by perpetrators. With the framework of Digital Forensics Research Workshop where the forensic identification, preservation, collection, examination, analysis, and presentation stages in finding evidence of digital crimes. Using 2 forensic tools namely Oxygen Forensic and Magnet Axiom to collect evidence, the results can be presented in the form of reports and evidence produces text chat files, video contexts, images, captions, usertags and hashtags. The comparison of the ability of forensic tools has the accuracy and different percentage levels of Oxygen Forensic, which is 100% and Magnet Axiom, which is 83.3% in obtaining evidence. Digital evidence can be used as corroborating evidence in a lawsuit.

Keywords: Social Media, Cyberchrime, Forensic Digital, DFRWS.

1. PENDAHULUAN

Pemanfaatan teknologi dalam sistem komunikasi memberikan keuntungan bagi individu manusia *Smartphone* berbasis *Android* dengan jumlah pengguna terbanyak adalah salah satu contoh kemajuan teknologi tersebut. Namun, dampak negatif dari penggunaan *smartphone* adalah resiko pencurian atau penghapusan data yang dapat menghilangkan bukti digital kejahatan yang dilakukan oleh pelaku. Berkembangnya media sosial dan aplikasi konten video beserta dengan *Instan Messenger* telah memudahkan terjadinya banyak kejahatan di dunia maya. Semakin banyak pengguna media sosial, maka semakin meningkat pula kasus kejahatan di dunia maya, seperti pencemaran nama baik, *bullying*, penipuan, serta penyebaran video ujaran kebencian dan video asusila yang semakin marak terjadi. Salah satu jejaring sosial yang populer di dunia maya adalah *Snack Video* yang rentan terhadap kejahatan *cybercrime Snack Video* sebuah aplikasi peranti bergerak yang memungkinkan pengguna untuk berbagi video. Pada tahun 2020, *Snack Video* menjadi aplikasi sosial media paling populer di Indonesia, dengan jumlah pengguna sekitar 100 juta yang menempatkan aplikasi ini diperingkat pertama pada *Play Store* Indonesia[1].

Aplikasi *Snack Video* adalah sebuah aplikasi media sosial berbasis video pendek yang dikembangkan oleh Kuaishou *Technology*, Perusahaan asal China dalam aplikasi *Snack Video*, pengguna dapat membuat dan membagikan

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 2 Bulan September - Page: 390-399

video pendek dengan durasi *maksimal* 60 detik yang dapat dihias dengan berbagai *filter*, musik, dan efek kreatif lainnya[2].

Kejahatan yang dilakukan tersebut dapat ditanggulangi dengan menggunakan kemajuan teknologi yaitu digital forensik. Digital forensik adalah sebuah bidang ilmu pengetahuan dan teknologi komputer yang digunakan untuk membantu dalam pembuktian hukum, terutama untuk mengungkap kejahatan yang terkait dengan penggunaan teknologi tinggi seperti kejahatan komputer. Dalam digital forensik, bukti-bukti digital diperoleh secara ilmiah sehingga dapat digunakan sebagai alat bukti yang sah dalam menjerat pelaku kejahatan[3]. Para ahli digital forensik dalam melakukan investigasi digital forensik, terdapat beberapa model mengenai proses investigasi digital forensik termasuk *National Institute of Justice* (NIJ*), National Institute of Standard and Technology* (NIST), *Digital Forensics Research Workshop* (DFRWS), *Association of Chief Police Officers* (ACPO), *Integrated Digital Forensic Investigation Framework v*2 (IDFIF)[4]

Bukti digital adalah informasi yang disimpan atau ditransmisikan dalam bentuk biner yang dapat diandalkan di pengadilan bukti digital tersebut dapat ditemukan pada *hard drive* komputer, ponsel, asisten pribadi digital (PDA), CD, dan kartu *flash* di kamera digital, dan tempat-tempat lainnya[5]. Terdapat banyak *Tools* Forensik yang dapat digunakan untuk menemukan jejak digital tersebut yaitu *Magnet Axiom, Oxygen Forensic, MOBILedit Forensic Express Pro,Autopsy,*dll[6]. Media sosial adalah Media Sosial merupakan fase perubahan bagaimana orang menemukan,membaca dan membagikan berita, informasi, dan konten kepada orang lain.[7]-[8]

