Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 4 No. 4 (2020) 682 - 690 ISSN Media Elektronik: 2580-0760

Analisis *Recovery* Bukti Digital Skype berbasis *Smartphone Android* Menggunakan *Framework* NIST

Anton Yudhana[1], Abdul Fadlil[2], Muhammad Rizki Setyawan[3]
[1,2] Program Studi Teknik Electro, Universitas Ahmad Dahlan
[3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan
[1]eyudhana@ee.uad.ac.id, [2]fadlil@mti.uad.ac.id, [3]muhammad1808048027@webmail.uad.ac.id

Abstract

Cybercrime is an activity utilizing electronic devices and network technology as tools or media to commit crimes. One of them uses the Skype application that is installed on the smartphone. In finding evidence from a cybercrime case, a forensic activity known as digital forensic must be carried out. This study aims to recover digital evidence that has been erased using the NIST framework and forensic tools such as Oxygen and Belkasoft. The results of digital evidence recovery from smartphone Samsung J2 in the removal scenario via the application manager, the Oxygen tool cannot recover deleted data and the percentage of success using Belkasoft is 26%. While the results of data recovery with the manual removal method the percentage of success using Oxygen was 63% and Belkasoft was 44%. Digital evidence recovery results from smartphones Andromax A on the erase scenario through the application manager, Oxygen and Belkasoft tools cannot recover deleted data. While manual removal of Oxygen by 61% and Belkasoft cannot restore data. It can be concluded the results of data recovery from both smartphones that are used according to the erasure method through the application manager, Belkasoft has better performance than Oxygen, and data recovery according to the method of erasing manually, Oxygen has better performance than Belkasoft.

Keywords: Cybercrime, Digital Forensics, Recovery, Skype, NIST

Abstrak

Cybercrime merupakan aktivitas memanfaatkan perangkat elektronik dan teknologi jaringan sebagai alat atau media untuk melakukan kejahatan. Salah satunya menggunakan aplikasi Skype yang ter-*install* pada *smartphone*. Dalam menemukan barang bukti dari kasus *cybercrime* perlu dilakukan kegiatan forensik yang dikenal dengan digital forensik. Penelitian ini bertujuan recovery bukti digital yang telah terhapus menggunakan *framework* NIST dan tool forensik berupa Oxygen dan Belkasoft. Hasil *recovery* bukti digital dari *smartphone* samsung J2 pada metode penghapusan melalui aplikasi manager, tool Oxygen tidak dapat mengembalikan data yang terhapus dan prosentase keberhasilan menggunakan belkasoft sebesar 26%. Sedangkan hasil recovery data dengan metode penghapusan secara manual prosentase keberhasilan menggunakan Oxygen sebesar 63% dan Belkasoft sebesar 44%. Hasil *recovery* bukti digital dari *smartphone* Andromax A pada skenario penghapusan melalui aplikasi manager, *tool* Oxygen dan Belkasoft tidak dapat mengembalikan data yang terhapus. Sedangkan penghapusan secara manual Oxygen sebesar 61% dan Belkasoft tidak dapat mengembalikan data. Dapat disimpulkan hasil recovery data dari kedua smartphone yang digunakan sesuai metode penghapusan melalui aplikasi manager, Belkasoft memiliki kinerja lebih baik dari Oxygen, dan recovery data sesuai metode penghapusan secara manual, Oxygen memiliki kinerja lebih baik dari Belkasoft.

Kata kunci: Kejahatan digital, Digital forensik, Recovery, Skype, NIST

1. Pendahuluan

Perkembangan teknologi berupa perangkat seluler saat ini mengalami perkembangan yang sangat pesat. Penggunaan perangkat seluler lambat laun dapat mengganti peran komputer, hal ini disebabkan dengan fitur dan aplikasi yang ada di perangkat smartphone. Instant Messaging (IM) adalah salah satu aplikasi yang paling sering digunakan oleh pengguna perangkat smartphone. IM mulai menggantikan peran Layanan Pesan Singkat (SMS) sebagai media dalam melakukan kegiatan berkomunikasi dan berbagi informasi [1].

Skype merupakan salah satu aplikasi IM yang populer yang digunakan oleh masyarakat dengan jumlah pengguna mencapai 300 juta pada tahun 2019 [2].

