LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
UNIVERSITAS AHMAD DAHLAN
Jl. Geodesi No. 3B Semaki Yogyakarta Telp. 0274 542835, 0274-563515 ext. 1502, 1503 Fax. 0274-542835, Website : lppm.uad.ac.id, email : lppm@uad.ac.id

LPPSURAT PERJANJIAN PELAKSANAAN PENELITIAN

Nomor: PUPS-025/SP3/LPPM-UAD/IV/2019

Pada hari ini, **Senin** tanggal **Delapan** bulan **April** tahun **Dua ribu sembilan belas (08-04-2019)**, kami yang bertandatangan di bawah ini:

1. Nama : **Dr. Widodo, M.Si.**
   Jabatan : Kepala Lembaga Penelitian dan Pengabdian Kepada Masyarakat Universitas Ahmad Dahlan (LPPM UAD), selanjutnya disebut sebagai **PIHAK PERTAMA.**
2. Nama : **SUNARDI, S.T., M.T., Ph.D.**
   Jabatan : Dosen/Peneliti pada Program Studi **S2 Teknik Informatika Program Pascasarjana** Universitas Ahmad Dahlan (UAD), selaku Ketua Peneliti, selanjutnya disebut **PIHAK KEDUA.**

Kedua belah pihak menyatakan setuju dan mufakat untuk mengadakan perjanjian pelaksanaan penelitian untuk selanjutnya disebut Surat Perjanjian Pelaksanaan Penelitian (SP3) dengan ketentuan dan syarat-syarat sebagai berikut.

JUDUL PENELITIAN

Pasal 1

(1) PIHAK PERTAMA memberikan pekerjaan kepada PIHAK KEDUA dan PIHAK KEDUA menyatakan menerima pekerjaan dari PIHAK PERTAMA berupa kegiatan pada skim **Penelitian Unggulan Program Studi (PUPS).**

(2) Judul penelitian sebagaimana dimaksud dalam ayat (1) di atas adalah: **"ORENSIK MEDIA SOSIAL PADA PERANGKAT MOBILE MENGGUNAKAN FRAMEWORK DIGITAL FORENSICS RESEARCH WORKSHOP (DFRWS) ."**

PERSONALIA PELAKSANA PENELITIAN

Pasal 2

Pelaksana kegiatan ini terdiri dari:

Ketua Peneliti	: SUNARDI, S.T., M.T., Ph.D.
Pembimbing/Konsultan	: -
Anggota Peneliti 1	: IMAM RIADI, Dr., M.Kom
Anggota Peneliti 2	:

BENTUK DAN JANGKA WAKTU PERJANJIAN

Pasal 3

PIHAK KEDUA melaksanakan penelitian dalam jangka waktu paling lama **6 (enam) bulan** sejak ditandatangani SP3 ini, dan menyerahkan hasil laporan penelitian sementara kepada PIHAK PERTAMA selambat-lambatnya pada **08 Oktober 2019.**

LUARAN/*OUTPUT* PENELITIAN

Pasal 4

PIHAK KEDUA berkewajiban untuk merealisasikan luaran/*output* penelitian seperti yang dijanjikan dalam proposal penelitian di luar Laporan Hasil Penelitian.

BIAYA PENELITIAN DAN CARA PEMBAYARAN

Pasal 5

PIHAK PERTAMA menyediakan dana pelaksanaan penelitian kepada PIHAK KEDUA sejumlah **Rp 18.500.000,00 (Delapan belas juta lima ratus ribu rupiah)** yang dibebankan pada Anggaran Pendapatan dan Belanja (APB) LPPM UAD Tahun Akademik 2018/2019 dibayarkan melalui rekening bank atas nama Ketua Peneliti oleh Bidang Finansial UAD dengan tahapan sebagai berikut.

(a) **Tahap I sebesar 70% x Rp 18.500.000,00 = Rp 12.950.000,00 (Dua belas juta sembilan ratus lima puluh ribu rupiah)** yang akan dibayarkan selambat-lambatnya dua minggu setelah SP3 ini ditandatangani oleh PARA PIHAK dan PIHAK KEDUA telah mengunggah file scan SP3 ini pada portal UAD.

(b) **Tahap II sebesar 30% x Rp 18.500.000,00 = Rp 5.550.000,00 (Lima juta lima ratus lima puluh ribu rupiah)** yang akan dibayarkan setelah PIHAK KEDUA menyelesaikan seluruh kewajibannya dalam jangka waktu seperti yang dimaksud dalam Pasal 3 serta dinyatakan benar dan lengkap.

PELAKSANAAN PEMBIMBINGAN

Pasal 6

(1) Khusus peneliti skema Penelitian Dosen Pemula (PDP) wajib melakukan pembimbingan atau konsultasi dengan dosen pembimbing penelitiannya paling sedikit 3 (tiga) kali pembimbingan

(2) Pembimbingan sebagaimana dimaksud dalam ayat (1) yaitu pembimbingan dalam hal:
a. penyusunan angket/kuesioner dan atau teknik pengumpulan data lainnya.
b. analisis data dan interpretasinya;
b. penyusunan hasil penelitian, pembahasan, penarikan kesimpulan.

(3) Pembimbingan sebagaimana dimaksud dalam ayat (1) dan ayat (2) dituliskan dalam form pembimbingan yang ditandatangani oleh peneliti dan dosen pembimbing penelitian.

JENIS LAPORAN PENELITIAN

Pasal 7

(1) PIHAK KEDUA wajib menyusun dan menyampaikan laporan penelitian baik secara *on line* melalui portal UAD maupun *hardcopy* kepada PIHAK PERTAMA yang terdiri atas:
a. Laporan Kemajuan
b. Laporan Sementara
b. Laporan Akhir Penelitian

(2) Berkas **Laporan Kemajuan** digunakan sebagai bahan monitoring dan evaluasi (monev) internal.

(3) Berkas **Laporan Sementara** digunakan sebagai bahan kolokium laporan penelitian.

(4) Berkas **Laporan Akhir Penelitian** merupakan revisi dari Laporan Penelitian Sementara yang telah dikolokiumkan.

MONITORING DAN EVALUASI

Pasal 8

(1) PIHAK PERTAMA berhak untuk melakukan monitoring dan evaluasi (monev) internal pelaksanaan penelitian, baik secara administrasi maupun substansi.

(2) Pemantauan kemajuan penelitian dilakukan oleh Tim Monev yang dibentuk oleh PIHAK PERTAMA.

(3) PIHAK KEDUA diharuskan MENYIAPKAN SEMUA DOKUMEN/BUKTI kemajuan pelaksanaan penelitiannya guna kepentingan monev.

(4) Waktu pelaksanaan monev akan ditentukan oleh PIHAK PERTAMA.

KOLOKIUM LAPORAN PENELITIAN

Pasal 9

(1) PIHAK KEDUA wajib menyerahkan **Laporan Penelitian Sementara** sebagai bahan kolokium selambat-lambatnya **08 Oktober 2019.**

(2) Ketua Peneliti wajib hadir dan mempresentasikan hasil penelitiannya pada kolokium **Laporan Penelitian Sementara** yang pelaksanaannya akan diatur oleh PIHAK PERTAMA.

(3) Revisi laporan penelitian yang sudah dikolokiumkan harus mendapatkan pengesahan dari *reviewer* dalam bentuk **Surat Pernyataan** dan dijilid dalam satu kesatuan laporan penelitian

LAPORAN AKHIR PENELITIAN

Pasal 10

(1) PIHAK KEDUA wajib menyerahkan **Laporan Akhir Penelitian** selambat-lambatnya **2 (dua) pekan** setelah dikolokiumkan.

(2) Sistematika dan format laporan penelitian mengacu pada ketentuan dalam Pedoman Penelitian yang dikeluarkan oleh LPPM dan ketentuan lain yang berlaku.

(3) Berkas Laporan Akhir Penelitian yang diserahkan kepada PIHAK PERTAMA harus dilampiri
   (a) artikel/draft publikasi ilmiah;
   (b) naskah/draft seminar (prosiding) dan sertifikat seminar
   (c) lampiran lain yang dianggap perlu (seperti angket atau lainnya);
   (d) Profil Penelitian;
   (e) Borang Capaian Luaran Penelitian;
   (f) Form Pembimbingan (khusus skema PDP)
   (g) Daftar hadir kolokium laporan penelitian; dan
   (h) produk penelitian (naskah buku ajar, modul, naskah akademik, dan sejenisnya) atau dokumentasi/fotonya jika produk penelitian berupa barang atau perangkat keras *(hardware)* yang disertai penjelasan ringkas alat dan petunjuk pemakaiannya

   Komponen (a) sampai dengan (g) dijilid dalam satu kesatuan sebagai berkas laporan akhir penelitian.

   Komponen (h) dijilid terpisah dari berkas laporan akhir penelitian, kecuali dokumentasi/foto produk penelitian.

(4) Laporan Akhir Penelitian sebagaimana tersebut pada ayat (1), (2), dan (3) memenuhi ketentuan sebagai berikut:
   a. bentuk/ukuran kertas A4;
   b. warna cover sesuai ketentuan;
   c. di bawah bagian cover ditulis:

PENELITIAN INI DILAKSANAKAN ATAS BIAYA
ANGGARAN DAN PENDAPATAN DAN BELANJA UNIVERSITAS AHMAD DAHLAN
TAHUN AKADEMIK 2018/2019
NOMOR KONTRAK: PUPS-025/SP3/LPPM-UAD/IV/2019

(5) Berkas Laporan Akhir Penelitian sebagaimana tersebut dalam ayat (1) diserahkan kepada PIHAK PERTAMA sebagai berikut
   1 eksemplar **ASLI** untuk PIHAK PERTAMA;
   1 eksemplar untuk PIHAK KEDUA;
   1 eksemplar untuk arsip Program Studi;

(6) PIHAK KEDUA wajib mengunggah file laporan akhir penelitian secara lengkap pada alamat *http://www.simpel.uad.ac.id* melalui akun portal ketua peneliti dengan format file PDF.

KEWAJIBAN UNGGAH LAPORAN PADA PORTAL UAD

Pasal 11

(1) PIHAK KEDUA wajib mengunggah berkas Laporan Akhir Penelitian pada *www.portal.uad.ac.id* melalui akun portal masing-masing peneliti
(2) Berkas Laporan Akhir Penelitian sebagaimana dimaksud pada ayat (1) yang terdiri dari:
   i. Abstrak (PDF).
   ii. Laporan Akhir Final (PDF).
   iii. Profil Penelitian (PDF).
   iv. Borang Capaian Luaran Penelitian (PDF).

SANKSI DAN PEMUTUSAN PERJANJIAN PENELITIAN

Pasal 12

(1) PIHAK PERTAMA berhak memberikan peringatan dan atau teguran atas kelalaian dan atau pelanggaran yang dilakukan oleh PIHAK KEDUA yang mengakibatkan tidak dapat terpenuhinya kontrak penelitian ini.
(2) PIHAK PERTAMA berhak melakukan pemutusan perjanjian penelitian, jika PIHAK KEDUA tidak mengindahkan peringatan yang diberikan oleh PIHAK PERTAMA.
(3) Segala kerugian material maupun finansial yang disebabkan akibat kelalaian PIHAK KEDUA, maka sepenuhnya menjadi tanggungjawab PIHAK KEDUA.
(4) Jenis sanksi yang diberikan dapat berupa:
   (a) tidak diperkenankannya mengajukan proposal penelitian pada tahun anggaran berikutnya sampai kewajibannya terselesaikan; dan atau
   (b) tidak dapat mencairkan dana tahap 2 dan atau
   (c) mengembalikan dana yang telah diterima oleh PIHAK KEDUA.

KEADAAN MEMAKSA (*FORCE MAJEUR*)

Pasal 13

Ketentuan dalam Pasal 10 tersebut di atas tidak berlaku dalam keadaan sebagai berikut:

a. Keadaan Memaksa (*force majeur*)
b. PIHAK PERTAMA menyetujui atas terjadinya keterlambatan yang didasarkan pada pemberitahuan sebelumnya oleh PIHAK KEDUA kepada PIHAK PERTAMA dengan **surat pemberitahuan** mengenai kemungkinan terjadinya keterlambatan dalam penyelesaian kegiatan penelitian sebagaimana dimaksud dalam Pasal 1 dan Pasal 3; dan sebaliknya PIHAK KEDUA menyetujui terjadinya keterlambatan pembayaran sebagai akibat keterlambatan dalam penyelesaian perjanjian penelitian.

Pasal 14

(1) Keadaan Memaksa (*force majeur*) sebagaimana yang dimaksud dalam Pasal 11 ayat (1) adalah peristiwa-peristiwa yang secara langsung mempengaruhi pelaksanaan perjanjian serta terjadi di luar kekuasaan dan kemampuan PIHAK KEDUA ataupun PIHAK PERTAMA.
(2) Peristiwa yang tergolong dalam keadaan memaksa (*force majeur*) antara lain berupa bencana alam, pemogokan, wabah penyakit, huru-hara, pemberontakan, perang, waktu kerja diperpendek oleh pemerintah, kebakaran dan atau peraturan pemerintah mengenai keadaan bahaya serta hal-hal lainnya yang dipersamakan dengan itu, sehingga PIHAK KEDUA ataupun PIHAK PERTAMA terpaksa tidak dapat memenuhi kewajibannya.
(3) Peristiwa sebagaimana dimaksud pada ayat (2) tersebut di atas, wajib dibenarkan oleh penguasa setempat dan diberitahukan dengan Surat oleh PIHAK KEDUA atau PIHAK PERTAMA kepada PIHAK PERTAMA atau PIHAK KEDUA selambat-lambatnya 7 (tujuh) hari sejak terjadinya peristiwa yang dikategorikan sebagai Keadaan Memaksa (*force majeur*).

(4) PIHAK PERTAMA memberikan kesempatan kepada PIHAK KEDUA untuk menyelesaikan perjanjian kontrak ini sampai pada batas waktu yang disepakati oleh kedua belah pihak jika keadaan *force majeur* dinyatakan telah selesai.

PENYELESAIAN PERSELISIHAN

Pasal 15

(1) Apabila dalam pelaksanaan perjanjian dan segala akibatnya timbul perbedaan pendapat atau perselisihan, PIHAK PERTAMA dan PIHAK KEDUA setuju untuk menyelesaikannya secara musyawarah untuk mencapai mufakat.

(2) Apabila penyelesaian sebagaimana termaksud dalam ayat (1) di atas tidak tercapai, maka PIHAK PERTAMA dan PIHAK KEDUA sepakat menyerahkan perselisihan tersebut melalui mediasi dengan Rektor sebagai atasan langsung dari PIHAK PERTAMA yang putusannya bersifat final dan mengikat.

PENGUNDURAN DIRI

Pasal 16

(1) Apabila PIHAK KEDUA mengundurkan diri atau membatalkan SP3 ini, maka PIHAK KEDUA wajib mengajukan Surat Pengunduran Diri yang ditujukan kepada PIHAK PERTAMA.

(2) Surat Pengunduran Diri sebagaimana dimaksud pada ayat (1) wajib disahkan oleh Dekan fakultas ketua peneliti yang bersangkutan dan bagi peneliti skim PDP ditambah persetujuan Dosen Pembimbing.

(3) PIHAK KEDUA wajib mengembalikan dana yang telah diterima kepada PIHAK PERTAMA.

LAIN-LAIN

Pasal 17

(1) Hal-hal yang dianggap belum cukup dan perubahan-perubahan perjanjian akan diatur kemudian atas dasar permufakatan kedua belah pihak yang akan dituangkan dalam bentuk Surat atau Perjanjian Tambahan (*addendum*), yang merupakan kesatuan dan bagian yang tidak terpisahkan dari perjanjian awal.

(2) Pemberitahuan dan/atau surat menyurat dari PIHAK KEDUA kepada PIHAK PERTAMA dialamatkan kepada Kepala Lembaga Penelitian dan Pengembangan Universitas Ahmad Dahlan.

Pasal 18

(1) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini berlaku sejak ditandatangani dan disetujui oleh kedua belah pihak.

(2) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini dibuat rangkap 2 (dua); bermeterai cukup pada kedua belah pihak; dan masing-masing memiliki kekuatan hukum yang sama. Biaya meterai dibebankan kepada PIHAK KEDUA.

PIHAK PERTAMA,	PIHAK KE DUA,
Dr. Widodo, M.Si.	**SUNARDI, S.T., M.T., Ph.D.**
NIP: 19600221198709101	NIP/NIY.

Kode/Nama Rumpun Ilmu: 458 / Teknik Informatika

LAPORAN AKHIR

PENELITIAN UNGGULAN PROGRAM STUDI

FORENSIK MEDIA SOSIAL PADA PERANGKAT MOBILE MENGGUNAKAN FRAMEWORK DIGITAL FORENSICS RESEARCH WORKSHOP (DFRWS)

Disusun Oleh:

Sunardi, Ph.D./0521057401

Dr. Imam Riadi/0510088001

MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS AHMAD DAHLAN

OKTOBER 2019

HALAMAN PENGESAHAN

LAPORAN PENELITIAN UNGGULAN PROGRAM STUDI
TAHUN AKADEMIK 2019 / 2020

Judul Penelitian	:	Forensik Media Sosial Pada Perangkat Mobile Menggunakan Framework Digital Forensics Research Workshop (DFRWS)
Kode/Nama Rumpun Ilmu	:	458 / Teknik Informatika
Butir RIP	:	
TSE Penelitian	:	Information, computer and communication
Ketua Peneliti		
a. Nama Lengkap	:	Sunardi, S.T., M.T., Ph. D.
b. NIY	:	60010313
c. Jabatan Fungsional	:	Lektor
d. Program Studi	:	Teknik Informatika
e. Nomor HP	:	082136021180
f. Alamat surel (e-mail)	:	sunardi @mti.uad.ac.id
Anggota Peneliti (1)		
a. Nama Lengkap	:	Dr. Imam Riadi, M. Kom.
b. NIY	:	60020397
c. Perguruan Tinggi	:	Universitas Ahmad Dahlan
Lokasi Penelitian	:	Yogyakarta
Lama Penelitian Keseluruhan	:	10 bulan
Biaya Penelitian Keseluruhan	:	Rp. 18.000.000, -
Tahun 1	:	Rp. 18.000.000, -
Tahun 2	:	-

Mengetahui,
Wakil Direktur Pascasarjana

Prof. Dr. Dwi Sulisworo, M.T.
NIY. 60970167

Yogyakarta, 30 Januari 2020
Ketua Peneliti,

Sunardi, S.T., M.T., Ph.D.
NIY. 60010313

Menyetujui,
Kepala Lembaga Penelitian dan Pengabdian Kepada Masyarakat
Universitas Ahmad Dahlan,

Dr. Widodo, M.Si.
NIP. 19600221 198709 1 001

SURAT PERNYATAAN TELAH REVISI

Dengan surat ini kami menyatakan bahwa penelitian:

1.	Judul Penelitian	:	Forensik Media Sosial Pada Perangkat Mobile Menggunakan Framework Digital Forensics Research Workshop (DFRWS)
2.	Ketua Peneliti		
	a. Nama Lengkap	:	Sunardi, S.T., M.T., Ph.D.
	b. NIY	:	60010313
	c. Jabatan Fungsional	:	Lektor
	d. Program Studi	:	Teknik Informatika
	e. Nomor HP	:	082136021180
	f. Alamat surel (e-mail)	:	sunardi @mti.uad.ac.id
3.	Jumlah Anggota Peneliti	:	1 Orang
	a. Anggota Peneliti	:	Dr. Imam Riadi, M. Kom.
4.	Lama Penelitian	:	10 bulan
5.	Biaya Penelitian Keseluruhan		
	a. Sumber UAD	:	Rp. 18.000.000, -
	b. Sumber Lain	:	-
	Jumlah	:	Rp. 18.000.000, -

Telah direvisi sesuai dengan masukan dan petunjuk yang petunjuk yang disampaikan *reviewer.*

Mengetahui,
Reviewer,

Dr. Tole Sutikno S.T., M.T.
NIY. 60010310

Yogyakarta, 30 Januari 2020
Ketua Peneliti,

Sunardi, S.T., M.T., Ph.D.
NIY. 60010313

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

ABSTRAK

Perkembangan di bidang teknologi komunikasi menyebabkan para pengguna beralih dari perangkat komputer kepada perangkat *mobile*, salah satunya adalah *smartphone*. *Smartphone* terdiri dari berbagai sistem operasi, sistem operasi dengan pengguna yang cukup banyak adalah Android. Fiturnya yang lengkap dan kemudahan yang ditawarkan membuat Android memiliki banyak pengguna. Aplikasi dari *smartphone* yang banyak digunakan oleh pengguna adalah aplikasi media sosial seperti Twitter, Whatsapp, dan Line. Salah satu aplikasi sosial media yang banyak digunakan adalah aplikasi Twitter, namun belakangan ini aplikasi Twitter menjadi salah satu aplikasi media sosial yang digunakan untuk melakukan ujaran kebencian, pencemaran nama baik dan tindak kejahatan lainnya.

Banyaknya pengguna aplikasi media sosial ini tentunya memiliki dampak positif dan negatif. Dampak negatif yang ditimbulkan dari penggunaan aplikasi media sosial adalah munculnya oknum-oknum yang melakukan kejahatan digital menggunakan aplikasi media sosial yang terinstall pada *smartphone*. Indikasi adanya kejahatan digital tersebut dapat dibuktikan dengan suatu metode forensik salah satunya *Digital Forensics Research Workshop* (DFRWS) dimana tahapan forensic ini meliputi *identification, preservation, collection, examination, analysis* dan *presentation* dalam menemukan bukti digital tindak kejahatan.

Penelitian ini bertujuan untuk memberikan gambaran proses pengangkatan bukti digital pada aplikasi Twitter yang terinstall pada *smartphone* berbasis Android. Hasil penelitian ini diharapkan dapat digunakan sebagai acuan peneliti selanjutnya yang berminat mengembangkan penelitian di bidang *mobile* forensik, terutama pada aplikasi media sosial yang terinstall pada *smartphone* dan berbasis Android.

Kata kunci: Forensik, Media, Bukti, Digital, DFRWS

ABSTRACT

Developments in the field of communication technology have caused users to switch from computers to mobile devices, one of which is smartphones. The smartphone consists of various operating systems, operating system with quite a lot of users is Android. Its full features and convenience offered to make Android have many users. Applications from smartphones that are widely used by users are social media applications such as Twitter, Whatsapp, and Line. One of the most widely used social media applications is the Twitter application, but lately, the Twitter application has become one of the social media applications used to conduct hate speech, defamation and other criminal acts.

The many uses of this social media application certainly have positive and negative impacts. The negative impact arising from the use of social media applications is the emergence of individuals who commit digital crimes using social media applications installed on smartphones. Indications of digital crime can be proven by a forensic method, one of which is the Digital Forensics Research Workshop (DFRWS) where the forensic stage includes identification, preservation, collection, examination, analysis and presentation in finding digital evidence of a crime.

This study aims to provide an overview of the process of appointment of digital evidence on Twitter applications installed on Android-based smartphones. The results of this study are expected to be used as a reference for further researchers interested in developing research in the field of mobile forensics, especially on social media applications installed on smartphones and based on Android.

Keywords: Forensics, Media, Evidence, Digital, DFRWS

PRAKATA

Alhamdulillah Kami ucapkan puji syukur kehadirat Allah SWT sehingga terselesaikannya Penelitian Unggulan Program Studi (PUPS) dengan dana Universitas Ahmad Dahlan tahun anggaran 2019. Dalam penelitian ini, Kami melibatkan 5 orang staf pendukung dan dua orang dosen yang berjudul Forensik Media Sosial Pada Perangkat Mobile Menggunakan Framework Digital Forensics Research Workshop (DFRWS).

Laporan penelitian ini telah mencapai tahap penyelesaian dan mendapatkan hasil seperti yang diinginkan. Sampai akhir dari waktu penelitian ini, yakni selama 10 bulan, penelitian yang dilakukan memberikan hasil 100%.

Terimakasih atas Kami sampaikan kepada LPP-UAD yang telah mengamanahi kami dengan memberikan hibah untuk penelitian kerjasama Kelembagaan. Terima kasih juga kepada Universitas Ahmad Dahlan dalam hal ini adalah LPP UAD sebagai wadah peneliti UAD. Terimakasih juga kami sampaikan kepada pihak-pihak terkait aras semua nasehat, masukan, dan kerjasama yang baik dalam upaya penyelesaian laporan penelitian ini.

Wassalammu'alaikum Wr. Wb.

Yogyakarta,05 Januari 2019

Tim Peneliti

Sunardi, ST., MT., Ph. D.

Dr. Imam Riadi, M. Kom.

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi serta jaringan internet yang semakin luas secara tidak langsung memberikan dampak pada pertumbuhan pengguna *smartphone*, penggunaan *smartphone* dimasa sekarang tidak hanya sekedar untuk melakukan panggilan telepon atau berkirim pesan singkat, tetapi penggunaan *smartphone* menjadi selayaknya komputer pribadi bagi penggunanya. Pada januari 2018 berdasarkan *system* operasi pengguna *smartphone* yang mengakses internet dengan perangkat *mobile* berbasis Android adalah sebanyak 73.5%, Apple IOS sebanyak 19.9%, dan *platform* lainnya sebanyak 6.6% (Kemp, 2018).

Manusia pada dasarnya merupakan makluk sosial, pada era teknologi sekarang media sosial menjadi salah satu alat untuk berinteraksi dengan manusia lainnya, selain untuk mengirim dan menerima informasi juga sebagai tempat untuk menyimpan suatu data infromasi dari pemilik akun media sosial. Berdasarkan pengguna aktif bulanan dari berbagai negara sebanyak 2.9 milyar pengguna media sosial menggunakan perangkat *mobile* dengan pengguna terbanyak dari Asia Timur sebanyak 64% (Kemp, 2018). Pada 2016 media sosial dengan pengguna paling banyak adalah Facebook 1.65 milyar, Instagram 500 juta pengguna dan Twitter 310 juta pengguna. Kejahatan pada media sosial Facebook dan Twitter meningkat sebanyak 780% selama 4 tahun dari tahun 2008 (556 kasus) sampai tahun 2012 (4908) kasus (Mukti, dkk, 2017).

Kemunculan suatu teknologi baru biasanya diiringi dengan munculnya suatu ancaman tindak kejahatan baru pula, perkembangan *smartphone* dan media sosial saat ini banyak disalahgunakan untuk melakukan tindak kejahatan (*cybercrime*) seperti *cyberbully*, penipuan, pemerasan, penyebaran *hoax*, ujaran kebencian dan lainnya. Pelaku kejahatan *cybercrime* biasanya dapat menghilangkan barang bukti kejahatan dengan cara menghapus data sehingga secara langsung data tersebut tidak dapat terlihat lagi, oleh karena itu perlu adanya proses forensik terhadap perangkat

mobile yang menggunakan media sosial untuk tindak kejahatan, dengan menggunakan *framework Digital Forensic Research Workshop* (DFRWS) untuk mendapatkan bukti digital tindak kejahatan dan diharapkan dapat menjadi bukti digital tindak kejahatan di media sosial.

1.2 Identifikasi Masalah

Dari uraian latar belakang di atas, dapat di indentifikasi beberapa permasalahan sebagai berikut:

a. Pertumbuhan penggunaan *smartphone* mendorong penggunaan aplikasi media sosial.
b. Terdapat potensi resiko kejahatan penggunaan media sosial pada *smartphone*.
c. Tantangan baru bagi penyidik menjadikan media sosial sebagai barang bukti digital suatu tindak kejahatan digital.

1.3 Rumusan Masalah

Berdasarkan uraian latar belakang dan identifikasi masalah, maka rumusan masalah penelitian ini adalah:

a. Bagaimana melakukan forensik tehadap media sosial pada perangkat *mobile* dengan menggunakan *framework Digital Forensic Research Workshop* (DFRWS).
b. Bagaimana bukti *digital forensic* yang didapat dari proses forensik tersebut dapat dijadikan sebagai barang bukti yang membantu pengungkapan kejahatan digital.

1.4 Batasan Masalah

Terdapat beberapa permasalahan yang ditemukan dalam penelitian, maka dari itu akan ditetapkan batasan masalah pada penelitian ini yaitu proses forensik dilakukan pada perangkat *mobile* dengan menggunakan *system* operasi Android yang terinstal aplikasi media sosial Twitter dengan menggunakan metode *Digital Forensic Research Workshop* (DFRWS).

1.5 Tujuan Penelitian

Tujuan penelitian ini adalah

a. Melakukan implementasi *digital framework forensic research workshop* (DFRWS) untuk mendapatkan barang bukti digital pada layanan media sosial Twitter di Android.
b. Berdasarkan analisis forensik yang dilakukan, barang bukti digital yang diangkat dapat digunakan sebagai salah satu elemen bantu dalam pengungkapan kejahatan digital.

1.6 Manfaat Penelitian

Manfaat penelitian ini adalah

a. Menambah pengetahuan tentang forensik pada perangkat *mobile* berbasis Android.
b. Menjadi bahan referensi untuk penelitian tentang *mobile forensic* dengan menggunakan metode *digital framework forensic research workshop* (DFRWS).

BAB 2. KAJIAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian sejenis ini sebelumnya pernah dilakukan oleh:

a. **Andri Lesmana Suryana, R.Reza El Akbar, Nur Widiyasono,2016, Jurnal Edukasi dan Penelitian Informatika (JEPIN) Vol. 2**, No.2. dengan judul: Investigasi *Email Spoofing* dengan Metode *Digital Forensics Research Workshop (DFRWS).*

b. Firmansyah Gustav Hikmatyar, Bambang Sugiantoro, 2018,(IJID) ***International Journal on Informatics for Development*** **Vol.7, No.2, 2018,** Pp. 19-22, dengan judul: *Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases.*

c. Irwansyah Saputra, Muhammad Nauval Azhar, 2018, Seminar Nasional dan Diskusi Panel Multidisiplin Hasil Penelitian & Pengabdian kepada Masyarakat, dengan judul: Analisis dan Investigasi Forensik *Digital Live Memory* untuk Deteksi Ttingkah laku Agresi pada Aplikasi Whatsapp.

d. Rahmat Inggi, Bambang Sugiantoro, Yudi Prayudi, 2018, semanTIK,Vol.4, No.2, 2018, pp.193-200, dengan judul: penerapan *System Development Life Cycle (SDLC)* Dalam Mengembangkan Framework Audio Forensik.

e. Wisnu Ari Mukti, Siti Ummi Masruroh, Dewei Khairini, 2017. Jurnal Teknik Informatika Vol.10 No.1. dengan judul: Analisa Dan Perbandingan Bukti Forensik Aplkasi Media Sosial Facebook Dan Twitter Pada *Smartphone* Android.

Penelitian-penelitian diatas digunakan sebagai rujukan dalam penelitian ini. Adapun peninjauan mengenai perbedaan dan persamaan penelitian-penelitian sebelumnya dengan penelitian yang dilakukan sekarang bisa dilihat pada Tabel 2.1:

Tabel 2.1 Perbedaan dan Persamaan Penelitian

Penulis	Topik	Judul-Jenis Tulisan-Sekolah/Universitas	Objek-Platform	*Tools*	Metode
Andri Lesmana Suryana, R.Reza El Akbar, Nur Widiyasono	Analisis Forensik	Investigasi Email Spoofing dengan Metode Digital Forensics Researh Workshop(DFRWS)-Jurnal Edukasi dan Penelitian Informatika (JEPIN) Vol 2, No.2, 2016	Komputer-email	Web hosting	DFRWS (Digital Forensics Research Workshop)
Wisnu Ari Mukti, Siti Ummi Masruroh, Dewei Khairini	Digital forensik	Analisa Dan Perbandingan Bukti Forensik Aplkasi Media Sosial Facebook Dan Twitter Pada *Smartphone* Android- Jurnal Teknik Informatika Vol.10 No.1.2017	Facebook-twitter-android	SQLite Manager-DB Browser for SQLite	Simulasi
Irwansyah Saputra, Muhammad Nauval Azhar	Analisis Forensik	Analisis dan Investigasi Forensik Digital Live Memory untuk Deteksi Ttingkah laku Agresi pada Aplikasi Whatsapp-Seminar Nasional dan Diskusi Panel Multidisiplin Hasil Penelitian & Pengabdian kepada Masyarakat, 2018	Whatsapp	FTK Imager	Cross Standard Industry for Data Mining(CRISP-DM)
Firmansyah Gustav Hikmatyar, Bambang Sugiantoro	Analisis forensik	Digital Forensic Analysis on Android *Smartphone*s for Handling Cybercrime Cases-(IJID) International Journal on Informatics for Development Vol.7, No.2, 2018, Pp. 19-22	Android-*smartphone*-SMS	FTK Imager	Experimental- Generic Computer Forensic Investigation Model (GCFIM)
Rahmat Inggi, Bambang Sugiantoro, Yudi Prayudi	Analisis forensik(audio)	Penerapan System Development Life Cycle (SDLC) Dalam Mengembangkan Framework Audio Forensik- semanTIK,Vol.4, No.2, 2018, pp.193-200	Audio recorder	framework	Systems Development Life Cycle (SDLC)

Berdasarkan Tabel 2.1. maka penelitian ini akan melakukan forensik media sosial pada perangkat mobile menggunakan metode DFRWS yang telah diteliti oleh Andri, Reza, Nur untuk menganalisis forensik media sosial pada twitter yang telah diteliti sebelumnya oleh Wisnu, Siti, Dewei.

2.2 Dasar Teori

2.2.1 Forensik Digital

Forensik digital merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (*pro justice*), yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi atau komputer *crime* secara ilmiah hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan (Al-Azhar, 2012).

2.2.2 *Digital Forensic Reasearch Workshop* (DFRWS)

Digital Forensics Research Workshop merupakan penggunaan metode ilmiah yang memiliki dasar dan terbukti untuk pemeliharaan, mengumpulkan, validasi, identifikasi, analisis, interpretasi, dokumentasi dan presentasi bukti digital yang berasal dari sumber-sumber digital untuk tujuan memfasilitasi atau melanjutkan rekontruksi peristiwa yang mengandung pidana, atau membantu untuk mengantisipasi tindakan yang tidak sah yang terbukti menggangu untuk operasi yang direncanakan (DFRWS,2001).

2.2.3 *Mobile Forensic*

Mobile device forensics merupakan ilmu yang melakukan *recovery* bukti digital dari perangkat *mobile* menggunakan data yang sesuai dengan forensik (W. Jansen, 2007). Forensik perangkat *mobile* merupakan forensik yang datanya diambil dari ponsel, dengan sendirinya bisa dijadikan sebagai bukti. Bukti-bukti ini bisa dijadikan landasan ketika menyelidiki suatu perkara oleh lembaga penegak hukum. terdapat sejumlah bukti yang dapat diekstraksi dari ponsel antara lain, nomor kontak, log panggilan, pesan sms, file audio, *email*, internet *history* dan bukti lain yang berkaitan dengan kasus yang sedang diselidiki. artefak ini bisa di ekstrak dengan metode *logic* atau fisik. Maksud dari secara *logic* adalah mengekstrak data dari file sistem dengan langsung berinteraksi dengan perangkat menggunakan *tools* atau software khusus untuk *mobile device forensics*. Terdapat empat elemen kunci forensik (Rahmadi 2013) diantaranya sebagai berikut:

a. Identifikasi bukti digital, dilakukan identifikasi dimana bukti itu berada, disimpan dan bagaimana penyimpanannya untuk memperoleh tahapan selanjutnya.
b. Penyimpanan bukti digital, pada tahapan ini bukti digital dapat saja hilang karena penyimpanan yang kurang baik.
c. Analisa bukti digital, pengambilan, pemrosesan dan interpretasi dari bukti digital merupakan bagian penting dalam analisa bukti digital.
d. Presentasi bukti digital, dimana bukti digital diuji otentifikasi dan korelasi dengan kasus yang ada. tahapan yang dilakukan investigator untuk melindungi bukti adalah *the chain of custody* yang mengandung arti bahwa pemeliharaan dengan meminimalisir kerusakan karena investigasi dengan tujuan, bahwa bukti benar-benar masih asli, bukti masih bisa dikatakan seperti saat ditemukan pada saat persidangan.

2.2.4 Media Sosial

Ardianto dalam buku Komunikasi 2.0 mengungkapkan, bahwa media sosial *online*, disebut jejaring sosial *online* bukan media massa *online* karena media sosial memiliki kekuatan sosial yang sangat mempengaruhi opini publik yang berkembang di masyarakat. Penggalangan dukungan atau gerakan massa bisa terbentuk karena kekuatan media *online* karena apa yang ada di dalam media sosial, terbukti mampu membentuk opini, sikap dan perilaku publik atau masyarakat. (Ardianto, 2011).

2.2.5 Android

Android merupakan subset perangkat lunak untuk perangkat *mobile* yang meliputi sistem operasi, *middleware* dan aplikasi inti yang dirilis oleh Google. Sebagai pelengkapnya berupa Android SDK (*Software Development Kit*) yang menyediakan *Tools* dan API yang diperlukan untuk mengembangkan aplikasi pada platform Android dengan menggunakan bahasa pemrograman Java. Kelebihan sistem operasi ini yaitu, sistem operasinya terbuka, sehingga dapat dikembangkan oleh siapa saja. Akses mudah ke Android Market. *Multitasking*, ponsel Android mampu menjalankan beberapa aplikasi sekaligus. Mudah dalam hal notifikasi

maksudnya sistem operasi ini dapat memberitahukan tentang adanya SMS, *Email*, atau bahkan artikel terbaru dan Mendukung semua layanan Google.