Penelitian terkait juga dilakukan dengan judul Akuisisi Bukti Digital Pada Aplikasi Tamtam Messenger Menggunakan Metode NIJ[9] dengan mendapatkan hasil Percakapan berupa pesan yang dikirim oleh pelaku kepada korban yang terindikasi adanya kejahatan *cyberbulyying* dalam aplikasi *TamTam Messenger* yang telah dihapus dapat dikembalikan melalui tools *MobileEdit forensic.* Metode national institute of justice (NIJ) dalam proses identifikasi barang bukti dari aplikasi *TamTam Messenger* pada *smartphone android* dapat digunakan untuk akuisisi bukti digital. *tools MobileEdit forensic* yang digunakan berjalan baik dan dapat memenuhi kebutuhan pencarian barang bukti. Penelitian dengan menggunakan metode DFRWS[10] mendapatkan hasil yaitu proses forensik berhasil mendapatkan informasi berupa data pengguna dan aktivitas transaksi yang ditersimpan pada perangkat *smartphone.* Dari perhitungan angka *indeks* data aktivitas yang dilakukan pada saat simulasi dan data yang berhasil ditemukan dengan *tools* forensik yaitu sebesar 100%. Pada penelitian Investigasi dan Analisis Forensik Digital Pada Percakapan Grub *Whatsapp* Menggunakan NIST SP 800-86 dan *Support Vector Machine* [11] hasil yang didapat Pada penelitian ini investigasi dan analisis forensik mengikuti standarisasi NIST SP 800-86, yaitu *Collection, Examination, Analysis,* dan *Reporting.* Pada proses *Collection* dan *Examination* telah sesuai dengan standart dalam menjaga keutuhan-barang bukti digital. Sedangkan pada proses Analysis dan *Reporting* dengan algoritma *Support Vector Machine* (SVM). Menghasilkan nilai sentimen negatif pada percakapan grup sebesar 96,21%. Hal ini disebabkan susunan kalimat yang digunakan pada percakapan grup sangat pendek. Percakapan grup tersebut belum menggunakan kaidah Subyek Predikat Obyek Keterangan. Sehingga hasil analisis percakapan pada penelitian ini menggunakan SVM belum optimal. Metode *Live* Forensik Untuk Investigasi Serangan Formjacking Pada *Website Ecommerce* hasil yang didapatkan formjacking dapat berjalan pada keempat *browser* dan dapat mengirimkan paket data berupa detail dari kartu kredit melalui perintah yang berada dalam kode Javascript. Menggunakan Metode NIJ *live* forensik yang kemudian dijalankan dengan tools forensik *FTK Imager 4.5.0*. Berdasarkan hasil dari tahapan-tahapan metode yang telah dilakukan, proses investigasi bukti digitak formjacking pada *website e-commerce* dapat dikatakan bahwa bukti digital berupa data yang valid [12]. Analisa dan Perbandingan Performa *Tools* Forensik Digital pada *Smartphone Android* menggunakan Instant *Messaging Whatsapp* hasil yang diperoleh mendapatkan ekstraksi data yang dilakukan dengan *MOBILedit* maka didapatkan bukti digital berupa 2 gambar, 1 video, *1 voice note*, 2 *log* dan 10 *database*. Sedangkan hasil ekstraksi data menggunakan *Oxygen Forensik,* didapatkan data yaitu 10 kontak, 1 video, 20 pesan percakapan, 1 panggilan, 21 *event log,* dan 2 *data file*, dengan status data yang berhasil *recovery* sebanyak 6 [13].

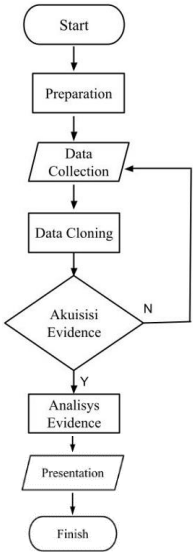
Penelitian ini bertujuan untuk memvalidasi serta menemukan jejak digital yang dihilangkan sebagai bukti dari kejahatan pelaku *cybercrime* dengan menggunakan alat forensik yaitu *Oxygen Forensic* dan *Magnet Axiom* dalam kasus ujaran kebencian dan penyebaran video asusila. Pada penelitian ini menggunakan penerapan metode DFRWS untuk mendapatkan kembali barang bukti digital yang dapat digunakan sebagai alat bukti yang sah dan dapat dipahami oleh penyidik saat menyelesaikan kejahatan *cybercrime.*

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Dalam penyelesaian penelitian ini digunakan tahapan penelitian dan struktur metode agar hasil akhir yang didapat tidak menyimpang dari tujuan sebelumnya. Berikut tahapan penelitian serta struktur metode yang digunakan untuk menyelesaikan penelitian ini

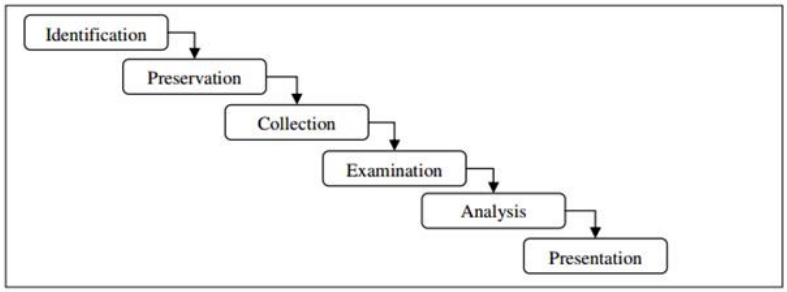
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 2 Bulan September - Page: 390-399