Diterima Redaksi : 26-07-2020 | Selesai Revisi : 09-08-2020 | Diterbitkan Online : 20-08-2020

Pengguna Skype yang semakin banyak tidak hanya memberikan dampak positif tetapi juga memberi dampak negatif. Salah satu dampak negatif yang dapat dilakuklan yaitu dengan memanfaatkannya untuk melakukan tindak kejahatan seperti *scamming*, menyebarkan konten illegal, transaksi narkoba, pemerasan dan lainya [3]. Setiap kejahatan yang dilakukan pasti meninggalkan barang bukti. Oleh karena itu dalam proses investigasi kasus *cybercrime* dibutuhkan pemahaman serta keahlian di bidang forensik digital [4].

Mobile forensik merupakan salah satu cabang dari digital forensik yang dilakukan untuk menemukan dan menganalisis barang bukti terkait kasus *cybercrime* agar dapat dipertanggungjawabkan secara hukum [5]. Barang bukti yang ditemukan dapat berupa bukti elektronik maupun bukti digital. Barang bukti elektronik merupakan barang bukti yang dapat dikenali secara fisik seperti perangkat komputer, smartphone maupun media penyimpanan. Sedangkan barang bukti digital merupakan hasil ekstrak atau recovery dari bukti elektronik seperti akun ID, kontak, text percakapan, dokumen, file multimedia (suara / gambar / video), atau file log [6][7]

Dalam melakukan tindakan *cybercrime*, sering kali pelaku mencoba untuk menyembunyikan jejak kejahatan dengan menghapus bukti digital dari perangkat elektronik [8]. Hal ini menjadi tantangan tersendiri bagi penyelidik ketika ingin menemukan bukti digital yang akan digunakan sebagai barang bukti dipersidangan [9]. Oleh karena itu, penyelidik dituntut agar memiliki kemampuan dalam menemukan serta mengembalikan (*recovery*) bukti digital yang telah dihapus [8].

Umumnya terdapat dua metode digunakan pada mobile forensik untuk melakukan ekstrak atau *recovery* data dari perangkat *smartphone* yaitu *logical acquisition* dan *physical acquisition. Logical acquisition* dimana *tool* forensik menggunakan API ini untuk berkomunikasi dengan sistem operasi perangkat *smartphone* dan meminta data dari sistem. Proses ini memungkinkan untuk memperoleh sebagian besar data langsung pada perangkat [10]. *Physical acquisition* sangat mirip dengan proses akuisisi forensik komputer, dimana akan membuat *image* salinan bit-to-bit dari semua data yang ada dalam perangkat seluler, termasuk file yang disembunyikan dan dihapus [11].

Saat melakukan investigasi kasus *cybercrime* dibutuhkan *framework* atau kerangka kerja forensik agar proses investigasi lebih efektif dan efisien [12]. Terdapat beberapa *framework* yang biasa digunakan oleh penyelidik diantaranya *Association of Chief Police Officers* (ACPO) [13], *National Institute of Justice* (NIJ) [14], *Digital Forensics Research Workshop* (DFRWS) [15], dan *National Institute of Standard and Technology* (NIST) [16].

Penelitian dengan tema sejenis pernah dilakukan dengan judul *Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method* [17]. Penelitian ini membahas penggunaan tools Oxygen forensics dan Axiom Magnets untuk mengembalikan data yang dihapus berupa file gambar dan chat dari aplikasi Instagram. Metode penelitian yang digunakan adalah NIST yang terbagi dalam empat tahap yaitu *collection*, *examination*, *analysis*, dan *reporting*.

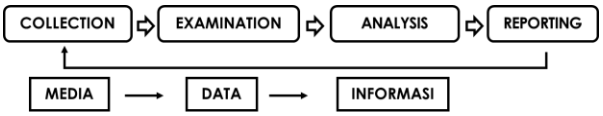
Penelitian kedua dengan tema sejenis pernah dilakukan dengan judul Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ) [9]. Penelitian ini membahas penggunaan tools MOBILedit Forensic, Wondershare dr. Fone for Android, dan Belkasoft Evidence Center untuk melakukan recovery bukti digital yaitu pesan, history kontak, panggilan, gambar dan video yang sebelumnya telah dihapus dari Samsung Galaxy J5. Metode penelitian yang digunakan adalah NIJ yang terbagi dalam lima tahap yaitu indentifikasi, solusi, uji coba, evaluasi, dan laporan.

