

Terakreditasi SINTA Peringkat 4

Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 28/E/KPT/2019
masa berlaku mulai Vol. 3 No. 1 tahun 2018 s.d Vol. 7 No. 1 tahun 2022

Terbit online pada laman web jurnal:
<http://publishing-widyagama.ac.id/ejournal-v2/index.php/jointecs>



Vol. 6 No. 2 (2021) 63 - 70

JOINTECS

(Journal of Information Technology and Computer Science)

e-ISSN:2541-6448

p-ISSN:2541-3619

Forensics Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice

Sunardi¹, Imam Riadi², Joko Triyanto³

¹Program Studi Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan

²Program Studi Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan

³Program Studi Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan

¹sunardi@mti.uad.ac.id, ²imam.riadi@is.uad.ac.id, ³joko1908048030@webmail.uad.ac.id

Abstract

Technological developments have a positive impact in the form of ease in gathering data and information includes the growth of smartphone users with Android-based. In other side, technology can also cause cybercrime. This study aims to reveal digital evidence in the process of identifying cybercrime activities by using WhatsApp application as communication media. The method for executing digital forensics in this study uses the framework of the National Institute of Justice (NIJ) with the stages of identification, examination, collection, analysis, and reporting. Wondershare Dr Fone is used as tool for analysis and extraction work. This research that are carried out has 100% success in collecting data in the form of photos, videos, contacts, and documents on the smartwatch but unable to read of the chat messenger and call history and unable to restore the lost data.

Keywords: whatsapp; cybercrime; NIJ; smartwatch; forensics.

Abstrak

Perkembangan teknologi memberikan dampak positif berupa kemudahan dalam memperoleh data dan informasi termasuk pesatnya penggunaan *smartphone* berbasis *Android*. Namun disisi lain, penggunaan teknologi juga dapat menimbulkan peluang terjadinya *cybercrime*. Penelitian ini bertujuan untuk mengungkap barang bukti digital dalam identifikasi kejahatan yang menggunakan aplikasi *WhatsApp* pada *Smartwatch* sebagai media komunikasi. Metode dalam mengeksekusi forensik digital pada penelitian ini memakai kerangka kerja *National Institute of Justice (NIJ)* dengan tahapan *identification, examination, collection, analysis, dan reporting*. *Tools* yang dipakai yaitu *Wondershare Dr Fone* untuk analisis dan ekstraksi. Penelitian ini mendapatkan keberhasilan 100% dalam mengumpulkan data berupa *photos, videos, contacts, dan documents* yang ada pada *Smartwatch*. Namun demikian tidak dapat membaca pada *chatt messenger* dan *call history* serta tidak bisa mengembalikan data yang telah hilang.

Kata Kunci: *whatsapp; cybercrime; NIJ; smartwatch; forensik.*

© 2021 Jurnal JOINTECS

1. Pendahuluan

Jumlah pengguna teknologi informasi yang paham media digital atau *digital savy* selalu mengalami perkembangan. Media digital adalah perkembangan teknologi informasi yang sangat penting untuk kehidupan masyarakat secara individu maupun organisasi [1]. Salah satu media digital yang berkembang di dunia termasuk Indonesia saat ini adalah *smartwatch* atau jam tangan pintar. Konsumen internet yang menggunakan piranti *smartwatch* mengalami pertumbuhan secara global. Sebagian besar pengguna merupakan usia produktif.

Smartwatch semakin populer sebagai alternatif *gadget* (gawai) pendamping ponsel. Ada banyak argumen yang mendorong popularitasnya, alasan paling mendasar yaitu fungsionalitasnya terkait kemudahan yang ditawarkan [2]. *Smartwatch* memiliki banyak fitur yang berguna, mulai dari notifikasi hingga navigasi peta digital. *Smartwatch* menjadi salah satu perangkat *wearable* yang populer dengan banyak produsen *smartphone* besar seperti Samsung dan Apple merilis *smartwatch* [3].

Smartwatch membawa dampak terhadap produk *wearable* lainnya seperti *fitness tracker* yang popularitasnya menurun karena fungsi utamanya kini menjadi salah satu fitur pada produk *smartwatch*. Perusahaan riset *CCS Insight* menyebutkan penjualan *fitness tracker* menurun hingga 23% di 2017, bertolak belakang dengan angka penjualan *smartwatch* yang meroket pada saat yang sama. Lembaga riset lainnya, Statista, bahkan memproyeksikan bahwa pertumbuhan angka penjualan *smartwatch* nyaris selalu meningkat setiap tahunnya yaitu mencapai dua kali lipat lebih, sejak tahun 2014 sampai terkini.

Pemakai *smartwatch* semakin meningkat terutama pada *android* karena banyak fitur yang bermanfaat. Bahkan *smartwatch* juga dilengkapi fitur-fitur yang hampir sama dengan yang ada pada *smartphone* seperti aplikasi *instant messaging* yang banyak manfaatnya. Aplikasi tersebut adalah *WhatsApp* (WA), *Facebook*, *Twitter*, dan lain sebagainya. Di sisi lain, aplikasi *instant messaging* membuka peluang untuk meningkatnya tindakan *cybercrime* atau kejahatan siber. *Cybercrime* muncul seiring dengan perkembangan teknologi informasi yang begitu cepat. *Cybercrime* memanfaatkan teknologi informasi berupa internet sebagai mediana [4]. Pidana internet/komputer adalah tindakan kriminal yang bukti kegiatan kriminalnya perlu diselidiki agar menjadi bahan data [5]. Tindak pidana *cybercrime* telah di atur dalam Undang-Undang nomor 19 tahun 2016 [6].