Gambar 2.1 Tahapan Penelitian

1) *Preparation*
   Tahap awal yang dilakukan untuk menyiapkan alat dan bahan serta pengecekan dalam kebutuhan yang diperlukan sebelum melakukan tindakan untuk pencarian bukti digital.
2) Data *Collection*
   Tahap ini melakukan inputan mulai dari pengumpulan data untuk *memfilte*r serta mengukur jenis data-data mana yang tepat dan harus digunakan untuk menuju ke tahap selanjutnya.
3) Data *Cloning*
   Meliputi proses mengambil salinan data yang ada dan menyalinnya ke lokasi baru, sehingga dapat digunakan tanpa mempengaruhi data asli salinan identik dari data yang telah ada. Digunakan data *cloning* juga sebagai antisipasi apabila terjadi kerusakan data.
4) Akuisisi *Evidence*
   Proses pengumpulan bukti digital atau data elektronik dari *smartphone* yang sudah dijalankan dapat berupa *file database*, *dokumen*, atau metadata. Apabila pada saat akuisisi bukti belum sempurna dapat menelusuri kembali pada tahap data *collection*
5) *Analysis Evidence*
   Setelah melakukan akuisisi bukti selanjutnya menganalisis bukti tersebut dilakukan proses untuk mengkoreksi,menafsirkan, dan mengevaluasi informasi atas bukti digital yang sudah diperoleh dari berbagai *tools* forensik sebagai dasar untuk membuat validasi bukti.
6) *Presentation*
   Pada tahap ini merupakan tahap akhir dimana setelah bukti digital sudah diperoleh secara rinci melakukan penyusunan serta pengambilan kesimpulan guna untuk mempersentasikan hasil akhirnya.
7) Selesai

pada proses investigasi yang digunakan metode DFRWS (*Digital Forensics Research Workshop*)[14] dengan langkah-langkah sebagai berikut:



Gambar 2.2 Metode DFRWS

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 2 Bulan September - Page: 390-399

1) Tahap persiapan (*identification* : Menentukan kebutuhan yang diperlukan pada saat proses penyidikan dan pencarian barang bukti oleh tim penyelidik, seperti : mengamankan barang bukti fisik berupa *smartphone* sipelaku kejahatan.
2) Tahap Pemeliharaan *(preservasion)*: Memelihara atau menjaga barang bukti digital dan memastikan keaslian bukt, menyangkal klaim jika barang bukti telah disabotase seperti : pada *smartphone* yang sudah diamankan oleh tim penyelidik di aktifkan fitur *mode* pesawat agar terhindar dari sistem telekomunikasi maupun *internet*.
3) Koleksi *(collection)* : Mengumpulkan barang bukti digital dengan menggunakan *tools* forensik yang dilakukan oleh *investigator* yaitu dengan *tools Oxygen Forensic* dan *Magnet Axiom*.
4) Pemeriksaan *(Examinition):* Setelah proses pengumpulan data. Dilakukan *filter* data untuk memilah data, membatasi data ke bagian tertentu dari sumber data yang dilakukan. Seperti pada *folder data base* yang sudah diekstraksi dengan *tools* forensik terdapat banyak *folder* dan *file* didalamnya, untuk mengetahui data mana yang ingin dilakukan proses analisis dapat melihat 1 per 1 data tersebut contoh terdapat pada *folder chace*.
5) Analisis *(Analisys)*: Proses menentukan dari mana data didapat, data berasal, jenis data. Termasuk kedalam pelacakan bukti, validasi bukti, seperti: menemukan tag video yang sudah dihapus oleh pelaku kejahatan. Menemukannya dengan menelusuri hasil yang sudah diekstraksi sebelumnya terdapat pada *folder database/chace/response/profile_feed.*
6) Presentasi (*Presentation):* Tahap akhir pada metode DFRWS, pembuatan penyajian laporan secara rinci dengan membuat tabel pelaporan dari jumlah barang bukti yang sudah ditemukan pada *tools Oxygen Forensic* maupun *Magnet Axiom*.

2.2 Alat dan Bahan

Alat dan bahan kebutuhan sistem yang digunakan untuk simulasi kasus dalam proses forensik, dan aktifitas penelitian menemukan jejak digital sipelaku kejahatan. Untuk dapat terlaksananya penelitian digunakan kebutuhan sistem yang berupa perangkat keras dan perangkat lunak sebagai berikut.