Penelitian ketiga dengan tema sejenis pernah dilakukan dengan judul Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST [18]. Penelitian ini membahas perbandingan kinerja tools Wondershare dr. Fone for Android dan Oxygen Forensics Suite 2014 dalam melakukan *recovery* bukti digital yaitu kontak, log panggilan, dan pesan yang sebelumnya telah dihapus dari Samsung J5 2015 dan Samsung J1 Ace. Metode penelitian yang digunakan adalah NIST yang terbagi dalam empat tahap yaitu *collection*, *examination*, *analysis*, dan *reporting*.

Penelitian ini bertujuan melakukan analisis *recovery* terhadap bukti digital yang telah dihapus menggunakan metode penghapusan data melalui aplikasi manager dan penghapusan data secara manual. Penelitian ini menggunakan *framework* NIST dalam menemukan bukti digital yang valid sehingga dapat digunakan sebagai barang bukti yang sah secara hukum dan memberikan pemahaman bagi penyelidik dalam menyelesaikan kasus-kasus kejahatan serupa.

2. Metode Penelitian

Metodologi menjelaskan tentang tahapan penelitian secara sistematis sehingga dapat digunakan sebagai pedoman yang jelas dalam menyelsaikan dan membuat analasis dari hasil penelitian yang dilakukan. Penggunaan *framework* yang tepat untuk mengumpulkan barang bukti digital dapat memiliki keberhasilan hampir 100% [19]. Penelitian ini menggunakan *framework* dari *National Institute of Standards and Technology* (NIST). Adapun tahapan dari NIST seperti yang disajikan pada Gambar 1.



Gambar 1. Tahapan NIST

Penjelasan tahapn dari *framework* NIST adalah sebagai berikut:

1. *Collection* : tahap ini melakukan pelabelan, identifikasi, rekaman, dan pengambilan data dari sumber data yang relevan sesuai prosedur untuk menjaga keaslian data.
2. *Examination* : tahap ini melakukan pengumpulan dan pemeriksaan data menggunakan teknik forensik kombinasi berbagai skenario, baik otomatis atau manual, serta menilai dan mengeluarkan data sambil menjaga keaslian data.
3. *Analysis* : tahap ini melakukan pencarian bukti digital dari hasil *examination* dengan menggunakan metode teknis dibenarkan dan hokum.
4. *Reporting* : tahap ini melakukan pembuatan laporan hasil dari hasil analisis yang didapatkan serta tahapan-tahapan yang dilakukan.

Adapun penelitian ini menggunakan alat dan bahan yaitu laptop Asus A46CB i5 Windows 10, *smartphone* Samsung J2 kondisi *rooted* dan Andromax A kondisi *rooted*, kabel USB, Skype untuk *smartphone* Android, *tools* forensik berupa Oxygen Forensic Suite 2014 dan Belkasoft Evidence Center (Trial Ver), dan data awal simulasi yang terdiri dari kontak, pesan dan file gambar seperti yang disajikan pada Tabel 1 dan Tabel 2.

Tabel 1. Data awal simulasi kasus barang bukti A

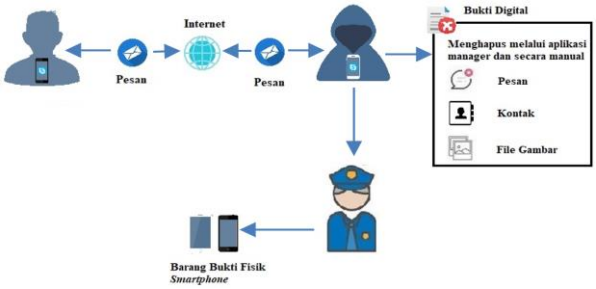
No	Bukti Digital	Jumlah
1	Kontak	11
2	Pesan	25
3	Gambar	13