Salah satu aplikasi *instant messaging* yang berpeluang untuk tindak kejahatan adalah WA. Aplikasi WA menjadi aplikasi yang terbanyak dipakai oleh berbagai

macam komunitas atau kelompok pada masyarakat di Indonesia, tidak luput juga oleh para ilmuwan dan para akademisi dari perguruan tinggi [7]. Kasus kejahatan dan bukti digital pada WA perlu diteliti atau diidentifikasi dengan melakukan analisis forensik menggunakan *tools* dan metode [8]. Beberapa *tools* yang dapat digunakan untuk mendapatkan bukti digital diantaranya *Wondershare Dr. Fone*, *MobilEdit*, *Oxygen Forensics*, *Belkasoft*, dan *Metsploit*. Penelitian ini menggunakan *tool Wondershare Dr. Fone*.

Selanjutnya, dalam melakukan analisis forensik juga dibutuhkan metode atau kerangka kerja agar bisa ditemukan barang bukti. Kerangka kerja yang dapat digunakan dalam proses pengambilan barang bukti digital diantaranya adalah *Integrated Digital Forensics Identification Framework* (IDFIF), *National Institute of Standards and Technology* (NIST), *National Institute of Justice* (NIJ), dan *Digital Forensics Research Workshop* (DFRWS). Masing-masing metode memiliki proses dan langkah kerja yang berbeda. Penelitian ini menggunakan metode NIJ sebagai kerangka kerja untuk membantu *investigator* dalam melakukan *digital forensics*.

Proses pengambilan barang bukti ini menggunakan metode NIJ karena memiliki tahapan yang lebih baik dibandingkan dengan metode lainnya. NIJ digunakan agar memperoleh atau mendapatkan bukti menurut keilmuan terhadap perawatan, validasi analisis, pengumpulan, identifikasi, dokumentasi, interpretasi, dan presentasi barang bukti dari sumber-sumber digital untuk melanjutkan atau memfasilitasi rekonstruksi kasus didapatkannya kriminalitas dan mendukung mengantisipasi berbagai macam perbuatan yang tidak sah mengindikasikan adanya proses yang diagendakan untuk mengganggu [9]. Pengangkatan data dan *file* dapat menggunakan *tools* yang sering digunakan dalam investigasi untuk mengekstrak sebagian besar informasi dengan cara yang efisien [10].

Teknologi informasi dan komunikasi di era globalisasi telah mengalami perkembangan yang sedemikian pesat. Hal tersebut disertai akibat bertambahnya pemakaian media sosial guna memperoleh data dengan mudah dan cepat. Media sosial merupakan salah satu media yang berkembang paling pesat [11]. Para pengguna lebih mudah berperan serta, membagikan, dan membuat konten berupa website, blog, dunia virtual, dan forum. Media sosial bisa menjadi inovasi perkembangan pembelajaran pada pendidikan dasar di Indonesia [12]. Terkait masyarakat dan negara, media sosial mengeratkan hubungan silaturahmi antara satu sama lain [13], memudahkan masyarakat agar berkomunikasi dengan orang banyak, memperbanyak pertemanan, waktu dan jarak sudah bukan masalah, mengekspresikan diri lebih mudah, penyiaran berita bisa lebih cepat, dan biayanya murah. Akibat buruk media sosial ialah menurunnya tatap muka, orang-orang yang sudah dekat

semakin jauh, internet yang membuat kecanduan banyak orang, semakin meningkatnya konflik dan masalah, mudah mengikuti perilaku buruk orang, dan menyebarnya privasi [14].

Aplikasi pesan *instant messaging* paling populer ialah WA (97,24%), LINE (88,49%), BBM (85,82%), Facebook (77,26%), dan Telegram (0,75%). Perkembangan ini memberikan kemudahan dalam kehidupan manusia. Namun terdapat hal-hal yang harus diperhatikan dalam pemanfaatannya, yaitu penyalahgunaan hak-hak atas privasi seperti tindakan kejahatan *cyber*. Dalam praktiknya, tindakan *cybercrime* dilakukan dengan cara yang dianggap ilegal oleh masyarakat, seperti melakukan penyadapan informasi dan pencurian data pribadi yang belakangan hal ini mendapatkan perhatian khusus oleh masyarakat internasional [15]. Penelitian ini memilih objek aplikasi pada WA dikarenakan termasuk aplikasi yang banyak digunakan masyarakat yaitu sebesar 97,24%. Penelitian bermaksud untuk menganalisis metode penyelidikan *cybercrime* serta menampilkan barang bukti yang telah terjadi pada WA.

Penelitian ini melakukan analisis forensik WA pada *smartwatch* dengan memakai pengembangan metode *digital forensics*. *Digital forensics* yaitu tindakan mendapatkan, menghasilkan, melestarikan, mengambil, serta memperlihatkan berbagai data yang sesuai dengan langkah kerja *forensics* dan *forensic tools* [16]. Ada *forensics tools* yang dapat digunakan untuk menjalankan investigasi diantaranya *Wondershare Dr. Fone*, *MobilEdit*, *Oxygen Forensics* dan sebagainya. *Tool forensics Wondershare Dr. Fone* memiliki kelebihan diantaranya mudah dan cepat dalam menjalankan investigasi *forensics* data atau *file* yang ada pada android.