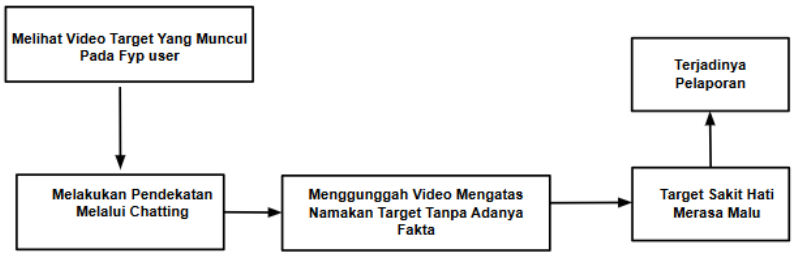
Tabel 2.3 Alat dan Bahan Penelitian

No	Alat dan Software	Deskripsi
1.	Laptop Lenovo	RAM 8 GB. System type 64-bit, Processor AMD 3020e, Windows 10
2.	Handphone Samsung J3	*Rooting*, *Object* penelitian, *Android* OS, v5.1.1 (Lollipop)
3.	*Odin*	*Tools* berbasis windows yang digunakan untuk melakukan rooting pada perangkat android dan laptop selama proses rooting berlangsung.
4.	CF Auto Root (TWRF)	*Tools* yang digunakan untuk melakukan *rooting* pada perangkat android menggunakan aplikasi Odin.
5.	*Root Cheker*	*Tools* yang digunakan untuk memastikan bahwa android sudah berhasil di *rooting.*
6.	*Root Explorer*	*Tool* berbasis android sebagai pendukung yang digunakan untuk mencari data pada android yang sudah di *rooting*
7.	*Magnet Axiom dan Oxygen Forensic*	Tools Forensik
8.	*Snack Video*	Tools yang akan dilakukan investigasi

2.3 Analisis Masalah

Proses mengidentifikasi suatu masalah yang sedang dihadapi dengan menyusun sistem yang saling berkaitan sehingga dapat mempermudah penyelesaian masalah secara efisien. Analisis sistem bertujuan untuk memperoleh jawaban dari sketsa yang sudah disusun.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 2 Bulan September - Page: 390-399

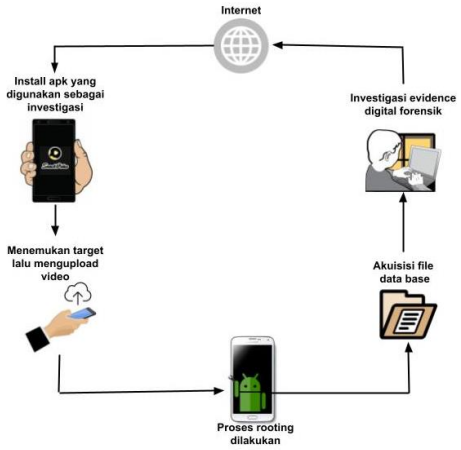


Gambar 2.4 Analisis Masalah

Dalam melakukan proses forensik seperti gambar diatas penelitian ini terlebih dahulu merekayasa dan membuat kasus ujar kebencian serta penyebaran video asusila yang diedukasikan dalam bentuk simulasi, memposting video asusila dengan memberi *caption, tag* pegguna lain dan *hastag* pada halaman beranda *Snack Video* serta *sending image* pada fitur *chatting* melakukan ujar kebencian secara sengaja tanpa adanya fakta yang membenarkan setelah video tersebut diposting dan sudah dilihat orang lain maka pelaku langsung berusaha menghapus postingan tersebut dari *smartphone* miliknya untuk mencoba menghilangkan jejak digital. Setelah terjadi peristiwa tersebut korban merasa sakit hati, malu, tersinggung bahkan kesal atas perbuatan si pelaku kejahatan maka dari itu korban melakukan pelaporan kepada pihak berwajib. Tim ahli forensik melakukan survei pengumpulan data investigasi forensik untuk menemukan akuisisi bukti digital sebagai barang bukti yang sah di dalam persidangan nantinya.

2.4 Analisis Konfigurasi Sistem

Analisis konfigurasi sistem meliputi proses memeriksa dan memahami konfigurasi atau pengaturan suatu sistem pada perangkat lunak. Dalam proses investigasi data digital untuk menemukan bukti digital pada android terlebih dahulu mengubah sistem android menjadi rooting, digunakan proses rooting untuk mendapatkan file data base jejak digital yang akan dieksekusi dengan menggunakan tool forensik.



Gambar 2.5 Analisis Konfigurasi Sistem

2.5 Perhitungan Keberhasilan

Dari rumus perbandingan yang sudah ditemukan dilakukan perhitungan persentase keberhasilan dari barang bukti yang didapatkan oleh *tools Oxygen Forensic dan Magnet Axiom* perhitungan dapat dilakukan sebagai berikut :

$$\text{Persentase Hasil} = \frac{Jumlah\ barang\ bukti\ yang\ ditemukan}{Total\ barang\ bukti\ yang\ akan\ dicari}\ x\ 100$$

Gambar 2.6 Rumus perbandingan [15]

Diketahui : Total barang bukti yang akan dicari : 6
Barang bukti yang ditemukan *Oxygen Forensic* : 6
Barang bukti yang ditemukan *Magnet Axiom* : 5

1) *Oxygen Forensic* : $\frac{6}{6}$ x 100% = 100%
2) *Magnet Axiom* : $\frac{5}{6}$ x 100% = 83,3%

Dari perhitungan yang sudah dilakukan *Oxygen Forensic* bekerja lebih baik dengan menemukan keseluruhan barang bukti

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 2 Bulan September - Page: 390-399

yakni 100%.