Tabel 2. Data awal simulasi kasus barang bukti B

No	Bukti Digital	Jumlah
1	Kontak	10
2	Pesan	22
3	Gambar	10

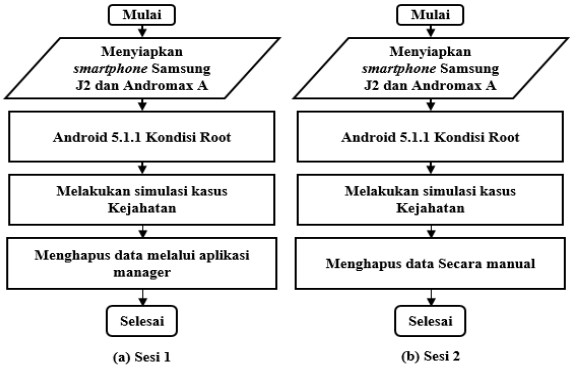
Data awal simulasi kasus digunakan sebagai pembanding dan penentu kinerja dari tool forensik yang digunakan untuk melakukan *recovery* data yang terhapus dari barang bukti sesuai dengan penghapusan data pada metode melalui aplikasi manager dan secara manual.

Pada penelitian ini tidak menggunakan kasus kejahatan dan barang bukti sesuai dengan yang terjadi melainkan dengan membuat simulasi kasus seperti yang disajikan pada gambar 2.



Gambar 2. Simulasi Kasus Kejahatan

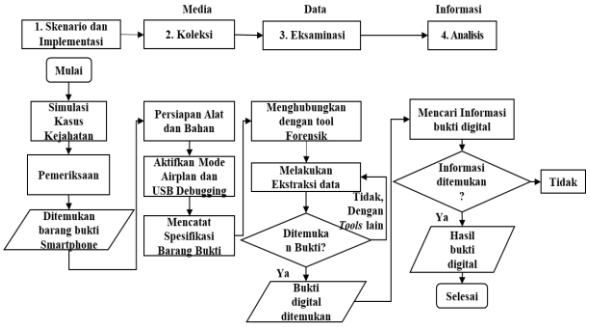
Penelitian ini melakukan simulasi kasus yaitu skenario penghapusan bukti, penyidik menemukan barang bukti berupa *smartphone* yang ter-*install* skype yang diduga digunakan untuk melakukan transaksi barang ilegal. Penelitian ini membagi skenario penghapusan data menjadi dua sesi. Dimana pada sesi pertama melakukan penghapusan data melalui aplikasi dan pada sesi kedua melakukan penghapusan data secara manual. Tahapan implementasi skenario penelitian seperti yang disajikan pada Gambar 3.



Gambar 3. Skenario metode penghapusan data

Penelitian ini akan melakukan *recovery* data yang telah terhapus berupa data kontak, pesan dan file gambar dari kedua smartphone yang digunakan sebagai barang bukti. Proses *recovery* data yang telah terhapus menggunakan *tool* forensik yaitu Oxygen Forensic Suite 2014 dan Belkasoft Evidience Center. Kedua smartphone yang ada pada penelitian ini digunakan untuk melihat kemampuan hasil *recovery* dari *tool* forensik yang di gunakan. Hasil penelitian kemudian disajikan dalam bentuk data kemampuan kinerja tool yang digunakan dalam mengembalikan data yang telah dihapus.

Adapun tahapan penelitian ini menggunakan tahapan dari framework NIST yang dirangkum menjadi tiga tahap dan ditambah satu tahapan yaitu skenario dan implemantasi. Flowchart penelitian seperti yang disajikan pada Gambar 4 [20].