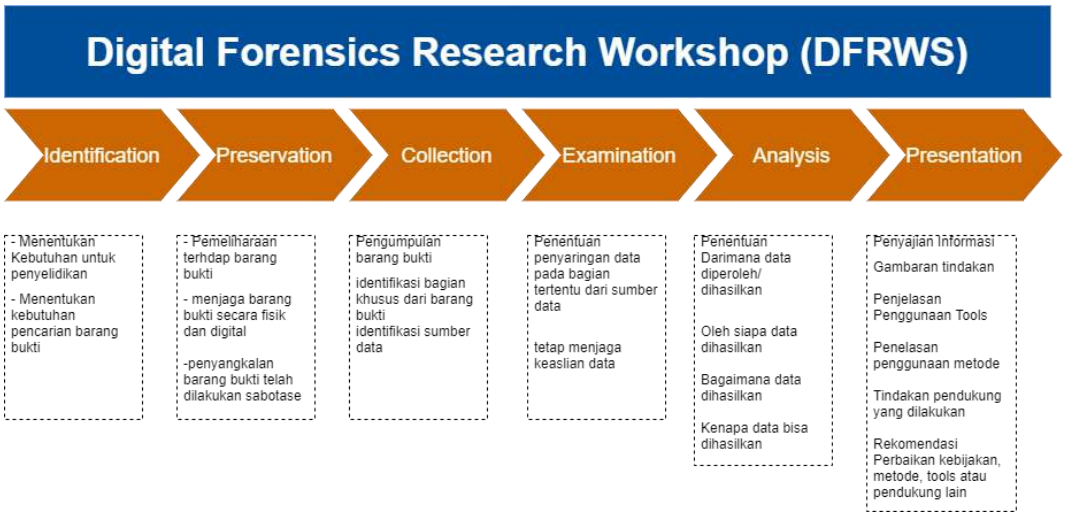
2.2.6 Twitter

Twitter adalah sebuah situs web yang menawarkan jaringan sosial berupa *mikroblog* sehingga memungkinkan penggunanya untuk mengirimkan dan membaca pesan yang disebut kicauan atau *tweets*, yang bebas mengekspresikan sesuatu seperti curhat/kritik terhadap kebijakan pemerintah. Kicauan adalah berupa teks tulisan hingga 140 karakter yang ditampilkan pada halaman profil penggunanya. Kelebihan Twitter dibanding dengan media sosial lainnya menurut Putra (2014: 33) diantaranya adalah jangkauannya luas, tidak hanya teman, tetapi juga mampu menjangkau publik figur, potensi periklanan di masa mendatang lebih besar, komunikasi terjadi sangat cepat (*update*), *mulitilink* (terhubung dengan banyak jaringan) dan lebih terukur dari Facebook. Twitter membantu penyebaran informasi secara lebih cepat yang kemudian akan menjadi sebuah topik yang dibahas oleh para penggunanya. Media massa seperti televisi, koran, majalah, tabloid pun menggunakan Twitter sebagai penyampai berita-beritanya. Hal ini mempermudah masyarakat memperoleh informasi secara cepat dan update karena berita dapat di update setiap saat oleh media massa melalui twitter.

BAB 3. METODOLOGI PENELITIAN

3.1 Metodologi

Metodologi yang digunakan dalam penelitian ini adalah DFRWS (*Digital Forensics Research Workshop*), metode ini membantu mendapatkan barang bukti dan mekanisme terpusat untuk merekam informasi yang dikumpulkan, DFRWS memiliki 6 tahapan untuk pengumpulan barang bukti, seperti pada Gambar 3.1



Gambar 3.1 Metode DFRWS

Alur kerja dari metode DFRWS pada gambar 3.1 adalah sebagai berikut:

3.1.1 *Identification* (Identifikasi)

Tahap identifikasi merupakan proses identifikasi dilakukan untuk menentukan kebutuhan yang apa saja yang diperlukan pada penyelidikan dan pencarian barang bukti kejahatan.

3.1.2 *Preservation* (Pemeliharaan)

Tahap ini merupakan tahap pemeliharaan dilakukan untuk menjaga barang bukti digital, memastikan keaslian barang bukti dan menyangkal klaim bahwa barang bukti telah dilakukan sabotase.

3.1.3 *Collection* (Pengumpulan)

Melakukan proses pengumpulan untuk proses identifikasi bagian yang khusus dari barang bukti digital dan melakukan identifikasi sumber data.

3.1.4 *Examination* (Pemeriksaan)

Melakukan tahap menentukan penyaringan data pada begian tertentu dari sumber data, penyaringan data dilakukan dengan melakukan perubahan bentuk data namun tidak melakukan perubahan pada isi data karena keaslian data merupakan hal yang sangat penting.

3.1.5 *Analysis* (Analisis)

Melakukan melakukan penentuan tentang dimana data tersebut dihasilkan, oleh siapa data tersebut dihasilkan, bagaimana data tersebut dihasilkan dan kenapa data tersebut dihasilkan.

3.1.6 *Presentation* (Presentasi)

Presentasi dilakukan dengan menyajikan informasi yang dihasilkan dari tahap analisis. tahap presentasi dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai *tool*, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, *tool*, atau aspek pendukung lainnya pada proses tindakan forensik digital.

3.2 Model dan Alat

a. Model penelitian

   Model penelitian akan menggunakan model eksperimen atau testing terhadap objek yang akan diteliti dan alat-alat pendukung penelitian.

b. Alat penelitian

   Alat-alat yang akan digunakan pada penelitian ini berupa perangkat keras (*hardware*) dan perangkat lunak (*software*) seperti pada Tabel 3.1.

Tabel 3.1 Alat Penelitian

Perangkat keras	Perangkat lunak
1. Perangkat komputer 2. Perangkat *smartphone*	1. Oxygen Forensic 2. Mobiledit Forensic 3. Belkasoft Evidence Center 4. SQLite Studio

Perangkat keras yang digunakan dalam penelitian berupa seperangkat komputer sebagai alat untuk melakukan pengumpulan serta alat yang digunakan dalam mencari barang bukti digital dan perangkat smartphone yang digunakan dalam simulasi kasus dengan pemasangan media sosial yang menjadi fokus dalam penelitian, pada pengumpulan dan pencarian barang bukti digital menggunakan beberapa percobaan tool dengan menerapkan metode DFRWS

BAB 4. HASIL DAN PEMBAHASAN

Berdasarkan pada metodologi penelitian menggunakan framework DFRWS maka tahapan yang dilakukan untuk melakukan forensik pada layanan media sosial twitter pada perangkat mobile yang berjalan diatas sistem operasi android dengan tujuan menemukan barang bukti kejahatan adalah sebagai berikut:

Sebelum memulai pada tahapan idenifikasi adalah pembuatan kerangka atau simulasi yang dilakukan dibuat terlebih dahulu dengan menggunakan akun twitter yang sudah di pasang pada perangkat android dengan memanfaatkan semua fitur yang terdapat pada twitter seperti pada Tabel 4.1 sebagai berikut:

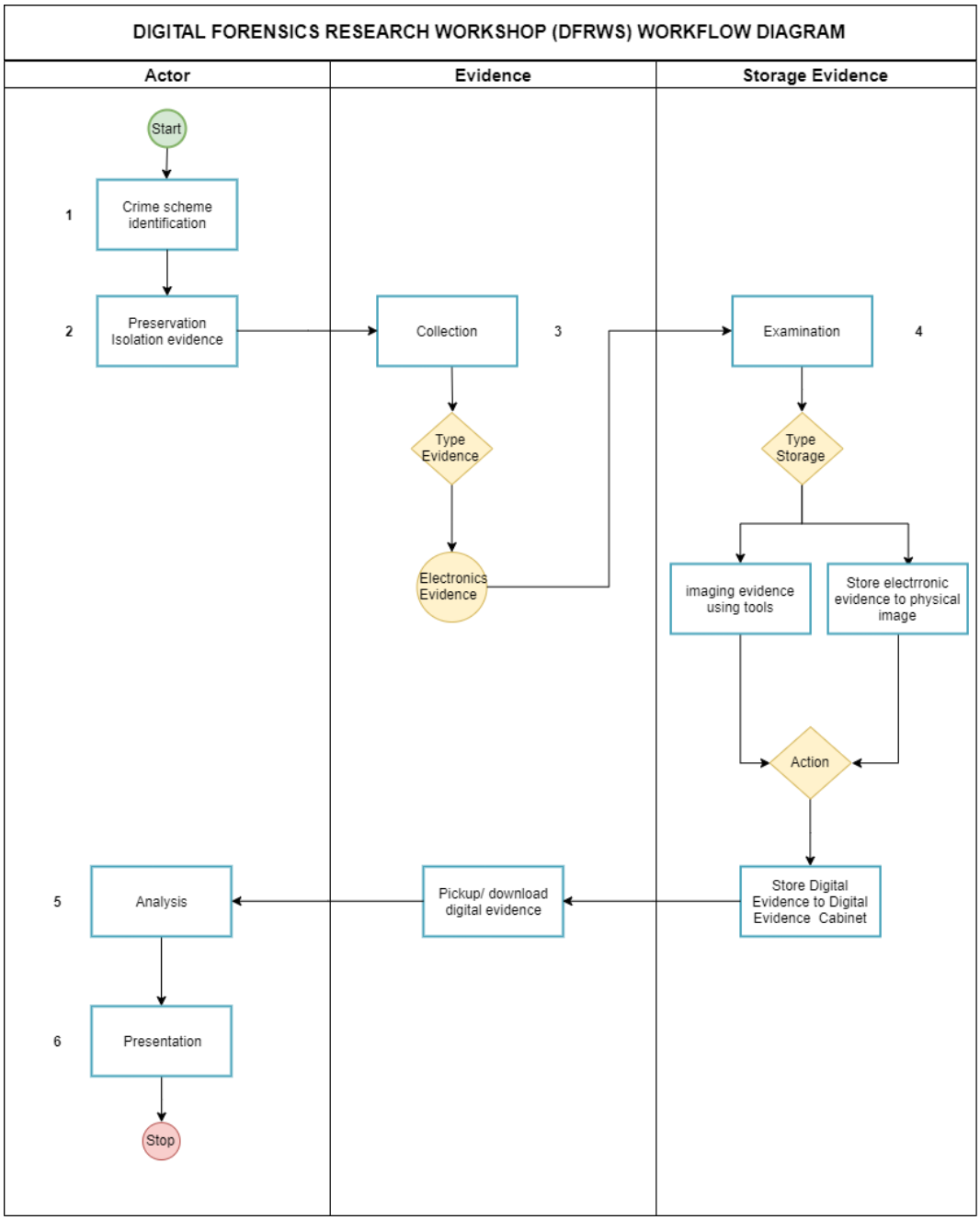
Tabel 4.1 fitur twitter

Aktivitas yang dilakukan	Bentuk data
Memposting audio/video	Video audio
Memposting teks/ tweet	Teks
Memposting gambar	Gambar
Membagikan kembali teks	Teks
Membagikan kembali gambar	Gambar
Mengikuti pengguna lain	
Mengumpulkan pengikut	
Nama akun	Teks
Lokasi perangkat	Teks
Nomor telepon	Teks
Cover photo	Gambar
Pesan teks pribadi	Teks
Pesan pribadi gambar	Gambar
Pesan pribadi video	Video

Pembuatan skenario yang dilakukan dalam proses simulasi adalah melakukan *recovery* data pada layanan twitter yang sebelumnya beberapa aktivitas dihapus pada smartphone dengan tujuan menghilangkan barang bukti.

Dari beberapa fitur twitter yang digunakan, gambar kerja untuk pencarian barang bukti menggunakan DFRWS adalah sebagai berikut, seperti pada gambar

4.1 Desain dan pengembangan



Gambar 4.1 *DFRWS Workflow Model*

Workflow model pada Gambar 4.1 menjelaskan tahapan dari skema kejahatan yang sudah dibuat serta pengumpulan barang bukti digital pada media sosial twitter dari tahap awal hingga tahap akhir dengan penjelasan sebagai berikut:

1. Melakukan investigasi fisik terhadap kejahatan menggunakan skema kejahatan yang sudah dibuat sebelumnya dengan *smartphone* dan akun twitter dengan memanfaatkan semua fitur yang ada di twitter untuk melakukan kejahatan.
2. Menjaga barang bukti untuk menjaga agar tidak ada perubahan baik penghapusan, penambahan atau perubahan dengan mengaktifkan mode pesawat dan memutus semua jaringan yang memungkinkan komunikasi dengan perangkat smartphone dan melakukan akuisisi langsung jika perlu dilakukan.
3. Mengidentifikasi dengan mengkategorikan bukti yang diperoleh menjadi bukti elektronik.
4. Penentuan penyaringan bukti elektronik pada bagian tertentu pada akun twitter, menggunakan *tools* mobiledit forensik dan belkasoft evidence center kedalam *backup* dan menyimpan barang bukti dalam bentuk *physical image*, bukti digital yang sudah disaring dalam proses ekstraksi kemudian disimpan untuk proses selanjutnya
5. Data yang sudah disaring kemudian di analisis untuk memperoleh informasi yang berguna untuk penyelesaian dan verifikasi.
6. Tahap akhir dalam alur rangkaian forensik DFRWS dengan pelaporan, dalam dokumen yang berisi data, temuan bukti, informasi yang diperoleh dari kasus.

4.1 Tahap Identifikasi

Tahap identifikasi dilakukan dengan mencari informasi dari kasus yang terjadi sebelumnya untuk dijadikan sebagai rujukan tentang pemahaman pada barang bukti yang sedang dilakukan pencarian. Pada tahap ini juga melakukan identifikasi tentang cara kerja twitter dengan berbagai fitur yang disematkan didalamnya, perangkat smartphone yang sudah terpasang media sosial twitter dan sudah digunakan untuk berbagai aktifitas dengan fitur yang ada di dalamnya, yang akan menjadi sumber dari pancarian bukti atau data yang akan diambil berdasarkan

skenario yang sudah dibuat dengan melakukan bebrapa aktivitas didalam layanan media sosial twitter dan menghapusnya.

4.1.1 Perangkat Smartphone

Perangkat smartphone yang digunakan dalam penelitian menggunakan sistem operasi android berikut Spesifikasi dari *smartphone* yang digunakan pada penelitian seperti pada Tabel 4.2

Tabel 4.2 Spesifikasi perangkat smartphone

Manufacture	**EVERCROSS**
Product	B75
HW Revision	LMY47D
Platform	Android
SW Revision	5.1(22)
Serial Number	0123456789ABCDEF
Unlocking Pattern	3452
IMEI	358441061746404
Rooted	Yes
SIM Card	Yes
Operator	3, MCC:510, MNC:89
IMSI	510897263097260
ICCID	89628990007753870152

4.1.2 Twitter

Media sosial twitter memiliki bebrapa fitur yang dapat digunakan oleh penggunanya, pada kasus ini twitter yang sudah dipasang pada perangkat akan digunakan untuk aktifitas normal sebagaimana umumnya yang nanti akan di identifikasi sebagai bentuk kejahatan yang dilakukan oleh pengguna akun, ada banyak fitur twitter yang dapat digunakan oleh pengguna diantaranya adalah, memperbarui profil pengguna, mengganti *username*, *password*, mengikuti atau menambah pertemanan, mengirim pesan secara pribadi, memberikan sanggahan pada sebuah *tweet* atau kiriman yang dikirimkan seseorang untuk diketahui khalayak umum, membagikan atau membagikan dengan memberi komentar, menyukai sebuah postingan, membagikan postingan melalui pesan pribadi, menjadikan *bookmark*, atau membagikan dengan aplikasi lain, fitur pencarian, *notifikasi*, menulis untuk postingan tertentu, berupa tulisan, gambar, *polling*, dan membagikan lokasi, namun dari banyak fitur hanya beberapa yang akan menjadi

fokus untuk menemukan barang bukti beberapa diantaranya seperti pada Tabel 4.3 berikut:

Tabel 4.3 fokus fitur twitter yang dicari

Fitur	Keterangan
Tweet	Menulis atau posting (layaknya ststus dalam facebook) ada beberapa kategori dalam posting seperti; Posting atau membagikan teks Membagikan audio/video Membagikan lokasi saat ini
Retweet	Mengulang atau membagikan kembali sebuah tweet yang sudah di posting atau dibagika oleh orang lain kemudian kita membagikan kembali, bisa juga sebagai alternatif dari *reply*
Direct Messages (DM)	Pesan secara langsung kepada pengguna lain secara personal
Mention	Cara membuat *link* terhadap suatu akun twitter, digunakan untuk menandai tweet kepada pengguna lain, juga dapat digunakan untuk mencari pengguna lain
Follower	Pengguna lain yang mengikuti kita
Following	Kita menikuti pengguna lain
Timeline	Semua aktivitas pengguna twitter yang kita ikuti akan tampil di halaman *timeline*

4.1.3 *Tools* forensik

Penggunaan *tools* forensik untuk menggali semua data dari perangkat *smartphone* yang menggunakan layanan media sosial twitter seperti pada Tabel 4.4.

Tabel 4.4 Tools Forensik yang digunakan

Nama *Tools*	Versi
MOBILedit Forensic Express	5.1.1
Belkasoft Evidence enter	Belkasoft Evidence Center 9.6 Build 3981 x64

4.2 Pemeliharaan

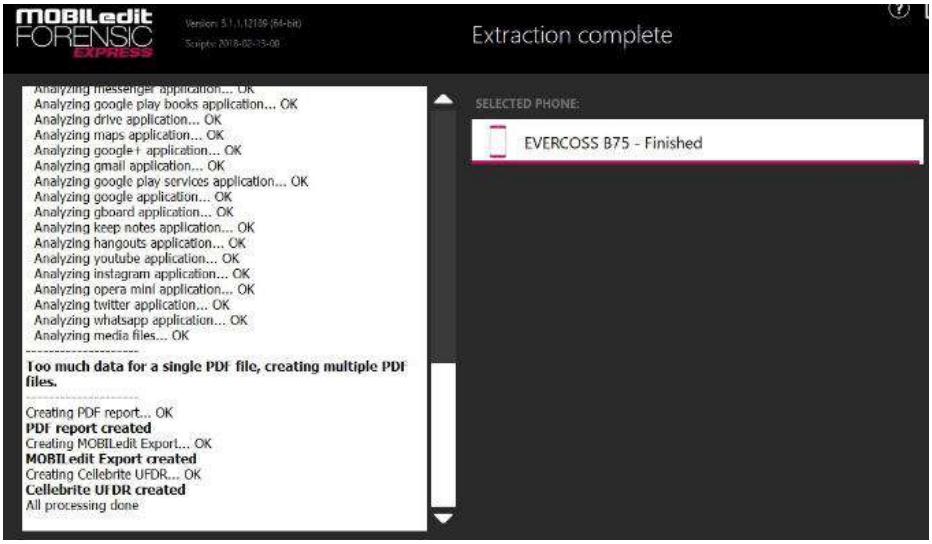
Tahap pemeliharaan bertujuan untuk menjaga barang bukti digital atau semua data yang ada pada perangkat dengan mengisolasi atau menjaga perangkat dari komunikasi dari luar ke dalam atau sebaliknya, pemasangan aplikasi, pencopotan aplikasi, penambahan atau penghapusan data. Pada tahap ini *smartphone* akan di isolasi dari semua jaringan komunikasi dengan cara mengaktifkan mode pesawat dan pemblokiran sementara pada port usb jika dimungkinkan.

4.3 Pengumpulan

Proses pengumpulan data pada perangkat dengan cara melakukan backup data dari perangkat dan membuat *physical image* dari perangkat agar keaslian tetap terjaga, menggunakan *tool* MOBILedit Forensic Express untuk mempermudah

pembacaan semua data yang ada pada perangkat. *Tools* MOBILedit akan meminta akses root untuk dapat melakukan backup perangkat secara menyeluruh.

Berikut pada gambar 4.2 proses pengumpulan data dari perangkat smartphone menggunakan MOBILedit Forensic Express.



Gambar 4.2 Backup Data Menggunakan MOBILedit Forensic Express

Pada gambar 4.2 apabila proses *backup* dari perangkat smartphone sudah selesai dapat dilihat pada log aktivitas menunjukkan semua proses telah selesai dengan membuat pdf report, MOBIL edit *report all processing done* dari *smartphone* yang dipilih EVERCROSS B75. *Tools* ini akan membuat laporan secara otomatis dapat berupa pdf, excel, atau html, yang akan mempermudah pembacaan serta pemeriksaan dalam pencarian barang bukti.

4.4 Pemeriksaan

Tahap pengumpulan data telah selesai dilakukan dan masuk pada proses pemeriksaan data, hasil *backup* dari Mobiledit Forensik dan Belkasoft Evidence Center kemudian dibaca berdasarkan *report* yang dibuat otomatis dari *tools*, dari *tools* MOBILedit Forensic Express dan Belkasoft Evidence Center didapatkan data yang diambil dari perangkat smartphone dengan layanan twitter seperti pada Tabel 4.5.

Tabel 4.5 Hasil pemeriksaan dengan kedua *tools*

Hasil yang diperoleh	*Tools*	
	MOBILedit Forensic Express	Belkasoft Evidence Center
Application info	√	×
Account info	√	×
Twitter ID	√	√
Friends	√	×
User/ follower/following	√	√
Conversation/direct messages	√	√
Cached search	√	×
Audio	×	×
Video	√	×
Text	√	√
Picture	√	√
Deleted messages/tweets	√	√
Ip adress	×	×
Url	√	√
Email/phone number	√	×
Location	√	×

Hasil yang didapatkan menggunakan MOBILedit Forensic Express dan Belkasoft Evidence Center pada masing masing *tool* sangat terbatas sehingga hanya beberapa data yang berhasil ditemukan bisa memberikan informasi yang jelas bahkan beberapa data tidak bisa terbaca.

4.4.1 MOBILedit Forensic Express

Info aplikasi media sosial twitter yang terpasang pada perangkat *smartphone* berisi informasi tentang versi aplikasi, ukuran aplikasi, ukuran data, tanggal aplikasi di *install* dan terakhir diperbarui seperti pada gambar 4.3.

Label	**Twitter**
Package	**com.twitter.android**
Version	**8.13.0-release.00**
Application Type	**User Application**
Application Size	**50.1 MB**
Data Size	**8.1 MB**
Cache Size	**88.8 MB**
First Installed	**2019-07-16 16:32:30 (UTC+7)**
Last Updated	**2019-09-20 18:25:28 (UTC+7)**
Last Active	**2019-09-26 15:43:00 (UTC+7)**

Gambar 4.3 Info Aplikasi Twitter yang Terpasang

Data selanjutnya yang ditemukan adalah informasi akun yang terpasang pada perangka *smartphone*, meliputi *nickname*, twitter id, deskripsi, jumlah pengikut, jumlah mengikuti, jumlah pesan pribadi, tanggal dipasang aplikasi serta tautan untuk gambar profil pengguna seperti pada Gambar 4.4.

Nickname	Wicakson8
Twitter ID	1151071365593628678
Description	J'؛j!Karna Soto Ayam Tak Pernah Bohongl؛'؛XIM؛XI؛X♦♦♦XX
Number of Followers	4
Following	5
Favorites	12
Number of Messages	46
Created	2019-07-16 17:09:34 (UTC+7)
Modified	2019-09-26 17:09:15 (UTC+7)
Picture Url	https://pbs.twimg.com/profile_images/1176690821690576900/hFt

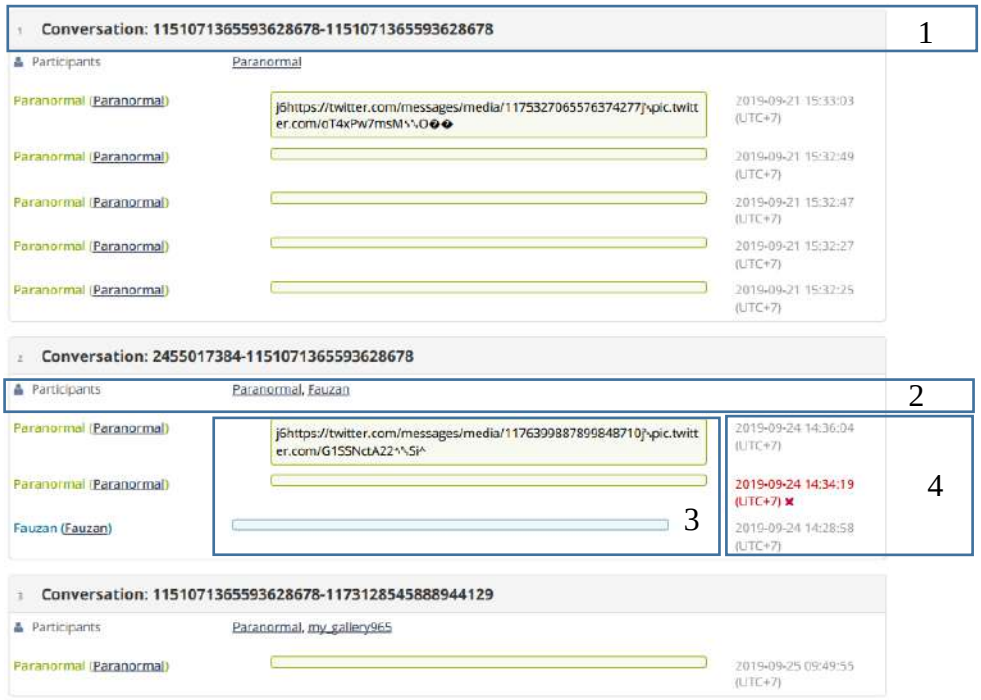
Gambar 4.4 Detail Informasi Pemilik Akun

Selanjutnya adalah informasi pertemanan yang di ikuti oleh pemilik akun berisi informasi yang cukup lengkap seperti nama akun dan twitter id pada kotak nomor 1, alamat yang dapat di akses menggunakan goole maps, serta deskripsi akun, tautan yang mengarah pada profil akun pada kotak nomor 2, jumlah pengikut dari akun tersebut, jumlah mengikuti, jumlah pesan (3), dan ulr gambar (4) data ini hampir sama dengan informasi akun pengguna seperti pada Gambar 4.5.

Nickname	NHKWORLD_News	1
Twitter ID	546657547	
Address (Google Maps)	Tokyo, Japan	2
Url	https://t.co/SQLqauwele	
Description	J'؛j~NHK WORLD's official news account brings you current events from Japan, Asia and beyond. Terms of use: https://t.co/Th0WdGYROzl؛'؛M'؛'؛J'؛'؛g'؛g'؛~j'؛https://t.co/Th0WdGYROzj)https://www3.nhk.or.jp/nhkworld/en/terms/B'؛www3.nhk.or.jp/nhkworld/en/te... XXI'؛g'؛~XXII'؛'؛♦♦XI'؛XM'؛X♦'؛ ♦'؛XX	
Number of Followers	43043	3
Following	0	
Number of Messages	43311	
Modified	2019-09-25 10:37:34 (UTC+7)	
Following User	✖ no	
Followed by User	✔ yes	
Picture Url	https://pbs.twimg.com/profile_images/781790577390039040/5-Umq3Kb_normal.jpg	4
Number of Messages	61	

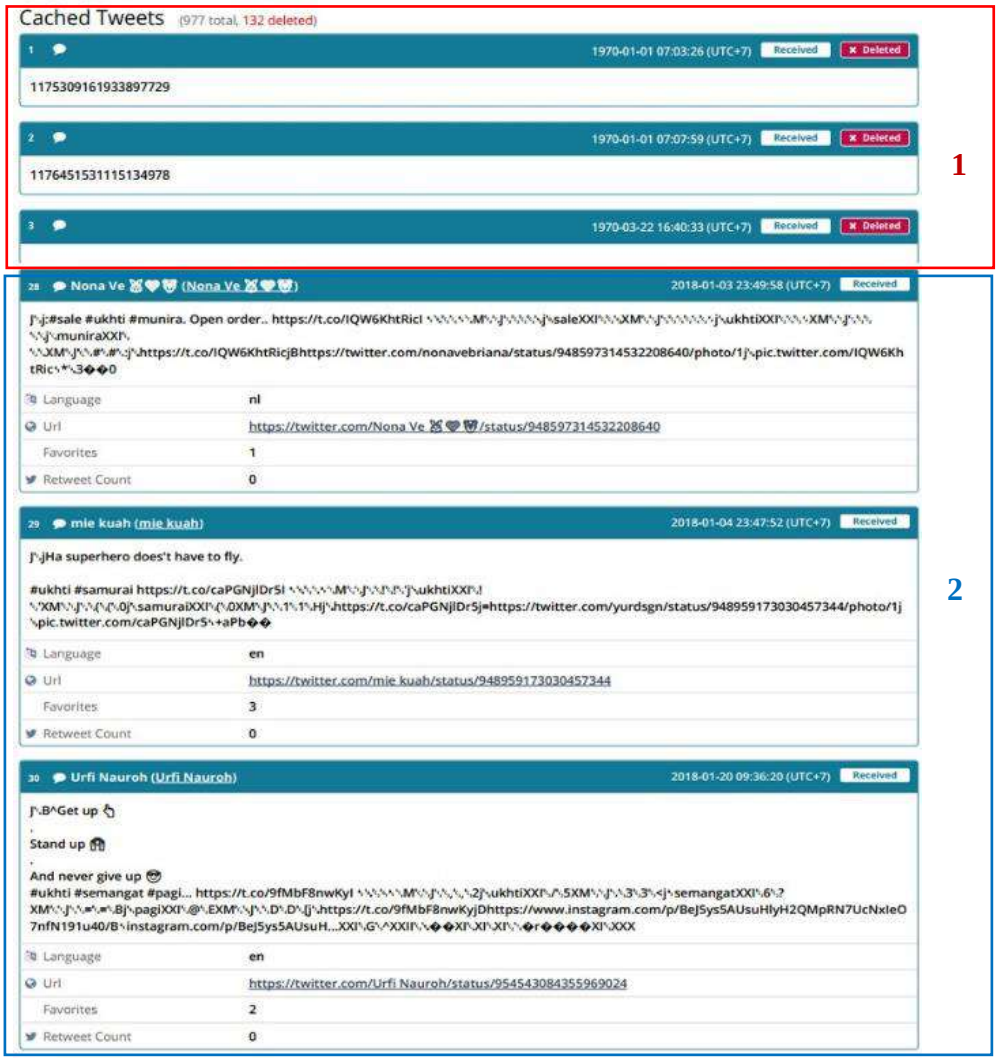
Gambar 4.5 detail informasi akun lain yang di ikuti

Percakapan yang dapat ditemukan menggunakan MOBILedit Forensic Express tidak dapat terbaca, informasi yang dapat ditemukan hanya ID twitter yang melakukan percakapan pada kotak dengan nomor 1, nama akun yang terlibat dalam percakapan pada kotak nomor 2, pada kotak nomor 3 merupakan isi dari percakapan yang tidak bisa terbaca pada tools MOBIL edit Forensic , kotak nomor 4 tanggal dan waktu percakapan dilakukan, jumlah percakapan, tanda percakapan atau pesan yang dihapus pada kotak nomor 4 dengan warna merah seperti pada Gambar 4.6.



Gambar 4.6 Percakapan Pribadi Pemilik Akun Dengan Akun Lain

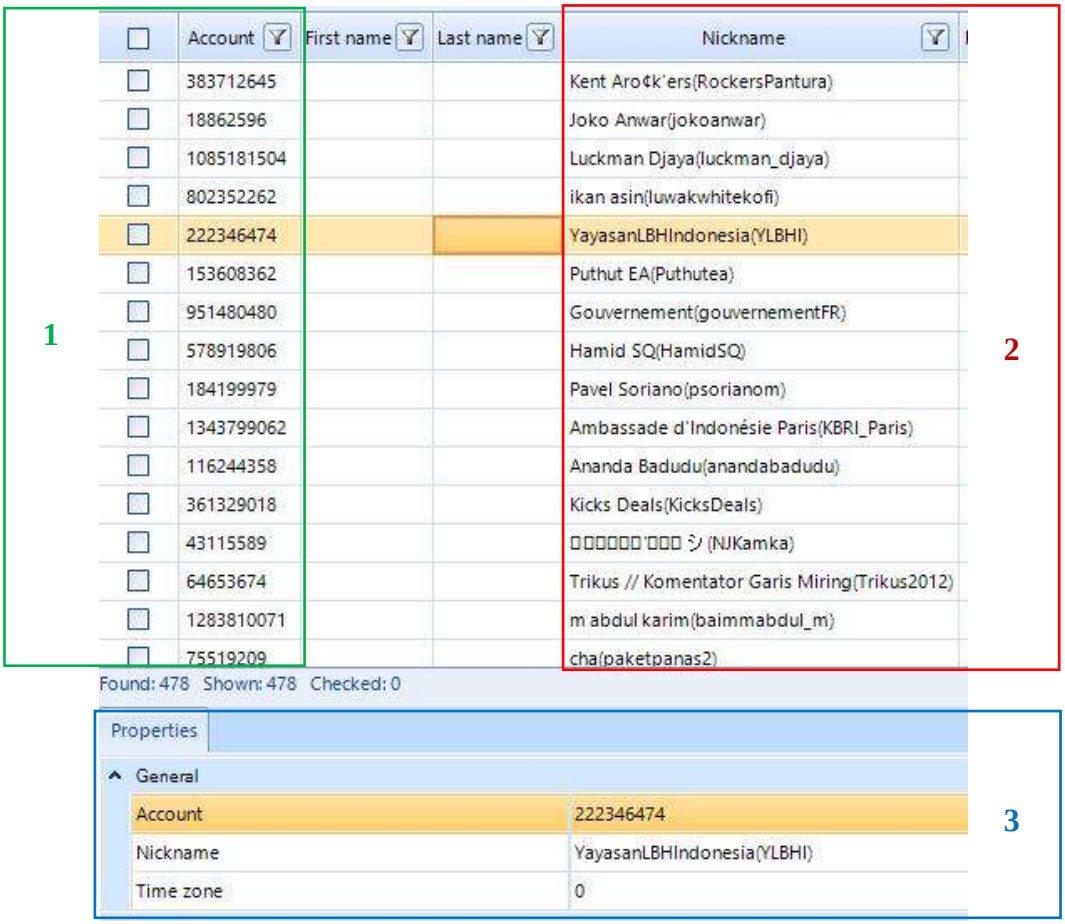
Selain percakapan, data lain yang dapat diambil dari layanan media sosial twitter adalah *cache tweets* atau *timeline* yang didalamnya berisi beberapa informasi diantaranya nama pengguna, *tweets* atau status yang diunggah, tanggal pengunggahan status tweet, hastag, bahasa, jumlah retweet atau seberapa banyak diunggah ulang, tautan yang menuju pada tweet pengguna seperti pada Gambar 4.7. Dapat dilihat juga tweet yang sudah dihapus oleh pemilik akun pada kotak berwarna merah dengan di tunjukkan nomor 1 serta cache tweet yang tampil pada timeline pemilik akun yang berhasil di ambil pada kotak biru dengan nomor 2 tertulis bahwa ada beberapa tweet yang sudah di hapus dari total keseluruhan tweet yang ada.



Gambar 4.7 Cache Tweets yang Muncul Pada Beranda Timeline

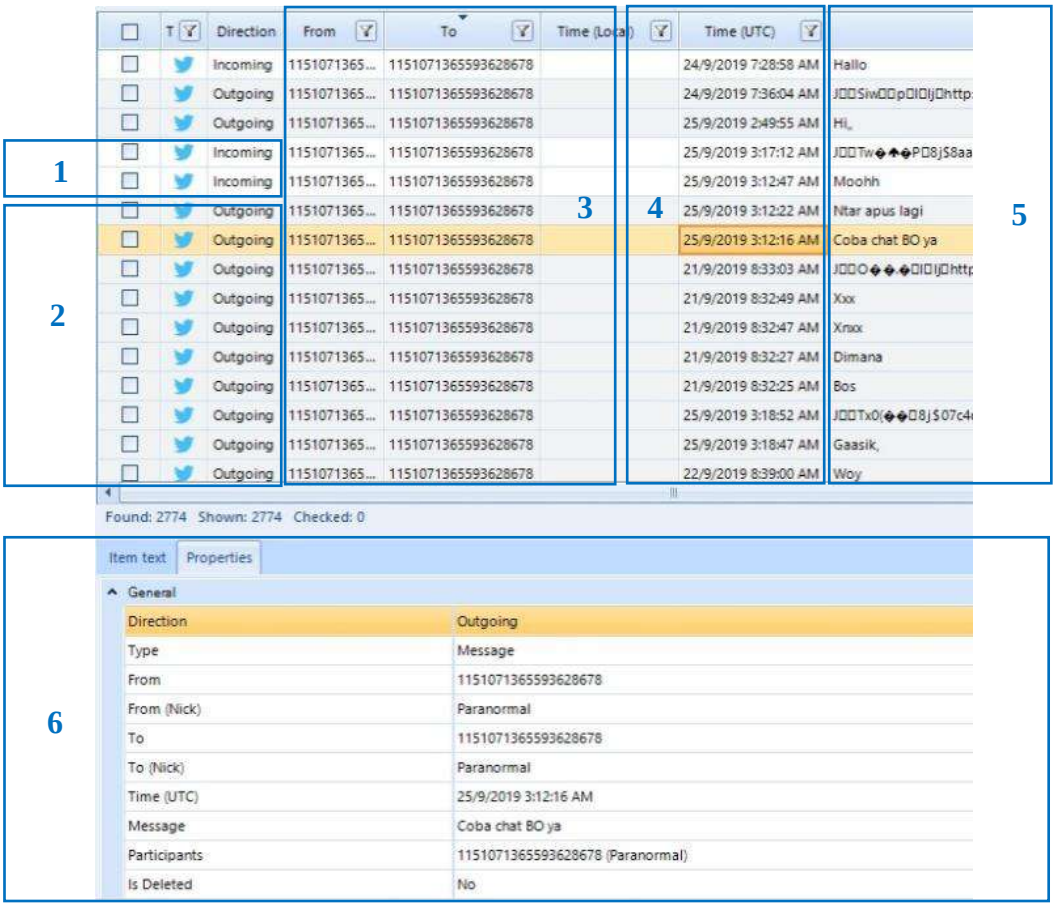
4.4.2 Belkasoft Evidence Center

Hasil pengambilan data menggunakan Belkasoft Evidence Center pada layanan media sosial twitter ditemukan lebih sedikit dari pengambilan mengggunakan tool MOBILedit Forensic Express seperti pada Gambar 4.8 ditemukan beberapa informasi ID akun pada kotak nomor 1 nama pengguna pada kotak nomor 2 serta dapat dibaca pada tab properties yang menunjukkan nama akun twitter serta id akun pengguna pada kotak nomor 3.