Berdasarkan latar belakang diatas, penelitian ini bertujuan melakukan analisis *forensics* WA pada *smartwatch* berbasis *android* menggunakan kerangka kerja NIJ. Metode NIJ adalah salah satu kerangka kerja yang mempunyai kelebihan dalam proses *forensics*. Penelitian fokus pada ada atau tidak adanya data *Photo*, *Video*, *Contact*, dan *Document* pada *smartwatch* menggunakan *tool Wondershare Dr. Fone* untuk mengangkat barang bukti agar dapat ditampilkan dan dijadikan barang bukti digital dari tindak kejahatan berbasis digital dan *cybercrime* lainnya.

2. Metode Penelitian

Objek penelitian berasal dari sifat manusia atau aktivitas yang mempunyai corak atau ragam tertentu untuk dipermanenkan dalam penelitian agar dapat dipahami dan kemudian diambil kesimpulan [17]. Objek penelitian ini adalah data dari aplikasi WA pada perangkat *smartwatch* android. Parameter bukti potensial dari NIJ dipakai untuk mengukur kemampuan

tool forensics dan parameter simulasi perlu disesuaikan dengan simulasi kasus [18]. Simulasi ini mengangkat kasus tindakan mencontek saat ujian tertulis seleksi karyawan yang berlangsung didalam suatu perusahaan. Pengecekan yang dijalankan dalam perusahaan tersebut menghasilkan barang bukti berupa *smartwatch* dari peserta ujian. Barang bukti digital tersebut diamankan petugas yang berwajib. Bukti potensial terkait *forensics* WA pada *Smartwatch* ialah identifikasi berupa foto, video, dan dokumen.

Skenario Aktivitas harus dijalankan agar mendapatkan barang bukti digital [19]. Penelitian ini membuat skenario rekayasa komprehensif dari kegiatan yang dijalankan di fitur WA pada *smartwatch* seperti dapat dilihat pada Gambar 1. Tujuan diadakannya skenario ini adalah untuk mempermudah investigasi dari kasus mencontek tersebut. Skenario tersebut sebagai berikut: pertama, tersangka (Akun A) membuat akun WA pada *smartwatch*, selanjutnya kedua, tersangka (Akun A) mendapat kesempatan dan menjadi peserta tes tertulis calon karyawan perusahaan. Ketiga, tersangka (Akun A) menyimpan data berupa foto, video dan dokumen pada WA, selanjutnya tersangka meminta bantuan rekannya yang berada diluar (Akun B), untuk mengirim jawaban melalui WA. terakhir tersangka (Akun A), menuliskan jawaban pada lembar jawab.



Gambar 1. Skenario Aktivitas

The Chain of custody adalah tahapan yang dijalankan *investigator* dalam melindungi bukti digital. Salah satu bukti digital yaitu berupa data atau dokumen WA pada *smartwatch*. Data yang disimpan dari WA akan dibedah dari piranti atau perangkat aktor menggunakan *tools*. Skenario investigasi dapat dilihat pada Gambar 2.



Gambar 2. Skenario Investigasi

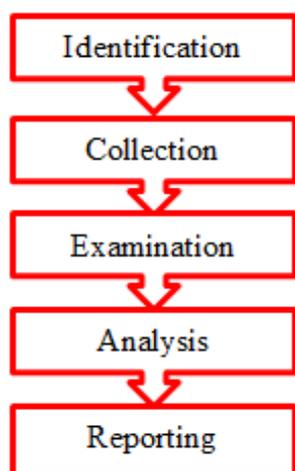
Penelitian ini memerlukan *hardware* dan *software* dalam proses analisis *forensics*. *Hardware* yang digunakan yaitu laptop Acer *dualboot* dan *Smartwatch* ZC01. *Software* yang digunakan yaitu *tools* Kingroot dan *Wondershare Dr Fone*. Alat dan bahan yang digunakan dalam *forensics* ini dapat dilihat pada Tabel 1.

Tabel 1 Alat dan Bahan

No	Alat dan Bahan	Spesifikasi	Keterangan
1	Laptop	Acer, <i>dualboot</i>	<i>Hardware</i>
2	<i>Smartwatch</i>	ZC01	<i>Hardware</i>
3	Kingroot	Melakukan <i>rooting</i>	<i>Software</i>
4	Wondershare Dr. Fone	<i>Tool forensics</i>	<i>Software</i>

2.1. Perancangan Sistem

Perancangan sistem pada penelitian ini mengimplementasikan kerangka kerja NIJ seperti pada Gambar 3. Kerangka kerja ini untuk menjelaskan tahapan pengkajian. Tahapan Pengkajian atau penelitian yang akan dijalankan sehingga bisa diketahui langkah-langkah dan alur penelitian secara terstruktur untuk dijadikan pedoman menyelesaikan masalah.



Gambar 3. Metode National Institute of Justice (NIJ)

Kerangka kerja NIJ memiliki lima tahapan yaitu *identification*, *collection*, *examination*, *analysis*, dan *reporting*. Setiap tahapan berkaitan dengan tahapan

lainnya yang teratur sehingga menghasilkan penelitian yang lebih baik. Tahapan-tahapan tersebut dijelaskan lebih lengkap sebagai berikut:

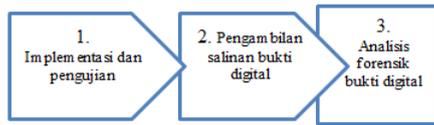
Identifikasi (*identification*) adalah kegiatan pemilihan data dan pemilahan barang bukti tindakan kejahatan digital untuk mendukung jalannya penyelidikan dalam rangka mencari bukti digital tindak kejahatan digital. Tahapan ini terdapat proses pelabelan, identifikasi, dan perekaman untuk keamanan barang bukti secara utuh. Pada tahapan ini diambil barang bukti yang ada.