HASIL DAN PEMBAHASAN

Dalam metode DFRWS *(Digital Forensic Research Work Shop)* dimulai dari pemeriksaan fisik pada *handphone* yang sudah di tetapkan sebagai barang bukti tahap ini ditentukan sebagai tahapan awal untuk mengidentifikasi oleh pihak penyelidik mendapatkan data yang di perlukan. Proses pengambilan data dilakukan pada saat *handphone* dalam keadaan hidup namun *data seluler* mati dan menggunakan *mode* pesawat dikarenakan untuk mendapatkan keaslian bukti digital. Hasilnya dapat dibuktikan menurut hukum yang berlaku melaporkan hasil awal hingga akhir dalam tahap penyajian yang berisi bukti fisik, bukti digital, dan hasil analisis.

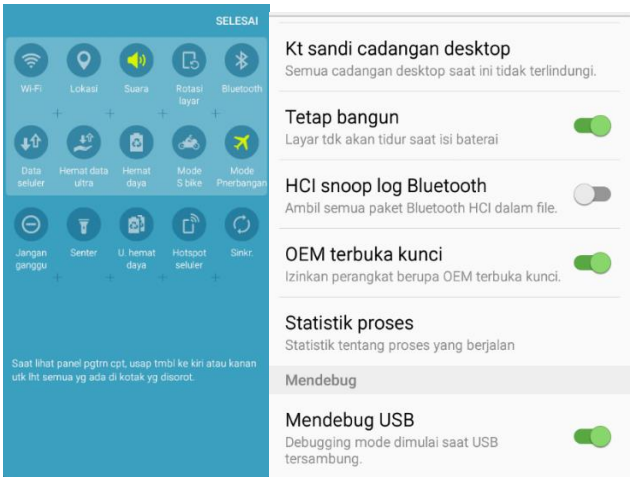
3.1 Identification

Melakukan pemeriksaan untuk kebutuhan penyelidik penelitian ini menggunakan *handphone* sebagai barang bukti fisik kasus ujar kebencian dan penyebaran video asusila dengan parameter bukti digital seperti *text chat, images, video, tag user, dan hastag*. Penelitian ini berhasil mengidentikasi *handphone Samsung Galaxy J3* seperti yang terlihat pada gambar berikut :

Gambar 3.1 Info perangkat

3.2 Preservasion

Menyimpan bukti secara digital demi menjamin keaslian yaitu dengan cara mengisolasi *handphone* dari jaringan telekomunikasi menjadi *mode* pesawat dan mengaktifkan mode *stay awake* agar perangkat tidak tidur dalam posisi *chargering.*



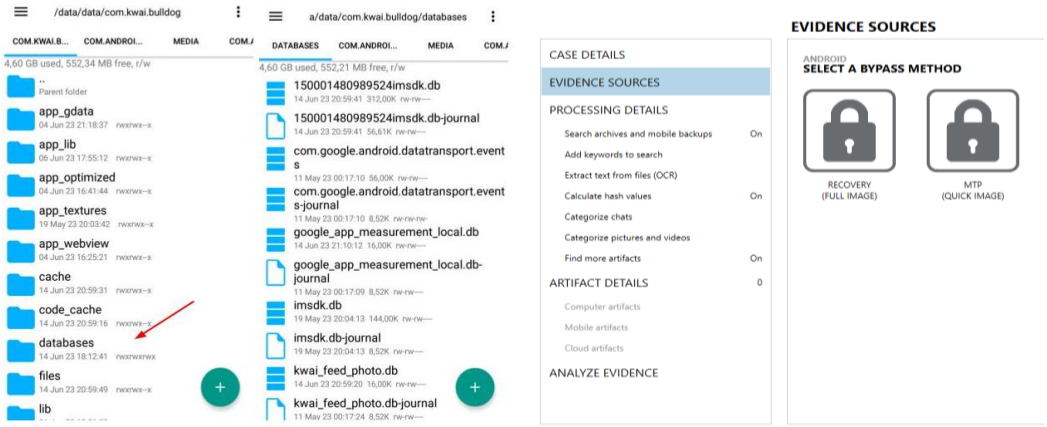
Gambar 3.2 Proses *Air Plan* dan *Stay Awake*

3.3 Collection

Dalam proses pengumpulan bukti digital ini dilakukan dengan bantuan aplikasi *Root Explorer* guna untuk melihat penyimpanan data base dari aplikasi yang sudah di*rooting* berfokus pada Kwaibulldog.com, namun untuk tools magnet axiom tidak diperlukan bantuan dari *root explorer*.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 2 Bulan September - Page: 390-399