Gambar 4.8 Informasi ID Akun dan Nama Akun Twitter

Data selanjutnya adalah bentuk aktifitas percakapan oleh pengguna, dapat terbaca pesan yang dikirimkan oleh pemilik akun, tanggal percakapan berlangsung, arah percakapan keluar dan masuk, pada kotak nomor 1 arah pesan atau percakapan masuk dari pengguna lain ke pemilik akun, terdapat juga logo media sosial twitter yang menunjukkan pengguna memakai aplikasi media sosial twitter, pada kotak nomor 2 arah percakapan keluar dari pemilik akun ke akun lain, kotak nomor 3 berisi nomor id pemilik akun pengirim dan penerima pesan, kotak nomor 4 adalah waktu percakapan terjadi yang menunjukkan tanggal dan waktu, sedangkan kotak nomor 5 berisi pesan yang dikirim maupun pesan yang diterima, untuk tab properties nomor 6 berisi detail dari sebuah percakapan yang dipilih seperti pada Gambar 4.9.

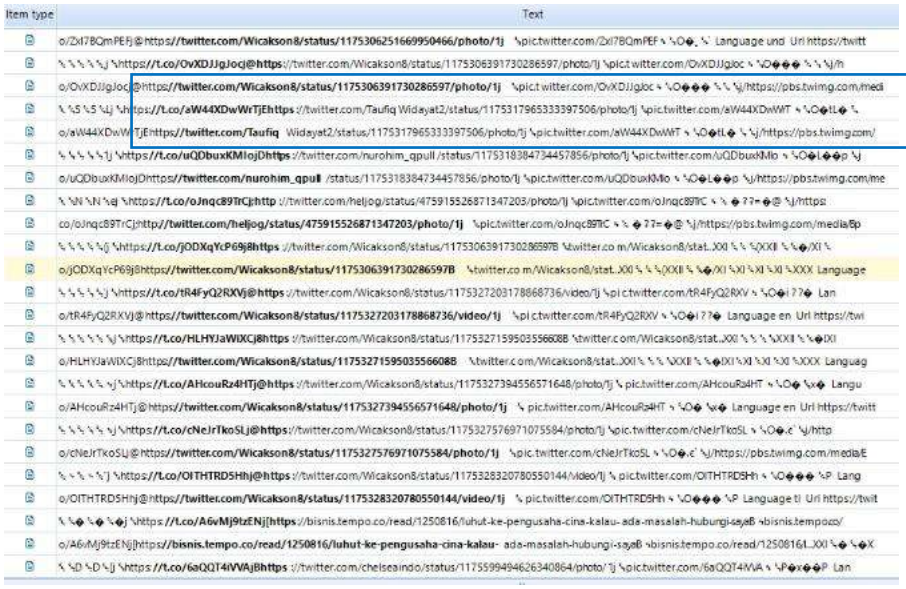


Gambar 4.9 Arah percakapan pemilik akun berserta isi percakapan

Data lain yang berhasil ditemukan menggunakan Belkasooft Evidence Center diantaranya adalah email seperti pada kotak nomor 1 ada beberapa email dari beberapa akun yang terhubung, selain email terdapat beberapa data seperti tautan, nomor telepon jumlah pengikut dari sebuah akun, jumlah mengikuti serta jumlah pesan pada kotak nomor 2, diambil contoh seperti pada kotak nomor 3 sebuah akun dengan nomor telepon (021) 3912377 memiliki email lbhjakarta@bantuanhukum.or.id mempunyai pengikut sebanyak 72797, mengikuti akun twitter lain sebanyak 6770 dan memiliki pesan atau percakapan 18670 seperti pada Gambar 4.10.

Gambar 4.10 Informasi alamat email dan jumlah pengikut dari sebuah akun

Sementara pada data lain dari Belkasoft menunjukkan bahwa tautan yang mengarah pada id akun dan aktifitas membagikan status atau aktifitas lain yang tampil pada *timeline* pada kotak nomor 1 seperti pada Gambar 4.11.

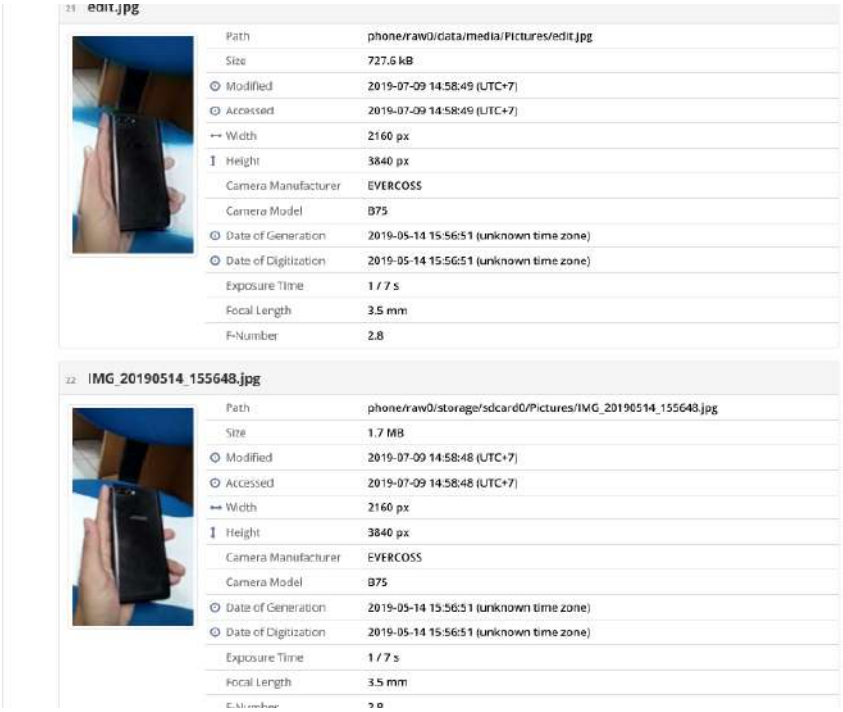


Gambar 4.11 tautan merujuk pada aktifitas pengguna

4.5 Analisis

4.5.1 Image Forensik

Hasil ekstraksi yang sudah dilakukan, didapat full report yang menunjukan bahwa ada beberapa file gambar, diantaranya adalah seperti pada Gambar 4.12.



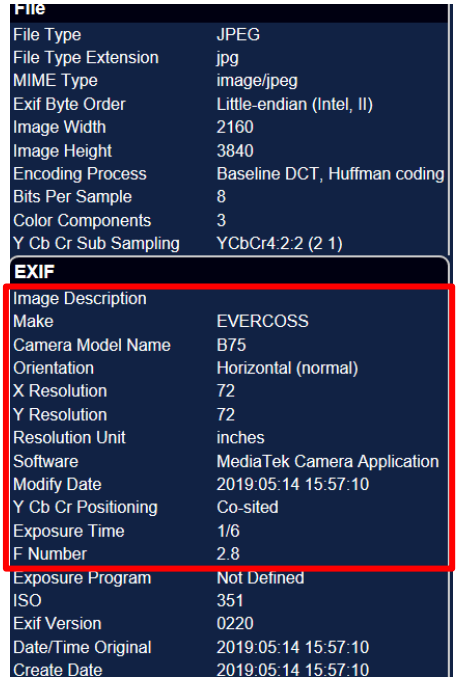
Gambar 4.12 Contoh File Gambar yang Didapat

Setelah menganalisis gambar yang didapat, terdapat 2 buah gambar yang serupa dengan gambar yang pelaku posting di Twitter, terlihat sangat jelas gambar pertama dan gambar kedua pada logo perangkat tersebut, kemudian dilakukan analisis pada 2 buah gambar tersebut. Gambar 4.13. adalah dua buah foto yang didapat.

(a) Foto Pertama (b) Foto Kedua

Gambar 4.13 Foto yang Mirip dengan Postingan

Tahap pertama dalam menganlisis keaslian gambar adalah mendeteksi metadata gambarnya, dalam mendeteksi gambar tersebut menggunakan FotoForensic (fotoforensic.com). Gambar 4.14 dan Gambar 4.15 merupakan hasil yang didapat dari pengecekan metadata kedua gambar.



File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)
Image Width	2160
Image Height	3840
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:2 (2 1)
EXIF	
Image Description	
Make	EVERCOSS
Camera Model Name	B75
Orientation	Horizontal (normal)
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	MediaTek Camera Application
Modify Date	2019:05:14 15:57:10
Y Cb Cr Positioning	Co-sited
Exposure Time	1/6
F Number	2.8
Exposure Program	Not Defined
ISO	351
Exif Version	0220
Date/Time Original	2019:05:14 15:57:10
Create Date	2019:05:14 15:57:10

Gambar 4.14 Metadata Foto Pertama

File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)
Current IPTC Digest	c7794901f643e177fd726c73c9a2bb6d
Image Width	2160
Image Height	3840
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:4:4 (1 1)
EXIF	
Photometric Interpretation	RGB
Make	EVERCOSS
Camera Model Name	B75
Orientation	Horizontal (normal)
Samples Per Pixel	3
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	Adobe Photoshop CC 2017 (Windows)
Modify Date	2019:05:20 15:23:47
Y Cb Cr Positioning	Co-sited
Exposure Time	1/7
F Number	2.8
Exposure Program	Not Defined
ISO	345
Exif Version	0220

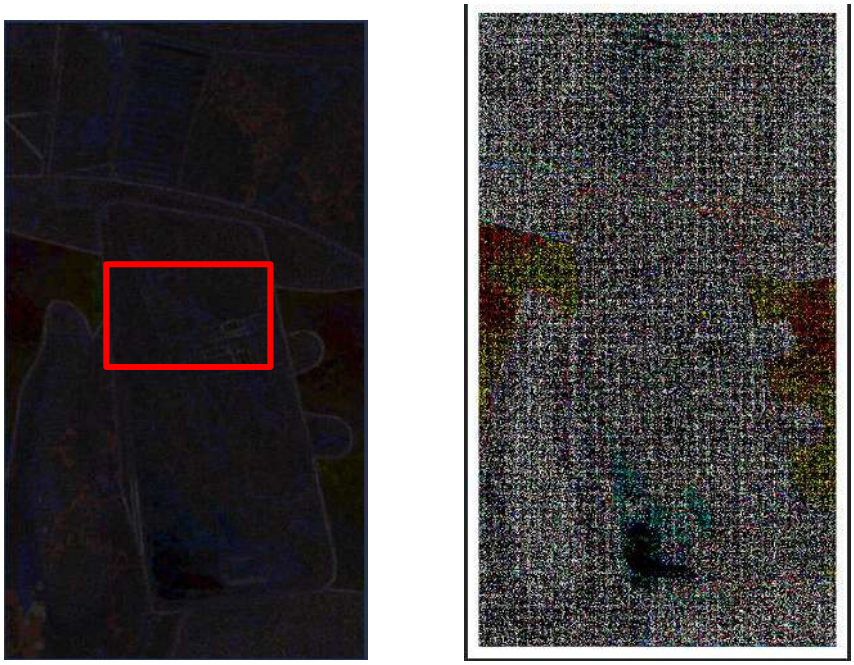
Photoshop	
IPTC Digest	c7794901f643e177fd726c73c9a2bb6d
Displayed Units X	inches
Displayed Units Y	inches
Print Style	Centered
Print Position	0 0
Print Scale	1
Global Angle	30
Global Altitude	30
URL List	
Slices Group Name	IMG_20190514_155648
Num Slices	1
Pixel Aspect Ratio	1
Photoshop Thumbnail	(Binary data 3379 bytes)
Has Real Merged Data	Yes
Writer Name	Adobe Photoshop
Reader Name	Adobe Photoshop CC 2017
Photoshop Quality	8
Photoshop Format	Standard
Progressive Scans	3 Scans
XMP	
XMP Toolkit	Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01
Creator Tool	MediaTek Camera Application
Metadata Date	2019:05:20 15:23:47+07:00
Date Created	2019:05:14 15:56:51.051
Color Mode	RGB
ICC Profile Name	sRGB IEC61966-2.1
Document ID	B739329E05185FA95FF7BFA6D5BE7009

Gambar 4.15 Metadata Foto Kedua

Gambar 4.14 diatas sudah menunjukan keaslian foto tersebut, karena dalam metadatanya tidak terdapat bukti yang menunjukan bahwa Foto (a) pernah diedit, sedangkan pada Gambar 4.15 Terdapat bukti metadata yang menunjukan foto tersebut sudah pernah diedit, yaitu terdapat tambahan berupa bukti yang menunjukan foto tersebut pernah diedit menggunakan Adobe PhotoShop CC 2017.

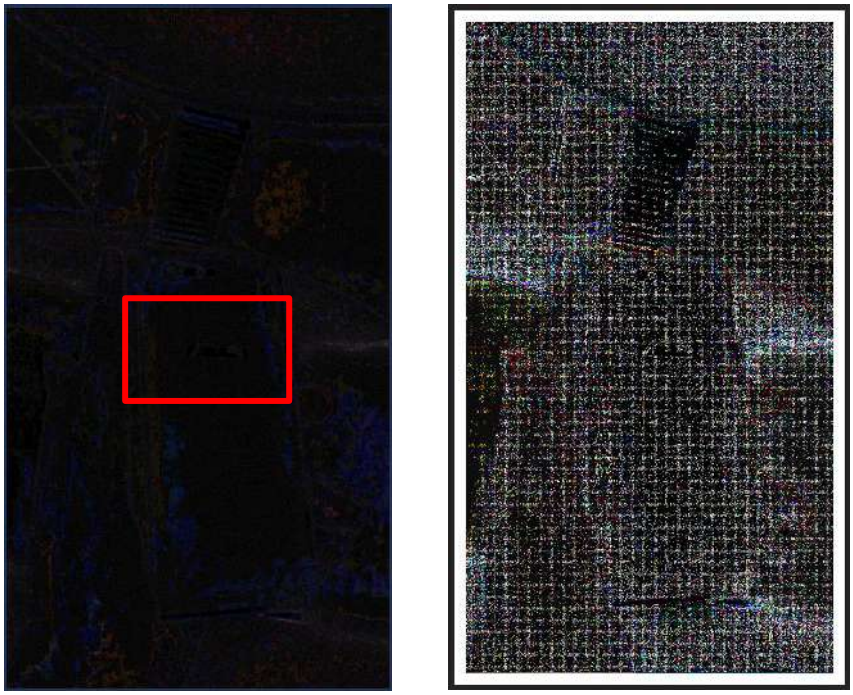
Setelah penentuan keaslian kedua foto tersebut, maka tahap selanjutnya adalah mencari bukti editan dengan membandingnya kedua buah foto tersebut

menggunakan *tools* FotoForensic (fotoforensic.com) dan ForensicallyBeta (29a.ch/photo-forensics). Gambar 4.16 merupakan analysis foto pertama (asli) dan Gambar 4.17. merupakan analysis foto kedua (editan).



(a) FotoForensik (b) ForensicallyBeta

Gambar 4.16 Analisis Foto Asli



(a) FotoForensik (b) ForensicallyBeta

Gambar 4.17 Analisis Foto Asli

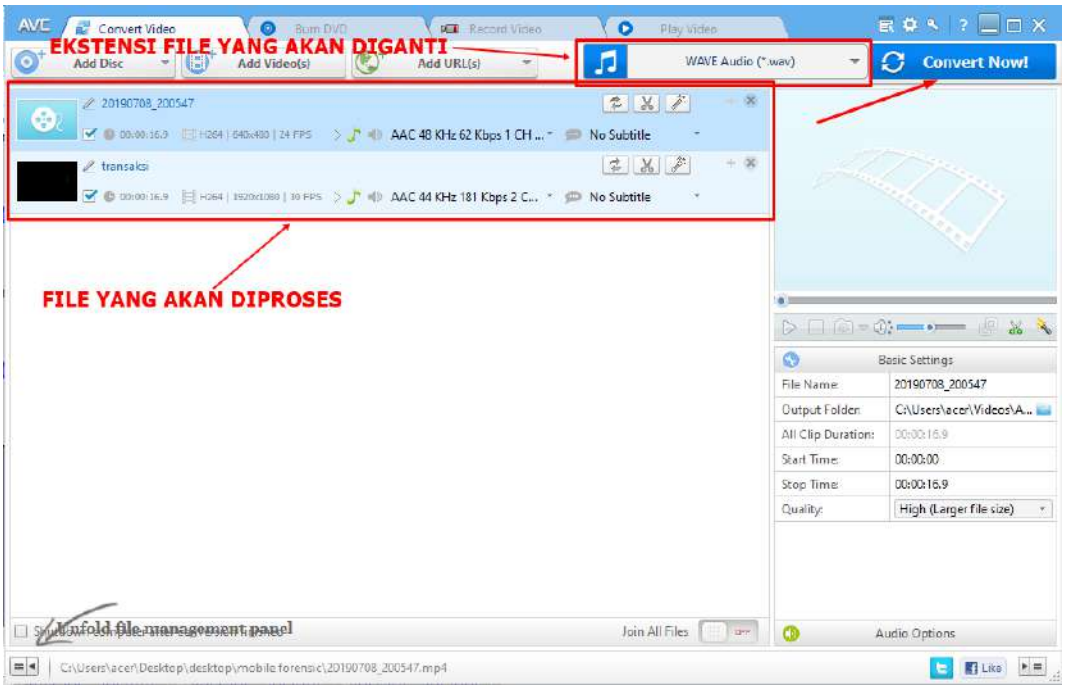
Setelah kedua foto diproses menggunakan 2 *tools* maka akan didapat seperti Gambar 4.16 yang merupakan proses dari foto asli dan Gambar 4.17 yang merupakan proses dari foto editan. Perbandingan kedua buah gambar terlihat jelas, terutama pada proses FotoForensic dengan teknik Teknik Level Error Analysis. Perbandingan yang terlihat salah satunya adalah perubahan pixel pada objek *smartphone*, selain itu juga terdapat beberapa perubahan pixel diarea lain yang berbeda dengan foto asli sehingga hal tersebut membuktikan bahwa pada bagian tersebut terdapat pengeditan foto. Sedangkan untuk ForensicallyBeta juga terdapat perbedaan pixel pada bagian tertentu yang menunjukan adanya noise pada foto tersebut.

4.5.2 Audio Forensik

Barang bukti digital yang didapat dari MOBILedit Forensic Express berupa video yang telah dimanipulasi tersebut akan diperoses untuk keperluan audio forensik. Analisis *spectrogram* adalah metode yang akan digunakan pada penelitian ini dengan tujuan untuk mengetahui pemilik suara dari video tersebut.

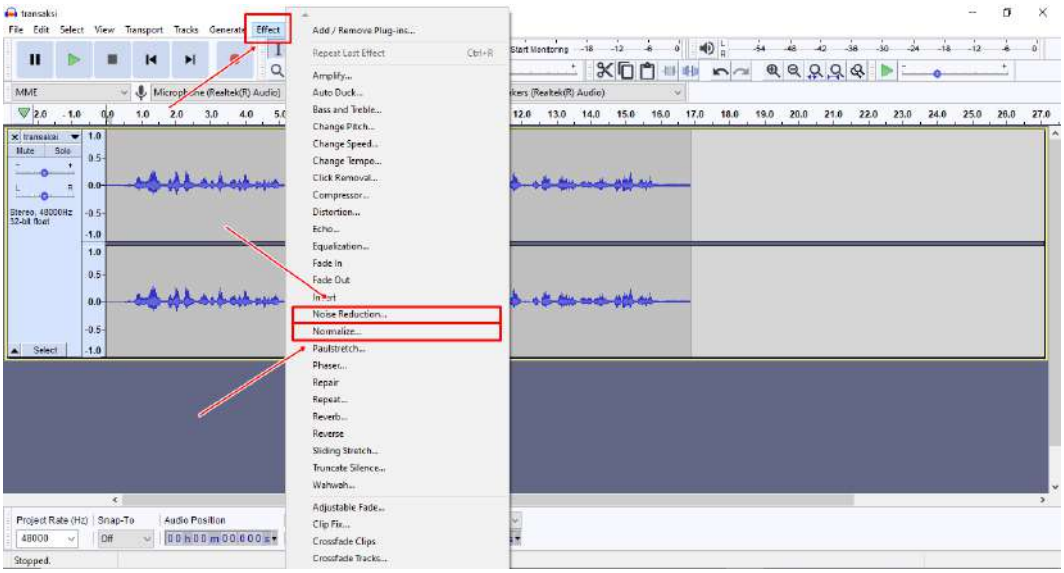
Didapatkannya file video yang telah dimanipulasi dan video asli dapat dilakukan analisis *spectrogram*.

Proses yang pertama dilakukan adalah mengambil audio dari file video yang didapatkan dengan menggunakan tool Any Video Converter Ultimate. Video tersebut dirubah yang semula ekstensi filenya .mp4 menjadi .wav seperti pada Gambar 4.18.



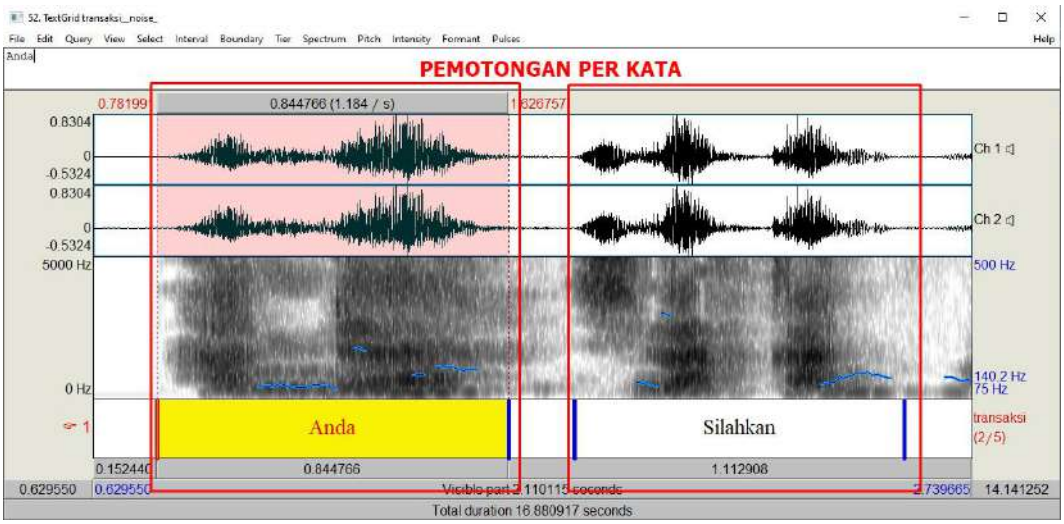
Gambar 4.18 Merubah Ekstensi File Video ke Audio

Pada Gambar 4.19 file audio tersebut akan dilkakukan filtrasi gangguan atau yang disebut *noise reduction* di aplikasi Audacity. Setelah dilakukan *noise reduction* kemudian dilakukan *normalize* yang akan memperjelas suara pada audio tersebut.



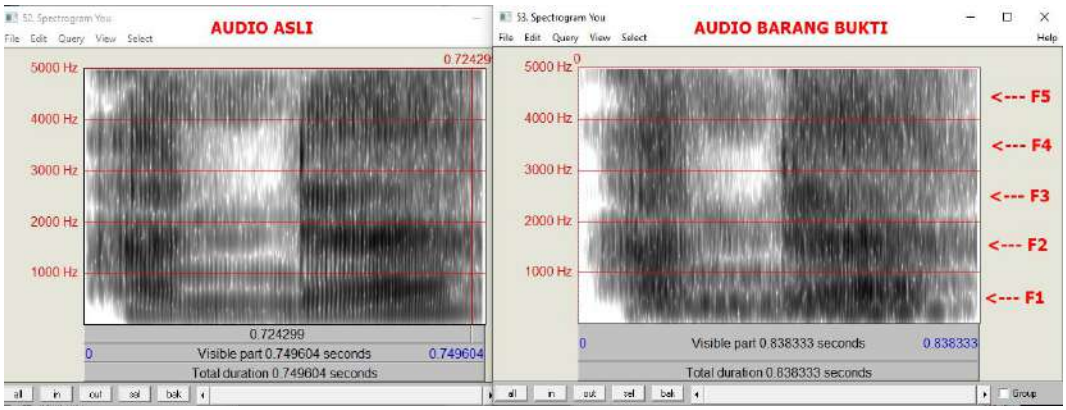
Gambar 4.19 Proses Noise Reduction dan Normalize

Audio yang telah didapatkan kemudian diolah dengan dipotong per suku kata dan diambil nilai *pitch* dari suku kata tersebut. Pemotongan kata dilakukan dengan menggunakan aplikasi Praat seperti pada Gambar 4.20.



Gambar 4.20 Proses Pemotongan Per Kata

Setelah proses diatas kemudian dilakukan analisa *spectrogram* perkata tersebut. Sebagai contoh kata “Anda” yang akan dilakukan analisa statistik *spectrogram* pada setiap rekaman suara yang ada pada Gambar 4.21.



Gambar 4.21 Analisis Spectrogram

Setelah semua potongan audio telah dianalisis untuk setiap forman dan hasilnya ada pada Tabel 4.6.

Tabel 4.6 Hasil Analisis

Syllables	Spectrogram Analysis
Anda	MATCH
Silahkan	MATCH
Melakukan	MATCH
Transfer	MATCH
Sejumlah	MATCH
Dua	MATCH
Puluh	MATCH
Juta	MATCH
Setelah	MATCH
Itu	UNMATCH
Barang	UNMATCH
Yang	MATCH
Dipesan	MATCH
Akan	MATCH
Dikirimkan	MATCH
Tiga	UNMATCH
Hari	MATCH
Kemudian	MATCH
Setelah2	MATCH
Transfer2	MATCH

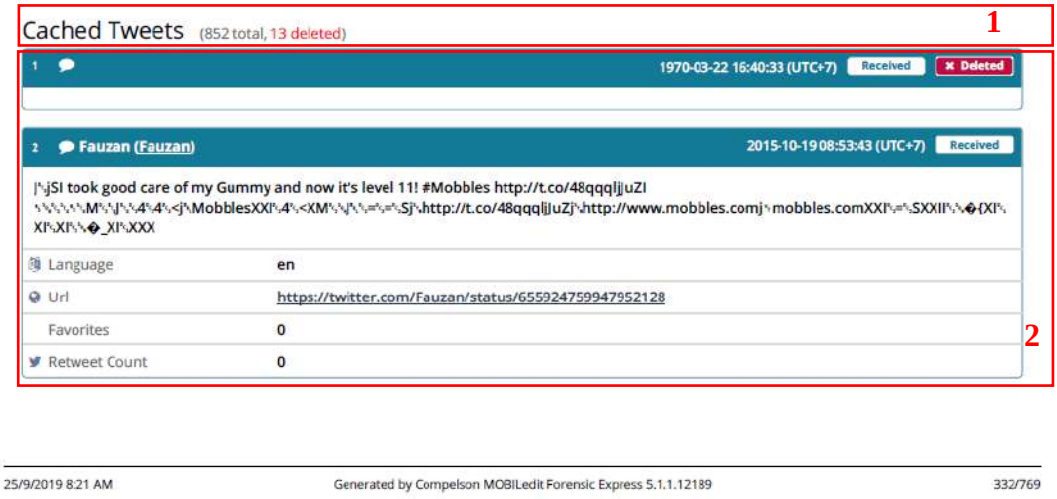
Dari analisis *spectrogram* yang dilakukan sampel audio dengan barang bukti video adalah MATCH. Pola spesifik pada setiap forman tidak memiliki perbedaan yang signifikan sehingga hasilnya dapat dikatakan identik dengan sampel audio.

4.5.3 Teks Forensik

Berdasarkan *file report* hasil ekstraksi data dari barang bukti *smartphone*, pada aplikasi *twitter* ditemukan data dalam bentuk *text* yaitu berupa infromasi akun *twitter* dan beberapa *posting tweet* yang berhasil tersimpan pada barang bukti *smartphone*, seperti pada Gambar 4.22 berikut:

Gambar 4.22 Hasil Report Informasi Akun Twitter

Pada laporan informasi akun *twitter*, terdapat 1 akun yang berhasil didapatkan dan dilaporkan dengan rincian: Nama Akun *Twitter, Nickname, Twitter ID, Description, Number of Followers, Following, Favorites, Number of Messages, Created, Modified,* dan *Picture URL*. Berdasarkan *file report* didapatkan 1 buah akun *twitter* dengan nama akun “Paranormal”.



Gambar 4.23 Hasil Report Cached Tweets

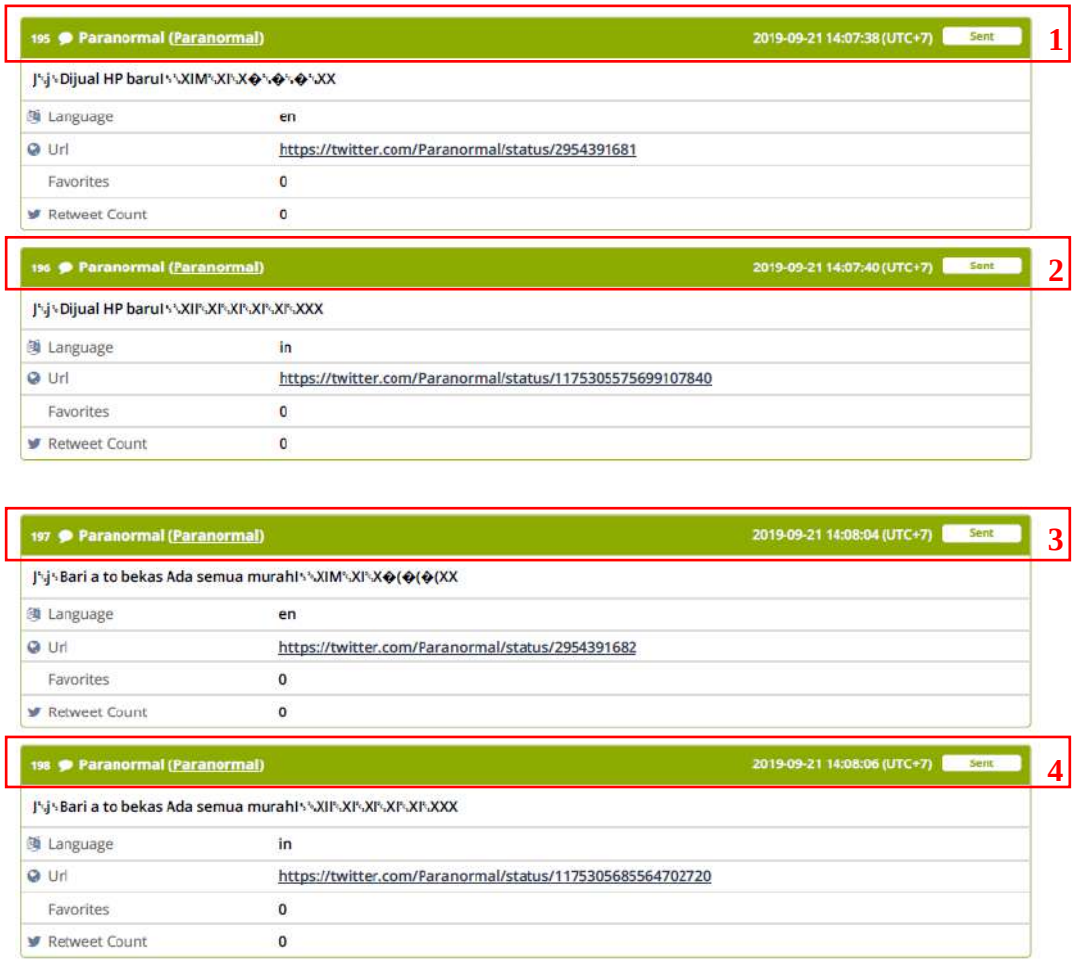
Pada *file report cached tweets*, Gambar 4.23 berhasil didapatkan total 852 *posting tweet*, dan 13 *file posting tweet* terhapus (1) dan dilaporkan dengan rincian: Nama Akun *Twitter*, Jam, Tanggal, Bulan, Tahun, *Timezone*, *Text Postingan Tweet*, Settingan Bahasa, *Url Tweet*, Jumlah *Favorites*, dan Jumlah *Retweet* (2).

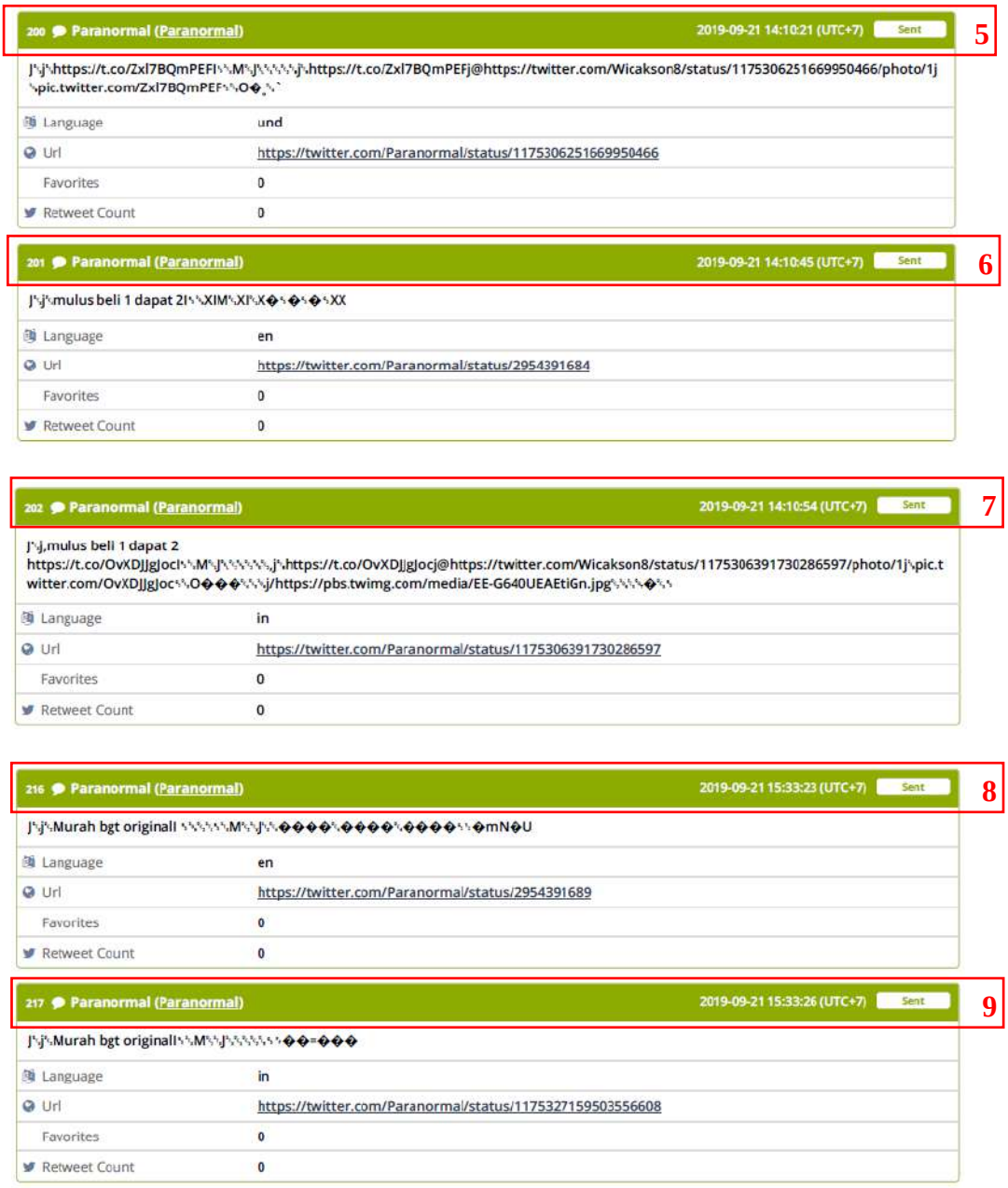
Gambar 4.24 Pembagian Kategori Cached Tweets

Postingan *tweet* yang didapat pada *file report* serperi Gambar 4.24 dibagi menjadi 2 kategori, yaitu *received* yang berarti *tweet* dari teman *following* (1) dan *sent* yang berarti *tweet* dari akun pelaku (Paranormal) pada kotak nomor 2. Berdasarkan studi kasus jual beli handphone yang dilakukan oleh akun *twitter* dengan nama akun "Paranormal", maka tahap pertama yang dilakukan adalah

mencari postingan *tweet* yang dilakukan oleh akun pelaku (Paranormal), pada *file report cached tweet* ditemukan terdapat 49 postingan *tweet* yang dikirimkan melalui akun pelaku (paranormal).