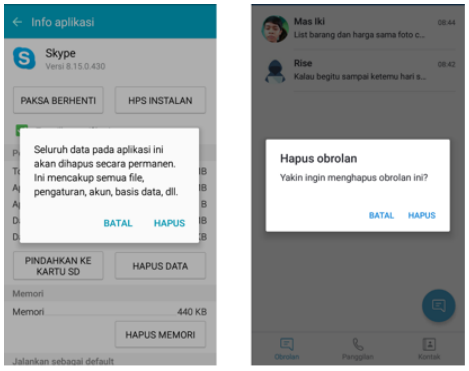


Gambar 4. Flowchart penelitian

3. Hasil dan Pembahasan

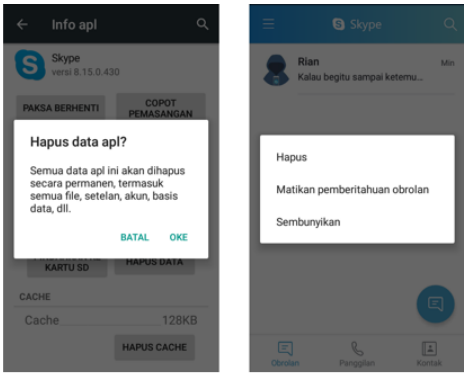
3.1. Skenario dan Implementasi

Simulasi kasus kejahatan pada penelitian ini sesuai pada Gambar 4. Pada penelitian ini simulasi kasus yang dilakukan yaitu melakukan penghapusan bukti digital tekait kejahatan transaksi barang ilegal yang dilakukan pelaku. Penghapusan bukti digital melalui dua sesi yaitu sesi pertama melalui aplikasi manager dan sesi kedua secara manual, penyelidik kemudian berhasil menemukan dua *smartphone* dari tangan pelaku sebagai barang bukti fisik. Implementasi penghapusan data dari barang bukti elektronik menggunakan metode penghapusan pada sesi 1 dan sesi 2 seperti yang disajikan pada Gambar 5 untuk barang bukti A dan Gambar 6 untuk barang bukti B.



(a) Sesi 1 (b) Sesi 2

Gambar 5. Implementasi penghapusan pada barang bukti A



(a) Sesi 1 (b) Sesi 2

Gambar 6. Implementasi penghapusan pada barang bukti B

3.2. Koleksi

Tahap koleksi merupakan pengumpulan barang bukti fisik berupa *smartphone* yang digunakan untuk melakukan penelitian. Penelitian ini menggunakan 2 smartphone yang dijadikan barang bukti seperti yang disajikan pada Gambar 7.

Gambar 7. Barang bukti berupa *smartphone*

Barang bukti berupa smartphone yang berhasil ditemukan, kemudian dilakukan pengamanan dengan mengaktifkan *Airplane Mode* dan mengaktifkan USB Debugging serta mencatat spesifikasi dari barang bukti yang ditemukan. Spesifikasi dari barang bukti berupa *smartphone* yang ditemukan seperti yang disajikan pada Tabel 3.

Tabel 3. Spesifikasi dari *smartphone* yang digunakan

Spesifikasi	Barang bukti A	Barang bukti B
Merek	Samsung J2	Smartfren Andromax A
Nomor Model	SM-J200G	Andromax A 16C3H
OS	Android	Android
Android Versi	5.1.1	5.1.1
Root	Ya	Ya

3.2. Eksaminasi

Tahap eksaminasi melakukan pemeriksaan dan pengambilan data dari *smartphone* untuk mendapatkan data yang telah dihapus. Hal pertama yang dilakukan sebelum melakukan pengambilan data yaitu menghubungkan smartphone dengan Laptop yang sebelumnya sudah ter-*install tool* forensik terlebih dahulu. Barang bukti A dan barang bukti B yang terhubung dengan Oxygen seperti yang disajikan pada Gambar 8.

Gambar 8. Barang bukti A dan barang bukti B yang terhubung dengan Oxygen

Gambar 8 menunjukkan bahwa barang bukti A dengan merek Samsung J2 dan barang bukti B dengan merek Smartfren Andromax A berhasil terhubung dengan Oxygen. Informasi yang didapatkan setelah kedua *smartphone* terhubung dengan Oxygen yaitu Model, IMEI, *Hardware revision* dan *Software revision*.

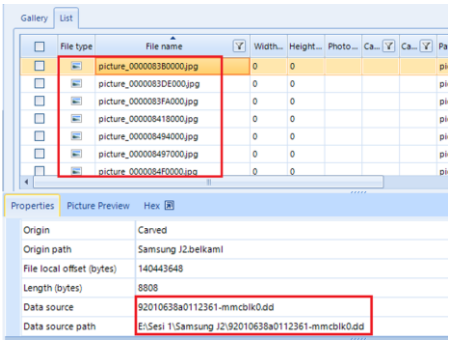
Berbeda dengan Oxygen, barang bukti yang berhasil terhubung dengan Belkasoft hanya memberi informasi tentang *Model*, *Manufacturer*, dan *Description* dari *smartphone* yang digunakan. Barang bukti A dan barang bukti B yang berhasil terhubung dengan Belkasoft seperti yang disajikan pada Gambar 9.