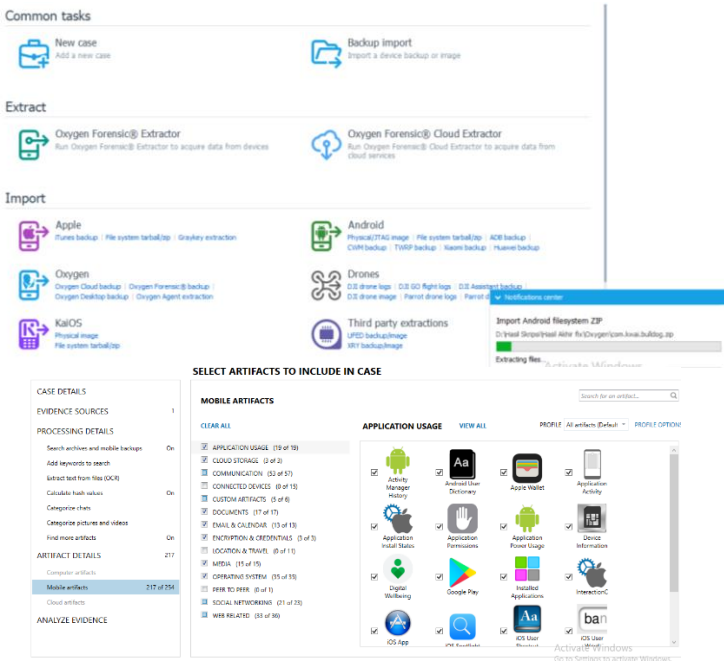


Gambar 3.3 Proses Pengumpulan Pada *Root Explorer dan Magnet Axiom*

3.4 Examinition

Data yang sudah diketahui /data/*com.kwai.bulldog*/ dari perangkat yang terdeteksi sebalumnya folder tersebut diubah dengan format RAR yang nantinya *file* yang ada didalam folder tersebut akan dibaca oleh *Oxygen Forensic* dalam proses pemindahan *file* menjadi RAR

Pada Magnet Axiom Tahap *Examination* dilakukan dengan menggunakan data dari *full image* barang bukti *smartphone* yang sudah dilakukan sebelumnya. Memilih artefak apa yang ingin dilakukan untuk proses analisis.



Gambar 3.4 Proses Examinition Pada *Oxygen Forensik* dan *Magnet Axiom*

3.5 Analysis

Tahap analisis *file* yang sudah di dapat sebelumnya akan saling dihubungkan dengan *tools Oxygen Forensic.* Untuk menemukan *text* chat yang sudah dihapus dapat di baca dengan menggunakan fitur *SQLite Viewer* dalam proses analisis pencarian *text chat* dengan menelusuri 150001480989524imsdk.db terdapat *file* dengan nama *kwai_message* terlihat pada gambar 3.5

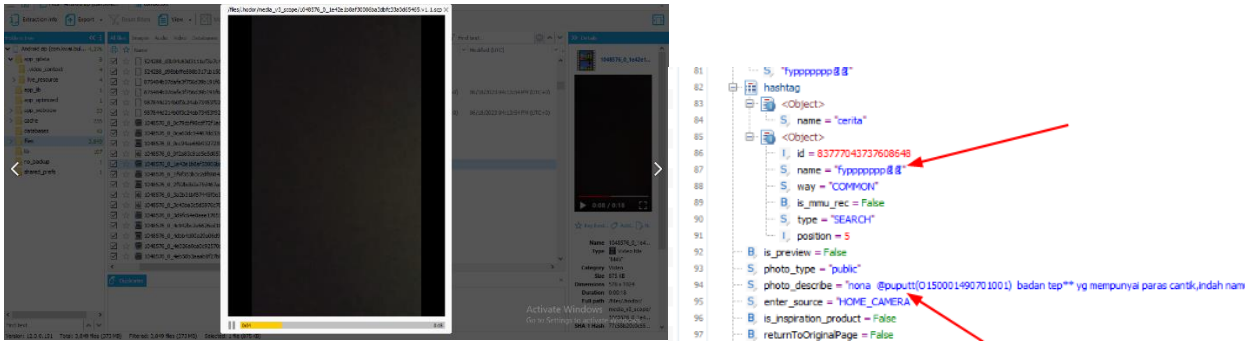
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 2 Bulan September - Page: 390-399

#	unknownTips	placeHolder	contentBytes
269			?Berbicara dan berkomunikasi dengan cara yang bera...
270			☐put
271			☐ayok kita ketemu
272			☐lagi jam istirahat kan
273			gak bisa
274			☐jadi gak mau ni??
275			iya GAK BISA!
276			☐fine liat ja ntr ????
277			1diajak ketemu aja susah jangan sok s*ci jad cwk
278			MUR4H*N!!
279			☐jaga mulutmu ya
280			☐jangan asal ngomong ibab
281			.apa maksud kau bagiin vid gak bener ttg aku ?
282			☐berani2 ya
283			☐jangan kurang AJAR WOI!
284			☐bodo
285			☐seru bukan haaahaha
286			☐jangan semena2 ya
287			☐aku bakal laporin
288			☐udah aku ss chtan ini
289		{"minSeq":0,"maxSeq":1686243317837999}	☐¯??´??