Tahap selanjutnya menganalisis postingan *tweet* yang berkaitan dengan studi kasus jual beli handphone, dan didapatkan 9 buah postingan *tweet* yang berisi tentang jual beli handphone, yaitu nomer *cached tweet*:195 (1), 196 (2), 197 (3) , 198 (4) , 200 (5), 201 (6) , 202 (7) , 216 (8) , dan 217 (9). Dengan rincian seperti Gambar 4.25 berikut:





Gambar 4.25 Rincian Tweet Jual Beli Handphone

Berdasarkan hasil analisis forensik pada *smartphone* pelaku, ditemukan 1 buah akun twitter dengan nama akun "Paranormal" dan ditemukan postingan *tweet* yang dilakukan dari akun twitter pelaku (Paranormal) sebanyak 49 *tweet* dan 9 diantaranya berisi postingan *tweet* jual beli handphone.

4.6 Presentasi

Hasil perolehan data menggunakan *tools* MOBILedit Forensic Express dan Belkasoft Evidence Center memiliki kelebihan dan kekurangan. Perolehan data dari masing masing tool disajikan dalam tabel agar lebih mudah dicermati.

4.6.1 MOBILedit Forensic Express

Hasil dari pengambilan data menggunakan tool MOBILedit Forensic Express berupa detail info akun, nama akun, pertemanan, pengguna lain yang masuk kedalam timeline, percakapan, pesan pribadi dan nomor telepon, seperti pada tabel 4.7.

Tabel 4.7 Hasil Pengambilan data dari MOBILedit Forensic Express

Evidences	MOBILedit Forensic Express	*Result*
Detail Account info	Account	1
	User Account	Paranormal
	Friends	6
	Users	587
	Conversation	4 conversation, 23 messages, 1 deleted
	Cached Tweets	852, 13 deleted
	Messages	23, 1 deleted
	Cached Searches	2
	List of Analyzed files	8 files
Account Name (1)	Nickname	Wicasono8
	Twitter ID	1151071365593628678
	Description	J☒j! Karna Soto Ayam Tak Pernah BohongI☒☒ XIM☒XI☒X�*�*�*XX
	Follower	4
	Following	5
	Favorite	12
	Number of Messages	46
	Created Date	2019-07-16 17:09:34 (UTC+7)
	Modified Date	2019-09-25 10:40:25 (UTC+7)
	Picture ID	https://pbs.twimg.com/profile_images/1176690821690576900/hFbrBj3H_normal.jpg
Friends (6)	Nickname	fauzangustafi
	Twitter ID	2455017384
	Adress (google maps)	Boyolali
	Description	J☒j☒Bio: I'm Awesome! I☒☒XIM☒XI☒X�☒ ☒☒☒XX
	Number of Followers	26
	Following	36
	Number of Messages	174
	Modified	2019-09-25 09:48:43 (UTC+7)
	Following User	Ok
	Followed by User	Ok
	Picture URL	https://pbs.twimg.com/profile_images/653594881508577281/qEdYmv0d_normal.jpg
	Number of Messages	20
User (587)	Nickname	PartaiSocmed
	Twitter ID	869327120
	Adress (google maps)	Indonesia
	Url	https://t.co/aDu3oGTVHr

	Description	J☒j🔲Social Media Party | Objectivity, Fairness and Justice for All | Non-Populist Party | Common Sense Party | Empowering People | No = 99I☒☒XIM☒XI☒X🔲🔲🔲🔲🔲XX
	Number of Followers	173470
	Following	3007
	Number of Messages	352939
	Modified	2019-09-24 14:02:56 (UTC+7)
	Picture URL	https://pbs.twimg.com/profile_images/1137182440907108352/iFHhYIh-_normal.jpg
Conversation (4 convers, 23 messages, 1 delete)	Sent Message	N/A
	Received Message	N/A
	Draft	N/A
	Failed Message	N/A
	Unknown Message	N/A
	Deleted Message	OK
	Conversation ID	2455017384-1151071365593628678
	Date/ Time	2019-9-24 14:36:04 (UTC+7)
	Participants	Paranormal, Fauzan
Cached tweets (852, 13 deleted)	Status/ timeline	OK
	Nama Akun	Rudiantara (Rudiantara)
	Tanggal Update	2019-05-25 20:15:31 (UTC+7)
	Words Status	J☒k☒☒Teman2, situasi sdh kondusif shg pembatasan akses fitur video & gambar pd medsos & instant messaging difungsikan kembali. Mari senantiasa jaga dunia maya digunakan unt hal2 yg positif. Mari perangi hoaks, fitnah, info2 yg memprovokasi spt yg banyak beredar saat kerusuhan kemarin.I☒☒XII☒XI☒XI☒XI☒XI☒XXX
	Hastag	NOK
	Language	In
	Url	https://twitter.com/Rudiantara/status/1132273995712090113
	Favorites	4078
	Retweet Count	1299
	Deleted/ Received	Received
Messages (23, 1 deleted)	Chat/ Sent- Received	Convesation ID Conversation: 2455017384-1151071365593628678
	Content	j6https://twitter.com/messages/media/1176399887899848710j☒pic.twitter.com/G1SSNctA22☒☒Si^
Cached Searches	Hastag	
	Account	OK
Application info	Label	Twitter
	Package	Com.twitter. android
	Version	8.13.0-release.00
	Application Type	User Application
	Application Size	50.1 MB
	Data Size	8.1 MB
	Cache Size	88.6 MB
	First Installed	2019-07-16 16:32:30 (UTC+7)
	Last Updated	2019-09-20 18:25:28 (UTC+7)
	Last Active	2019-09-25 11:26:00 (UTC+7)
Video		ok
Gambar		Ditemukan
Suara		Nok
Email		andihiyat@gmail.com
Url		https://twitter.com/Rudiantara/status/1132273995712090113
IP Adress		-
Kontak Telepon		0812 8899 3248

4.6.2 Belkasoft Evidence Center

Data pada Tabel 4.8 berisi nama akun, id akun, aktifitas pengguna, arah pada pesan pribadi, perubahan status, *email*, tautan dan *timeline*, merupakan data yang dapat diambil menggunakan Belkasoft Evidence Center, jumlah data lebih sedikit dari pengambilan menggunakan MOBILedit Forensic Express, penelusuran data yang lebih spesifik pada Belkasoft akan membutuhkan banyak waktu dalam menganalisis, terlebih jika pengguna sudah melakukan banyak aktifitas dalam akun twitternya.

Tabel 4.8 Hasil pengambilan data dari Belkasoft Evidence Center

Evidences	Belkasoft Evidence Center	*Result*
Nama Akun	Found	Paranormal
ID Akun	found	1151071365593628678
User Activity	Status changed	Message; Jj Besok gowesIXIIXIXIXIXIXXX
Incoming Messages	Found	gaasik
Outgoing Messages	Found	Baku hantam, minat?
Status change/ tweets	Found	Jj4Maunya apa ?@rudiantara_id #saveri #freedominternetIMJ��Uij rudiantara_idj RudiantaraXXIXMJ#jsaveriXXI#XMJ$$4jfreedomintern etXXI$4XXIIXIXI@XI s XIXXX;
Email	Found	korbanaksi@gmail.com
Detail account	Found	Follower 46742; messages 5523 modified 2019-09-28
Url	Found	https://pbs.twimg.com/profile_images/852355177260621 824/usivwpwx_normal.jpg
Timeline	Found	JjTKampus A "Initiate Retreat!" Kampus B "Request Back Up!" anak STM "LAUNCH ATTACK!!!"IMJ d jmeisyacvjmeisya and 666 othersXXIXXIIXIXI[XIXIXX

BAB 5. KESIMPULAN

1. Langkah kerja dari *Digitl Forensics Research Workshop* (DFRWS) dapat diimplementasikan untuk proses pengambilan barang bukti sebagai alat pembuktian hukum atau membantu mengantisipasi aksi kejahatan, pembuktian kejahatan menggunakan teknologi hingga mendapat bukti-bukti digital pada layanan media sosial twitter dari perangkat smartphone dengan sistem operasi Android.
2. Penggunakan beberapa *tools* forensik telah mendapatkan barang bukti berupa foto, video, suara, kontak dan beberapa fitur yang tersedia pada layanan media sosial twitter. Pada masa sekarang atau masa yang akan datang dapat dengan mudah untuk mencari petunjuk atau barang bukti yang berkaitan dengan media sosial twitter untuk melakukan penyelidikan dan penyidikan atau hal lain dalam media sosial twitter yang sekiranya menjadi sebuah pelanggaran. Beberapa hal yang dapat diambil dari twitter dengen menerapkan metode *Digital Forensic Research Workshop* (DFRWS):
    a. Pengambilan data berupa informasi akun twitter, pesan atau percakapan pribadi yang dilakukan dengan akun lain, status yang dibuat, pembagian video, serta status atau tweet yang sudah dihapus oleh pengguna dapat ditelusuri dengan baik.
    b. Pada analisis gambar yang dibagikan di twitter juga menjadi indikasi akun twitter digunakan untuk membagikan gambar yang sudah dimodifikasi untuk tujuan kejahatan, didapat dengan membaca metadata dari dua gambar sama yang dapat diambil dari perangkat kemudian dianalisis menggunakan teknik analisis kesalahan, kebisingan, deteksi klon, serta teknik analisis jpeg.
    c. Bukti audio yang diperoleh juga menjadi perhatian karena banyak audio yang di modifikasi.

d. Penggunaan beberapa *tools* forensic juga dapat diterapkan menggunakan metode DFRWS, barang bukti utuh bisa ditemukan dari perangkat
e. Dari *tools* yang digunakan untuk mengambil barang bukti menjadi perhatian karena salah satu *tools* yang digunakan bisa mendapat barang bukti lebih banyak dari *tools* lain, dengan laporan yang disajikan mudah untuk dianalisis, tetapi juga terdapat beberapa kelemahan untuk pengambilan informasi tertentu yang menjadi fitur dari twitter karena data terenkripsi dan tidak bisa dibaca bahkan data tidak ditemukan.

DAFTAR PUSTAKA

Al-Azhar, Nuh Muhammad (2012). "Digital Forensic, Panduan Praktis Investigasi Komputer". Jakarta. Salemba Infotek.

Ari Mukti, W., Masruroh, S. U., & Khairani, D. (2018). Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook Dan Twitter Pada *Smartphone* Android. *Jurnal Teknik Informatika Uin Syarif Hidayatullah*, *10*(1).

Ambaranie. N.K.M. 2017. Ini Hasil Kerja Polri Perangi Kejahatan Siber Sepanjang 2017. Https://Nasional.Kompas.Com/Read/2017/12/29/17233911/Ini-Hasil-Kerja-Polri Perangi-Kejahatan-Sibersepanjang-2017. Diakses 29 sJanuari 2019

Bintang, R. A. K. N., Umar, R., & Yudhana, A. (2018). Perancangan Perbandingan Live Forensics Pada Keamanan Media Sosial Instagram, Facebook Dan Twitter Di Windows 10. *Prosiding Snst Fakultas Teknik*, *1*(1).

Hikmatyar, F. G., & Sugiantoro, B. (2019). Digital Forensic Analysis On Android *Smartphone*s For Handling Cybercrime Cases. *Ijid (International Journal On Informatics For Development)*, *7*(2).

Inggi, R., Sugiantoro, B., & Prayudi, Y. (2018). Penerapan System Development Life Cycle (Sdlc) Dalam Mengembangkan Framework Audio Forensik. *Semantik*, *4*(2).

Kemp, S. Digital In 2018 : World's Internet Users Pass The 4 Billion Mark Https://Wearesocial.Com/Blog/2018/01/Global-Digital-Report-2018. Diakses 29 Januari 2019

Mukti, Wisnu Ari, Siti Ummi Masruroh, & Dewi Khairani. 2017. "Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial." Jurnal Teknik Informatika 10(1): 73–84.

Saputra, I., & Azhar, M. N. (2018, September). Analisis Dan Investigasi Forensik Digital Live Memory Untuk Deteksi Tingkah Laku Agresi Pada Aplikasi Whatsapp. In *Seminar Nasional Dan Diskusi Panel Multidisiplin Hasil Penelitian Dan Pengabdian Kepada Masyarakat 2018* (Vol. 1, No. 1).

Suryana, A. L., El Akbar, R., & Widiyasono, N. (2016). Investigasi Email Spoofing Dengan Metode Digital Forensics Research Workshop (Dfrws). *Jurnal Edukasi Dan Penelitian Informatika (Jepin)*, *2*(2).

Wardana, A. C., Pedrason, R., & Prasetyo, T. B. (2018). Implementasi Digital Forensik Brunei Darussalam Dalam Membangun Keamanan Siber. *Peperangan Asimetrik*, *4*(1).

Yudhistira, D. S. (2018). *Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop* (Master's Thesis, Universitas Islam Indonesia).

Zuhriyanto, I., Yudhana, A., & Riadi, I. (2018, November). Perancangan Digital Forensik Pada Aplikasi Twitter Menggunakan Metode Live Forensics. In *Seminar Nasional Informatika (Semnasif)* (Vol. 1, No. 1).

LAMPIRAN 1

(Salinan Kontrak)

LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
UNIVERSITAS AHMAD DAHLAN
Jl. Gondosuli No. 18 Semaki Yogyakarta. Telp. 0274-542886, 0274-583515 ext. 1502, 1503 Fax. 0274-542886, Website : lppm.uad.ac.id, email : lppm@uad.ac.id

LPPSURAT PERJANJIAN PELAKSANAAN PENELITIAN

Nomor: PUPS-025/SP3/LPPM-UAD/IV/2019

Pada hari ini, **Senin** tanggal **Delapan** bulan **April** tahun **Dua ribu sembilan belas (08-04-2019)**, kami yang bertandatangan di bawah ini:

1. Nama : **Dr. Widodo, M.Si.**
   Jabatan : Kepala Lembaga Penelitian dan Pengabdian Kepada Masyarakat Universitas Ahmad Dahlan (LPPM UAD), selanjutnya disebut sebagai **PIHAK PERTAMA.**
2. Nama : **SUNARDI, S.T., M.T., Ph.D.**
   Jabatan : Dosen/Peneliti pada Program Studi **S2 Teknik Informatika Program Pascasarjana** Universitas Ahmad Dahlan (UAD), selaku Ketua Peneliti, selanjutnya disebut **PIHAK KEDUA.**

Kedua belah pihak menyatakan setuju dan mufakat untuk mengadakan perjanjian pelaksanaan penelitian untuk selanjutnya disebut Surat Perjanjian Pelaksanaan Penelitian (SP3) dengan ketentuan dan syarat-syarat sebagai berikut.

JUDUL PENELITIAN

Pasal 1

(1) PIHAK PERTAMA memberikan pekerjaan kepada PIHAK KEDUA dan PIHAK KEDUA menyatakan menerima pekerjaan dari PIHAK PERTAMA berupa kegiatan pada skim **Penelitian Unggulan Program Studi (PUPS).**

(2) Judul penelitian sebagaimana dimaksud dalam ayat (1) di atas adalah: **"ORENSIK MEDIA SOSIAL PADA PERANGKAT MOBILE MENGGUNAKAN FRAMEWORK DIGITAL FORENSICS RESEARCH WORKSHOP (DFRWS) ."**

PERSONALIA PELAKSANA PENELITIAN

Pasal 2

Pelaksana kegiatan ini terdiri dari:

Ketua Peneliti	: SUNARDI, S.T., M.T., Ph.D.
Pembimbing/Konsultan	: -
Anggota Peneliti 1	: IMAM RIADI, Dr., M.Kom
Anggota Peneliti 2	:

BENTUK DAN JANGKA WAKTU PERJANJIAN

Pasal 3

PIHAK KEDUA melaksanakan penelitian dalam jangka waktu paling lama **6 (enam) bulan** sejak ditandatangani SP3 ini, dan menyerahkan hasil laporan penelitian sementara kepada PIHAK PERTAMA selambat-lambatnya pada **08 Oktober 2019.**

LUARAN/*OUTPUT* PENELITIAN

Pasal 4

PIHAK KEDUA berkewajiban untuk merealisasikan luaran/*output* penelitian seperti yang dijanjikan dalam proposal penelitian di luar Laporan Hasil Penelitian.

BIAYA PENELITIAN DAN CARA PEMBAYARAN

Pasal 5

PIHAK PERTAMA menyediakan dana pelaksanaan penelitian kepada PIHAK KEDUA sejumlah **Rp 18.500.000,00 (Delapan belas juta lima ratus ribu rupiah)** yang dibebankan pada Anggaran Pendapatan dan Belanja (APB) LPPM UAD Tahun Akademik 2018/2019 dibayarkan melalui rekening bank atas nama Ketua Peneliti oleh Bidang Finansial UAD dengan tahapan sebagai berikut.

(a) **Tahap I sebesar 70% x Rp 18.500.000,00 = Rp 12.950.000,00 (Dua belas juta sembilan ratus lima puluh ribu rupiah)** yang akan dibayarkan selambat-lambatnya dua minggu setelah SP3 ini ditandatangani oleh PARA PIHAK dan PIHAK KEDUA telah mengunggah file scan SP3 ini pada portal UAD.

(b) **Tahap II sebesar 30% x Rp 18.500.000,00 = Rp 5.550.000,00 (Lima juta lima ratus lima puluh ribu rupiah)** yang akan dibayarkan setelah PIHAK KEDUA menyelesaikan seluruh kewajibannya dalam jangka waktu seperti yang dimaksud dalam Pasal 3 serta dinyatakan benar dan lengkap.

PELAKSANAAN PEMBIMBINGAN

Pasal 6

(1) Khusus peneliti skema Penelitian Dosen Pemula (PDP) wajib melakukan pembimbingan atau konsultasi dengan dosen pembimbing penelitiannya paling sedikit 3 (tiga) kali pembimbingan.

(2) Pembimbingan sebagaimana dimaksud dalam ayat (1) yaitu pembimbingan dalam hal:
a. penyusunan angket/kuesioner dan atau teknik pengumpulan data lainnya;
b. analisis data dan interpretasinya;
b. penyusunan hasil penelitian, pembahasan, penarikan kesimpulan.

(3) Pembimbingan sebagaimana dimaksud dalam ayat (1) dan ayat (2) dituliskan dalam form pembimbingan yang ditandatangani oleh peneliti dan dosen pembimbing penelitian.

JENIS LAPORAN PENELITIAN

Pasal 7

(1) PIHAK KEDUA wajib menyusun dan menyampaikan laporan penelitian baik secara *on line* melalui portal UAD maupun *hardcopy* kepada PIHAK PERTAMA yang terdiri atas:
a. Laporan Kemajuan
b. Laporan Sementara
b. Laporan Akhir Penelitian

(2) Berkas **Laporan Kemajuan** digunakan sebagai bahan monitoring dan evaluasi (monev) internal.

(3) Berkas **Laporan Sementara** digunakan sebagai bahan kolokium laporan penelitian.

(4) Berkas **Laporan Akhir Penelitian** merupakan revisi dari Laporan Penelitian Sementara yang telah dikolokiumkan.

MONITORING DAN EVALUASI

Pasal 8

(1) PIHAK PERTAMA berhak untuk melakukan monitoring dan evaluasi (monev) internal pelaksanaan penelitian, baik secara administrasi maupun substansi.

(2) Pemantauan kemajuan penelitian dilakukan oleh Tim Monev yang dibentuk oleh PIHAK PERTAMA.

(3) PIHAK KEDUA diharuskan MENYIAPKAN SEMUA DOKUMEN/BUKTI kemajuan pelaksanaan penelitiannya guna kepentingan monev.

(4) Waktu pelaksanaan monev akan ditentukan oleh PIHAK PERTAMA.

KOLOKIUM LAPORAN PENELITIAN

Pasal 9

(1) PIHAK KEDUA wajib menyerahkan **Laporan Penelitian Sementara** sebagai bahan kolokium selambat-lambatnya **08 Oktober 2019.**

(2) Ketua Peneliti wajib hadir dan mempresentasikan hasil penelitiannya pada kolokium **Laporan Penelitian Sementara** yang pelaksanaannya akan diatur oleh PIHAK PERTAMA.

(3) Revisi laporan penelitian yang sudah dikolokiumkan harus mendapatkan pengesahan dari *reviewer* dalam bentuk **Surat Pernyataan** dan dijilid dalam satu kesatuan laporan penelitian.

LAPORAN AKHIR PENELITIAN

Pasal 10

(1) PIHAK KEDUA wajib menyerahkan **Laporan Akhir Penelitian** selambat-lambatnya **2 (dua) pekan** setelah dikolokiumkan.

(2) Sistematika dan format laporan penelitian mengacu pada ketentuan dalam Pedoman Penelitian yang dikeluarkan oleh LPPM dan ketentuan lain yang berlaku.

(3) Berkas Laporan Akhir Penelitian yang diserahkan kepada PIHAK PERTAMA harus dilampiri:
   (a) artikel/draft publikasi ilmiah;
   (b) naskah/draft seminar (prosiding) dan sertifikat seminar;
   (c) lampiran lain yang dianggap perlu (seperti angket atau lainnya);
   (d) Profil Penelitian;
   (e) Borang Capaian Luaran Penelitian;
   (f) Form Pembimbingan (khusus skema PDP)
   (g) Daftar hadir kolokium laporan penelitian; dan
   (h) produk penelitian (naskah buku ajar, modul, naskah akademik, dan sejenisnya) atau dokumentasi/fotonya jika produk penelitian berupa barang atau perangkat keras *(hardware)* yang disertai penjelasan ringkas alat dan petunjuk pemakaiannya.

   Komponen (a) sampai dengan (g) dijilid dalam satu kesatuan sebagai berkas laporan akhir penelitian.

   Komponan (h) dijilid terpisah dari berkas laporan akhir penelitian, kecuali dokumentasi/foto produk penelitian.

(4) Laporan Akhir Penelitian sebagaimana tersebut pada ayat (1), (2), dan (3) memenuhi ketentuan sebagai berikut:
   a. bentuk/ukuran kertas A4;
   b. warna cover sesuai ketentuan;
   c. di bawah bagian cover ditulis:

PENELITIAN INI DILAKSANAKAN ATAS BIAYA
ANGGARAN DAN PENDAPATAN DAN BELANJA UNIVERSITAS AHMAD DAHLAN
TAHUN AKADEMIK 2018/2019
NOMOR KONTRAK: PUPS-025/SP3/LPPM-UAD/IV/2019

(5) Berkas Laporan Akhir Penelitian sebagaimana tersebut dalam ayat (1) diserahkan kepada PIHAK PERTAMA sebagai berikut.
   1 eksemplar **ASLI** untuk PIHAK PERTAMA;
   1 eksemplar untuk PIHAK KEDUA;
   1 eksemplar untuk arsip Program Studi;

(6) PIHAK KEDUA wajib mengunggah file laporan akhir penelitian secara lengkap pada alamat *http://www.simpel.uad.ac.id* melalui akun portal ketua peneliti dengan format file PDF.

KEWAJIBAN UNGGAH LAPORAN PADA PORTAL UAD

Pasal 11

(1) PIHAK KEDUA wajib mengunggah berkas Laporan Akhir Penelitian pada *www.portal.uad.ac.id* melalui akun portal masing-masing peneliti.
(2) Berkas Laporan Akhir Penelitian sebagaimana dimaksud pada ayat (1) yang terdiri dari:
   i. Abstrak (PDF).
   ii. Laporan Akhir Final (PDF).
   iii. Profil Penelitian (PDF).
   iv. Borang Capaian Luaran Penelitian (PDF).

SANKSI DAN PEMUTUSAN PERJANJIAN PENELITIAN

Pasal 12

(1) PIHAK PERTAMA berhak memberikan peringatan dan atau teguran atas kelalaian dan atau pelanggaran yang dilakukan oleh PIHAK KEDUA yang mengakibatkan tidak dapat terpenuhinya kontrak penelitian ini.
(2) PIHAK PERTAMA berhak melakukan pemutusan perjanjian penelitian, jika PIHAK KEDUA tidak mengindahkan peringatan yang diberikan oleh PIHAK PERTAMA.
(3) Segala kerugian material maupun finansial yang disebabkan akibat kelalaian PIHAK KEDUA, maka sepenuhnya menjadi tanggungjawab PIHAK KEDUA.
(4) Jenis sanksi yang diberikan dapat berupa:
   (a) tidak diperkenankannya mengajukan proposal penelitian pada tahun anggaran berikutnya sampai kewajibannya terselesaikan; dan atau
   (b) tidak dapat mencairkan dana tahap 2; dan atau
   (c) mengembalikan dana yang telah diterima oleh PIHAK KEDUA.

KEADAAN MEMAKSA (*FORCE MAJEUR*)

Pasal 13

Ketentuan dalam Pasal 10 tersebut di atas tidak berlaku dalam keadaan sebagai berikut:

a. Keadaan Memaksa (*force majeur*)
b. PIHAK PERTAMA menyetujui atas terjadinya keterlambatan yang didasarkan pada pemberitahuan sebelumnya oleh PIHAK KEDUA kepada PIHAK PERTAMA dengan **surat pemberitahuan** mengenai kemungkinan terjadinya keterlambatan dalam penyelesaian kegiatan penelitian sebagaimana dimaksud dalam Pasal 1 dan Pasal 3; dan sebaliknya PIHAK KEDUA menyetujui terjadinya keterlambatan pembayaran sebagai akibat keterlambatan dalam penyelesaian perjanjian penelitian.

Pasal 14

(1) Keadaan Memaksa (*force majeur*) sebagaimana yang dimaksud dalam Pasal 11 ayat (1) adalah peristiwa-peristiwa yang secara langsung mempengaruhi pelaksanaan perjanjian serta terjadi di luar kekuasaan dan kemampuan PIHAK KEDUA ataupun PIHAK PERTAMA.
(2) Peristiwa yang tergolong dalam keadaan memaksa (*force majeur*) antara lain berupa bencana alam, pemogokan, wabah penyakit, huru-hara, pemberontakan, perang, waktu kerja diperpendek oleh pemerintah, kebakaran dan atau peraturan pemerintah mengenai keadaan bahaya serta hal-hal lainnya yang dipersamakan dengan itu, sehingga PIHAK KEDUA ataupun PIHAK PERTAMA terpaksa tidak dapat memenuhi kewajibannya.
(3) Peristiwa sebagaimana dimaksud pada ayat (2) tersebut di atas, wajib dibenarkan oleh penguasa setempat dan diberitahukan dengan Surat oleh PIHAK KEDUA atau PIHAK PERTAMA kepada PIHAK PERTAMA atau PIHAK KEDUA selambat-lambatnya 7 (tujuh) hari sejak terjadinya peristiwa yang dikategorikan sebagai Keadaan Memaksa (*force majeur*).

(4) PIHAK PERTAMA memberikan kesempatan kepada PIHAK KEDUA untuk menyelesaikan perjanjian kontrak ini sampai pada batas waktu yang disepakati oleh kedua belah pihak jika keadaan *force majeur* dinyatakan telah selesai.

PENYELESAIAN PERSELISIHAN

Pasal 15

(1) Apabila dalam pelaksanaan perjanjian dan segala akibatnya timbul perbedaan pendapat atau perselisihan, PIHAK PERTAMA dan PIHAK KEDUA setuju untuk menyelesaikannya secara musyawarah untuk mencapai mufakat.

(2) Apabila penyelesaian sebagaimana termaksud dalam ayat (1) di atas tidak tercapai, maka PIHAK PERTAMA dan PIHAK KEDUA sepakat menyerahkan perselisihan tersebut melalui mediasi dengan Rektor sebagai atasan langsung dari PIHAK PERTAMA yang putusannya bersifat final dan mengikat.

PENGUNDURAN DIRI

Pasal 16

(1) Apabila PIHAK KEDUA mengundurkan diri atau membatalkan SP3 ini, maka PIHAK KEDUA wajib mengajukan Surat Pengunduran Diri yang ditujukan kepada PIHAK PERTAMA.

(2) Surat Pengunduran Diri sebagaimana dimaksud pada ayat (1) wajib disahkan oleh Dekan fakultas ketua peneliti yang bersangkutan; dan bagi peneliti skim PDP ditambah persetujuan Dosen Pembimbing.

(3) PIHAK KEDUA wajib mengembalikan dana yang telah diterima kepada PIHAK PERTAMA

LAIN-LAIN

Pasal 17

(1) Hal-hal yang dianggap belum cukup dan perubahan-perubahan perjanjian akan diatur kemudian atas dasar permufakatan kedua belah pihak yang akan dituangkan dalam bentuk Surat atau Perjanjian Tambahan (*addendum*), yang merupakan kesatuan dan bagian yang tidak terpisahkan dari perjanjian awal.

(2) Pemberitahuan dan/atau surat menyurat dari PIHAK KEDUA kepada PIHAK PERTAMA dialamatkan kepada Kepala Lembaga Penelitian dan Pengembangan Universitas Ahmad Dahlan.

Pasal 18

(1) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini berlaku sejak ditandatangani dan disetujui oleh kedua belah pihak.

(2) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini dibuat rangkap 2 (dua); bermeterai cukup pada kedua belah pihak; dan masing-masing memiliki kekuatan hukum yang sama. Biaya meterai dibebankan kepada PIHAK KEDUA.

PIHAK PERTAMA,	PIHAK KE DUA,
Dr. Widodo, M.Si.	**SUNARDI, S.T., M.T., Ph.D.**
NIP: 19600221198709101	NIP/NIY.

LAMPIRAN 2

(Borang Capaian Luaran Penelitian)

BORANG CAPAIAN LUARAN PENELITIAN
SUMBERDANA UAD TAHUN AKADEMIK 2019/2020
SKEMA PENELITIAN UNGGULAN PROGRAM STUDI

I. IDENTITAS PENELITI

Judul penelitian	: Forensik Media Sosial pada Perangkat Mobile Menggunakan Framework Digital Forensics Research Workshop (DFRWS)
Ketua Peneliti	: Sunardi, S.T., M.T., Ph.D
NIDN / e-mail	: 0521057401/sunardi@mti.uad.ac.id
Prodi/Fakultas	: Pascasarjana/Magister Teknik Informatika
Anggota Peneliti 1	: Dr. Imam Riadi, M.Kom
Jenis/Tahap Penelitian	: Pengembangan
TKT/TRL	:

II. CAPAIAN LUARAN PENELITIAN

A. PUBLIKASI ILMIAH

	Keterangan
ARTIKEL JURNAL KE-1*[1]	**FORENSIK *MOBILE* PADA APLIKASI SOSIAL MEDIA MENGGUNAKAN METODE DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS)**
Nama jurnal yang dituju	Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)
Level jurnal	Nasional
Status	Terakreditasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	http://jtiik.ub.ac.id/index.php/jtiik

*[1] Jika masih ada artikel ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

B. BUKU AJAR

Buku ke-1*[2]	**Keterangan**
Judul buku	
Penulis	
Penerbit	
No. ISBN	
Buku ke-2, dst.	

*[2] Jika masih ada buku ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

C. PEMBICARA PADA PERTEMUAN ILMIAH (SEMINAR/SIMPOSIUM)

Mengikuti seminar*[3]	**Keterangan**
Pertemuan Ilmiah ke-1	
- Judul Makalah	
- Nama pertemuan ilmiah	

- Tempat pelaksanaan	
- Waktu pelaksanaan	
- Jenis pertemuan	
- Status naskah	
Pertemuan Ilmiah ke-2, dst.	

*[3] Jika masih ada undangan ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

D. PEMBICARA KUNCI/*KEYNOTE* SPEAKER PADA PERTEMUAN ILMIAH (SEMINAR/SIMPOSIUM)

	Keterangan
- Judul makalah	
- Penulis	
- Penyelenggara	
- Waktu Pelaksanaan	
- Tempat Pelaksanaan	
- Skala pertemuan	Regional/Nasional/Internasional
- Status pertemuan	Sudah dilaksanakan / belum
- Alamat URL artikel	
-	

*[3] Jika masih ada undangan ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

E. Menjadi Peneliti Tamu (*Visiting Scientist)*

Menjadi peneliti tamu (*visiting scientist*) pada perguruan tinggi lain*[4]	**Nasional**	**Internasional**
- Perguruan tinggi pengundang		
- Lama kegiatan		
- Kegiatan penting yang dilakukan		

*[4] Jika masih ada undangan ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

F. Hak Kekayaan Intelektual dan Lainnya

Jenis HKI	**Uraian**
Paten	Tuliskan judul paten adan tanggal pengajuannya
Hak Cipta	Tuliskan bentuk dan atau nama/judul hak cipta dan tanggal pengajuannya
TEKNOLOGI TEPAT GUNA	Jelaskan nama TTG dan pemanfaatan serta penggunanya

REKAYASA SOSIAL	Uraikan kebijakan publik yang sedang atau sudah dapat diubah
JEJARING KERJA SAMA	Uraikan kapan jejaring dibentuk dan kegiatannya sampai saat ini, baik antarpeneliti maupun antarlembaga
PENGHARGAAN	Uraikan penghargaan yang diterima sebagai peneliti, baik dari pemerintah atau asosiasi profesi
LAINNYA	Tulis dan uraikan luaran HKI lainnya

Yogyakarta, 31 Oktober 2019
Ketua Peneliti,

Sunardi, S.T., M.T., Ph.D

LEMBAR TAMBAHAN

	Keterangan
ARTIKEL JURNAL KE-2	**Audio Forensic on Smartphone with Digital Forensic Research Workshop Method (DFRWS)**
Nama jurnal yang dituju	IGI Global International Journal of Technoethics (IJT)
Level jurnal	Internasional
Status	Bereputasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	https://www.igi-global.com/
ARTIKEL JURNAL KE-3	**FORENSIK MOBILE PADA SMARTPHONE ANDROID MENGGUNAKAN METODE DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS)**
Nama jurnal yang dituju	Jurnal Penelitian Pos dan Informatika (JPPI)
Level jurnal	Nasional
Status	Terakreditasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	jurnal-ppi.kominfo.go.id
ARTIKEL JURNAL KE-4	Analisis Perbandingan *Tools* Forensik Metode
Nama jurnal yang dituju	Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)
Level jurnal	Nasional
Status	Terakreditasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	http://www.jurnal.iaii.or.id/index.php/RESTI
ARTIKEL JURNAL KE-5	Image Forensic with *Digital Forensic Research Workshop* Method
Nama jurnal yang dituju	IGI GLOBAL Internasional journal of digital crime and forensics
Level jurnal	Internasional
Status	Bereputasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	https://www.igi-global.com/

LAMPIRAN 3

(Profil Penelitian)

FORENSIK MEDIA SOSIAL PADA PERANGKAT MOBILE MENGGUNAKAN FRAMEWORK DIGITAL FORENSICS RESEARCH WORKSHOP (DFRWS)

Peneliti

Sunardi, S.T., M.T., Ph.D

Pascasarjana/Magister Informatika
Universitas Ahmad Dahlan
sunardi@mti.uad.ac.id

Dr. Imam Riadi, M.Kom.

Pascasarjana/Magister Informatika
Universitas Ahmad Dahlan
Imam.riadi@mti.uad.ac.id

Ringkasan Eksekutif

Perkembangan di bidang teknologi komunikasi menyebabkan para pengguna beralih dari perangkat komputer kepada perangkat *mobile*, salah satunya adalah *smartphone*. *Smartphone* terdiri dari berbagai sistem operasi, sistem operasi dengan pengguna yang cukup banyak adalah Android. Fiturnya yang lengkap dan kemudahan yang ditawarkan membuat Android memiliki banyak pengguna. Aplikasi dari *smartphone* yang banyak digunakan oleh pengguna adalah aplikasi media sosial seperti Twitter, Whatsapp, dan Line. Salah satu aplikasi sosial media yang banyak digunakan adalah aplikasi Twitter, namun belakangan ini aplikasi Twitter menjadi salah satu aplikasi media sosial yang digunakan untuk melakukan ujaran kebencian, pencemaran nama baik dan tindak kejahatan lainnya.

Banyaknya pengguna aplikasi media sosial ini tentunya memiliki dampak positif dan negatif. Dampak negatif yang ditimbulkan dari penggunaan aplikasi media sosial adalah munculnya oknum-oknum yang melakukan kejahatan digital menggunakan aplikasi media sosial yang terinstall pada *smartphone*. Indikasi adanya kejahatan digital tersebut dapat dibuktikan dengan suatu metode forensik salah satunya *Digital Forensics Research Workshop* (DFRWS) dimana tahapan forensic ini meliputi *identification, preservation, collection, examination*, *analysis* dan *presentation* dalam menemukan bukti digital tindak kejahatan.

Penelitian ini bertujuan untuk memberikan gambaran proses pengangkatan bukti digital pada aplikasi Twitter yang terinstall pada *smartphone* berbasis Android. Hasil penelitian ini diharapkan dapat digunakan sebagai acuan peneliti selanjutnya yang berminat mengembangkan penelitian di bidang *mobile* forensik, terutama pada aplikasi media sosial yang terinstall pada *smartphone* dan berbasis Android.