Pengumpulan (*collection*) yaitu serangkaian agenda menghimpun data untuk mendorong proses penyidikan dalam rangka mencari bukti digital dari kejahatan. Tahapan ini terdapat proses pengumpulan data dari sumber data yang akurat serta menjaga integritas barang bukti digital dari perubahan. Pengumpulan yang dilakukan adalah dengan studi kasus, eksperimen dan observasi. Data asli yang digunakan dalam penelitian ini yaitu *photo* sebanyak 71, video sebanyak 2, *contact* sebanyak 4, *document* sebanyak 2, *call history* sebanyak 5, *chat messenger* sebanyak 30.

Pemeriksaan (*examination*), yaitu tahap pemeriksaan data yang dikumpulkan secara *forensics* dan secara manual ataupun otomatis, dan menjamin agar data yang telah diambil berupa *file digital* tersebut asli sama dengan yang didapat ditempat kejadian sehingga *digital file* perlu dilakukan validasi dan identifikasi file dengan teknik *hashing*. Teknik *hashing* merupakan fungsi yang mengkonversi setiap string menjadi bilangan [20]. Pemeriksaan ini dapat menjadi petunjuk kebenaran atau kesalahan suatu barang bukti.

Analisis (*analysis*) dijalankan setelah menghasilkan data digital dan *file* yang dicari dari proses pemeriksaan sebelumnya. Data tersebut selanjutnya dianalisis secara komprehensif dan detail menggunakan metode yang akurat secara hukum dan teknik atau cara untuk membuktikan data tersebut. Hasil dari analisis terhadap data digital selanjutnya dipakai sebagai bukti digital dan bisa dipertanggungjawabkan secara hukum dan secara ilmiah

Pelaporan (*reporting*) dijalankan setelah didapat barang bukti digital dari proses analisis dan pemeriksaan. Tahapan ini dijalankan pelaporan hasil analisis yang terdiri dari pemaparan tentang *tool*, penggambaran tindak kejahatan yang dilakukan, metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi dalam perbaikan kebijakan, *tool*, metode atau aspek pendukung lainnya pada proses tindakan *forensics* digital. Tahapan pengkajian yang dilalui pada penelitian ini mengacu pada lima tahapan dari NIJ dan langkah-langkah dari penulisan ini terdiri dari tiga tahapan utama yaitu implementasi dan pengujian, pengambilan salinan bukti digital dan analisis *forensics* bukti digital. Tahapan penelitian tersebut dapat dilihat pada Gambar 4.



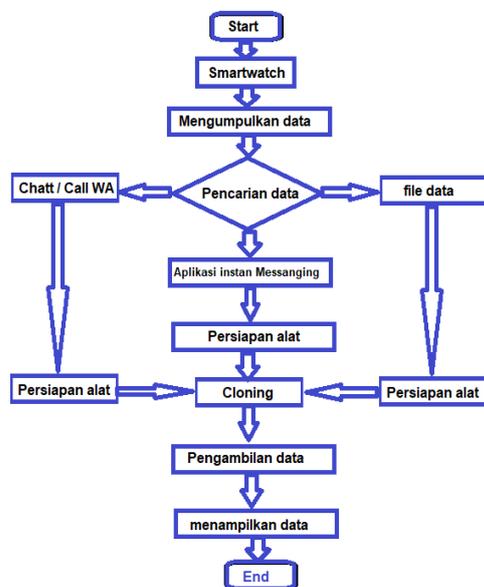
Gambar 4. Tahapan Penelitian

2.2. Pengujian Sistem

Maksud dan tujuan pengujian sistem ialah agar dapat mengetahui apakah sistem yang dijalankan sudah layak dipakai dan sesuai dengan tujuan awal pembuatan [21]. Proses ini dikerjakan menggunakan skenario yang telah ditetapkan pada langkah sebelumnya. Pengujian sistem dilakukan sesuai parameter berupa bukti potensial terkait *forensics* WA pada *smartwatch*. Sebelum pengujian sistem dilakukan, dijalankan beberapa persiapan seperti *rooting* piranti *smartwatch* dengan *tool kingroot*, pemasangan aplikasi atau *tool Wondershare Dr. Fone*, instalasi WA, dan pemasangan aplikasi *database* lainnya.

Kriteria keberhasilan dapat dilihat dari kemunculan atau terangkatnya bukti digital dari WA pada *smartwatch*. Analisis hasil digital diambil dari bukti digital yang telah diakuisisi oleh *tool forensics Wondershare Dr. Fone*. Analisis ini meliputi analisis *photos*, *videos*, dan *documents* pada aplikasi WA pada *smartwatch* yang dianggap sebagai bukti potensial.