Gambar 9. Barang bukti A dan barang bukti B yang terhubung dengan Belkasoft

Barang bukti A dan barang bukti B yang terhubung dengan belkasoft berhasil menampilkan informasi dari *smartphone* yang digunakan.

Setelah *smartphone* terhubung dengan tool forensik, selanjutnya melakukan ekstrasi data yang terhapus dari *smartphone*. Proses menghubungkan *smartphone* dengan *tool* forensik dan eksraksi data akan dilakukan dua kali mengikuti dengan skenario penghapusan data yang telah dibuat seperti yang disajikan pada Gambar 2 sebelumnya.

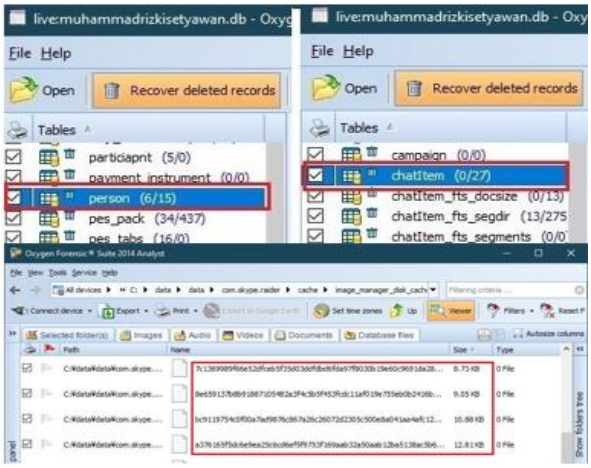
Proses ekstraksi pertama yaitu melakukan *recovery* data dari barang bukti A yang telah di implementasi metode penghapusan sesi 1 dan sesi 2. Hasil ekstraksi barang bukti A pada metode penghapusan sesi 1 menggunakan Oxygen tidak berhasil melakukan *recovery* data yang telah terhapus. Sedangkan hasil ekstraksi menggunakan Belkasoft seperti yang disajikan pada Gambar 10.



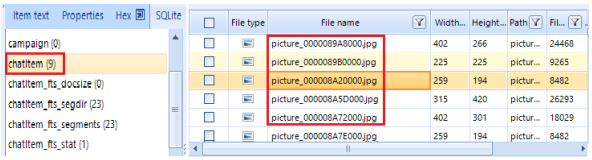
Gambar 10. Contoh hasil ekstraksi barang bukti A pada Sesi 1 dengan Belkasoft

Hasil ekstraksi pada barang bukti A pada metode penghapusan sesi 2 menggunakan Belkasoft hanya berhasil mengembalikan bukti digital berupa 13 file gambar, sementara data kontak dan pesan tidak berhasil di dikembalikan

Proses selanjutnya melakukan ekstraksi dari barang bukti A pada metode penghapusan sesi 2. Hasil ekstraksi data yang telah dilakukan seperti yang disajikan pada Gambar 11 (a) menggunakan Oxygen dan Gambar 11 (b) menggunakan Belkasoft.