HKI dan Publikasi

1. Analisis Digital forensik aplikasi twitter menggunakan Digital Forensik Research Workshop (DFRWS) (Submitted)
2. Audio Forensic on Smartphone with *Digital Forensic Research Workshop* Method (DFRWS) (Submitted)
3. Mobile Forensik Aplikasi Pembayaran Digital Menggunakan Metode DFRWS (Submitted)
4. Analisis Perbandingan *Tools* Forensik Metode *Digital Forensic Research Workshop* Method (Submitted)
5. Image Forensic with *Digital Forensic Research Workshop* Method (Submitted)

Latar Belakang

Perkembangan di bidang teknologi komunikasi menyebabkan para pengguna beralih dari perangkat komputer kepada perangkat *mobile*, salah satunya adalah *smartphone*. *Smartphone* terdiri dari berbagai sistem operasi, sistem operasi dengan pengguna yang cukup banyak adalah Android. Fiturnya yang lengkap dan kemudahan yang ditawarkan membuat Android memiliki banyak pengguna. Aplikasi dari *smartphone* yang banyak digunakan oleh pengguna adalah aplikasi media sosial seperti Twitter, Whatsapp, dan Line. Salah satu aplikasi sosial media yang banyak digunakan adalah aplikasi Twitter, namun belakangan ini aplikasi Twitter menjadi salah satu aplikasi media sosial yang digunakan untuk melakukan ujaran kebencian, pencemaran nama baik dan tindak kejahatan lainnya.

Hasil dan Manfaat

1. Menambah pengetahuan tentang forensik pada perangkat *mobile* berbasis Android.
2. Menjadi bahan referensi untuk penelitian tentang *mobile forensic* dengan menggunakan metode *digital framework forensic research workshop* (DFRWS).

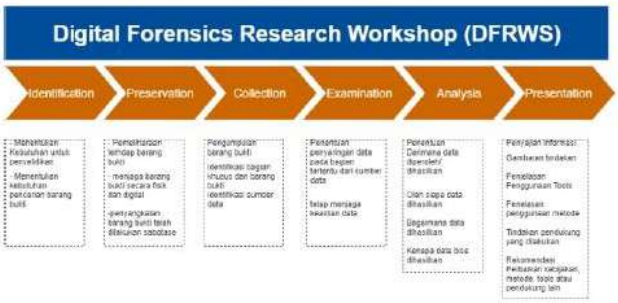
Banyaknya pengguna aplikasi media sosial ini tentunya memiliki dampak positif dan negatif. Dampak negatif yang ditimbulkan dari penggunaan aplikasi media sosial adalah munculnya oknum-oknum yang melakukan kejahatan digital menggunakan aplikasi media sosial yang terinstall pada *smartphone*. Indikasi adanya kejahatan digital tersebut dapat dibuktikan dengan suatu metode forensik salah satunya *Digital Forensics Research Workshop* (DFRWS) dimana tahapan forensic ini meliputi *identification, preservation, collection, examination, analysis* dan *presentation* dalam menemukan bukti digital tindak kejahatan.

Metode

Digital Forensics Research Workshop merupakan penggunaan metode ilmiah yang memiliki dasar dan terbukti untuk pemeliharaan, mengumpulkan, validasi, identifikasi, analisis, interpretasi, dokumentasi dan presentasi bukti digital yang berasal dari sumber-sumber digital untuk tujuan memfasilitasi atau melanjutkan rekontruksi peristiwa yang mengandung pidana, atau membantu untuk mengantisipasi tindakan yang tidak sah yang terbukti menggangu untuk operasi yang direncanakan.

Digital Forensics Research Workshop merupakan penggunaan metode ilmiah yang memiliki dasar dan terbukti untuk pemeliharaan, mengumpulkan, validasi, identifikasi, analisis, interpretasi, dokumentasi dan presentasi bukti digital yang berasal dari sumber-sumber digital untuk tujuan memfasilitasi atau melanjutkan rekontruksi peristiwa yang mengandung pidana, atau membantu untuk mengantisipasi tindakan yang tidak sah yang terbukti menggangu untuk operasi yang direncanakan (Ademu, Imafidon, Preston, 2011).

Berbagai metode computer forensics dan juga digital forensics dikembangkan demi menghadapi berbagai jenis metode ancaman siber yang terdiri dari berbagai tingkatan dan saluran, selain itu metode digital forensics juga dikembangkan guna menghadapi peningkatan jumlah serangan siber yang sekarang telah menjadi tren global.



Gambar 1. Metode DFRWS

LAMPIRAN 4

(Presensi Kolokium)

DAFTAR HADIR KOLOKIUM
LAPORAN PENELITIAN DANA UAD T.A. 2018/2019

Hari, Tanggal : Senin, 25 Nov 2019
Pukul : 13.00
Tempat : R. Sidang Industri
Reviewer/Pemonev : .....

No.	Nama Pengusul	Skema	Tanda Tangan
1.	Taufiq Ismail, S.T. M.G.	PUPS.	
2.	Adhi Prahara	PUPS	
3.	M. Fauzan Gustafi	PUPS	
4.	Ghufron Zaida Muflih	PUPS	
5.	Annie Purwani STP, MT	PUPS	
6.	Utaminingsih Linarti ST, MT	PUPS	
7.	Irsyad Riadi	PUPS	
8.			
9.			
10.			

Yogyakarta, ...
Kepala LPPM UAD,

Dr. Widodo, M.Si.
NIP. 19600221 198709 1 001

LAMPIRAN 5

(Personalia Peneliti)

PERSONALIA PENELITIAN

Judul Penelitian : Forensik Media Sosial pada Perangkat Mobile Menggunakan Framework Digital Forensics Research Workshop (DFRWS)

Skema : Penelitian Unggulan Program Studi

1. Ketua Peneliti

a. Nama Lengkap dan Gelar : Sunardi, S.T., M.T., Ph.D
b. NIDN/NIY/NIP : 0521057401/ 60010313/19700206 200501 1 001
c. Fakultas/Program Studi : Pascasarjana/Magister Teknik Informatika
d. Jabatan Akademik : TP/AA/L/LK/GB
e. Alokasi waktu untuk penelitian : 10 minggu
f. Tugas dalam penelitian : 1. Koordinasi team work

2. Anggota Peneliti 1

a. Nama Lengkap dan Gelar : Dr. Imam Riadi, M.Kom
b. NIDN/NIY/NIP : 0510088001/ 60020397/ 19700206 200501 1 001
c. Fakultas/Program Studi : Pascasarjana/Magister Teknik Informatika
d. Jabatan Akademik : TP/AA/L/LK/GB
e. Alokasi waktu untuk penelitian : 10 minggu
f. Tugas dalam penelitian : 1. Koordinasi team work

3. Keterlibatan Mahasiswa

No	Nama Mahasiswa dan NIM	Program Studi	Tugas dalam Tim	Judul Tugas Akhir
1	Ikhsan Zuhriyanto NIM:1807048012	Magister Teknik Informatika	Penulisan Jurnal	Analisis Digital Forensik Aplikasi Twitter Menggunakan Digital Forensik Research Workshop (DFRWS)
2	Muhammad Fauzan Gustafi NIM: 1807048015	Magister Teknik Informatika	Penulisan Jurnal	Forensik Audio di Smartphone Menggunakan Metode Digital Forensic Research Workshop (DFRWS) Untuk Keperluan Barang Bukti Digital
3	Muhammad Noor Fadillah NIM:1807048006	Magister Teknik Informatika	Penulisan Jurnal	Mobile Forensik Aplikasi Pembayaran Digital Menggunakan Metode DFRWS

	Ghufron Zaida Muflih NIM: 1807048002	Magister Teknik Informatika	Penulisan Jurnal	Analisis Perbandingan Metode Backpropagation dan Adaptive Neuro Fuzzy Inference System untuk Prediksi Curah Hujan
	Wicaksono Yuli Sulistyo NIM: 1807048009	Magister Teknik Informatika	Penulisan Jurnal	Image Forensik untuk Mendeteksi Image Forgery Pada Foto Digital

LAMPIRAN 6

(Jurnal Internasional dan Jurnal Nasional)

FORENSIK *MOBILE* PADA APLIKASI SOSIAL MEDIA MENGGUNAKAN METODE DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS)

[1]Imam Riadi , Sunardi[2], Anton Yudhana[3] dan Ikhsan Zuhriyanto[4]

[1] Program Studi Sistem Informasi, Universitas Ahmad Dahlan
[2,3] Program Studi Teknik Elektro, Universitas Ahmad Dahlan
[4] Program Studi Teknik Informatika, Universitas Ahmad Dahlan
Email: [1]imam.riadi@mti.ac.id, [2]sunardi@mti.uad.ac.id , [3]eyudhana@mti.uad.ac.id,
[4]ikhsan1807048012@webmail.uad.ac.id

(Naskah masuk: dd mmm yyyy, diterima untuk diterbitkan: dd mmm yyyy)

Abstrak

Peningkatan teknologi dunia internet dan smartphone bersamaan dengan peningkatan pengguna aplikasi media sosial yang menggunakan smartphone salah satunya menggunakan operasi Android. Salah satu dampak permasalahan yang kemudian sering terjadi di sosial media adalah menambahnya kejahatan pada bidang teknologi sosial media, walaupun tidak ada kejahatan yang tidak meninggalkan bukti digital. Aplikasi Twitter adalah salah satu sosial media yang banyak digunakan oleh penggunanya. Penelitian ini dilakukan untuk menemukan bukti forensic pada aplikasi sosial media Twitter yang diakses menggunakan media browser dan juga smartphone. Tindakan kejahatan seperti penipuan, penghinaan, ujaran benci dan tindak kejahatan lainnya belakangan ini banyak menggunakan aplikasi sosial media khususnya Twitter. Penelitiain ini menggukan metode *Digital Forensics Research Workshop* (DFRWS) untuk melakukan forensic dengan teknik *live forensic* pada *smartphone* yang menggunakan aplikasi Twitter. Tahapan forensik ini meliputi *identification, preservation, collection, examination, analysis* dan *presentation* dalam menemukan bukti digital tindak kejahatan dengan menggunakan software MOBILedit dan Belkasoft dimana pada *smartphone* yang di forensic dapat ditemukan informasi account yang digunakan, status, chat dan media baik berupa foto maupun video.

Kata Kunci: *Digital Forensik, Live Forensic, Mobile Forensics*, Twitter

MOBILE FORENSICS IN SOCIAL MEDIA APPLICATIONS USING THE DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS) METHOD

Abstract

The increase in internet and smartphone technology, together with the increase in the use of social media applications using smartphones, one of which uses Android operations. One that causes problems that then often occur in social media is adding it to the field of social media technology, while there is no crime that does not accept digital evidence. Twitter application is one of the social media that is widely used by its users. This research was conducted to find forensic evidence on Twitter's social media applications provided using a media browser and smartphone. Acts of crime such as debates, insults, hate speech, and other riots using a particular social media application Twitter. This research uses the Digital Forensics Research Workshop (DFRWS) method to conduct forensics with forensic life techniques on smartphones that use the Twitter application. This forensic stage contains identification, preservation, collection, examination, analysis, and presentation in finding digital evidence of criminal acts using MOBILedit and Belkasoft software, where on the forensic smartphone can be found the account information used, status, chat and good media using photo or video.

Keywords: *Digital Forensik, Live Forensic, Mobile Forensic, Twitter*

1. PENDAHULUAN

Salah satu sifat dasar yang dimiliki oleh manusia yaitu saling berkomunikasi dan berinteraksi dengan sesama manusia lainnya. Komunikasi selanjutnya berbentuk kelompok dalam berinteraksi, sifat dalam kelompok ini didasari pada kemampuan dalam berkomunikasi, mengungkapkan rasa dan kemampuan untuk saling bersosial. Pada era digital saat ini menjadi salah satu faktor dalam menggunakan teknologi informasi yang dipengaruhi oleh kemudahan dalam komunikasi.Selain memberikan manfaat, perkembangan era digital juga memberikan dampak negative juga yaitu banyaknya kasus kejahatan meningkat menggunakan aplikasi di internet. Kejahatan dunia maya semakin meningkat setiap tahunnya (Larasati & Hidayanto, 2017).

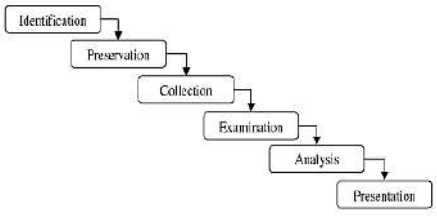
Perkembangan dibidang teknologi informasi seperti sosial media Facebook, Twitter dan Instagram telah menjangkau kehidupan bermasyarakat, terutama generasi remaja. Dampak buruk yang dihasilkan dari penggunaan teknologi ini adalah penyalahgunaan dalam melakukan kejahatan. Penyalahgunaan penggunaan sosial media tersebut biasanya dikenal dengan nama cybercrime (Handrizal, 2017).

Sosial media Twitter telah menjadi penghubung telekomunikasi antar manusia di dunia siber (cyber). Pertumbuhan sosial media dan aplikasi pesan instan telah mempermudah pengembangan banyak kejahatan cyber dan aktivitas jahat yang serius (Anwar & Riadi, 2017). Penggunaan sosial media Twitter yang semakin mudah, terutama dalam mendaftarkan akun baru membuat memunculkan banyak akun palsu yang selain digunakan untuk berkomunikasi juga digunakan untuk menuliskan berita tidak benar, penipuan dan juga pencemaraan nama baik terhadap seseorang sehingga pada akhirnya merugikan banyak pihak (Zuhriyanto, Yudhana, & Riadi, 2018). Kejahatan di dunia digital sulit di deteksi secara fisik melainkan harus menggunakan pemrosesan digital, dikarenakan jejak pelaku semakin berkembang menuju kejahatan asimetris (Aryo C Ki Wardana, Pedrason, & Prasetyo, 2018).

Perkembangan teknologi internet juga di dasari oleh perkembangan *smartphone*, saat ini memudahkan banyak orang dalam mengakses informasi dan diikuti oleh pertumbuhan penggunaan sosial media. Data akun yang aktif setara dengan 31% dari jumlah penduduk dunia atau sekitar 2,31 Triliun. Pengguna aplikasi sosial media Twitter sendiri pada bulan juni 2016 telah menembus 310 juta pengguna, dimana kejahatan pada media sosial Twitter semakin meningkat tiap tahunnya (Mukti, Masruroh, & Khairani, 2017).

2. METODE PENELITIAN

Penelitian ini menggunakan metode digital forensik yang dibuat oleh *Digital Forensic Research Workshop* (DFRWS). Metode DFRWS membantu dalam memperoleh barang bukti dan merekam informasi yang dibutuhkan untuk kemudian dikumpulkan menggunakan data mekanisme terpusat (Suryana, Akbar, & Widiyasono, 2016a). Metode tersebut mempunyai beberapa tahap yaitu seperti pada gambar 1.



Gambar 1. Alur DFRWS

1. Identification

Tahap ini merupakan proses identifikasi dalam pencarian barang bukti digital dan menentukan kebutuhan yang diperlukan untuk proses penyelidikan.

2. Preservation

Tahap ini merupakan tahap pemeliharaan yang diperlukan untuk menjaga bahwa barang bukti digital masih terjaga keasliannya. Barang bukti tidak dilakukan perubahan atau disabotase.

3. Collection

Melakukan proses pengumpulan dan mengidentifikasi bagian yang dibutuhkan untuk melakukan identifikasi dari sumber data berdasarkan barang bukti digital.

4. Examination

Tahap ini menentukan *filtering* pada salah satu bagian yang berasal dari sumber data, tetapi tetap menjaga keaslian dari isi data tersebut dikarenakan sifat dari keaslian data sangat penting oleh karena itu *filtering* data dilakukan hanya dari sisi perubahan bentuk pada data dengan tetap menjaga keaslian data.

5. Analysis

Melakukan penelitian untuk dapat mengetahui dimana, oleh siapa dan bagaimana data dari sebuah kasus tersebut dapat dihasilkan.

6. Presentation

Tahapan presentasi dilakukan dengan menampilkan informasi yang diperoleh dari tahap sebelumnya, kemudian dilakukan pendataan data hasil dari analisis yang diperoleh meliputi pelaporan tindakan yang sudah dilakukan. Penjelasan mengenai metode dan *tools* yang di terapkan untuk menentukan tindakan yang dibutuhkan serta memberikan saran dan masukan untuk perbaikan sebuah kebijakan, metode, *tools* atau aspek pendukung lainnya jika dibutuhkan.

2.1 Twitter

Twitter merupakan aplikasi dari sebuah situs website dan mobile yang bergerak pada jaringan sosial dan menghubungkan penggunanya untuk berkim pesan berupa gambar, teks, video, audio, dengan batasan teks hingga hingga 140 karakter kata. Salah satu fitur dari jejaring sosial ini adalah jangkauan yang luas, selain itu potensi untuk beriklan dan komunikasi yang begitu cepat, serta terhubung oleh banyak jaringan dan lebih terukur dari aplikasi facebook (Kwak, Lee, Park, & Moon, 2010). Media massa konvensional dalam penyampaian berita-beritanya juga terkadang menggunakan aplikasi Twitter. Aplikasi sosial media Twitter menyebarkan informasi dengan cepat dan dijadikan topik yang dibahas oleh para penggunanya. Hal ini membuat masyarakat mendapatkan informasi begitu cepat dan terbaru karena berita dipebarui melalui jejaring sosial.

2.2 *Tools Forensic*

Perangkat *tools* forensik yang bisa digunakan untuk mengambil data dari ponsel atau *tools* ekstraksi bisa berupa software atau hardware. Banyak *tools* ekstraksi yang beredar saat ini mulai dari *tools* yang gratis dengan keterbatasan fitur dan berbayar dengan banyak fitur didalamnya yang digunakan untuk menggali bukti yang di perlukan (Febriyanto & Sembiring, 2016). Perangkat *tools* yang sifatnya komersil sulit didapatkan terkait dengan privasi dan keamanan serta biaya yang sangat tinggi, berikut beberapa *tools* yang digunakan dalam penelitian ini.

2.2.1 MOBILedit Forensic

MOBILedit merupakan *tools forensic* yang memungkinkan penyidik memperoleh secara *logic*, mencari dan memeriksa ponsel. Menggunakan beberapa mekanisme konektivitas terutama nirkabel, cukup baik digunakan untuk memperoleh informasi sistem telepon dan informasi lain seperti kontak dan pesan (Yadi & Kunang, 2014).

2.2.2 Belkasoft Evidence Center

Belkasoft Evience Center, dapat digunakan untuk mendapatkan, mencari, menganalisa dan menyimpan berbagai bukti digital yang ada pada perangkat komputer atau *mobile*, *tools* ini untuk mengekstrak bukti digital dari berbagai sumber dengan menganalisis penyimpanan *hard drive*, memory dump, iOs BlackBerry dan android backup kemudian secara otomatis menganalisis sumber data dan menyimpannya dalam sebuah laporan (Parekh & Jani, 2018a).

3. HASIL DAN PEMBAHASAN

Metode *Live forensic* adalah proses analisis pengambilan barang bukti pada data yang sedang berjalan di *system* (Yudhana, Riadi, & Anshori, 2018). Metode *Live Forensic* memiliki sebagian kesamaan dengan teknik forensik tradisional yaitu tahapan pertama identifikasi penyimpanan, tahapan kedua analisis dan terakhir presentasi. Metode *live forensics* adalah hasil dari kurangnya teknik forensik tradisional yang tidak dapat memperoleh hasil barang bukti ketika sistem sedang melakukan proses misalnya aktivitas memory berjalan, proses *network*, *swap file* data dan proses *running system*. Data yang diperoleh dari file sistem ini menjadi kelebihan dari teknik *live forensics* (Ahmad, Riadi, & Prayudi, 2017).

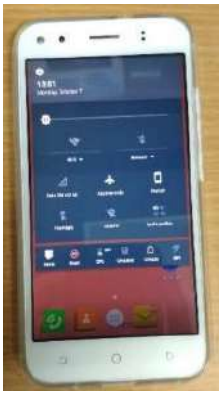
3.1 Tahapan Forensik

Metode Digital Forensik Research Workshop (DFRWS) merupakan salah satu metode forensic yang memiliki tahapan cukup

lengkap dalam menjalakan proses forensic dan banyak digunakan oleh penyidik forensic. *Digital Forensic Research Workshop* merupakan penggunaan metode dengan tujuan memfasilitasi atau melanjutkan rekontruksi peristiwa tindak kejahatan yang mengandung pidana, atau membantu untuk mengantisipasi tindakan yang tidak sah yang terbukti menggangu untuk operasi yang direncanakan. Metode DFRWS memiliki 6 tahapan utama, yaitu *identification, preservation, collection, examination, analysis* dan *presentation.*

Tahapan pertama yang dilakukan adalah identifikasi untuk dijadikan bahan acuan pada barang bukti yang sedang dilakukan pencarian berdasarkan kasus yang telah terjadi sebelumnya.

Tahap kedua adalah preservation, yaitu tahap pemeliharaan barang bukti digital dan memastikan keadaan barang bukti asli. Proses penjagaan integrasi dilakukan untuk menjaga barang bukti itu asli dan tidak rusak, barang bukti fisik dan pembuatan backup data atau proses image file dari barang bukti yang diperoleh dengan teknik isolasi. Tahap yang dilakukan adalah melakukan isolasi perangkat *smartphone* dari komunikasi. Teknik isolasi perlu dilakukan untuk menghindari hal-hal yang dapat merusak bukti digital atau mempengaruhi integritas data didalamnya. Kegiatan isolasi yang dilakukan adalah merubah status perangkat kedalam Mode Pesawat seperti ada gambar 2.



Gambar 2. Mode Pesawat

Tahapan selanjutnya adalah tahapan dilakukannya proses pengumpulan identifikasi bagian yang khusus dari barang bukti digital dan melakukan identifikasi sumber data. Barang bukti yang diusulkan adalah sebuah perangkat *smartphone.* Penelitian ini menggunakan *smartphone* Evercross seperti pada gambar 3.

Gambar 3. *Smartphone*

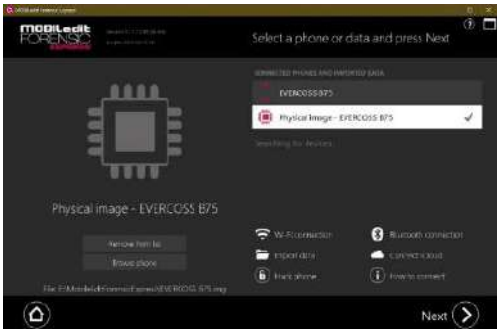
Spesifikasi lebih detail dapat dilihat pada tabel 1 seperti berikut.

Tabel 1. Spesifikasi *Smartphone*

Jenis	Spesifikasi
Merek	Evercross
Seri	Elevote
Model	Y3+
IMEI	358441061746404
OS	Android
Versi OS	5.1 (Lolipop)
Processor	Quad Core 1.0 GHz

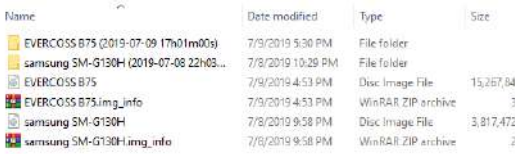
Tahap pengambilan barang bukti digital pada *smartphone* memiliki resiko yang tinggi, jika terjadi kesalahan fatal, data dan bukti digital yang ada pada *smartphone* dapat hilang atau *corrupted* sehingga tidak terbaca, oleh karena itu perlu dilakukan preservasi barang bukti, yaitu melakukan *backup* atau *imaging smartphone* yang menjadi barang bukti, proses ini disebut juga *logical acquisition*.

Perangkat *tools* yang digunakan untuk melakukan proses backup adalah MOBILedit Forensic Express. Kemampuan tool ini adalah dapat membuat sebuah backup sistem *smartphone* dan mengekstraksinya. gambar 4. merupakan proses backup pada *smartphone* dengan MOBILedit Forensic Express.



Gambar 4. Aplikasi MOBILedit

Hasil dari proses backup ini berupa dokumen image dari *smartphone* dengan ekstensi .img dengan ukuran dokumen yang bervariasi tergantung banyaknya data pada *smartphone* tersebut. Gambar 5 merupakan hasil backup dari proses yang sudah dilakukan.

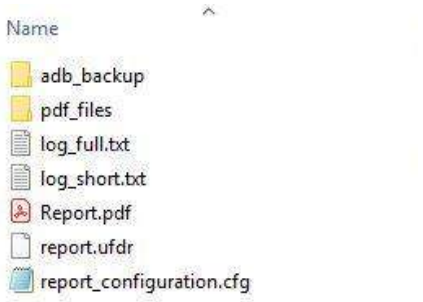


Gambar 5. Physical Image

Setelah dilakukan backup, langkah selanjutnya adalah melakukan ekstraksi data dengan menggunakan *tools* MOBILedit Forensic Express, pada tahap ini barang bukti atau *smartphone* harus terkoneksi terlebih dahulu pada computer tempat MOBILedit Forensik Express di-instal. Gambar 6 merupakan proses ekraksi data.

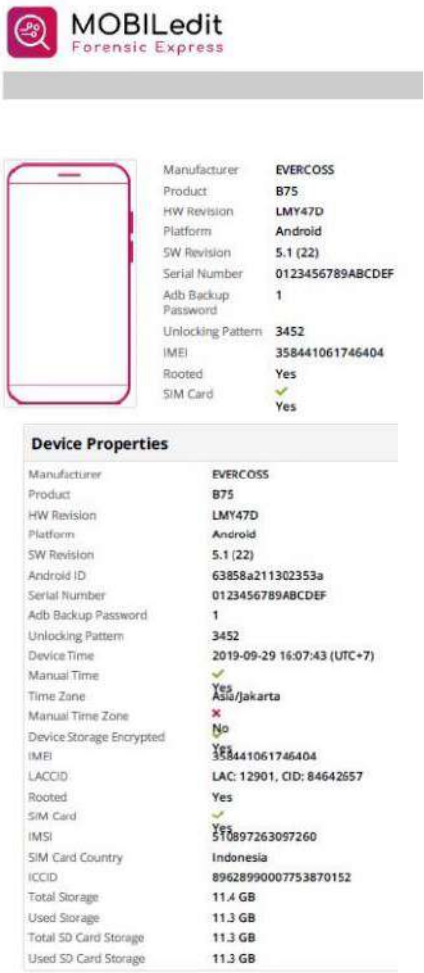
Gambar 6. Proses Extraction

Hasil ekstraksi yang telah dilakukan akan ditampilkan dalam full *report* pada penelitian ini. Full *report* yang dipilih adalah dalam bentuk format.pdf, tampilan full *report* untuk barang bukti seperti yang ditunjukan pada gambar 7.



Gambar 7. Hasil Extraction

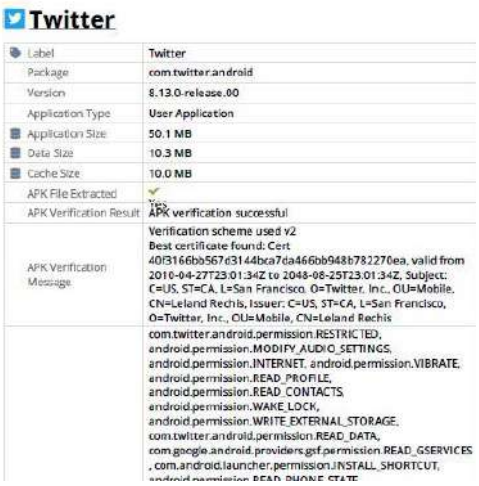
Hasil dari laporan Report.pdf dapat menunjukan bahwa *smartphone* yang digunakan adalah bermerk Evercross dan spesifikasinya secara lebih detail, Selain spesifikasi didapat juga informasi lain seperti *time zone*, IMEI, Storage dan lainnya, sesuai dengan yang di tunjukan pada gambar 8.



Gambar 8. Full *Report* MOBILedit

Hasil dari analisa aplikasi Twitter yang di dapat dari report.pdf adalah informasi yang menunjukan version aplikasi yang dipakai, data

size, dan permission yang digunakan untuk mengakses *smartphone* sesuai dengan gambar 9.



Gambar 9. Aplikasi Twitter

File *report* juga menampilkan nama *account* yang digunakan dalam aplikasi Twitter di *smartphone*, disini munjukan dengan nama akun Wicakson8 dan sebutan *account* Paranormal, sesuai gambar 10.

Gambar 10. Informasi *Account* Twitter

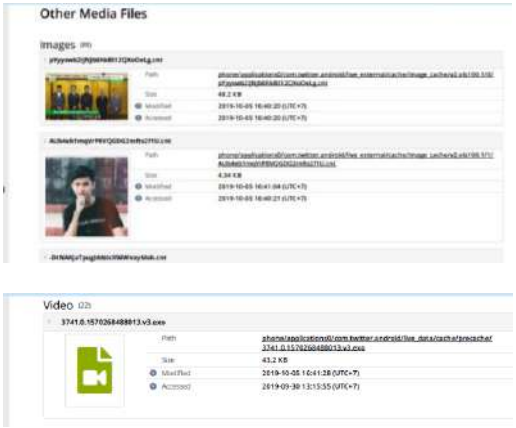
Selain nama *account* yang digunakan juga dapat diambil status Twitter yang sudah di delete dari timeline sepeti pada gambar 11.

Gambar 11. Status Twitter *Delete*

Data c*hat* yang sudah di delete juga dapat diketahui tetapi untuk percakapannya di enkripsi sehingga tidak dapat dibaca yang terdapat pada gambar 12.

Gambar 12. Percakapan di Twitter

Hasil analisa gambar dan video juga dapat ditemukan, pada aplikasi Twitter ini terdapat 88 images dan 22 video yang di dapatkan. Seperti gambar 13.

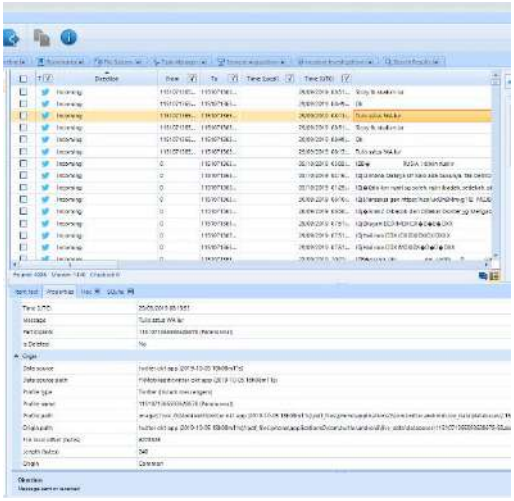


Gambar 13. Media Twitter

Tahapan akhir adalah tahapan presentasi, tahapan ini dilakukan dengan menampilkan kembali informasi yang dihasilkan dari tahap sebelumnya setelah memperoleh barang bukti dari proses pemeriksaan kemuian dilakukan dianalisis. Pelaporan hasil analisis yang telah dilakukan berdasarkan tahapan metode sebelumnya, penjelasan mengenai penggunaan metode dan *tools* yang digunakan. Pada tahap akhir untuk membantu menentukan rekomendasi untuk perbaikan pada proses forensik digital.

Gambar 14. Aplikasi Belkasoft

Menggunakan aplikasi *tools* forensic Belkasoft Evidence Center, dimana aplikasi ini digunakan untuk membaca *image* data yang sudah dianalisis sehingga menampilkan informasi yang lebih detail. Pada gambar 15 menunjukan jumlah data yang diambil di aplikasi Twitter khususnya sejumlah 4.086 *chat* baik yang masuk maupun keluar.



Gambar 15. Overview Aplikasi Twitter

Pada aplikasi Belkasoft Evidence Center ini juga memudahkan untuk pembacaan mana pesan Twitter yang masuk (*incoming*) dan pesan yang dikirim keluar (*outcoming*). Selain itu waktu pengiriman,isi pesan dan *accoun*t yang digunakan juga dapat diketahui sesuai dengan gambar 15.

4. KESIMPULAN

Berdasarkan hasil yang didapat pada pembahasan, dapat disimpulkan yaitu untuk data pada aplikasi Twitter yang dapat diambil adalah berupa *account* Twitter, pesan, status, foto dan video. Data status dan timeline yang sudah dihapus juga dapat diketahui dengan aplikasi MOBILedit dan Belkasoft. Beberapa data *messege* yang sudah terhapus bersifat enkripsi yang susah untuk dibaca baik di MOBILedit maupun Belkasoft.

DAFTAR PUSTAKA

Ahmad, M. S., Riadi, I., & Prayudi, Y. (2017). Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Serangan Man in the Middle Attack Berbasis Evil Twin, *9*(April), 1–8.

Anwar, N., & Riadi, I. (2017). Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *3*(1), 1. https://doi.org/10.26555/jiteki.v3i1.6643

Febriyanto, A., & Sembiring, I. (2016). Uji Perbandingan Tools Mobile Forensic Pada Platform Java, Blackberry dan Android, (November).

Handrizal. (2017). Analisis Perbandingan Toolkit Puran File Recovery , Glary Undelete Dan Recovery Untuk Digital Forensik. *Jurnal Sains Komputer & Informatika*, (1), 84–94.

Kwak, H., Lee, C., Park, H., & Moon, S. (2010). What is Twitter , a Social Network or a News Media ?, 591–600.

Larasati, T. D., & Hidayanto, B. C. (2017). Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10. *Seminar Nasional Sistem Informasi Indonesia, 6 November 2017*, (November).

Mukti, W. A., Masruroh, S. U., & Khairani, D. (2017). Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial. *Jurnal Teknik Informatika*, *10*(1), 73–84. https://doi.org/10.15408/JTI.V10I1.5617

Parekh, M., & Jani, S. (2018). Memory Forensic : Acquisition And Analysis Of Memory And Its Tools Comparison. *Communiacation, Integrated Networks & Signal Processing-CNISP 2018*, *5*(2: SE : February 2018), 90–95. https://doi.org/10.5281/zenodo.1198968

Suryana, A. L., Akbar, R. R. El, & Widiyasono, N. (2016). Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS), *2*(2), 111–117.

Wardana, A. C. K., Pedrason, R., & Prasetyo, T. B. (n.d.). Implementasi Digital Forensik

Brunei Darussalam Dalam Membangun Keamanan Siber, 1–22.
Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist, *3*(1), 13–21.
Zuhriyanto, I., Yudhana, A., & Riadi, I. (2018). Perancangan Digital Forensik Pada Aplikasi Twitter Menggunakan Metode Live Forensics, *2018*(November), 86–91.

Audio Forensic on Smartphone with Digital Forensic Research Workshop Method (DFRWS)

ABSTRACT

Audio is one of the digital items that can reveal a case that has happened, but audio evidence can also be manipulated and changed to hide information. Forensic audio is one technique to be able to know that the owner of the sound from the audio uses pitch, formant, and spectrogram parameters. This research will be conducted to examine the similarity of the original sound with the voice manipulated to determine the owner of the sound. This study analyzed to find the level of similarity/identical using spectrogram analysis to determine the identity of the owner of the sound with Digital Forensic Research Workshop Method (DFRWS).

Keywords: Audio, DFRWS, Forensic, Smartphone, Spectrogram

INTRODUCTION

The era of increasingly advanced technology makes the digital world is already ordinary among the people, including matters of sending messages in the form of text, audio, and video. The ease of application on a smartphone opens up opportunities for someone to commit a crime, for example, hoaxes, photo forgery, illegal transactions, and bullying. Crime involving technology is a cybercrime category (Utama Siahaan, 2018).

Illegal transactions using voice and video messages are digital crimes. Audio can be in the form of voice messages, the sound that is in the video, sound recordings, and recordings of the results of wiretapping. Voice and video messages have many drawbacks, which are readily manipulated using the software on a computer or application on a smartphone that can hide the identity of the voice owner (Wu, Wang, & Huang, 2014). The form of manipulation of audio can be done by changing the timbre and pitch that will hide the identity of the owner of the sound. In a court case, The evidence is needed that can resolve a case, if the audio is unknown to the owner of the vote, the audio evidence cannot be used as evidence.

Manipulation of data that began to bloom practice is needed forensic methods to deal with these causes, one way to treat it using the *Digital Forensic Research Workshop* (DFRWS) method. The *tools* used for the forensic process are Oxygen Forensic Suite 2014 and PRAAT.

LITERATURE REVIEW

1. Mobile Forensic

Increased smartphone users are increasing criminal crimes involving Android smartphones and the need for mobile forensics to solve this problem (Riadi, Umar, & Firdonsyah, 2018). Mobile forensic is a live forensic process (Umar, Yudhana, & Faiz, 2018). Mobile forensics is the science of recovering digital evidence from mobile devices using data that is compatible with forensics (Jansen & Ayers, 2007). Mobile device forensics is a forensic whose data taken from a cell phone by itself can be used as evidence. This evidence can be used as a basis when investigating a case by law enforcement agencies. There is some evidence that can be extracted from mobile phones, among others, contact numbers, call logs, SMS messages, audio files, emails, internet history and other evidence relating to the case being investigated. Logical or physical methods can extract this artifact. The purpose of logically is to extract data from system files by directly interacting with the device using *tools* or software specifically for mobile device forensics.

Presentation of digital evidence, where digital evidence is tested for authentication and correlation with existing cases. The stage carried out by the investigator to protect evidence is the chain of custody, which implies that maintenance by minimizing damage due to investigations with the aim, that the evidence is actually still original, the evidence can still be said as when it was found during the trial.

2. Forensic Audio

Forensic audio is a field of science that analyzes audio, sound, or recording evidence. Voice recordings contain data that contains information, one of which is the frequency characteristic used to determine identity (Huizen, Jayanti, & Hostiadi, 2017). In audio forensic investigations, the method often used is listening and analyzing visual sound spectrograms, often leading to wrong conclusions due to loss of data when transferring data or editing electronically (Gural & Pazarc, 2017). With the audio forensic method that has been developed, analysis can reduce the possibility of errors in the conclusions obtained.

In general, digital forensics aims to analyze the suitability or authenticity of the multimedia content with the original content. Analysis of Audio, Video, Image, forensics is usually not to find evidence but to test the suitability or authenticity of the content of the evidence with the original content (Böhme, Freiling, Gloe, & Kirchner, 2009). Forensic audio can be concluded as the application of science to investigate and construct evidence in court. Audio that will be analyzed can be through the parameters of pitch, formant and spectrogram to show identities (Putri & Sunarmo, 2014).