Bukti digital yang dipakai pada penelitian ini tidak dihasilkan pada kondisi yang sebenarnya atau barang bukti tidak dihasilkan dari tindak *cyber* yang sebenarnya, melainkan bukti digital diciptakan dan didapat dari hasil skenario. Untuk mendapatkan bukti digital dari skenario perlu dibuatkan *flowchat* tahapan pengujian dan implementasi secara sistematis sesuai metode NIJ. Tahap pengujian dan implementasi analisis *forensics* digital WA pada *smartwatch* ditunjukkan pada Gambar 5.



Gambar 5. Implementasi dan Pengujian

3. Hasil dan Pembahasan

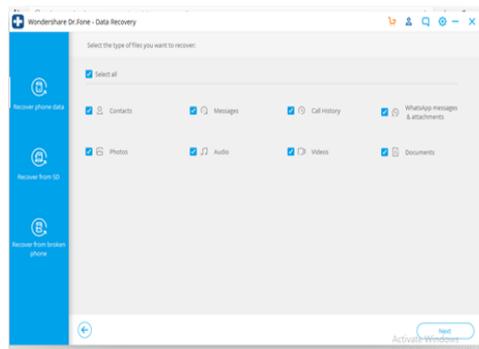
Penelitian ini merupakan hasil dari uji coba pada pengembangan metode yang telah dibuat. Penelitian pertama yang dikerjakan adalah menjalankan identifikasi masalah yang telah terjadi dan mengumpulkan informasi tentang data yang akan dicari. Tahapan kemudian mencari dan mengumpulkan solusi yang akan dikerjakan dalam mengumpulkan bukti-bukti digital yang ada di WA pada *Smartwatch*. Selanjutnya mempersiapkan alat dan bahan yang akan digunakan dalam mengumpulkan bukti-bukti. Secara lebih detil hasil dan pembahasan yang didapatkan dalam penelitian ini diuraikan berikut.

Tampilan awal *tool Wondershare Dr. Fone* dapat dilihat pada Gambar 6. *Tool* ini merupakan *software recovery* yang dipakai khusus untuk mengangkat data atau bukti digital. Pengangkatan data bukti digital pada Android dengan *tool* ini dapat dilakukan dengan mudah dan cepat.



Gambar 6. Wondershare Dr. Fone

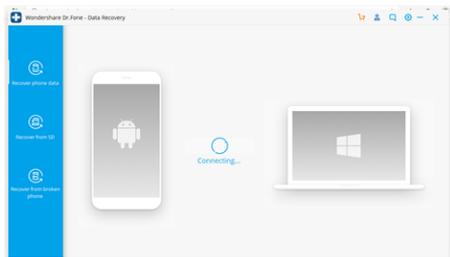
Tool ini memiliki banyak menu pilihan seperti pada Gambar 7. Beberapa macam data dan *file* yang dapat ditampilkan, dianalisis, diangkat, dan dikembalikan menggunakan *Wondershare Dr.Fone* diantaranya adalah *contacts*, *message*, *call history*, *WA*, *photos*, *audios*, *videos*, dan *documents*. Pada menu ini ditentukan pilihan yang akan di angkat sebagai barang bukti. Menu pilihan pada tahap ini adalah *WhatsApp*.



Gambar 7. Menu Pilihan

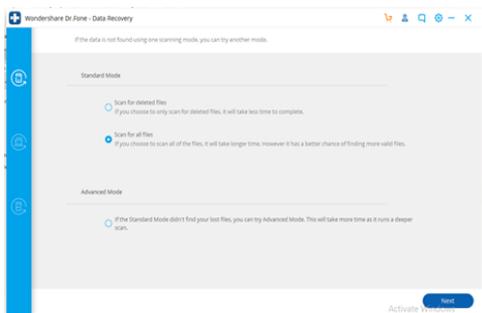
Koneksi *smartwatch* dapat dilihat pada Gambar 8. Koneksi perangkat ini adalah proses menghubungkan barang bukti di dalam *smartwatch* dengan laptop atau *Personal Computer (PC)*. Proses menghubungkan

barang bukti ini memerlukan waktu yang cukup lama, hal ini dipengaruhi oleh besar dan kecilnya kapasitas pada *smartwatch* maupun laptop yang dipakai. Tahapan ini dilakukan proses pengambilan dan deteksi data yang ditemukan pada barang bukti.



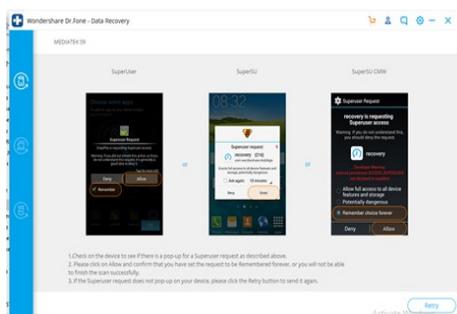
Gambar 8 Koneksi dengan *Smartwatch*

Scan recovery dengan *Smartwatch* dapat dilihat pada Gambar 9. Tahapan ini merupakan pemilihan data apa saja yang akan diangkat dalam proses forensik. Data yang diangkat yaitu semua file yang ada pada *smartwatch*. Pada menu terdapat dua pilihan yaitu *scan for deleted files* dan *scan for all files*. Berdasarkan data yang diangkat adalah semua file maka pilih menu *scan for all files*. Pada menu ini menjadi salah satu langkah dalam melanjutkan proses penelitian selanjutnya.