Gambar 3.5 Tampilan *Text Chat* Hujatan yang sudah dihapus

Untuk menemukan bukti video yang sudah dihapus oleh user dengan keterangan *caption* hujatan serta melakukan *tag* pada target dapat ditemukan dengan menelusuri *file* dengan nama 1048576 terlihat pada gambar 3.6. serta terlihat caption hujatan serta taguser atas nama puput

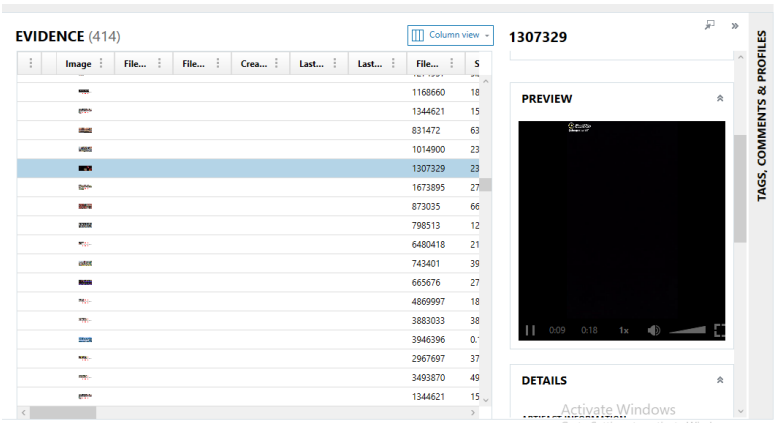


Gambar 3.5 Tampilan Video yang sudah dihapus dan tag *caption* dengan hujatan

Pada *tools forensik Magnet Axiom* melakukan analisis data-data yang sudah didapat dari hasil ekstraksi sebelumnya. Hasil ekstraksi yang didapatkan dari proses penghapusan *text chat*, unggahan video, *sending image* melalui perangkat *Samsung Galaxy J3 2016* pada aplikasi *Snack Video*. Proses analisis bukti untuk mendapatkan video, *image* yang sudah dihapus serta *text* percakapan dengan menelurusi artefak media yang terdapat diperangkat *user*. Mendapatkan video yang sudah dihapus dengan menelusuri artefak video terlihat pada gambar 3.6

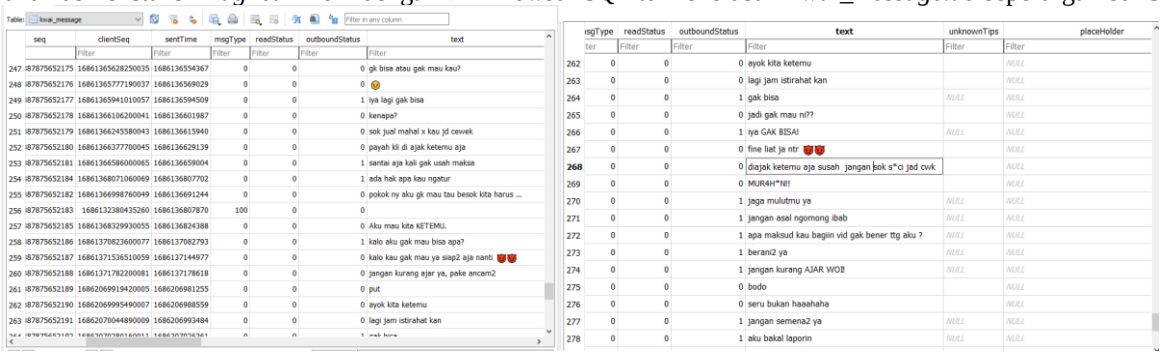
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 2 Bulan September - Page: 390-399



Gambar 3.6 Hasil Ekstaksi Video

Menampilkan hasil *text* percakapan ancaman serta hujatan yang dilakukan *user* kepada target dengan menelusuri membuka hasil ekstaksi *Magnet Axiom* dengan *DB Browser SQ lite* menelusuri *kwai_message.db* seperti gambar 3.7



Gambar 3.7 *Text* Percakapan

3.6 Presentation

Tahapan akhir pada metode DFRWS pembuatan laporan hasil analisis dari proses proses yang sudah dilakukan sebelumnya dan menjelaskan informasi data apa saja yang di temukan serta aspek pendukung oleh tim penyidik. Hasil *repot* yang sudah dilakukan pada *tools Oxygen Forensic* dan *Magnet Axiom* dapat dilihat pada Tabel 3.8

Result Obtained	***Tools Oxygen Forensic***	***Tools Magnet Axiom***
Info User	Ditemukan	Ditemukan
Text Chat	Ditemukan	Ditemukan
Sending Image	Ditemukan	Ditemukan
Video *Context*	Ditemukan	Ditemukan
Tag, Caption Has Tag	Ditemukan	Tidak Ditemukan
Video Fyp	Ditemukan	Ditemukan

4. KESIMPULAN

Teknik yang didapat dalam proses validasi jejak digital pada kasus ujar kebencian dan penyebaran video asusila di *Snack Video* dengan penerapan DFRWS lebih terstruktur. Tahap demi tahap yang digunakan dalam memvalidasi jejak digital berupa identifikasi, pemeliharaan, koleksi, pemeriksaan, analisis, presentasi sangat baik untuk memperoleh bukti digital secara keseluruhan. Sesuai dengan praktik terbaik dalam bidang forensik digital dengan penggunaan *tools Oxygen*