3. *Digital Forensic Research Workshop* (DFRWS)

Digital Forensics Research Workshop is the use of scientific methods that have a basis and proven for the maintenance, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence originating from digital sources for the purpose of facilitating or continuing the reconstruction of events containing criminal, or helps to anticipate unauthorized actions that are proven to interfere with planned operations (Ademu, Imafidon, & Preston, 2011).

Various methods of computer forensics and also digital forensics were developed to deal with various types of cyber threat methods consisting of various levels and channels, in addition to that digital forensic methods were also developed to deal with the increasing number of cyber-attacks which have now become a global trend (Aryo C K Wardana, Pedrason, & Prasetyo, 2018).

4. *Spectrogram*

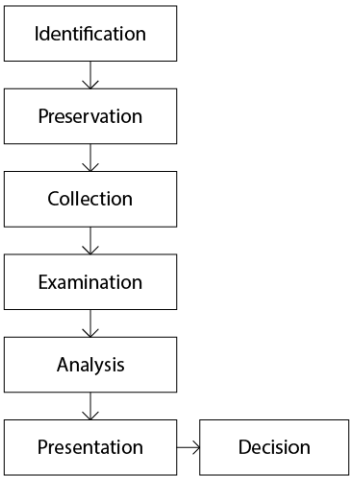
Spectrogram Analysis has the objective to see identical common patterns spoken and identical specific patterns on each formant of each word analyzed. Spectrogram Analysis will look at energy levels in each formant. If the pronunciation of certain words from the recording that has been changed by voice changer and the original recording does not show

a definite change then it can be concluded that the pronunciation of the sentence has the same spectrogram(Subki, Sugiantoro, & Prayudi, 2018) which refers to (AL-Azhar, 2011).

METHOD

This study uses a digital forensic method created by the *Digital Forensic Research Workshop* (DFRWS). The DFRWS method helps obtain evidence and a centralized mechanism for recording the information collected. The method has several stages, such as in Figure 1. (Suryana, Akbar, & Widiyasono, 2016c).

Figure 1. Schema of the DFRWS Method



a. Identification determine the needs needed for the investigation and search for evidence.
b. Maintenance, requesting digital evidence to ensure the authenticity of the evidence and refute sabotage claims
c. Collection, stages of identifying certain parts of digital evidence and identifying data sources.
d. Examination, which determines the filtering of data on certain parts of the data source, is done by changing the shape of the data but not changing the contents of the data to maintain the authenticity of the very important data.
e. Analysis, determines where the data is produced, by whom and how the data is produced and why the data is produced.
f. Presentation by presenting information generated from the analysis phase.

RESULT

DFRWS method is one of the forensic methods that has quite complete stages in carrying out the forensic process and is widely used by forensic investigators. In general, according to the DFRWS method, the stages of the investigation process of digital evidence both computers and smartphones have 6 main stages, namely Identification, Preservation, Collection, Examination, Analysis, and Presentation.

STAGES OF IDENTIFICATION

The identification phase is carried out by searching for information from previous cases to serve as a reference for understanding the evidence being searched. This identification stage also identifies how the image forgery case works. The image forgery case simulation is carried out to obtain digital evidence, because by getting the evidence sought, the identification stage can be continued at the maintenance stage in accordance with the framework of the DFRWS method.

STAGES OF PRESERVATION

The second stage is preservation, which is the maintenance stage to safeguard digital evidence, ensure the authenticity of evidence and refute claims that evidence has been sabotaged. The process of maintaining integration is carried out to keep the evidence authentic and undamaged, with the technique of isolating physical evidence and making backups in the form of cloning or image file processing of the evidence. The step taken is isolating the smartphone device from communication. Isolation needs to be done to avoid things that can damage digital evidence or affect the integrity of the data in it. Isolation activities carried out are changing the status of the device into Airplane Mode as shown in Figure 2.

Figure 2. Preservation

STAGES OF COLLECTION

The third stage is collection, which is the stage of the process of collecting identification of specific parts of digital evidence and identifying the source of data. Proof of evidence proposed is a smartphone device. This study uses the Samsung Galaxy Young as shown in Figure 3. and the spesification in Table 1.

Figure 3. Samsung Galaxy Young

Table 1. Smartphone Specification

Types of Specifications	Specification
Brand	Samsung
Series	Galaxy
Model	Young
Number Model	SM-G130H
IMEI	352716071399351 / 00 352717071399359 / 00
OS	Android
OS Version	4.4.2 (KitKat)
Processor	ARM Cortex-A7

Activate Developer Option for the forensic process, to activate it by pressing Build Number on the smartphone 7 times as shown in Figure 4. If the activation process is successful, the Developer Options menu can be found in the settings section. The next step is to enable the Stay Awake and USB Debugging options for the forensic process as shown in Figure 5. Stay Awake is needed so that the smartphone device is not in sleep mode if it is not used for a while during the forensic process because it can activate the smartphone device security system. USB Debugging is used to give permission to smartphone devices to communicate with workstations using USB and ADB cables.

Figure 4. Build Number of Smartphone

Figure 5. Developer Options

The stage of taking digital evidence on a smartphone has a high risk, if a fatal error occurs, the data and digital evidence available on a smartphone can be lost or corrupted so that it cannot be read, therefore it is necessary to preserve the evidence, i.e. Backup or imaging smartphone that becomes Evidence, this process is also called logical acquisition.

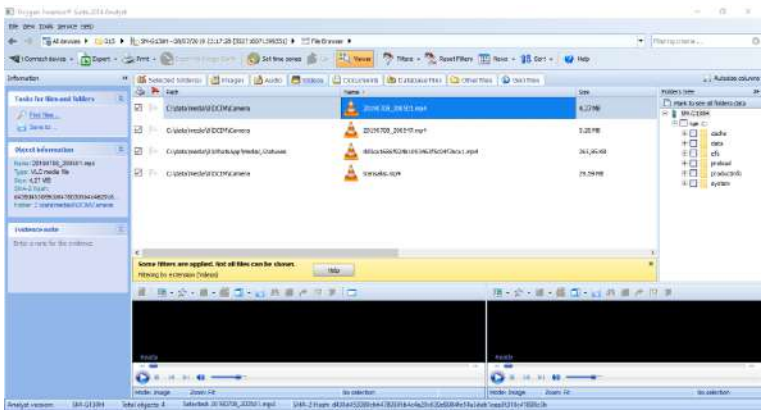
The *tools* used to carry out the backup process are Oxygen Forensic. The ability of this tool in making a smartphone system backup is quite good. Figures 6. show the backup process of the backup process on smartphone with Oxygen Forensic and Figure 7. is the result of the imaging process on a *smartphone*.

Figure 6. Smartphone Backup Process

The results of this backup process are document images from each Android smartphone can be open with Oxygen Forensic, document sizes that vary depending on the amount of data on the smartphone, as shown in Figure 7. and Figure 8.

Figure 7. Smartphone Backup Results

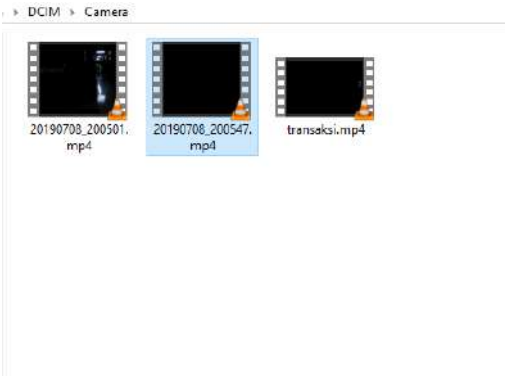
Figure 8. File Preview of Backup Results



STAGES OF EXAMINATION

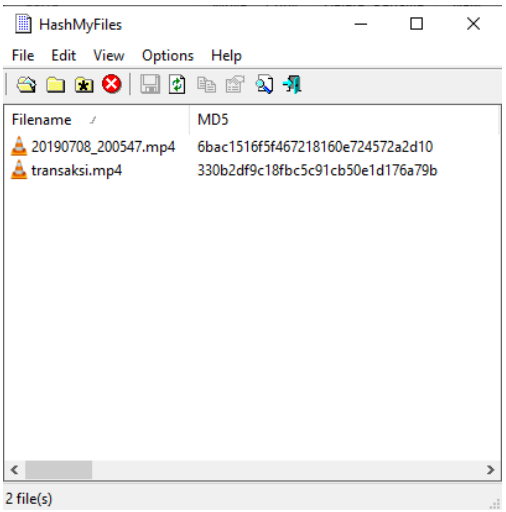
The results of extraction in the form of video files can be seen in Figure 9. Extraction produces 2 files in the form of sample files and evidence files. Figure 10. proves that the hashing results differ between the two files.

Figure 9. The Results of Extraction



After the extraction results have been removed the hashing is done to determine the hash value in the file.

Figure 10. Hashing Process

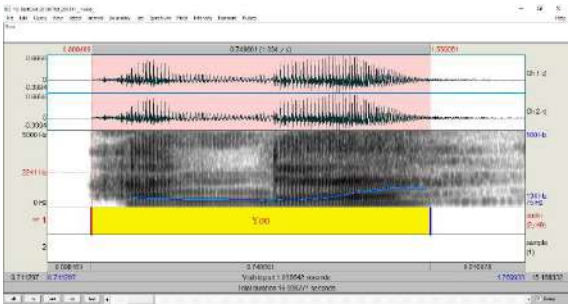


Next step videos will be converted to audio in the form of .wav extension which will then be analyzed.

STAGES OF ANALYSIS

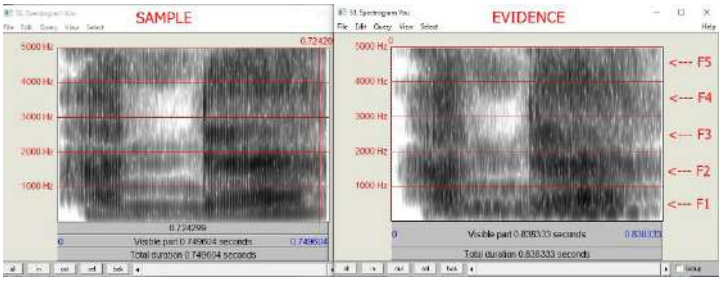
At this stage a spectrogram analysis will be performed. The first stage of audio analysis removes the noise in the audio. Then the audio is divided into words to do spectrogram analysis as seen in Figure 11.

Figure 11. Dividing Audio



Then the speech audio will be approved formant patterns to be analyzed for special patterns. Figure 12 shows that your words from audio evidence are identical to sample audio.

Figure 12. Spectrogram Analysis



After all the audio pieces have been analyzed for each formant and the results are in Table 2.

Table 2. Result of the Analysis

Syllables	Spectrogram Analysis
You	MATCH
Please	MATCH
Make a	MATCH
Transfer	MATCH
Of	MATCH
Twenty	MATCH
Million	MATCH
After	MATCH
That	MATCH
The	UNMATCH

Order	UNMATCH
Goods	MATCH
Will	MATCH
Be	MATCH
Sent	MATCH
Three	UNMATCH
Days	MATCH
Later	MATCH
After2	MATCH
Transfer2	MATCH

STAGES OF PRESENTATION

From the analysis conducted, the audio sample with audio evidence is MATCH. The specific pattern on each formant does not have a significant difference so the results can be said to be identical with the audio sample.

CONCLUSION

In this study information was obtained in the form of audio samples with audio evidence said to be suitable. There are similarities between the special patterns in the formants that are in the audio and only a few are not suitable so it can be concluded that the two audios have in common.

REFERENCES

Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A New Approach of Digital Forensic Model for Digital Forensic Investigation. *International Journal of Advanced Computer Science and Applications*, *2*(12), 175–178. https://doi.org/10.14569/ijacsa.2011.021226

AL-Azhar, M. N. (2011). *AudioForensic Theory and Analysis* (p. 1). p. 1. Bidang Fisika dan Komputer Forensik.

Böhme, R., Freiling, F. C., Gloe, T., & Kirchner, M. (2009). Multimedia forensics is not computer forensics. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5718 LNCS*, 90–103. https://doi.org/10.1007/978-3-642-03521-0_9

Gural, E., & Pazarc, M. (2017). A supporting method to detect manipulated zones in digitally edited audio files. *Medicine Science | International Medical Journal*, 1. https://doi.org/10.5455/medscience.2017.06.8699

Huizen, R. R., Jayanti, N. K. D. A., & Hostiadi, D. P. (2017). *Model Evaluasi Rekaman Percakapan Di Audio Forensik*. 133–140.

Jansen, W., & Ayers, R. (2007). Guidelines on Cell Phone Forensics Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*, *800*(101), 1–104. https://doi.org/10.6028/NIST.SP.800-124

Putri, V. R. C., & Sunarmo. (2014). *Analisis Rekaman Suara Menggunakan Teknik Audio Forensik Untuk Keperluan Barang Bukti Digital*. *3*(1), 7–13.

Riadi, I., Umar, R., & Firdonsyah, A. (2018). Forensic tools performance analysis on android-based blackberry messenger using NIST measurements. *International*

Journal of Electrical and Computer Engineering, *8*(5), 3991–4003. https://doi.org/10.11591/ijece.v8i5.pp3991-4003

Subki, A., Sugiantoro, B., & Prayudi, Y. (2018). Membandingkan Tingkat Kemiripan Rekaman Voice Changer Menggunakan Analisis Pitch, Formant dan Spectogram. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *5*(1), 17. https://doi.org/10.25126/jtiik.201851500

Suryana, A. L., Akbar, R. El, & Widiyasono, N. (2016). Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS). *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *2*(2), 111–117. https://doi.org/10.26418/jp.v2i2.16821

Umar, R., Yudhana, A., & Faiz, M. N. (2018). Experimental analysis of web browser sessions using live forensics method. *International Journal of Electrical and Computer Engineering*, *8*(5), 2951–2958. https://doi.org/10.11591/ijece.v8i5.pp.2951-2958

Utama Siahaan, A. P. (2018). Pelanggaran Cybercrime Dan Kekuatan Yurisdiksi Di Indonesia. *Jurnal Teknik Dan Informatika*, *5*(1), 6–9.

Wardana, A. C. K., Pedrason, R., & Prasetyo, T. B. (2018). Implementasi digital forensik brunei darussalam dalam membangun keamanan siber implementation of digital forensic brunei darussalam in building cyber security. *Jurnal Prodi Perang Asimetris*, *4*(1), 1–22.

Wu, H., Wang, Y., & Huang, J. (2014). Identification of electronic disguised voices. *IEEE Transactions on Information Forensics and Security*, *9*(3), 489–500. https://doi.org/10.1109/TIFS.2014.2301912

FORENSIK MOBILE PADA SMARTPHONE ANDROID MENGGUNAKAN METODE DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS)

MOBILE FORENSICS ON ANDROID SMARTPHONES USING DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS) METHOD

Imam Riadi[1], Sunardi[2], Rusydi Umar[3], Muhammad Noor Fadillah[4]

[1]Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan, Yogyakarta
[2] Teknik Elektro, Fakultas Teknik Industri, Universitas Ahmad Dahlan, Yogyakarta
[3,4] Teknik Informatika, Fakultas Teknik Industri, Universitas Ahmad Dahlan, Yogyakarta
Kampus 3 Universitas Ahmad Dahlan Jalan Prof. Dr. Soepomo, S.H., Janturan, Warungboto, Umbulharjo, Yogyakarta
imam.riadi@is.uad.ac.id, sunardi@mti.uad.ac.id, rusydi@mti.uad.ac.id, muhammad1807048006@webmail.uad.ac.id

Naskah diterima: Bagian ini akan diisi oleh redaksi pelaksana jurnal Penelitian Pos dan Informatika

Abstrak

Perangkat *smartphone* sudah menjadi barang yang dimiliki semua orang, semua kegiatan penggunanya dapat didukung dengan adanya *smartphone*. Berdasarkan sistem operasi, pengguna *smartphone* Android sebanyak 73,5% pengguna. Selain untuk hal positif, penggunaan *smartphone* kerap digunakan untuk hal negatif. Sehingga tidak jarang *smartphone* dijadikan salah satu bukti dalam suatu tindak kejahatan. Dalam kasus *cybercrime* di Indonesia memiliki UU ITE yang pada salah satu pasalnya membahas tentang kekuatan hukum alat bukti digital. Bukti digital dapat dibuktikan dengan proses forensik pada *smartphone* Android menggunakan metode *Digital Forensic Research Workshop* (DFRWS) dimana tahapan forensik meliputi *identification, preservation, collection, examination, analysis,* dan *presentation*. Sehingga barang bukti yang berhasil didapatkan dapat dipertanggungjawabkan secara hukum yang berlaku. Berdasarkan proses forensik terhadap perangkat *mobile smartphone* Android dengan metode *Digital Forensic Research Workshop* (DFRWS) menggunakan *tools MOBILedit Forensik* berhasil ditemukan data berupa *file image, audio, video, document, archive file* dan *SQLite database*. Selanjutnya data tersebut dapat digunakan sebagai barang bukti digital.

Kata kunci: *Mobile* Forensik**,** bukti digital*, Android smartphone, DFRWS.*

Abstract

Smartphone devices have become the property of everyone, all user activities can be supported by a smartphone. Based on the operating system, Android smartphone users are as much as 73.5% of users. in addition to positive things, smartphone usage is often used for negative things. So it is not uncommon for a smartphone to be one of the pieces of evidence in a crime. In the case of cybercrime in Indonesia, it has a UU ITE which is one of its articles discusses the legal force of digital evidence Digital evidence can be proven by the forensic process on an Android smartphone using the Digital Forensic Research Workshop (DFRWS) method where the forensic stage includes identification, preservation, collection, examination, analysis, and presentation. So that the evidence that has been obtained can be justified legally in force. Based on the forensic process of Android smartphone mobile devices using the Digital Forensic Research Workshop (DFRWS) method using the MOBILedit Forensic tools, data found in the form of image files, audio, video, documents, archive files, and SQLite databases. Furthermore, the data can be used as digital evidence

Keywords*: Mobile Forensics, Digital Evidence, Android Smartphone, DFRWS*

PENDAHULUAN

Di era digital sekarang hampir semua orang sudah memiliki *smartphone*, pertumbuhan pengguna *smartphone* semakin meningkat seiring dengan meratanya koneksi internet di semua wilayah, berdasarkan data APJII (2018), sebanyak 64.8% dari 264,16 juta penduduk Indonesia sudah menggunakan internet di kehidupan sehari hari mereka dan 93,9% mengakses internet menggunakan *smartphone*. Berdasarkan system operasi yang digunakan pada perangkat *smartphone*, sebanyak 73,5% adalah pengguna *Android, Apple IOS* sebanyak 19,9%, dan lainnya 6,6% (Kemp, 2018).

Penggunaan *smartphone* tidak hanya sekedar untuk berkomunikasi tetapi sudah menjadi perangkat *mobile* yang bisa mendukung semua kegiatan penggunanya. Dengan beragam aplikasi pendukung yang tersedia, *smartphone* bisa digunakan dari sebagai media bersosialisasi dengan aplikasi *messenger* dan *social media* sampai menjadi alat pembayaran dengan aplikasi *mobile payment*. Perkembangan teknologi selain memberikan dampak positif juga memunculkan resiko kejahatan. Seperti pada media sosial dapat ditemui beberapa kasus penipuan, pencemaran nama baik, pemerasan dan *cyberbully* (Zuhriyanto et al., 2018), dengan cara pihak tertentu bisa memanipulasi *image* sehingga keaslian *image* tersebut tidak bisa dipercaya lagi (Sulistyo, Riadi, & Yudhana, 2018a). Pada *file audio* juga dapat dimanipulasi langsung dengan

bantuan aplikasi yang tersedia pada *smartphone* (Gustafi, Umar, & Sunardi, 2018). Selain itu, kewaspadaan terkait informasi penting yang ada pada *smartphone* masih rendah sehingga rawan menjadi korban *cybercrime*.

Dalam kasus *cybercrime*, Indonesia memiliki UU ITE yang pada UU 11/2018 berisi tentang dasar hukum mengenai kekuatan hukum alat bukti elektronik dan syarat formil dan materil alat bukti elektronik sehingga dapat diterima di pengadilan (Sitompul, 2012). Berdasarkan permasalahan di atas, peneliti akan melakukan proses forensik pada perangkat mobile *smartphone* dengan sistem operasi Android menggunakan metode *Digital Forensic Research Workshop* (DFRWS) untuk mencari informasi elektronik / dokumen elektronik yang dapat dijadikan sebagai barang bukti digital.

LANDASAN TEORI

Mobile Forensic

Mobile forensic merupakan cabang dari keilmuan *digital forensic* untuk mendapatkan bukti digital pada perangkat *mobile* dengan menggunakan metode yang diterima secara umum serta memperhatikan aspek legal, seluruh prosedur dan pelaksanaan *mobile forensic* harus berlandaskan metode yang umum diterima oleh ilmu *digital forensic* (Heriyanto, 2016).

Digital Evidence

Menurut Sitompul (2012), berdasarkan UU ITE alat bukti hukum yang sah adalah informasi elektronik, yaitu satu atau sekumpulan data elektronik, termasuk tidak terbatas pada tulisan, suara, gambar, peta, foto, surat elektronik, huruf, tanda, angka, kode akses, symbol yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. (pasal 1 butir 1 UU ITE) dan dokumen elektronik, yaitu setiap informasi elektronik yang dibuat, diteruskan, dikirim, atau disimpan dalam bentuk analog, digital, atau sejenisnya, yang dapat ditampilkan, dilihat, dan didengarkan melalui sistem elektronik tetapi tidak terbatas pada tulisan, suara, gambar, foto atau sejenisnya, huruf, angka, kode akses, *symbol* yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. (pasal 1 butir 4 UU ITE)

DFRWS

Digital Forensics Research Workshop (DFRWS) merupakan metode ilmiah yang digunakan pada *digital forensic* dan telah teruji untuk melakukan proses *identification, preservation, collection, examination, analysis,* dan *presentation* terhadap barang bukti digital yang diperoleh dengan tujuan untuk memperdalam dan memfasilitasi rekonstruksi kejadian yang diduga sebagai suatu tindak kejahatan (Harris, 2006a).

Penelitian dengan tema sejenis pernah dilakukan beberapa peneliti sebagai berikut:

- Imam Riadi, Sunardi, & Sahiruddin (2019) dengan judul "Analisis *Forensic Recovery* Pada *Smarphone* Android Menggunakan Metode *Nasional Institute Of Justice* (NIJ)". Penelitian ini melakukan forensik mengembalikan data yang hilang atau terhapus pada *smartphone* Android dengan menggunakan metode *National Institute of Justice* (NIJ), perbedaan dengan penelitian yang dilakukan yaitu pada metode yang digunakan
- Rusydi Umar & Sahiruddin (2019) dengan judul "Metode NIST Untuk Analisis Forensik Bukti Digital Pada Perangkat Android". Penelitian ini membahas pengangkatan bukti digital pada *smartphone* Android menggunakan *tools* forensik *Wondershare Dr. Fone For Android* dan *Oxygen Forensic Suite* dengan metode *National Institute Of Standard And Technology* (NIST). Perbedaan dengan penelitian yang dilakukan adalah metode dan *tools* forensik yang digunakan.
- Roni Anggara Putra, Abdul Fadlil, & Imam Riadi (2017) dengan judul "*Forensic Mobile* Pada *Smartwatch* Berbasis Android". Penelitian ini berfokus pada pengangkatan barang bukti yang ada pada *smartwatch* menggunakan metode *National Institute of Justice* (NIJ), perbedaan dengan penelitian yang dilakukan yaitu pada objek penelitian dan metode yang digunakan.

METODE

Penelitian ini menggunakan metode *Digital Forensic Research Workshop* (DFRWS), metode ini

merupakan metode ilmiah yang digunakan pada *digital forensic* dan telah teruji untuk membantu mendapatkan barang bukti digital (Harris, 2006a).

Gambar 1. Metode *Digital Forensic Research Workshop* (DFRWS)

Berdasarkan Metode *Digital Forensic Research Workshop* (DFRWS), terdapat beberapa tahapan yang harus dilakukan, seperti:

a. Identification

Tahap ini merupakan proses identifikasi dilakukan untuk menentukan kebutuhan yang apa saja yang diperlukan pada penyelidikan dan pencarian barang bukti.

b. Preservation

Tahap ini merupakan tahap pemeliharaan dilakukan untuk menjaga barang bukti digital, memastikan keaslian barang bukti dan menyangkal klaim bahwa barang bukti telah dilakukan sabotase.

c. Collection

Melakukan proses pengumpulan identifikasi bagian yang khusus dari barang bukti digital dan melakukan identifikasi sumber data.

d. Examination

Melakukan tahap menentukan penyaringan data pada begian tertentu dari sumber data, penyaringan data dilakukan dengan melakukan perubahan bentuk data namun Tidak melakukan perubahan pada isi data karena keaslian data merupakan hal yang sangat penting.

e. Analysis

Melakukan melakukan penentuan tentang dimana data tersebut dihasilkan, oleh siapa data tersebut dihasilkan, bagaimana data tersebut dihasilkan dan kenapa data tersebut dihasilkan.

f. Presentation

Presentasi dilakukan dengan menyajikan informasi yang dihasilkan dari tahap analisis. Tahap presentasi dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai tool, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan

kebijakan, metode, tool, atau aspek pendukung lainnya pada proses tindakan forensik digital.

HASIL DAN PEMBAHASAN

Penelitian dilakukan dengan menggunakan *smartphone* yang disimulasikan sebagai salah satu barang bukti terkait suatu tindak kejahatan. Penelitian menggunakan 1 buah *smartphone* Android dengan merk Evercross Tipe Elevate Y3+. Berdasarkan metode penelitian yang digunakan, berikut tahapan proses forensik pada perangkat *mobile smartphone* untuk mencari informasi elektronik / dokumen elektronik yang dapat dijadikan sebagai barang bukti digital:

a. Identification

Tahapan Identifikasi merupakan tahap awal yang dilakukan untuk penentuan kebutuhan yang diperlukan saat proses penyelidikan dan pencarian bukti.

Perangkat *smartphone*

Berdasarkan barang bukti yang digunakan, yaitu 1 buah *smartphone* Android dengan spesifikasi sebagai berikut:

Tabel 1. ***Spesifikasi* smartphone**

Manufacture	Evercross
Product	B75
Hw version	LMY47D
Platform	Android
Sw version	5.1
Serial number	010516100002641
Imei	358441061746404
Ram	2gb
Rom	16gb
Rooted	yes

Tools forensic

Tools forensic yang digunakan untuk proses mencari informasi elektronik / dokumen elektronik yang dapat dijadikan sebagai barang bukti digital pada *smartphone* Android adalah *Tools MOBILedit Forensic Express* versi 7.0.

b. Preservation

Pada tahapan *preservation* yaitu untuk menjaga barang bukti digital, memastikan keaslian bukti dan membantah klaim bukti di sabotase. Maka barang bukti perangkat *smartphone* akan di simpan ditempat yang aman dan terisolasi dari komunikasi maka semua koneksi pada *smartphone* dimatikan dengan mengaktifkan *airplane mode*. Selain itu juga dilakukan proses *imaging* atau *cloning* terhadap *smartphone* sehingga keaslian barang bukti tetap terjaga sesuai dengan aturan forensik yaitu

proses forensik tidak dilakukan terhadap barang bukti asli.

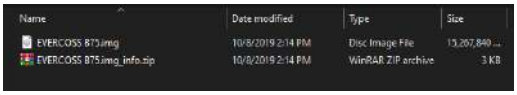
c. Collection

Tahapan *collection* dilakukan dengan menggunakan *tools MOBILedit Forensic Express*, *tools* ini dapat melakukan proses *imaging* dan *extract* data pada *smartphone* Android.

Proses pertama yang dilakukan yaitu menghubungkankan *smartphone* dengan laptop yang sudah terinstal aplikasi *MOBILedit Forensic Express*.

Gambar 1. Tahap awal collection

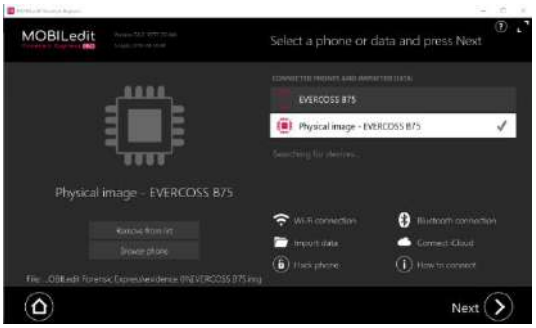
Lalu langkah berikutnya yaitu membuat *physical image* dari *smartphone* Android yang jadi barang bukti, sehingga proses forensik tidak dilakukan pada perangkat asli untuk menghindari perubahan atau kerusakan data pada perangkat asli. Hasil dari proses *physical image* akan menghasilkan file dengan ekstensi .img dengan besaran *file* sesuai dengan besaran data yang ada pada *smartphone* target.



Gambar 2. File *physical image smartphone*

d. Examination

Tahapan *examination* akan dilakukan dengan menggunakan data dari file *physical image* yang sudah dibuat sebelumnya bukan langsung pada perangkat *smartphone*.



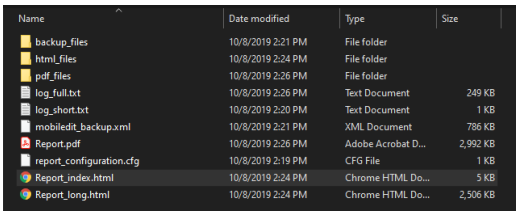
Gambar 3. Proses *extract* dari *physical image*

Selanjutnya adalah proses ekstraksi dari file *physical image* sehingga semua data pada *smartphone* target akan terekstraksi.

Gambar 4. Proses *extraction complete*

Setelah proses *extraction* selesai, maka *tools MOBILedit Forensik Express* akan

menghasilkan file *full report* hasil ekstraksi semua data dengan ekstensi *file* yang sudah ditentukan berupa *file* .pdf.



Gambar 5. *Output file report* hasil *extraction data*

e. Analysis

Tahapan *analysis* berdasarkan *file report* hasil dari *exctration data* dari *file physical image* dapat dikemukakan sebagai berikut:

laporan pertama menampilkan informasi terkait perangkat yang dijadikan barang bukti yaitu *smartphone* merk Evercoss tipe B75 dengan *operating system* Android 5.1.

Gambar 6. Informasi perangkat

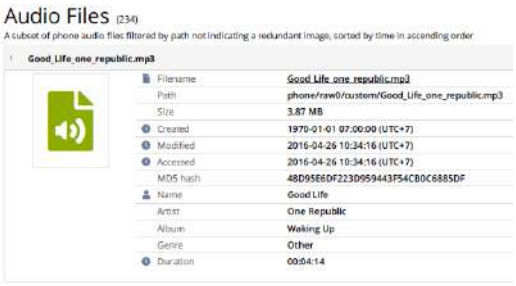
Laporan kedua, berisi daftar jenis *file* yang didapatkan beserta jumah *file* yang didapatkan dari hasil *extraction* dari *file physical image* Evercoss B75.

Gambar 7. Daftar Jenis *file*

Pada jenis *file contact*, *application*, *photos*, dan *location* tidak terdapat *file* yang didapatkan. Sedangkan pada *file image*, terdapat 6 *file* yang berhasil didapatkan dan dilaporkan dengan rincian: *preview image, file name, path, size, created date, modified date, accessed date, width, height,* dan *format file*.

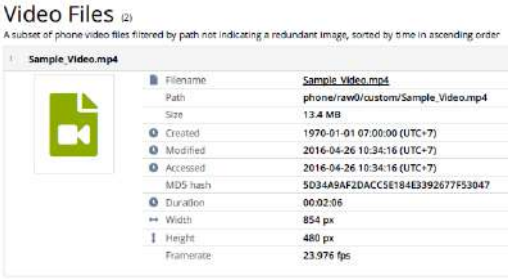
Gambar 8. Informasi *image file*

pada *file audio*, terdapat 234 *file* yang berhasil didapatkan dan dilaporkan dengan rincian: *thumbnail image, filename, path, size, created date, modified date, accessed date, MD5 hash, name, artist, album, genre* dan *duration*.



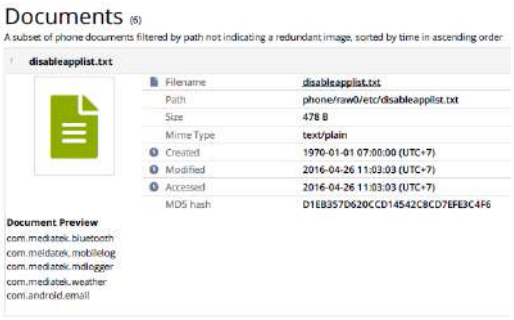
Gambar 9. Informasi *audio file*

pada *file video*, terdapat 2 *file* yang berhasil didapatkan dan dilaporkan dengan rincian: *thumbnail image, filename, path, size, created date, modified date, accessed date, MD5 hash, duration, width, height* dan *framerate*.



Gambar 10. Informasi *video file*

pada *file documents*, terdapat 6 *file* yang berhasil didapatkan dan dilaporkan dengan rincian: *thumbnail image, filename, path, size, mime type, created date, modified date, accessed date, MD5 hash* dan *document preview*.



Gambar 11. Informasi document file

pada *filesystem* terdapat 2 jenis *file* yaitu *internal filesystem* sebanyak 3313 *file* dan 2 *deleted* dan *misc filesystem* 0 *files. File* yang berhasil didapatkan dilaporkan dengan rincian: *filename, size, created date, modified date, accessed date* dan pada *file* yang sudah di *delete* diberikan keterangan *deleted.* Seperti pada gambar berikut:

Gambar 12. Informasi *file filesystem*

Semua data *extraction* dari proses *forensic* menggunakan *MOBILedit Forensic Express* akan menghasilkan *log* yang berisi tanggal dan waktu proses *extraction* beserta keterangan proses *extraction.*

Gambar 13. Data *extraction log*

f. Presentation

tahapan *presentation* meliputi penjelasan *tools* yang digunakan, metode yang dipakai dan menyampaikan informasi berdasarkan dari hasil analisis yang didapatkan dari barang bukti

berdasarkan barang bukti 1 buah *smartphone* dengan spesifikasi sebagai berikut:

Tabel 2. ***Spesifikasi barang bukti*** **smartphone**

Manufacture	Evercross
Product	B75
Hw version	LMY47D
Platform	Android
Sw version	5.1
Serial number	010516100002641
Imei	358441061746404
Ram	2gb
Rom	16gb
Rooted	yes

Telah dilakukan proses forensik dengan menggunakan *tools MOBILedit Forensic Express* dan menggunakan *Metode Digital Forensic Research Workshop* (DFRWS). Hasil yang didapatkan dari proses forensik terhadap barang bukti *smartphone* dengan rincian sebagai berikut:

Tabel 3. ***Rincian hasil forensik***

Jenis file	Jumlah
Archive file	143
Document	6
Audio file	234
Image file	6
Video file	2
Sqlite databases	1
XML file	53
Other file	2868

PENUTUP

Berdasarkan penelitian yang dilakukan didapatkan hasil berupa beberapa data dari *smartphone* Android yang sebelumnya sudah dilakukan proses *physical image* dengan menggunakan *tools* forensik *MOBILedit Forensic Express* dan hasil extraksi dari file *physical image* berupa *file image, audio, video, document*. Selanjutnya data hasil dari extraksi dapat digunakan sebagai barang bukti digital sesuai dengan kasus yang ditangani.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada tim Penelitian Unggulan Program Studi Magister Teknik Informatika Universitas Ahmad Dahlan Yogyakarta yang membantu untuk menyelesaikan penelitian ini.

DAFTAR PUSTAKA

APJII. (2018). *Penetrasi & Profil Perilaku Pengguna Internet Indonesia*.

Gustafi, M. F., Umar, R., & Sunardi. (2018). Analisis Manipulasi Suara Yang Telah di Edit Dengan Aplikasi Smartphone Menggunakan Teknik Audio Forensik Sebagai Barang Bukti Digital (Vol. 2018, pp. 76–80).

Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation*. https://doi.org/10.1016/j.diin.2006.06.005

Heriyanto, A. P. (2016). *Mobile Phone Forensics: Theory Mobile Phone Forensics and Security Series, 1'st Edition*. Yogyakarta: Andi.

Kemp, S. (2018). *Digital in 2018 : World's Internet Users Pass The 4 Billion Mark*. Diakses dari https://wearesocial.com/blog/2018/01/global-digital-report-2018 Tanggal 2 Oktober 2019

Putra, R. A., Fadlil, A., & Riadi, I. (2017). Forensik Mobile Pada Smartwach Berbasis Android. *Jurti*, *1*(1), 41–47. https://doi.org/25798790

Riadi, I., Sunardi, & Sahiruddin. (2019). Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ), *3*(1), 87–95.

Sitompul, J. (2012). *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*. (Tatanusa, Ed.). Jakarta.

Sulistyo, W. Y., Riadi, I., & Yudhana, A. (2018). Analisis Deteksi Keaslian Citra Menggunakan Teknik Error Level Analysis Dengan Forensicallybeta (Vol. 2018, pp. 154–159).

Umar, R., & Sahiruddin. (2019). Metode NIST Untuk Analisis Forensik Bukti Digital Pada Perangkat Android (pp. 978–979).

Zuhriyanto, I., Yudhana, A., & Riadi, I. (2018). Perancangan Digital Forensik Pada Aplikasi Twitter Menggunakan Metode Live Forensics (Vol. 2018, pp. 86–91).