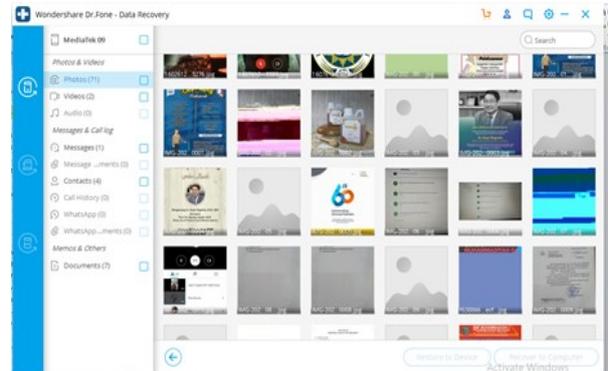
Gambar 9. *Scan Recovery*

Petunjuk USB *debugging* dapat dilihat pada Gambar 10. *Tool* ini mudah digunakan untuk mendapatkan informasi yang ada pada barang bukti. Tahap ini merupakan proses mendeteksi bug atau potensial *error* untuk kode yang bisa menyebabkan sistem tidak dapat berfungsi dengan baik. Pada menu ini akan dilakukan proses *recovery* data dan menampilkan *software* yang akan diangkat sebagai barang bukti. Tahap proses *debugging* memerlukan waktu yang cukup lama untuk mengecek atau deteksi potensi *error*.



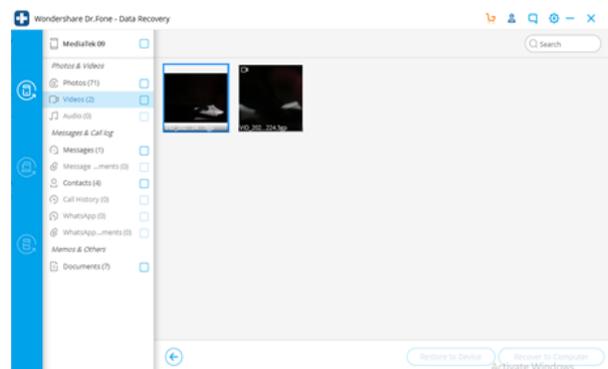
Gambar 10. Petunjuk USB Debugging

Hasil *Photos* dapat dilihat pada Gambar 11. Pengangkatan barang bukti foto menghasilkan 71 gambar. Rincian gambar yang ditampilkan yaitu 64 gambar terbaca dan 7 gambar tersembunyi atau telah dihapus. Tersembunyinya 7 gambar ini memperlihatkan bahwa *tools Wondershare Dr. Fone* hanya dapat menampilkan data berupa gambar yang belum terhapus.



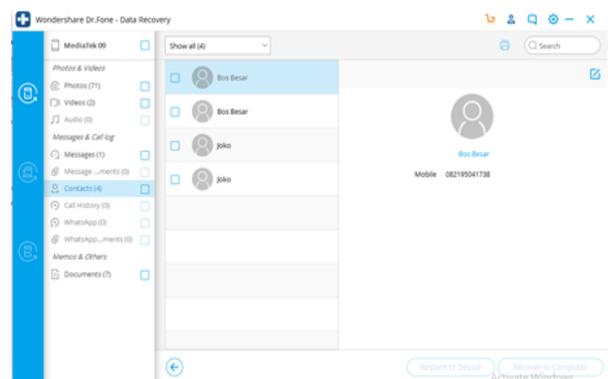
Gambar 11. Hasil Photo

Simulasi proses pengangkatan barang bukti ini hanya menampilkan video pada *smartwatch*. Hasil Video dapat dilihat pada Gambar 12. Pengangkatan barang bukti foto menghasilkan dua video.



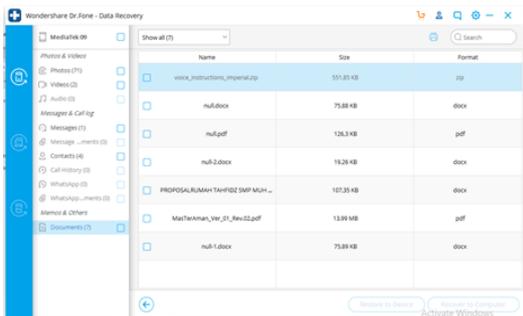
Gambar 12 Hasil Video

Hasil *contacts* dapat dilihat pada Gambar 13. Pengangkatan barang bukti foto menghasilkan 4 kontak dengan rincian dua nama Bos Besar dan dua nama Joko. Hal ini menunjukkan bahwa hasil forensik sesuai dengan nomer yang tersimpan pada *smartwatch*.



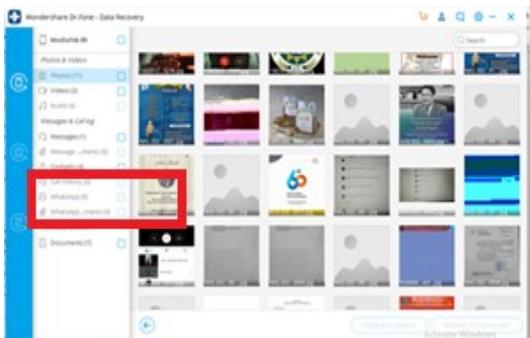
Gambar 13 Hasil *Contacts*

Hasil *document* dapat dilihat pada Gambar 14. Pengangkatan barang bukti *document* menghasilkan tujuh dokumen yang semuanya masih valid. Nama *document* sesuai yang ada di WA pada *smartwatch*. Format *document* yang tampil yaitu *zip*, *docx*, dan *pdf*.