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 2 Bulan September - Page: 390-399

Forensic dan *Magnet Axiom* dalam ekstraksi datanya yang menemukan bukti digital tersebut dari kasus kejahatan *cybercrime*. Berdasarkan barang bukti digital yang ditemukan pada *tools Oxygen Forensic* sebanyak 6 dari total 6 bukti yang didapat. Untuk barang bukti digital pada *tools Magnet Axiom* sebanyak 5 dari 6 total barang bukti. Persentase keberhasilan barang bukti yang ditemukan dari *tools Oxygen Forensic* jauh lebih akurat dibanding dengan *tools Magnet Axiom* yaitu 100% untuk *Oxygen Forensic* dan 83,3% untuk *Magnet Axiom*. Sehingga dari kedua *tools* yang digunakan memiliki perbandingan sekitar 16,7%. Saran untuk penelitian selanjutnya dapat mencoba menggunakan 2 *platform* objek penelitian yang serupa agar mengetahui hasil perbedaan bukti digital yang didapat serta mengetahui tingkat keamanan pada aplikasi yang digunakan. Menggunakan metode penelitian yang berbeda seperti *static forensic* sehingga dapat mengetahui alur yang berbeda dengan penelitian sebelumnya. Serta diharapkan dengan menggunakan lebih banyak data yang diujikan agar hasil yang didapat jauh lebih akurat.

REFERENCES

[1] F. Dehotman, "Perkembangan Snack Video," *Jabar.com, Tribun*, 2020. https://www.google.com/amp/s/jabar.tribunnews.com/amp/2020/07/04/snack-video-masuk-peringkat-pertama-aplikasi-paling-populer-di-google-play-store-indonesia

[2] Sijori.id, "Snack Video," *Minka*, 2020. https://sijori.id/read/snack-video-aplikasi-baru-saingan-berat-tik-tok

[3] Azhar, *Digital Forensic Practical Guidelines For Computer Investigation*. Jakarta: Salemba, 2012.

[4] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. Media Inform. Budidarma*, vol. 6, no. 2, p. 1263, 2022, doi: 10.30865/mib.v6i2.3946.

[5] NIJ.gov, "Defenition of Evidence Forensic," *kemdikbud*, 2022.

[6] H. Herman and A. Yudhana, "Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers," *JURIKOM (Jurnal Ris. Komputer)*, vol. 9, no. 4, p. 1117, 2022, doi: 10.30865/jurikom.v9i4.4738.

[7] L. Tysara, "Pengertian Media Sosial adalah Laman dalam Jaringan Sosial," *Liputan 6.com*. https://www.liputan6.com/hot/read/4844021/pengertian-media-sosial-adalah-laman-dalam-jaringan-sosial-ini-fungsi-dan-jenis-jenisnya

[8] J. Gerung, "Media Sosial Dalam Digital Marketing Kesehatan," in *Geupedia*, 2021, p. 62 halaman. [Online]. Available: https://www.google.co.id/books/edition/Media_Sosial_dalam_Digital_Marketing_Kes/JNZMEAAAQBAJ?hl=id&gbpv=1&dq=media+sosial+adalah&pg=PA62&printsec=frontcover

[9] D. Mualfah, A. Viransa, F. I. Komputer, and U. M. Riau, "Jurnal Software Engineering and Information Systems (SEIS) AKUISISI BUKTI DIGITAL PADA APLIKASI TAMTAM MESSENGER," vol. 3, no. 1, 2023.

[10] M. N. Fadillah *et al.*, "ANALISIS FORENSIK APLIKASI DOMPET DIGITAL PADA SMARTPHONE ANDROID MENGGUNAKAN," vol. 09, no. 02, pp. 265–279, 2022.

[11] M. W. Indriyanto, D. Hariyadi, and M. Habibi, "INVESTIGASI DAN ANALISIS FORENSIK DIGITAL PADA PERCAKAPAN GRUP WHATSAPP MENGGUNAKAN NIST SP 800-86 dan SUPPORT VECTOR MACHINE DIGITAL FORENSICS INVESTIGATION AND ANALYSIS ON WHATSAPP GROUP CHATS USING NIST SP 800-86 AND SUPPORT VECTOR MACHINE," vol. 3, no. 2, pp. 34–38, 2020.

[12] N. Setiawan, A. R. Pratama, and E. Ramadhani, "Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce," *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 7, no. 1, pp. 1–9, 2022, doi: 10.32528/justindo.v7i1.5356.

[13] I. A. Plianda and R. Indrayani, "Analisa dan Perbandingan Performa Tools Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp," vol. 6, pp. 500–506, 2022, doi: 10.30865/mib.v6i1.3487.

[14] M. N. Faiz, *Tahapan-Investigasi-forensik-1*. Purwokerto, 2022.

[15] UMA, "Menghitung Persentase Keberhasilan," 2021. https://manajemen.uma.ac.id/2021/09/cara-menghitung-persentase-beserta-penjelasan-dan-contohnya/