Perbandingan *Tools* Forensik Pada Layanan Sosial Media Menggunakan *Metode Digital Forensic Research Workshop* (DFRWS)

Sunardi[1], Imam Riadi[2], Anton Yudhana[3], Ghufron Zaida Muflih[4]

[1,3]Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
[2]Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan, Yogyakarta
[4]Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
[1]sunardi@mti.uad.ac.id, [2]imam.riadi@mti.uad.ac.id, [3]eyudhana@mti.uad.ac.id,
[4]ghufron1807048002@webmail.uad.ac.id

Abstract

Social media applications currently play a role and become a part in various human activities, on the other hand social media is also very vulnerable to various crime. Some of the crimes on social media can be in the form of hate speech, defamation, fraud, gambling, pornography, and other actions that are very detrimental. In this study, the Digital Forensic Research Workshop (DFRWS) method is used to search all data on the Twitter social media service running on the Android operating system by using the MOBILedit Forensic Express tool and Belkoft evidence center, from the two tools, it is found that the MOBILedit Forensic Express find more Data on Twitter social media from Belkasoft Evidence Center, the findings of these two tools make some contributions to social media investigations that run on the Android operating system.

Keywords: Forensics, DFRWS, Twitter, MOBILedit, Belkasoft

Abstrak

Aplikasi media sosial saat ini banyak berperan dan menjadi bagian dalam berbagai aktifitas manusia, disisi lain media sosial juga sangat rawan terhadap berbagai tindak kejahatan. Beberapa tindak kejahatan pada media sosial dapat berupa ujaran kebencian, pencemaran nama baik, penipuan, perjudian, pornografi, serta tindakan lain yang sangat merugikan. Pada penelitian ini menerapkan metode *Digital Forensic Research Workshop* (DFRWS) untuk mencari semua data pada layanan media sosial twitter yang berjalan di sistem operasi Android dengan menggunakan *tools* MOBILedit Forensic Express dan Belkasoft Evidence Center, dari kedua *tools* didapatkan perbandingan bahwa pada MOBILedit Forensic Express lebih banyak menemukan data pada media sosial twitter dari belkasoft evidence center, temuan pada dua *tools* ini membuat beberapa kontribusi pada investigasi media sosial yang berjalan pada sistem operasi android.

Kata Kunci: Forensik, DFRWS, Twitter, MOBILedit, Belkasoft

1. Pendahuluan

Aplikasi media sosial berperan dan menjadi bagian dalam berbagai aktifitas manusia seperti bersosialisasi *grup chat*, aktifitas niaga, media iklan, pendidikan, serta konten kreatif lainnya, disisi lain media sosial juga sangat rawan terhadap berbagai tindak kejahatan. Aplikasi media sosial twitter yang menjadi salah satu aplikasi media sosial populer saat ini di antara aplikasi media sosial lain. Beberapa tindak kejahatan pada media sosial dapat berupa ujaran kebencian, pencemaran nama baik, peniupuan, perjudian, pornografi, serta tindak kejahatan yang lain yang sangat merugikan. Laporan dari UNICEF pada tahun 2017 terdapat 40% anak indonesia mengalami peristiwa *bully* akibat dari dampak *cyberagression* dari penggunaan media sosial. Selanjutnya terdapat 32% anak yang melaporkan mendapat kekerasan fisik. Hal ini disebabkan banyaknya pengguna aplikasi dari berbagai usia (I. Saputra & Azhar, 2018).

Sampel data pada 9 maret hingga 14 April 2019, Penetrasi pengguna internet Indonesia mencapai 171,17 Juta Jiwa atau 64,8 % dari total populasi penduduk Indonesia 264,16 juta orang tahun 2018 (proyeksi BPS), kontribusi pengguna paling banyak berada di Jawa 55.7% dari keseluruhan wilayah Indonesia disusul Sumatera 21.6%, Sulawesi-Maluku-Papua

10.9%, Kalimantan 6.6%, dan Bali-NTT 5.2%. Perangkat yang terhubung dengan internet paling banyak adalah smartphone mencapai 93,9% perharinya, kemudian komputer laptop 17,2% dengan kisaran waktu lebih dari 8 jam. Pelecehan atau tindakan bully juga banyak terjadi di media sosial sebesar 49%, konten porno 55,9%. Alasan utama masyarakat menggunakan internet untuk komunikasi melalui pesan dengan porsi 24,7%, media sosial 18,9% dan mencari info pekerjaan 11,5%. Alasan kedua sebanyak 19,1 % untuk mengakses media sosial, 16,4% untuk komunikasi lewat pesan dan 15,2% untuk mengisi waktu luang, konten terbanyak/ hiburan yang sering dikunjungi adalah menonton film/video serta bermain game, media sosial paling sering dikunjungi adalah facebook 50,7%, instagram 17,8% youtube 15,1% twitter menempati posisis ke empat 1,7%. (APJII, 2018b).

Metode *Digital Forensics Research Workshop* (DFRWS) untuk investigasi email *spoofing* atau manipulasi data pada *header* email dan diperoleh email *spoofing* dapat dikirmkan dengan layanan web hosting yang menyediakan layanan untuk pengiriman email selanjutnya dapat diketahui perbedaan email asli dan email *spoofing* dengan jelas ketika membuka *header* email rinci.(Suryana, Akbar, & Widiyasono, 2016b).

Framework audio forensik dengan menerapkan *Systems Development Life Cycl*e (SDLC) memungkinkan peneliti mengembangkan audio forensik sebagai standar dalam melakukan proses investigasi audio forensik, melakukan ekstraksi tahapan-tahapan dari framework hasil identifikasi, eliminasi, penambahan tahapan yang penting dalam investigasi audio forensik, implementasi dengan membuat *framework* hasil pengembangan dan *menintenance framework* (Inggi, Sugiantoro, & Prayudi, 2018).

Penelitian pada media sosial facebook dan twitter untuk menemukan dan membandingkan bukti forensik yang di akses pada *smartphone* android, menggunakan metode simulasi dengan 11 skenario, pengembalian file yang dihapus, pencarian nama akun, lokasi, nomor telpon, tanggal lahir, foto profil, cover foto, posting berupa text, gambar, pesan pribadi berupa text dan gambar, dengan hasil 100% pada facebook dan 60% pada twitter (Mukti, Masruroh, & Khairani, n.d.). Selain pada sistem operasi Android pada firefox OS juga dapat dilakukan pemeriksaan forensik pada media sosial Facebook, Twitter, dan Google + dengan hasil gambar yang sebagian besar informasi forensik berda pada memori tidak stabil *(volatile memory)*, serta menunjukkan bahwa memori pada firefox OS tidak ter enkripsi (Yusoff, Dehghantanha, & Mahmod, 2017).

Penggunaan *tools* forensik belkasoft evicence center dalam akuisisi dan analisis, menekankan alat forensik digital baik yang berbayar atau gratis yang tersedia. untuk mencari bukti kejahaan digital dalam membantu pihak kepolisian melakukan investigasi terhadap suatu kejahatan seperti data lokasi, foto, pesan, atau penelusuran internet. (Popovic, Kuk, & Kovacevic, 2018). Selain itu penting untuk mengetahui alat yang akan digunakan untuk mencari bukti seperti bukti kejahatan pada perangkat atau media sosial, meskipun sebagian besar alat memberi bukti yang masuk akal hanya pada satu alat saja, juga perlu dibandingan dengan alat lain (Salave & Wakdikar, 2017).

Penelitian ini bertujuan mencari semua data yang ada pada media sosial twitter yang berjalan di sistem operasi android dengan menerapkan metode *Digital Forensics Research Workshop* (DFRWS), menggunakan *tools* forensik MOBILedit Forensic Express dan Belkasoft Evidence Center untuk menggali data yang ada pada media sosial twitter dengan melakukan pengujian skenario eksperimen berupa penambahan data audio, gambar, video, text dan dilakukan beberapa penghapusan data, serta ingin diketahui *tools* yang tepat untuk memperoleh data digital pada media sosial twitter dengan membandingkan keduanya.

2. Metodologi Penelitian

2.1 *Digital Forensic Research Workshop* (DFRWS)

Forensik digital merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum *(pro justice)*, dalam hal ini untuk membuktikan kejahatan berteknologi tinggi hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan, membantu mengantisipasi aksi ilegal yang dapat merusak jalannya rencanan operasi, elemen terpenting dalam digital forensik adalah kredibilitas bukti digital, dapat berupa audio digital, video, handphone/*smartphone*, text, gambar, dan lain sebagainya. (Aryo C Ki Wardana et al., 2018).

The Digital Forensics Research Workshop (DFRWS) mendefinisikan digital forensik sebagai ilmu pengetahuan pasti dan metode telah teruji untuk melakukan proses *preservation*, *validation*, *identification*, *analysis*, *interpretation*, *documentation*, dan *presentation* dari seluruh bukti digital yang diperoleh dari sumber digital untuk memfasilitasi rekontruksi dari kejadian yang diduga seabgai sebuah tindak kejahatan atau membantu proses untuk mengantisipasi terjadinya kejahatan tersebut (Harris, 2006b).

2.2. *Tools* Forensik

Tools forensik yang bisa digunakan untuk mengambil data dari *smartphone* atau *tools* ekstraksi bisa berupa perangkat lunak atau perangkat keras, banyak *tools* ekstraksi yang beredar mulai dari *tools* gratis untuk uji coba dan berbayar untuk mendapatkannya dengan banyak fitur didalamnya yang bisa digunakan untuk menggali bukti yang diperlukan, saat ini *tools* forensik lebih banyak yang sifatnya komersil dan cukup sulit untuk mendapatkannya terkait dengan privasi dan keamanan.

2.3 MOBILedit Forensic Express

Tools forensik ini sangat banyak versinya dari yang versi standar hingga pro, MOBILedit Forensic Express memungkinkan untuk mendapatkan data secara logic, mencari dan memeriksa isi dari perangkat, pembuatan image, backup serta cloning, menggunakan beberapa mekanisme konektifitas yang dapat dipilih dari usb hingga nirkabel, cukup baik digunakan untuk memperoleh informasi sistem perangkat atau *smartphone* dan informasi lain seperti pesan dan kontak (Yadi & Kunang, 2014).

2.4 Belkasoft Evidence Center

Belkasoft Evience Center, dapat digunakan untuk mendapatkan, mencari, menganalisa dan menyimpan berbagai bukti digital yang ada pada perangkat komputer atau *mobile*, *tools* ini untuk mengekstrak bukti digital dari berbagai sumber dengan menganalisis penyimpanan *hard drive*, *memory dump*, iOs BlackBerry dan android *backup* kemudian secara otomatis akan menganalisis sumber data dan menyimpannya dalam sebuah laporan (Parekh & Jani, 2018b).
Metode *Digital Forensic Research Workshop* DFRWS menggunakan langkah-langkah berikut:

g. Identifikasi, melakukan penentuan kebutuhan yang diperlukan untuk penyelidikan dan pencarian bukti.
h. Pemeliharaan, menjaga bukti digital agar memastikan keaslian bukti dan membantah klaim bukti telah dilakukan sabotase
i. Pengumpulan, tahapan melakukan identifikasi bagian tertentu dari bukti digital dan melakukan identifikasi sumber data.
j. Pemeriksaan, yaitu menentukan filterisasi data pada bagin tertentu dari sumber data, dilakukan dengan melakukan perubahan bentuk data tetapi tidak melakukan perubahan isi data untuk menjaga keaslian data yang sangat penting.
k. Analisis, melakukan penentuan tentang dimana data tersebut dihasilkan, oleh siapa dan bagaimana cara data dihasilkan serta kenapa data tersebut dihasilkan.
l. presentasi dengan menyajikan informasi yang dihasilkan dari tahapan analisis.

3. Hasil Dan Pembahasan

7.1. Tahap Identifikasi

Tahap identifikasi diperlukan perangkat *smartphone* yang sudah terpasang media sosial twitter dan sudah digunakan untuk berbagai aktifitas dengan fitur yang ada di dalamnya, yang akan menjadi sumber dari pancarian bukti atau data yang akan diambil.

3.1.1. Perangkat Smartphone

Spesifikasi dari *smartphone* yang digunakan pada penelitian seperti pada tabel 1, dan berjalan diatas sistem operasi android.

Tabel 1. Spesifikasi perangkat smartphone

Manufacture	EVERCROSS
Product	B75
HW Revision	LMY47D

Platform	Android
SW Revision	5.1(22)
Serial Number	0123456789ABCDEF
Unlocking Pattern	3452
IMEI	358441061746404
Rooted	Yes
SIM Card	Yes
Operator	3, MCC:510, MNC:89
IMSI	510897263097260
ICCID	89628990007753870152

3.1.2 Akun Twitter

Media sosial twitter memiliki bebrapa fitur yang dapat digunakan oleh penggunanya antara lain adalah, memperbarui profil pengguna, mengganti *username*, *password*, mengikuti atau menambah pertemanan, mengirim pesan secara pribadi, memberikan sanggahan pada sebuah tweet atau kiriman yang dikirimkan seseorang untuk diketahui khalayak umum, membagikan atau membagikan dengan memberi komentar, menyukai sebuah postingan, membagikan postingan melalui pesan pribadi, menjadikan *bookmark*, atau membagikan dengan aplikasi lain, fitur pencarian, *notifikasi*, menulis untuk postingan tertentu, berupa tulisan, gambar, *polling*, dan membagikan lokasi.

3.1.3 *Tools* forensik

Penggunaan *tools* forensik untuk menggali semua data dari perangkat *smartphone* yang menggunakan layanan media sosial twitter seperti pada tabel 2.

Tabel 2. *Tools* Forensik yang digunakan

Nama *Tools*	Versi
MOBILedit Forensic Express	5.1.1
Belkasoft Evidence enter	Belkasoft Evidence Center 9.6 Build 3981 x64

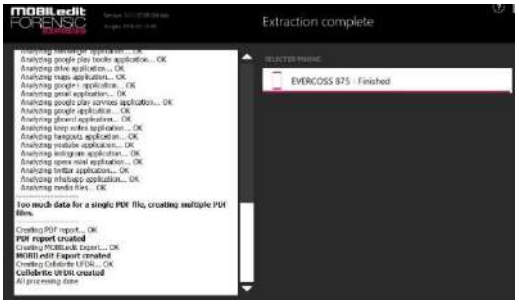
7.2. Pemeliharaan

Tahap pemeliharaan bertujuan untuk menjaga barang bukti digital atau semua data yang ada pada perangkat dengan mengisolasi atau menjaga perangkat dari komunikasi dari luar ke dalam atau sebaliknya, pemasangan aplikasi, pencopotan aplikasi, penambahan atau penghapusan data dengan cara mengaktifkan mode pesawat pada perangkat.

7.3. Pengumpulan

Proses pengumpulan data pada perangkat dengan cara melakukan kloning perangkat atau membuat *physical image* dari perangkat agar keaslian tetap terjaga, dan membuat backup menggunakan MOBILedit Forensic Express untuk mempermudah pembacaan semua data yang ada pada perangkat.

Berikut pada gambar 1 proses pengumpulan data dari perangkat smartphone menggunakan MOBILedit Forensic Express .



Gambar 1. Backup data menggunakan MOBILedit Forensic Express

7.4. Pemeriksaan

Tahap pemeriksaan data setelah tahap pengumpulan data selesai, dari *tools* MOBILedit Forensic Express dan Belkasoft Evidence Center didapatkan data yang diambil dari perangkat smartphone dengan layanan twitter seperti pada tabel 3.

Tabel 3. Hasil pemeriksaan dengan kedua *tools*

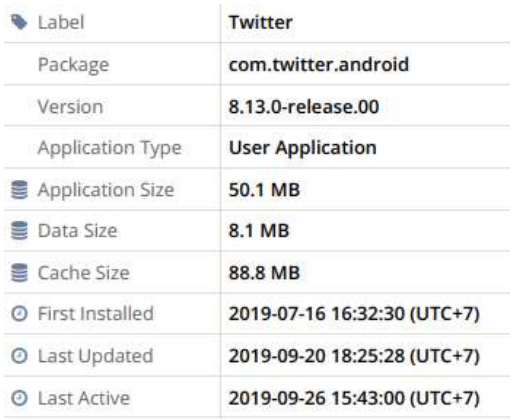
Hasil yang diperoleh	*Tools*	
	MOBILedit Forensic Express	Belkasoft Evidence Center
Application info	√	×
Account info	√	×
Twitter ID	√	√
Friends	√	×
User/ Follower/Following	√	√
Conversation/Direst Messages	√	√
Cached Search	√	×
Audio	×	×
Video	√	×
Text	√	√
Picture	√	√
Deleted Messages/Tweets	√	√
IP Adress	×	×
url	√	√
Email/Phone Number	√	×
Location	√	×

7.5. Analisis

Hasil yang didapatkan menggunakan MOBILedit Forensic Express dan Belkasoft Evidence Center pada masing masing *tool* sangat terbatas sehingga hanya beberapa data yang berhasil ditemukan bisa memberikan informasi yang jelas bahkan beberapa data tidak bisa terbaca.

3.5.1 MOBILedit Forensic Express

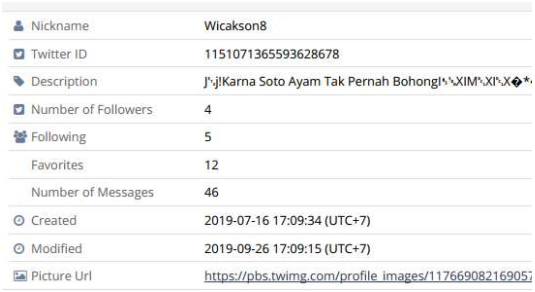
Info apilkasi media sosial twitter yang terpasang pada perangkat *smartphone* berisi informasi tentang versi aplikasi, ukuran aplikasi, ukuran data, tanggal di *install* dan terakhir diperbarui seperti pada gambar 2.



Label	Twitter
Package	com.twitter.android
Version	8.13.0-release.00
Application Type	User Application
Application Size	50.1 MB
Data Size	8.1 MB
Cache Size	88.8 MB
First Installed	2019-07-16 16:32:30 (UTC+7)
Last Updated	2019-09-20 18:25:28 (UTC+7)
Last Active	2019-09-26 15:43:00 (UTC+7)

Gambar 2. Info Aplikasi twitter yang terpasang

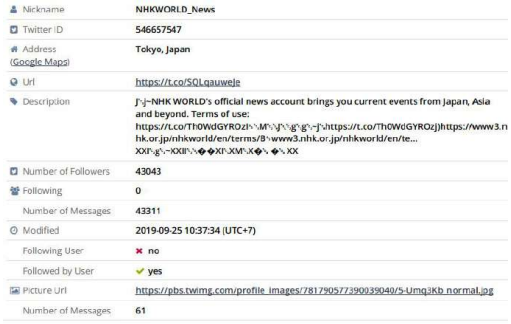
Data selanjutnya yang ditemukan adalah informasi akun yang terpasang pada perangka smartphone, meliputi nickname, twitter id, deskripsi, jumlah pengikut, jumlah mengikuti, jumlah pesan, tanggal dipasang aplikasi serta tautan untuk gambar profil pengguna seperti pada gambar 3.



Nickname	Wicakson8
Twitter ID	1151071365593628678
Description	J^·j!Karna Soto Ayam Tak Pernah Bohong!^·\·\XIM^\XI^\X@*·
Number of Followers	4
Following	5
Favorites	12
Number of Messages	46
Created	2019-07-16 17:09:34 (UTC+7)
Modified	2019-09-26 17:09:15 (UTC+7)
Picture Url	https://pbs.twimg.com/profile_images/117669082169057

Gambar 3. Detail informasi pemilik akun

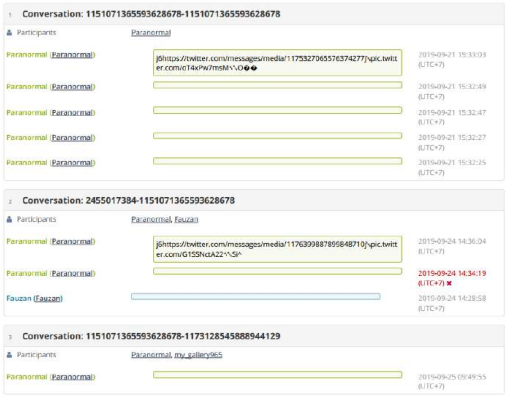
Selanjutnya adalah informasi pertemanan yang di ikuti oleh pemilik akun berisi informasi yang cukup lengkap seperti nama, twitter id, alamat yang dapat dilihat dengan goole maps, deskripsi akun, tautan yang mengarah pada profil akun, jumlah pengikut, data ini hampir sama dengan informasi akun pengguna seperti pada gambar 4.



Nickname	NHKWORLD_News
Twitter ID	546657547
Address (Google Maps)	Tokyo, Japan
Url	https://t.co/SQLqauweJe
Description	J^·j~NHK WORLD's official news account brings you current events from Japan, Asia and beyond. Terms of use: https://t.co/Th0WdGYROzJ^\·M^\·\J^\·\g^\g\~J^·\https://t.co/Th0WdGYROzJjhttps://www3.nhk.or.jp/nhkworld/en/terms/8^\www3.nhk.or.jp/nhkworld/en/te... XXI^\g\~XXII^\·\·\··XI^\XM^\X·\·\·\·XX
Number of Followers	43043
Following	0
Number of Messages	43311
Modified	2019-09-25 10:37:34 (UTC+7)
Following User	no
Followed by User	yes
Picture Url	https://pbs.twimg.com/profile_images/781790577390039040/5-Umq3Kb_normal.jpg
Number of Messages	61

Gambar 4. Detail informasi akun lain yang di ikuti

Percakapan yang dapat ditemukan menggunakan MOBILedit Forensic Express tidak dapat terbaca, informasi yang dapat ditemukan hanya ID twitter yang melakukan percakapan, nama akun, tanggal percakapan dilakukan, jumlah percakapan, tanda percakapan atau pesan yang dihapus seperti pada gambar 5.



Gambar 5. Percakapan pribadi pemilik akun dengan akun lain

Selain percakapan, data lain yang dapat diambil dari layanan media sosial twitter adalah *cache tweets* atau *timeline* yang didalamnya berisi beberapa informasi diantaranya nama pengguna, *tweets* atau status yang diunggah, tanggal pengunggahan status tweet, hastag, bahasa, jumlah retweet atau seberapa banyak diunggah ulang, tautan yang menuju pada tweet pengguna seperti pada gambar 6. Dapat dilihat juga tweet yang dihapus oleh pemilik akun.

Gambar 6. Cache tweets yang muncul pada beranda timeline

3.5.2 Belkasoft Evidence Center

Hasil pengambilan data menggunakan Belkasoft Evidence Center pada layanan media sosial twitter ditemukan lebih sedikit dari pengambilan mengggunakan tool MOBILedit Forensic Express seperti pada gambar 7 ditemukan beberapa informasi ID akun yang menunjukkan nama akun.

Account	First name	Last name	Nickname
383712645			Kent Aro4k'ers(RockersPantura)
18862596			Joko Anwar(jokoanwar)
1085181504			Luckman Djaya(luckman_djaya)
802352262			ikan asin(luwakwhitekofi)
222346474			YayasanLBHIndonesia(YLBHI)
153608362			Puthut EA(Puthutea)
951480480			Gouvernement(gouvernementFR)
578919806			Hamid SQ(HamidSQ)
184199979			Pavel Soriano(psorianom)
1343799062			Ambassade d'Indonésie Paris(KBRI_Paris)
116244358			Ananda Badudu(anandabadudu)
361329018			Kicks Deals(KicksDeals)
43115589			□□□□□□'□□□ シ (NJKamka)
64653674			Trikus // Komentator Garis Miring(Trikus2012)
1283810071			m abdul karim(baimmabdul_m)
75519209			cha(paketpanas2)

Found: 478 Shown: 478 Checked: 0

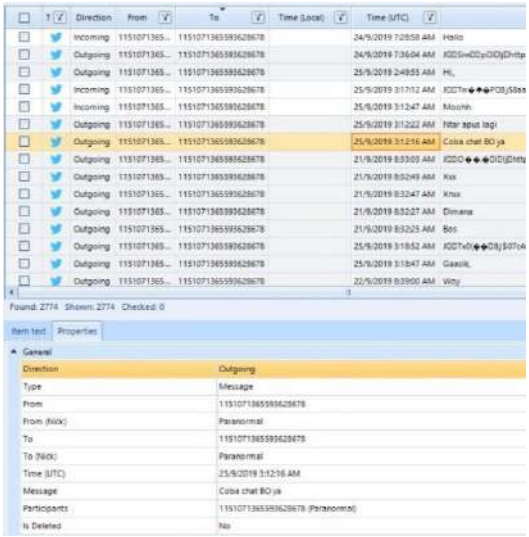
Properties

General

Account	222346474
Nickname	YayasanLBHIndonesia(YLBHI)
Time zone	0

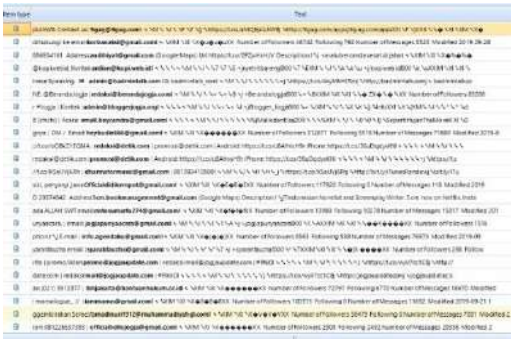
Gambar 7. Informasi ID akun dan nama akun twitter

Data selanjutnya adalah bentuk aktifitas percakapan oleh pengguna, dapat terbaca pesan yang dikirimkan oleh pemilik akun, tanggal percakapan berlangsung, arah percakapan keluar dan masuk seperti pada gambar 8.



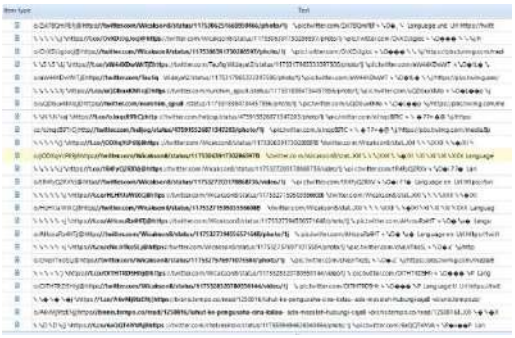
Gambar 8. Arah percakapan pemilik akun berserta isi percakapan

Data lain yang berhasil ditemukan menggunakan Belkasooft diantaranya adalah email dari beberapa akun yang terhubung, selain email terdapat beberapa data seperti tautan, nomor telepon jumlah pengikut dari sebuah akun, jumlah mengikuti serta jumlah pesan seperti pada gambar 9.



Gambar 9. Informasi alamat email dan jumlah pengikut dari sebuah akun

Sementara pada data lain dari Belkasoft menunjukkan bahwa tautan yang mengarah pada id akun dan aktifitas membagikan status atau aktifitas lain yang tampil pada timeline seperti pada gambar 10.



Gambar 10. tautan merujuk pada aktifitas pengguna

7.6. Presentasi

Hasil perolehan data menggunakan *tools* MOBILedit Forensic Express dan Belkasoft Evidence Center memiliki kelebihan dan kekurangan. Perolehan data dari masing masing tool disajikan dalam tabel agar lebih mudah dicermati.

3.6.1 MOBILedit Forensic Express

Hasil dari pengambilan data menggunakan tool MOBILedit Forensic Express berupa detail info akun, nama akun, pertemanan, pengguna lain yang masuk kedalam timeline, percakapan, pesan pribadi dan nomor telepon, seperti pada tabel 4.

Tabel 4. Hasil Pengambilan data dari MOBILedit Forensic Express

Evidences	MOBILedit Forensic Express	*Result*
Detail Account info	Account	1
	User Account	Paranormal
	Friends	6
	Users	587
	Conversation	4 conversation, 23 messages, 1 deleted
	Cached Tweets	852, 13 deleted
	Messages	23, 1 deleted
	Cached Searches	2
	List of Analyzed files	8 files
Account Name (1)	Nickname	Wicasono8
	Twitter ID	1151071365593628678
	Description	J□j!Karna Soto Ayam Tak Pernah Bohongl□ □XIM□XI□ X□*□*□*XX
	Follower	4
	Following	5
	Favorite	12
	Number of Messages	46
	Created Date	2019-07-16 17:09:34 (UTC+7)
	Modified Date	2019-09-25 10:40:25 (UTC+7)
	Picture ID	https://pbs.twimg.com/profile_images/1176690821690576900/hFbrBj3H_normal.jpg
Friends (6)	Nickname	fauzangustafi
	Twitter ID	2455017384
	Adress (google maps)	Boyolali
	Description	J□j□Bio: I'm Awesome! I□□XIM□ XI□X□□□□□XX
	Number of Followers	26
	Following	36
	Number of Messages	174
	Modified	2019-09-25 09:48:43 (UTC+7)
	Following User	Ok
	Followed by User	Ok
	Picture URL	https://pbs.twimg.com/profile_images/653594881508577281/qEdYmv0d_normal.jpg
	Number of Messages	20
User (587)	Nickname	PartaiSocmed
	Twitter ID	869327120
	Adress (google maps)	Indonesia
	Url	https://t.co/aDu3oGTVHr
	Description	J□j□Social Media Party | Objectivity, Fairness and Justice for All | Non-Populist Party | Common Sense Party | Empowering People | No = 99I□□XIM□XI□ X□□□□□□XX
	Number of Followers	173470
	Following	3007
	Number of Messages	352939
	Modified	2019-09-24 14:02:56 (UTC+7)
	Picture URL	https://pbs.twimg.com/profile_images/1137182440907108352/iFHhYIh-_normal.jpg
Conversation (4 convers, 23 messages, 1 delete)	Sent Message	N/A
	Received Message	N/A
	Draft	N/A
	Failed Message	N/A
	Unknown Message	N/A
	Deleted Message	OK
	Conversation ID	2455017384-1151071365593628678
	Date/ Time	2019-9-24 14:36:04 (UTC+7)

	Participants	Paranormal, Fauzan
Cached tweets (852, 13 deleted)	Status/ timeline	OK
	Nama Akun	Rudiantara (Rudiantara)
	Tanggal Update	2019-05-25 20:15:31 (UTC+7)
	Words Status	J□k□□Teman2, situasi sdh kondusif shg pembatasan akses fitur video & gambar pd medsos & instant messaging difungsikan kembali. Mari senantiasa jaga dunia maya digunakan unt hal2 yg positif. Mari perangi hoaks, fitnah, info2 yg memprovokasi spt yg banyak beredar saat kerusuhan kemarin. I□ □XII□XI□XI□XI□ XI□XXX
	Hastag	NOK
	Language	In
	Url	https://twitter.com/Rudiantara/status/1132273995712090113
	Favorites	4078
	Retweet Count	1299
	Deleted/ Received	Received
Messages (23, 1 deleted)	Chat/ Sent-Received	Convesation ID Conversation: 2455017384-1151071365593628678
	Content	j6https://twitter.com/messages/media/1176399887899848710j□ pic.twitter.com/G1SSNctA22□□Si^
Cached Searches	Hastag Account	OK
Application info	Label	Twitter
	Package	Com.twitter. android
	Version	8.13.0-release.00
	Application Type	User Application
	Application Size	50.1 MB
	Data Size	8.1 MB
	Cache Size	88.6 MB
	First Installed	2019-07-16 16:32:30 (UTC+7)
	Last Updated	2019-09-20 18:25:28 (UTC+7)
	Last Active	2019-09-25 11:26:00 (UTC+7)
Video		ok
Gambar		Ditemukan
Suara		Nok
Email		andihiyat@gmail.com
Url		https://twitter.com/Rudiantara/status/1132273995712090113
IP Adress		-
Kontak Telepon		0812 8899 3248

3.6.2 Belkasoft Evidence Center

Data pada tabel 5 berisi nama akun, id akun, aktifitas pengguna, arah pada pesan pribadi, perubahan status, email, tautan dan timeline, merupakan data yang dapat diambil menggunakan Belkasoft Evidence Center, jumlah data lebih sedikit dari pengambilan menggunakan MOBILedit Forensic Express, penelusuran data yang lebih spesifik pada Belkasoft akan membutuhkan banyak waktu dalam menganalisis, terlebih jika pengguna sudah melakukan banyak aktifitas dalam akun twitternya.

Tabel 5. Hasil pengambilan data dari Belkasoft Evidence Center

Evidences	Belkasoft Evidence Center	Result
Nama Akun	Found	Paranormal
ID Akun	found	1151071365593628678
User Activity	Status changed	Message; Jj Besok gowesIXIIXIXIXIXIXXX
Incoming Messages	Found	gaasik
Outgoing Messages	Found	Baku hantam, minat?
Status change/ tweets	Found	Jj4Maunya apa ?@rudiantara_id #saveri #freedominternetIMJ ��Uij rudiantara_idj RudiantaraXXIXMJ#jsaveriXXI#XMJ$$4jfreedominternetXXI$4XXIIXIXI@XI s ��XIXXX;
Email	Found	korbanaksi@gmail.com
Detail account	Found	Follower 46742; messages 5523 modified 2019-09-28
Url	Found	https://pbs.twimg.com/profile_images/852355177260621824/usivwpwx_normal.jpg

Timeline	Found	JjTKampus A "Initiate Retreat!" Kampus B "Request Back Up!" anak STM "LAUNCH ATTACK!!!"IMJ

Image Forensic Social Media Using Digital Forensic Research Workshop (DFRWS) Method

Imam Riadi, Department of Information System, Universitas Ahmad Dahlan, Indonesia
Sunardi, Department of Electrical Engineering, Universitas Ahmad Dahlan, Indonesia
Anton Yudhana, Department of Electrical Engineering, Universitas Ahmad Dahlan, Indonesia
Wicaksono Yuli Sulistyo, Department of Informatics, Universitas Ahmad Dahlan, Indonesia

ABSTRACT

Developments in the information technology era are increasing both positively and negatively. One of the negative impacts is the uncontrolled attitude of the people in using the applications they have, thus creating crime in cyberspace (cybercrime), an example of the most widely used social media application is the Facebook, Twitter and Instagram applications. The case of cybercrime that is common on social media is uploading photos that have been used to bully someone or provide information, fraud, and defamation. Changes to photos can be easily created or edited so that they can change information that is conveyed differently and is vulnerable to use for a crime. This is the basis of this research for experiments in the detection of digital photo forgery. This study uses a Forensic method stage called Digital Forensic Research Work Shop (DFRWS).

Keywords: Digital, Forensics, Image, Mobile, Photo, Forgery, DFRWS, Social Media

INTRODUCTION

The development of technology from time to time is more advanced, so that makes everything all digital, including photo business. Digital photos have advantages, but besides that, they also have disadvantages such as the ease of manipulating photos with editing software so that they can change the message conveyed on the picture (Sulistyo, Riadi, & Yudhana, 2018b). Advances in editing software make manipulating photos even easier for someone. Manipulation of photos is divided into three types, namely image splicing, copy-move, and image retouching, and it makes it difficult to distinguish original photos from manipulated photos because manipulation techniques are getting better and developing (Fadlil, Riadi, & Sari, 2017). The ease in making and manipulating an image can damage the credibility of the authenticity of the photo in various aspects, so it is prone to be made a crime because changes in the photo can cause changes in the information conveyed (Rosidin, 2018).

Mobile phones today are called smartphones that are equipped with operating systems so that they can perform several functions like a computer, one of which is accessing the

internet. January 2016 smartphone users access the internet with an Android-based platform as much as 66%, Apple iOS 19%, and other platforms as much as 15%, while the number of smartphone users active social media throughout the world reaches 2.31 Trillion (Mukti et al., n.d.). Image retouching is a manipulation technique that is commonly found in social media applications such as Twitter, Facebook, and Instagram with a variety of positive and negative goals. Technology-based crime has increased in various ways. Therefore we need a precise mechanism to trace and analyze the digital evidence obtained (A. P. Saputra & Widiyasono, 2017). A picture or photo can be used as evidence in the field of law or court, if the photo submitted by the court is known to have been manipulated then the validity of the photo is lost and can not be used as court evidence (Kresnha, Susilowati, & Adharani, 2016).

Manipulation techniques that have increasingly developed, we need a forensic method that can solve these problems, one of which is using the *Digital Forensic Research Workshop* (DFRWS) method. Some *tools* that can be used for this process are MOBILedit Forensic Express, Fotoforensic, and ForensicallyBeta.

LITERATURE REVIEW

1. Mobile Forensic

Mobile forensics is a branch of digital forensics that deals with the recovery of digital evidence from mobile devices. The investigation process is usually focused on simple data such as data calls, SMS, e-mail, and data that has been erased from mobile storage. Information taken from a mobile device can be useful in various legal or court matters and investigations such as corporate fraud cases, cyberbully, evidence of the crime (Putra et al., 2017).

2. Digital Image Processing

Image processing is a general term for various techniques whose existence is to manipulate and modify images in various ways. Photos are two-dimensional images that can be quickly processed. Each photo in digital form can be processed with certain applications (Permata, 2016). image processing techniques have been successful in improving image quality so that it is easy to interpret (Effendi, Fitriyah, & Effendi, 2017).

3. *Digital Forensic Research Workshop* (DFRWS)

Image processing is a general term for various techniques whose existence is to manipulate and modify images in various ways. Photos are two-dimensional images that can be easily processed. Each photo in digital form can be processed with certain applications (Faiz, Prabowo, & Muhammad Fajar Sidiq, 2018).