Gambar 14. Hasil Documents

Hasil *call history* dan *chat messenger* dapat dilihat pada Gambar 15. Pada tahap pengangkatan barang bukti *call history* dan *chat messenger* tidak dapat dibuka dan terbaca serta tidak bisa mengembalikan data yang telah hilang. Hal ini menjadi salah satu kekurangan *tools forensics Wondershare Dr. Fone*.



Gambar 15. Hasil *call history* dan *chat messenger*

Tabel 2. Hasil forensik

Data	Photo	Video	Call history	Chat messenger	Contact	Document
Asli	71	2	5	30	4	7
Hasil	71	2	0	0	4	7
Persentase	100%	100%	0%	0%	100%	100%

Berdasarkan data pada Tabel 2 menggunakan *Wondershare Dr. Fone*, yaitu data asli *photo* pada *smartwatch* sebanyak 71 mendapatkan hasil *forensics file photo* sebanyak 71 dengan persentase keberhasilan sebesar 100%. Data asli *video* pada *smartwatch* sebanyak 2 menghasilkan *forensics file video* sebanyak 2 dengan persentase keberhasilan sebesar 100%. Data asli *contact* pada *smartwatch* sebanyak 4 menghasilkan *file contact* sebanyak 4 dengan persentase keberhasilan 100% dan juga untuk 2 data asli *document* pada *smartwatch* mendapatkan hasil *forensics file document* sebanyak 2 dengan persentase keberhasilan sebesar 100%. Sedangkan data *call history* pada *smartwatch* sebanyak 5 hasil *forensics file call history* sebanyak 0

dengan persentase keberhasilan sebesar 0%. Begitupun untuk 30 data asli *chat messenger* pada *smartwatch* mendapatkan hasil 0 atau tidak ditemukan *file chat messenger* dengan persentase keberhasilan sebesar 0%. Setelah dilakukan *forensics* beberapa kali, hasil dari pengangkatan data *call history* dan *chat messenger* tetap 0%, ini disebabkan oleh kelemahan tool *forensics Wondershare Dr. Fone* karena hanya mempunyai konektivitas menggunakan kabel data saja. Pengambilan data tidak dapat menggunakan *wireless* dan hanya bisa menggunakan kabel data untuk konektivitasnya.

Tabel 3. Perbandingan Durasi

Durasi	Photo	Video	Call history	Chat messenger	Contact	Document
Menit	9	8	3	11	2	8

Berdasarkan data pada Tabel 3 perbandingan durasi yang diperlukan membutuhkan waktu yang berbeda-beda. Durasi yang dibutuhkan untuk memproses *photo* yaitu 9 menit. Durasi yang dibutuhkan untuk memproses *video* yaitu 8 menit. Durasi yang di perlukan untuk memproses *call history* yaitu 3 menit. Durasi yang di perlukan untuk memproses *chat messenger* yaitu 11 menit. Durasi yang diperlukan untuk memproses *contact* yaitu 2 menit. Durasi yang diperlukan untuk memproses *document* yaitu 9 menit. Dari data tersebut dapat dilihat bahwa durasi paling lama yaitu memproses *chat messenger* dan durasi paling cepat yaitu memproses *contact*. Perbedaan durasi dalam proses ini disebabkan oleh ukuran data yang berbeda-beda.

4. Kesimpulan

Analisis *forensics WA* dan uji coba menggunakan tool *Wondershare Dr. Fone* pada *Smartwatch* dapat disimpulkan bahwa teknik yang dijalankan berdasarkan Metode *National Institute of Justice* dengan beberapa tahap yaitu identifikasi, pengumpulan data, pengujian, analisis dan pelaporan ini mempunyai tingkat keberhasilan 100% untuk mengumpulkan data berupa *photos*, *videos*, *contacts*, dan *documents* yang ada pada *smartwatch*. Berdasarkan hasil uji coba dan analisis *forensics* menggunakan *Wondershare Dr. Fone* ditemukan kekurangan dari tool tersebut, yaitu tidak dapat membaca *call history* dan *chat messenger* dengan persentase 0%. Selain itu tidak bisa mengembalikan data yang telah hilang. *Wondershare Dr. Fone* tidak dapat mengambil data menggunakan *Wireless* melainkan hanya dapat menggunakan kabel data untuk konektivitasnya.

Daftar Pustaka

[1] A. Wiraniagara and F. Wijaya, “Analisis Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Domain Deliver Support And Service (Studi Kasus : Yayasan Eka Tjipta

- , Jakarta),” *J. Sebatik*, vol. 23, no. 2, pp. 663–671, 2019, [Online]. Available: <https://jurnal.wicida.ac.id/index.php/sebatik/article/view/831>.
- [2] R. A. Putra, A. Fadlil, and I. Riadi, “Forensik Mobil Pada Smartwath Berbasis Android,” *J. Rekayasa dan Teknol.*, vol. 1, no. 1, pp. 41–47, 2017, doi: <http://dx.doi.org/10.30872/jurti.v1i1.638>.
- [3] D. Lorinso and Irwansyah, “Penggunaan Wearable Internet of Things (WIoT) oleh Kaum Milenial,” *J. Ilmu Komun. Source*, vol. 6, no. 2, pp. 190–205, 2020, doi: <https://doi.org/10.35308/source.v6i2.1861>.
- [4] D. Setiawan, “Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Terhadap Budaya,” *J. Simbolika*, vol. 4, no. 1, pp. 62–72, 2018, doi: <https://doi.org/10.31289/simbollika.v4i1.1474>.
- [5] I. Riadi, Sunardi, and P. Widiandana, “Investigating Cyberbullying on Whatsapp Using Digital Forensics Research Workshop,” *Resti*, vol. 4 No 4, pp. 730–735, 2020.
- [6] I. G. A. S. K. Singgi, I. G. B. Suryawan, and I. N. G. Sugiarta, “Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime),” *J. Konstr. Huk.*, vol. 1, no. 2, pp. 334–339, 2020, doi: [10.22225/jkh.2.1.2553.334-339](https://doi.org/10.22225/jkh.2.1.2553.334-339).
- [7] K. Sukrillah, Ratnamulyani, “Pemanfaatan Media Sosial Melalui Whatsapp Group Fei Sebagai Sarana Komunikasi,” *Komunikatio*, vol. 3, 2017.
- [8] M. S. Ahmad, I. Riadi, and Y. Prayudi, “Investigasi Live Forensik dari Sisi Pengguna Untuk Menganalisa Serangan Man in The Midle Attactk Berbasis Evil Twin,” *Ilkom*, vol. 9 no 1, pp. 1–8.
- [9] I. Riadi, Sunardi, and Sahirudin, “Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ),” *J. Rekayasa Teknol. Jurti*, vol. 3, no. 1, pp. 87–95, 2019, doi: <http://dx.doi.org/10.30872/jurti.v3i1.2292>.
- [10] I. Riadi, R. Umar, and A. Firdonsyah, “Forensic Tools Performance Analysis on Android-based Blackberry Messenger using NIST Measurements,” *Int. J. Elektricial Comput. Enginering IJECE*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: [10.11591/ijece.v8i5.pp3991-4003](https://doi.org/10.11591/ijece.v8i5.pp3991-4003).
- [11] F. Anwar, “Perubahan dan Permasalahan Media Sosial,” *J. Muara Ilmu Sos. Humaniora, dan Seni*, vol. 1, no. 1, pp. 137–144, 2017, doi: <http://dx.doi.org/10.24912/jmishumsen.v1i1.343>.
- [12] S. Fitri, “Dampak Positif Dan Negatif Sosial Mediaterhadap Perubahan Sosial Anak,” *J. Nat.*, vol. 1, no. 2, pp. 118–123, 2017, doi: <https://doi.org/10.35568/naturalistic.v1i2.5>.
- [13] C. S. B. Mustaffa and nan Z. M. Ibrahim, “Persepsi dan Penggunaan Media Sosial dari Perspektif Ibu Bapa: Satu Analisis Kualitatif,” *J. Komun. Malaysian J. Comun.*, vol. 30, no. 4, pp. 43–47, 2014, doi: <https://doi.org/10.17576/JKMJC-2014-30SI-04>.
- [14] A. S. Cahyono, “Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat di Indonesia,” *J. Publiciana Univ. Tulungagung*, vol. 9, no. 1, pp. 140–157, 2016.
- [15] Suherman, P. Widodo, and D. Gunawan, “Efektivitas Keamanan Informasi dalam Menghadapi Ancaman Social Engineering,” *J. Peperangan Asimetris*, vol. 3, no. 1, pp. 73–89, 2017, [Online]. Available: <http://jurnalprodi.idu.ac.id/index.php/PA/article/view/94/78>.
- [16] Sunardi, I. Riadi, and I. M. Nasrulloh, “Analisis Forensik Solid State Drive (SSD) Menggunakan Framework Rapid Response,” *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 5, p. 509, 2019, doi: [10.25126/jtiik.2019651516](https://doi.org/10.25126/jtiik.2019651516).
- [17] N. Ridha, “Proses Penelitian, Masalah, Variabel dan Paradigma Penelitian,” *J. Hikmah*, vol. 14, no. 1, pp. 62–69, 2017, [Online]. Available: <http://jurnalhikmah.staisumatera-medan.ac.id/index.php/hikmah/article/view/18>.
- [18] I. Riadi, A. Fadlil, and T. Sari, “Image Forensic For Detecting Splicing Image With Distance Function,” *Int. J. Comput. Appl.*, vol. 169, no. 5, pp. 6–10, 2017, doi: [10.5120/ijca2017914729](https://doi.org/10.5120/ijca2017914729).
- [19] A. Fauzan, I. Riadi, and A. Fadlil, “Analisis Forensik Digital Pada Line Messenger untuk Penanganan Cybercrime,” *J. Ilk. Unsri*, vol. 2, no. 1, pp. 159–163, 2016.
- [20] N. Alamsyah, “Perbandingan Algoritma Winnowing Dengan Algoritma Rabin Karp Untuk Mendeteksi Plagiarisme Pada Kemiripan Teks Judul Skripsi,” *J. Technol.*, vol. 8, no. 3, pp. 124–134, 2017, doi: [10.31602/tji.v8i3.1116](https://doi.org/10.31602/tji.v8i3.1116).
- [21] U. Hanifah, R. Alit, and Sugiarto, “Penggunaan Metode Black Box pada Pengujian Sistem Informasi Surat Keluar Masuk,” *J. Scan Teknol. Inf. dan Komun.*, vol. 11, no. 2, pp. 33–40, 2016, [Online]. Available: <http://ejournal.upnjatim.ac.id/index.php/scan/article/view/643/517>.