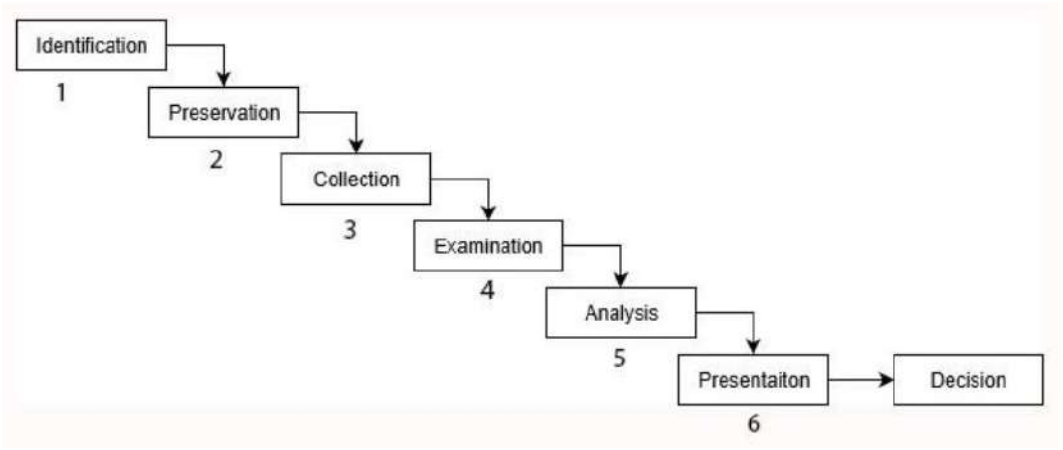
Previous research before this research included research on Fotoforensic, with the results obtained that fotoforensics.com can be used as accurate detection of images. The facilities provided by fotoforensics.com can be used and are very efficient in the ELA (Error Level Analysis) and JPEG% techniques. The accuracy obtained from the results of this research experiment is three samples, namely sample 1 and sample 2, as much as 87% accuracy rate while sample 3 is 71% (Mahardika, Khatulistian, & Kuncoro, 2018). Research on ELA shows that the ELA (Error Level Analysis) technique introduced by Krawets has many analysis features for analyzing an image that has a function of each, but this analysis may give wrong results and also has many interpretations, for that requires Special system for providing quantitative results for the performance of the ELA technique (Sari, Riadi, & Fadlil, 2016). Then another study that discusses the based on ordinal

measure coefficient of discrete cosine transform (OM-DCT), based on the results of analysis and experiments that have been carried out in this study, it can be concluded that OM-DCT can be used well for detection of falsity of images with copy-move techniques (Zulfan, Arnia, & Muharar, 2018). Other research is about the Level Error Analysis technique that can be used to detect image modification. This method works by resetting the image at 75% or 95% compression and evaluating the difference with the original. Modified areas are easily seen because of their characteristic aspects in ELA representation (Febrianda, Andreswari, & Wulandari, 2018). In addition to these studies, there is also research that discusses the DyWT and SIFT methods, the results of this study indicate that testing with the DyWT and SIFT methods can detect copy-move falsification in different image areas that have undergone modifications in image processing, such as rotations and scales that have been applied to the test image (Tresnaningsih, Endina Putri Purwandari, & Desi Andreswari, 2017).

METHOD

This study uses a digital forensic method created by the *Digital Forensic Research Workshop* (DFRWS). The DFRWS method helps obtain evidence and a centralized mechanism for recording the information collected. The method has several stages, such as in Figure 1. (Suryana et al., 2016c).

Figure 1. Schema of the DFRWS



1. *Identification*

This stage is an identification process carried out to determine what needs are needed in the investigation and search for evidence.

2. *Preservation*

This stage is the maintenance stage carried out to safeguard digital evidence, ensure the authenticity of evidence, and refute claims that evidence has been sabotaged.

3. *Collection*

Conducting the process of collecting identification of a specific part of digital evidence and identifying the source of data.

4. *Examination*

Performing the stage of determining the filtering of data at certain parts of the data source, filtering the data is done by doing the form of data but does not make changes to the contents of the data because the authenticity of the data is important.

5. *Analysis*

Determine where the data is produced, by whom the data is produced, how the data is produced, and why the data is generated.

6. *Presentation*

The presentation is done by presenting information generated from the analysis phase. The presentation stage is carried out after evidence is obtained from the inspection process and analyzed. Furthermore, at this stage, an explanation is made of the *tools* and methods used, determining the supporting actions taken and providing recommendations for improving policies, methods, *tools*, or other supporting aspects of the digital forensic action process.

Case simulation carried out was a case of fraudulent sales of used smartphones using social media Twitter. the perpetrators have posted items sold on Twitter, but before that the perpetrators first edit the smartphone images to be sold so that they look more attractive and eliminate defects in their products. In this study, the acquisition method used is the Live Forensics method with the forensic framework referring to the standards of the *Digital Forensic Research Workshop* (DFRWS).

RESULT

The *Digital Forensic Research Workshop* (DFRWS) method is one of the forensic methods that have quite complete stages in running the forensic process and is widely used by forensic investigators. Digital Forensics Research Workshop is the use of scientific methods that have a basis and proven for the maintenance, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence originating from digital sources for the purpose of facilitating or continuing the reconstruction of events containing criminal, or helps to anticipate unauthorized actions that are proven to interfere with planned operations. The DFRWS method has six main stages, namely, identification, preservation, collection, examination, analysis, and presentation.

First step taken is identification by searching for information from previous cases to be used as a reference for understanding the evidence being explored. This identification stage also identifies how the image forgery case works. The image forgery case simulation is carried out to obtain digital evidence, because by getting the evidence sought, the identification stage can be continued at the maintenance stage in accordance with the framework of the DFRWS method.

The second stage is preservation, which is the maintenance phase to safeguard digital evidence, ensure the authenticity of evidence, and refute claims that evidence has been sabotaged. The process of maintaining integration is carried out to keep the evidence authentic and undamaged, with the technique of isolating physical evidence and making backups in the form of cloning or image file processing of the evidence. The step taken is

isolating the smartphone device from communication. Isolation needs to be done to avoid things that can damage digital evidence or affect the integrity of the data in it. Isolation activities carried out are changing the status of the device into Airplane Mode.

The next stage is the stage in which the process of collecting identification of specific portions of digital evidence and identifying data sources is carried out. Proof of evidence proposed is a smartphone device. This research uses branded smartphone Evercross, as in Figure 2.

Figure 2. A Smartphone Used for Case Simulation

Table 1. Smartphone Specifications

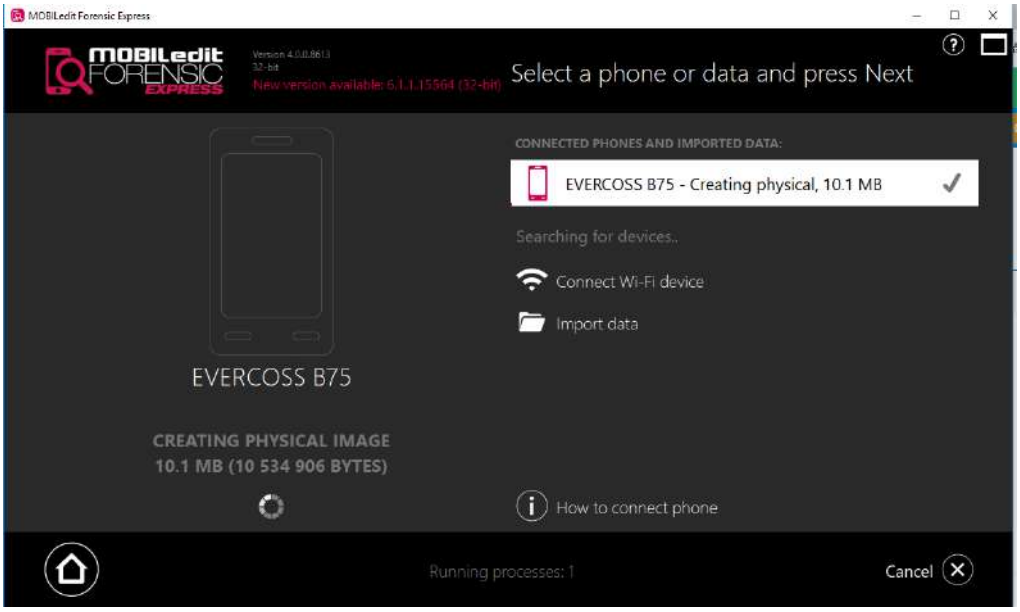
Type of Specification	Spesifications
Brand	Evercross
Series	Elevote
Model	Y3+
IMEI	358441061746404
OS	Android
OS Version	5.1 (Lolipop)
Processor	Quad Core 1.0 GHz

Activate Developer Option for the forensic process, to activate it by pressing Build Number on the smartphone seven times. If the activation process is successful, the next step on the Developer Options menu is to activate the Stay Awake and USB Debugging options for forensic procedures. Stay Awake is needed so that the smartphone device is not in sleep mode if it is not used for a while during the forensic process because it can activate the smartphone device security system. USB Debugging is used to give permission to smartphone devices to communicate with workstations using USB and ADB cables.

The stage of taking digital Evidence on a smartphone has a high risk, if a fatal error occurs, the data and digital Evidence available on a smartphone can be lost or corrupted so that it cannot be read, therefore it is necessary to preserve the Evidence, which is to backup or imaging the smartphone which is becoming Evidence, this process is also called logical acquisition.

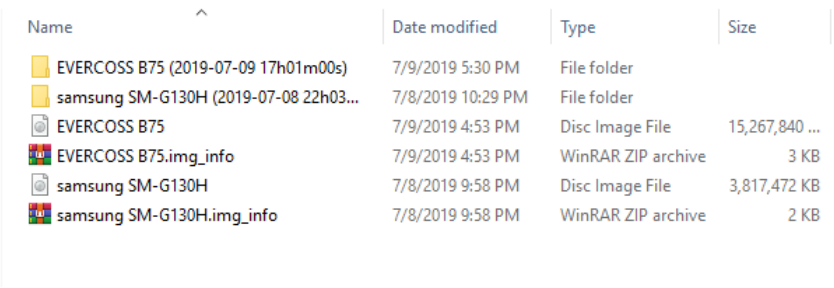
The *tools* used to carry out the backup process are MOBILedit Forensic Express. The ability of this tool is that it can make a smartphone system backup and extract it. Figure 3. is a backup process on smartphones with MOBILedit Forensic Express.

Figure 3. Smartphone Backup Process



The result of this backup process is an image document from a smartphone with an .img extension with document sizes that vary depending on the amount of data on the smartphone. the results of backups are used to maintain the authenticity of primary data to avoid changing data when in court. Figure 4. is the result of a backup of the process that has been done.

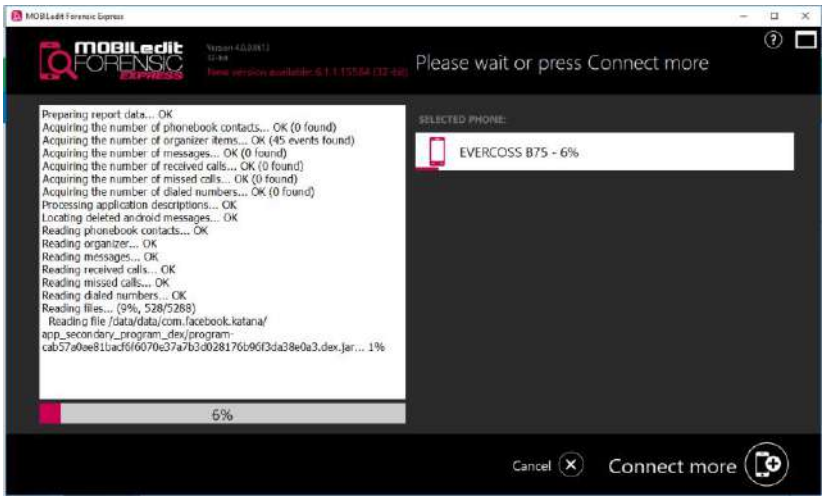
Figure 4. Smartphone Backup Process Result



Name	Date modified	Type	Size
EVERCOSS B75 (2019-07-09 17h01m00s)	7/9/2019 5:30 PM	File folder	
samsung SM-G130H (2019-07-08 22h03...	7/8/2019 10:29 PM	File folder	
EVERCOSS B75	7/9/2019 4:53 PM	Disc Image File	15,267,840 ...
EVERCOSS B75.img_info	7/9/2019 4:53 PM	WinRAR ZIP archive	3 KB
samsung SM-G130H	7/8/2019 9:58 PM	Disc Image File	3,817,472 KB
samsung SM-G130H.img_info	7/8/2019 9:58 PM	WinRAR ZIP archive	2 KB

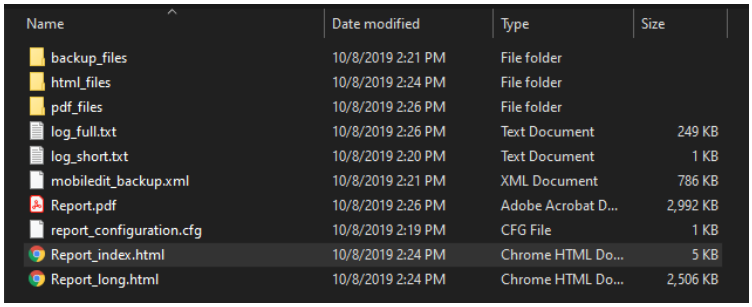
After the backup, the next step is to extract data using the MOBILedit Forensic Express tool, at this stage the evidence or smartphone must be connected first to the computer where the MOBILedit Forensic Express is installed. This process is the process of collecting data using an image file from the previous process so that the authenticity of the data is maintained. Figure 5. is the data extraction process.

Figure 5. Smartphone Data Extraction Process



The results of data collection that have been completed will get all content from chat, SMS, images, and others. Figure 6. is the result of this process.

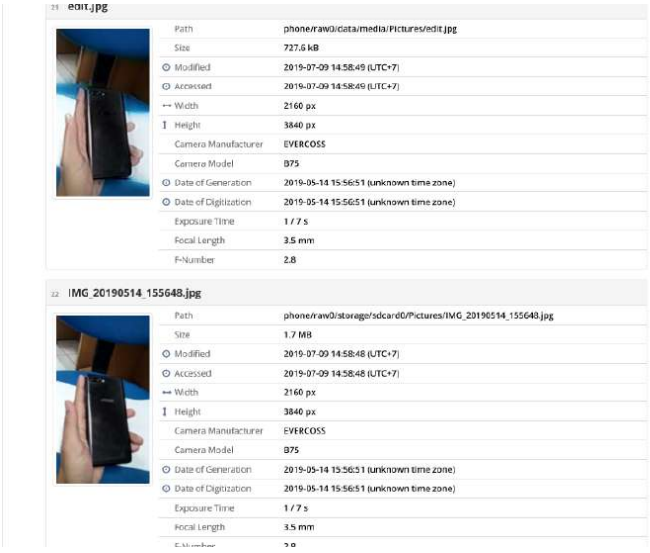
Figure 6. Data Collection Results



Name	Date modified	Type	Size
backup_files	10/8/2019 2:21 PM	File folder	
html_files	10/8/2019 2:24 PM	File folder	
pdf_files	10/8/2019 2:26 PM	File folder	
log_full.txt	10/8/2019 2:26 PM	Text Document	249 KB
log_short.txt	10/8/2019 2:20 PM	Text Document	1 KB
mobiledit_backup.xml	10/8/2019 2:21 PM	XML Document	786 KB
Report.pdf	10/8/2019 2:26 PM	Adobe Acrobat D...	2,992 KB
report_configuration.cfg	10/8/2019 2:19 PM	CFG File	1 KB
Report_index.html	10/8/2019 2:24 PM	Chrome HTML Do...	5 KB
Report_long.html	10/8/2019 2:24 PM	Chrome HTML Do...	2,506 KB

The extraction results that have been carried out will be displayed in the full report in this study. The selected full report is in .pdf format, full report display for evidence. Extraction results that have been done obtained a complete report that shows that there are 39 image files, including those as in Figure 7.

Figure 7. Example of Image File Obtained



21 edit.jpg

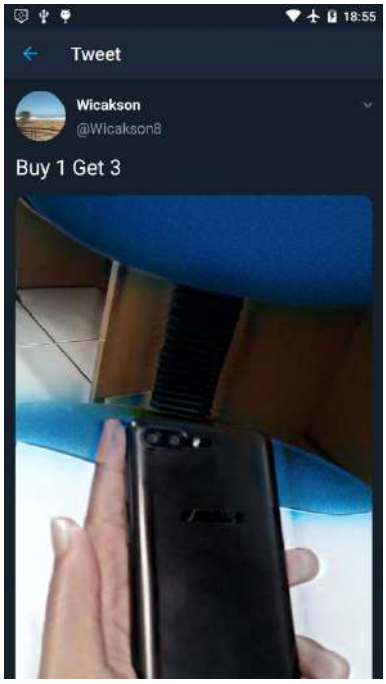
Path	phone/raw0/data/media/Pictures/edit.jpg
Size	727.6 kB
Modified	2019-07-09 14:58:49 (UTC+7)
Accessed	2019-07-09 14:58:49 (UTC+7)
Width	2160 px
Height	3840 px
Camera Manufacturer	EVERCOSS
Camera Model	B75
Date of Generation	2019-05-14 15:56:51 (unknown time zone)
Date of Digitization	2019-05-14 15:56:51 (unknown time zone)
Exposure Time	1 / 7 s
Focal Length	3.5 mm
F-Number	2.8

22 IMG_20190514_155648.jpg

Path	phone/raw0/storage/sdcard0/Pictures/IMG_20190514_155648.jpg
Size	1.7 MB
Modified	2019-07-09 14:58:48 (UTC+7)
Accessed	2019-07-09 14:58:48 (UTC+7)
Width	2160 px
Height	3840 px
Camera Manufacturer	EVERCOSS
Camera Model	B75
Date of Generation	2019-05-14 15:56:51 (unknown time zone)
Date of Digitization	2019-05-14 15:56:51 (unknown time zone)
Exposure Time	1 / 7 s
Focal Length	3.5 mm

After getting proof of the image, the next step is to look for pictures that match the actors posting on Twitter in carrying out the action. The case in this study is smartphone sales fraud by refining the appearance of the smartphone so that it looks without damage. Figure 8. is a picture and post of the perpetrator.

Figure 8. Post Actor



After analyzing the images obtained, there are two pictures that are similar to the images that the perpetrators post on Twitter, then an analysis of the two pictures is carried out. Figure 9. is two photos obtained.

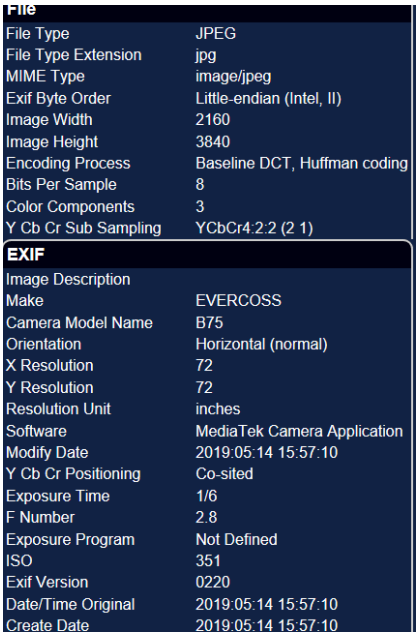
Figure 9. Photos Similar to Posts (a) First Photo. (b) Second Photo

(a)

(b)

The first step in analyzing the authenticity of an image is to detect the image metadata, in identifying the image using FotoForensic (fotoforensic.com). Figure 10. and Figure 10 are the results obtained from checking the metadata of the two images.

Figure 10. First Photo Metadata



File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)
Image Width	2160
Image Height	3840
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:2 (2 1)
EXIF	
Image Description	
Make	EVERCOSS
Camera Model Name	B75
Orientation	Horizontal (normal)
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	MediaTek Camera Application
Modify Date	2019:05:14 15:57:10
Y Cb Cr Positioning	Co-sited
Exposure Time	1/6
F Number	2.8
Exposure Program	Not Defined
ISO	351
Exif Version	0220
Date/Time Original	2019:05:14 15:57:10
Create Date	2019:05:14 15:57:10

Figure 11. Second Photo Metadata

File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)
Current IPTC Digest	c7794901f643e177fd726c73c9a2bb6d
Image Width	2160
Image Height	3840
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:4:4 (1 1)
EXIF	
Photometric Interpretation	RGB
Make	EVERCOSS
Camera Model Name	B75
Orientation	Horizontal (normal)
Samples Per Pixel	3
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	Adobe Photoshop CC 2017 (Windows)
Modify Date	2019:05:20 15:23:47
Y Cb Cr Positioning	Co-sited
Exposure Time	1/7
F Number	2.8
Exposure Program	Not Defined
ISO	345
Exif Version	0220

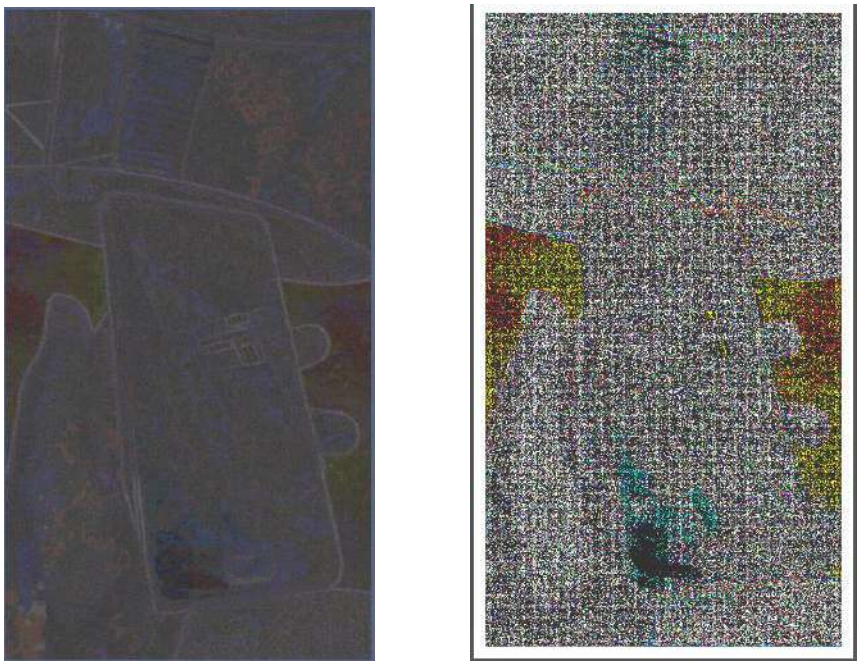
Photoshop	
IPTC Digest	c7794901f643e177fd726c73c9a2bb6d
Displayed Units X	inches
Displayed Units Y	inches
Print Style	Centered
Print Position	0 0
Print Scale	1
Global Angle	30
Global Altitude	30
URL List	
Slices Group Name	IMG_20190514_155648
Num Slices	1
Pixel Aspect Ratio	1
Photoshop Thumbnail	(Binary data 3379 bytes)
Has Real Merged Data	Yes
Writer Name	Adobe Photoshop
Reader Name	Adobe Photoshop CC 2017
Photoshop Quality	8
Photoshop Format	Standard
Progressive Scans	3 Scans
XMP	
XMP Toolkit	Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01
Creator Tool	MediaTek Camera Application
Metadata Date	2019:05:20 15:23:47+07:00
Date Created	2019:05:14 15:56:51.051
Color Mode	RGB
ICC Profile Name	sRGB IEC61966-2.1
Document ID	B739329E05185FA95FF7BFA6D5BE7009

Figure 10. above has shown the authenticity of the photo because in the metadata, there is no evidence to show that the Photo (a) was edited, whereas in Figure 11. There is evidence of metadata that shows the photo has been edited, that is, an additional form of evidence that shows the photo has been edited using Adobe Photoshop CC 2017.

After determining the authenticity of the two photos, the next step is to find proof of editing by comparing them using the FotoForensic *tools* (fotoforensic.com) and

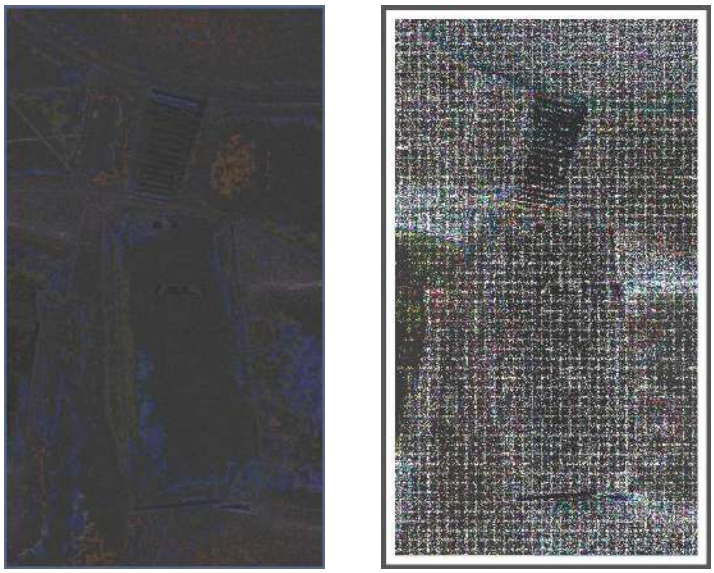
ForensicallyBeta (29a.ch/photo-forensics). Figure 12. and Figure 13. are the first photo analysis (original), and Figure 16. is the second photo analysis (edited).

Figure 12. Analysis of Original Photo (a) With FotoForensic. (b) With ForensicallyBeta



(a) (b)

Figure 13. Analysis Manipulation Photo (a) With FotoForensic. (b) With ForensicallyBeta



(a) (b)

After the two photos are processed using two *tools*, they will get like Figure 12. which is the process of the original photo and Figure 13. which is the process of photo editing.

The comparison of the two images is clearly visible, especially in the FotoForensic process, with the Technical Level Error Analysis technique. The comparison that is seen one of them is the pixel change on the smartphone object, besides that there are also some pixel changes in other areas that are different from the original photo so that it proves that in that section there is photo editing. As for ForensicallyBeta, there are also pixel differences in certain parts that indicate the presence of noise in the photo.

CONCLUSION

The results obtained from the research process regarding forensic image analysis using the *Digital Forensic Research Workshop* (DFRWS) method provide several conclusions that digital evidence obtained from several images related to the case simulation discussed. The extraction process uses the MOBILedit Forensic Express tool, using an EVERCROSS smartphone device. Based on digital evidence obtained on two forensic devices, it can be concluded that FotoForensic metadata content from photos can be obtained, where the second photo is an edited photo because there are indications that it has been edited using Adobe Photoshop CC 2017. In addition to checking metadata, FotoForensic can be used for analysis of parts of photos that have been edited, so it can be concluded FotoForensic has good performance in detecting photo authenticity. ForensicallyBeta can be used for analysis of parts of photographs that have been edited with various techniques, such as Error Analysis, Noise Analysis, Clone Detection, and JPEG Analysis Techniques.

REFERENCES

Effendi, M., Fitriyah, F., & Effendi, U. (2017). Identification of Tea Type and Quality Using Digital Image Processing with Artificial Neural Network Methods. *Jurnal Teknotan*, *11*(2), 67. https://doi.org/10.24198/jt.vol11n2.7

Fadlil, A., Riadi, I., & Sari, T. (2017). Image Forensic for detecting Splicing Image with Distance Function. *169*(5), 6–10.

Faiz, M. N., Prabowo, W. A., & Muhammad Fajar Sidiq. (2018). Comparative Study of Digital Forensic Investigations in Crimes. *1*(1), 47–53. https://doi.org/10.20895/INISTA.V1I1

Febrianda, D. A., Andreswari, D., & Wulandari, E. P. (2018). Integrated Digital Image Authentication System with Web Based Error Level Analysis (ELA) and Color Filter Array (CFA). *4*(March 2016), 45–56.

Kresnha, P. E., Susilowati, E., & Adharani, Y. (2016). Detecting Image Manipulation Based on Copy-Move Forgery Using Euclidean Distances with Single Value Decomposition. *Seminar Nasional Teknologi Informasi Dan Multimedia 2016*, 6–7.

Mahardika, F., Khatulistian, A. D., & Kuncoro, A. P. (2018). Review Photos Forensic.Com with Error Level Analysis and JPEG Techniques to Know the Original Image. *Jurnal Informatika: Jurnal Pengembangan IT Poltek Tegal*, *03*(01), 71–75.

Mukti, W. A., Masruroh, S. U., & Khairani, D. (2018). Analysis and Comparison of Forensic Evidence of Facebook and Twitter Social Media Applications on Android Smartphones. *Jurnal Teknik Informatika*, *10*(1), 73–84. https://doi.org/10.15408/jti.v10i1.6820

Permata, E. (2016). Identification of Sharp Objects Using Digital Image Processing on X-Ray Images. *Volt*, *1*(1), 1–14.

Putra, R. A., Fadlil, A., & Riadi, I. (2017). Mobile Forensics On Android-Based

Smartwach. *Jurti*, *1*(1), 41–47. https://doi.org/25798790

Rosidin. (2018). Analysis of Object Match Detection in Digital Images Using Matlab With SIFT Algorithm Method. Universitas Islam Indonesia.

Saputra, A. P., & Widiyasono, N. (2017). Digital Forensic Analysis in File Steganography (Case Study: Drug Circulation). *Jurnal Teknik Informatika Dan Sistem Informasi*, *3*(1), 179–190. https://doi.org/10.28932/jutisi.v3i1.594

Sari, T., Riadi, I., & Fadlil, A. (2016). Image Forensics for File Engineering Detection Using Error Level Analysis. *Annual Research Seminar 2016*, *2*(1), 133–138. Retrieved from http://ars.ilkom.unsri.ac.id

Sulistyo, W. Y., Riadi, I., & Yudhana, A. (2018). Image Authentication Detection Analysis Using Level Error Analysis Technique With ForensicallyBeta. *2018*(November), 154–159.

Suryana, A. L., Akbar, R. El, & Widiyasono, N. (2016). Email Spoofing Investigation with Digital Forensics Research Workshop (DFRWS) Method. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *2*(2), 111–117. https://doi.org/10.26418/jp.v2i2.16821

Tresnaningsih, W. R., Endina Putri Purwandari, & Desi Andreswari. (2017). Copy Move Image Falsification Using Dyadic Wavelet And Scale Invariant Feature Transform. *Jurnal Pseudocode*, *4*(1).

Zulfan, Arnia, F., & Muharar, R. (2018). Detection of Image Counterfeiting Using Copy-Move Technique Using the Ordinal Measure Method of the Discrete Cosine Transform Coefficient. *Jurnal Nasional Teknik Elektro*, *5*(2), 165. https://doi.org/10.25077/jnte.v5n2.230.2016

Daftar Publikasi:

No	Author	Judul	Jurnal	Status
1.	Imam Riadi, Sunardi, Anton Yudhana, Ikhsan Zuhriyanto,	Analisis Digital forensik aplikasi twitter menggunakan Digital Forensik Research Workshop (DFRWS)	Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)	Submitted
2.	Sunardi, Imam Riadi, Rusydi Umar, Muhammad Fauzan Gustafi	Audio Forensic on Smartphone with *Digital Forensic Research Workshop* Method (DFRWS)	IGI Global International Journal of Technoethics (IJT)	Submitted
3.	Imam Riadi, Sunardi, Rusydi Umar, Muhammad Noor Fadillah	Mobile Forensik Aplikasi Pembayaran Digital Menggunakan Metode DFRWS	Jurnal Penelitian Pos dan Informatika (JPPI)	Submitted
4.	Sunardi, Imam Riadi, Anton Yudhana, Ghufron Zaida Muflih	Analisis Perbandingan *Tools* Forensik Metode	Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)	Submitted
5.	Imam Riadi, Sunardi, Anton Yudhana, Wicaksono Yuli Sulistyo	Image Forensic with *Digital Forensic Research Workshop* Method	IGI GLOBAL Internasional journal of digital crime and forensics	Submitted

LAMPIRAN 6

(Bukti Submit)

UNIVERSITAS
AHMAD DAHLAN

wicaksono SULISTYO <wicaksono1807048009@webmail.uad.ac.id>

Manuscript Submission: Image Forensic Social Me...

1 pesan

(Shared) Journal Submission System Admin <journalsubmissionsystemadmin@igi-global.com>10 Oktober 2019 16.49
Kepada: "wicaksono1807048009@webmail.uad.ac.id" <wicaksono1807048009@webmail.uad.ac.id>

Dear Wicaksono Sulistyo,

This email is to confirm that we received your manuscript submission, "Image Forensic Social Media Using Digital Forensic Research Workshop (DFRWS) Method." Your manuscript will be evaluated by the journal's editor(s) and you will be advised as soon as possible through email of its status, as well as any revisions that may be necessary. Your manuscript can be managed from the Manuscripts page: https://www.igi-global.com/submission/manuscripts/. Please bookmark this page for easy access.

If you have any questions, please contact the journal editor, Feng Liu, at liufeng@iie.ac.cn.

If you need to contact IGI Global regarding your submission, please include the journal name and/or acronym and the title of your article in the subject line of all correspondence. This will ensure your correspondence reaches the correct Development Editor at IGI Global and will result in a much quicker response.

Thanks again for your submission - we look forward to working with you!

IGI Global
eEditorial Discovery

Gmail Fauzan Gustafi <fauzangustafi@gmail.com>

Manuscript Submission: Audio Forensic on Smartp...

1 message

(Shared) Journal Submission System Admin <journalsubmissionsystemadmin@igi-global.com> Thu, Oct 10, 2019 at 9:07 PM
To: "fauzan.gustafi@gmail.com" <fauzan.gustafi@gmail.com>

eEditorial Discovery
Supporting Your Editorial Experience

Dear Muhammad Gustafi,

This email is to confirm that we received your manuscript submission, "Audio Forensic on Smartphone with Digital Forensic Research Workshop Method (DFRWS)." Your manuscript will be evaluated by the journal's editor(s) and you will be advised as soon as possible through email of its status, as well as any revisions that may be necessary. Your manuscript can be managed from the Manuscripts page: https://www.igi-global.com/submission/manuscripts/. Please bookmark this page for easy access.

If you have any questions, please contact the journal editor, Rocci Luppicini, at rluppici@uottawa.ca.

If you need to contact IGI Global regarding your submission, please include the journal name and/or acronym and the title of your article in the subject line of all correspondence. This will ensure your correspondence reaches the correct Development Editor at IGI Global and will result in a much quicker response.

Thanks again for your submission - we look forward to working with you!

IGI Global
eEditorial Discovery

UNIVERSITAS
AHMAD DAHLAN

Ghufron Muflih <ghufron1807048002@webmail.uad.ac.id>

[RESTI] Submission Acknowledgement

2 pesan

Yuhefizar <ephi.lintau@gmail.com> 10 Oktober 2019 16.15
Kepada: Ghufron Zaida Muflih <ghufron1807048002@webmail.uad.ac.id>

Ghufron Zaida Muflih:

Thank you for submitting the manuscript, "Perbandingan Tools Forensik Pada Layanan Sosial Media Menggunakan Metode Digital Forensic Research Workshop (DFRWS)" to Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi). With the online journal management system that we are using, you will be able to track its progress through the editorial process by logging in to the journal web site:

Submission URL: http://www.jurnal.iaii.or.id/index.php/RESTI/authorDashboard/submission/1313
Username: ghufron3112

If you have any questions, please contact me. Thank you for considering this journal as a venue for your work.

Yuhefizar

Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)

Gmail **Ikhsan Zuhriyanto <ikhzann@gmail.com>**

[JTIIK] Pernyataan Naskah

1 message

Redaksi JTIIK <jtiik@ub.ac.id> Tue, Nov 5, 2019 at 7:23 AM
To: ikhzann Ikhsan zuhriyanto <ikhzann@gmail.com>

ikhzann Ikhsan zuhriyanto:

Terima kasih untuk menyerahkan manuskrip, "FORENSIK MOBILE PADA APLIKASI SOSIAL MEDIA MENGGUNAKAN METODE DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS)" untuk Jurnal Teknologi Informasi dan Ilmu Komputer. Dengan sistem manajemen jurnal online yang digunakan oleh JTIIK, kemajuan naskah dapat dilihat selama proses editorial/review dengan login ke web site jurnal:

URL Manuskrip: http://jtiik.ub.ac.id/index.php/jtiik/author/submission/2669
Nama pengguna Penulis: ikhzann94

Jika mempunyai pertanyaan, silakan hubungi email jtiik@ub.ac.id. Terima kasih untuk mengirimkan naskah ke JTIIK, semoga diterima dan bermanfaat.

Redaksi JTIIK
Jurnal Teknologi Informasi dan Ilmu Komputer

Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)
Fakultas Ilmu Komputer, Universitas Brawijaya, Malang

JURNAL Penelitian Pos & Informatika

Puslitbang Sumber Daya Perangkat dan Penyelenggaraan Pos dan Informatika Badan Litbang SDM Kemkominfo

Show Menu

#292 Summary

Submission

Authors	Imam Riadi, Sunardi Sunardi, Rusydi Umar, Muhammad Noor Fadillah
Title	FORENSIK MOBILE PADA SMARTPHONE ANDROID MENGGUNAKAN METODE DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS)
Original file	292-992-1-SM.DOC 2019-10-10
Supp. files	None ADD A SUPPLEMENTARY FILE
Submitter	Muhammad Noor Fadillah
Date submitted	October 10, 2019 - 09:58 AM
Section	Informatics
Editor	Vidyantina Anandhita
Author comments	Tolong segera direview, terima kasih

Status

Status	In Review
Initiated	2019-10-10
Last modified	2019-10-24