(a) Mengguanakan Oxygen



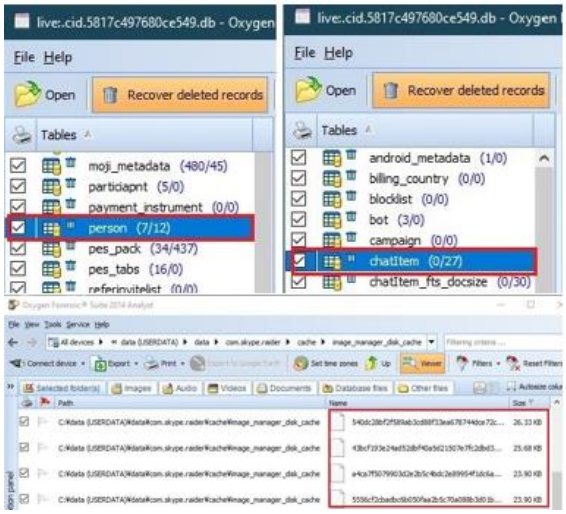
(b) Menggunakan Belkasoft

Gambar 11. Contoh hasil ekstraksi barang bukti A pada Sesi 2

Hasil ekstraksi dari barang bukti A pada metode penghapusan sesi 2 menggunakan Oxygen berhasil mengembalikan bukti digital yang terhapus berupa 12 kontak, 27 pesan dan 11 file gambar. Sedangkan hasil ekstrasi menggunakan Belkasoft berhasil mengembalikan bukti digital berupa 9 pesan, dan 13 file gambar, sementara data kontak tidak berhasil di kembalikan.

Proses ekstraksi kedua yaitu melakukan *recovery* data dari barang bukti B yang telah di implementasi metode penghapusan sesi 1 dan sesi 2. Hasil ekstraksi barang bukti B pada metode penghapusan sesi 1 menggunakan Oxygen dan Belkasoft tidak berhasil mengembalikan data yang telah terhapus.

Proses selanjutnya melakukan ekstraksi dari barang bukti B pada metode penghapusan sesi 1 menggunakan Oxygen seperti yang disajikan pada Gambar 12. Sedangkan hasil ekstraksi menggunakan Belkasoft tidak berhasil mengembalikan data yang terhapus.



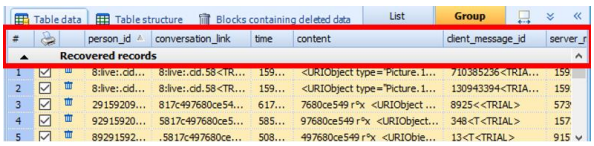
Gambar 12. Contoh Hasil ekstraksi barang bukti B menggunakan Oxygen pada Sesi 1

Hasil ekstraksi dari barang bukti B pada skenario sesi 1 menggunakan Oxygen berhasil mengembalikan bukti digital yang terhapus berupa 15 kontak, 27 pesan dan 10 file gambar.

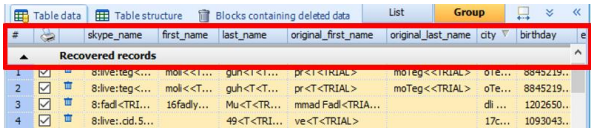
3.2. Analisis

Tahap analisis melakukan pencarian informasi berguna dari data yang telah didapat pada tahap sebelumnya. Proses analisis dilakukan atau mencari informasi penting dilakukan dengan mengecek hasil ekstraksi kedua barang bukti.

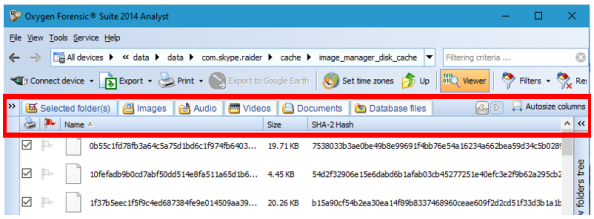
Proses analisis pada tool Oxygen melakukan pencarian informasi pesan, kontak, dan gambar seperti yang disajikan pada Gambar 13 (a) pesan, Gambar 13 (b) kontak, dan Gambar 13 (c) file gambar.



(a) Pesan



(b) Kontak



(c) File Gambar

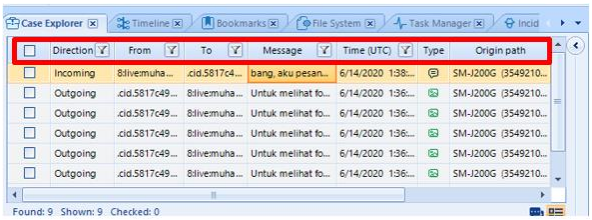
Gambar 13 Contoh proses analisis menggunakan Oxygen

Dari Gambar 13 (a) informasi yang bisa didapatkan dari bukti digital pesan berupa *person id, conversation link, time, content*, dan informasi lainnya.

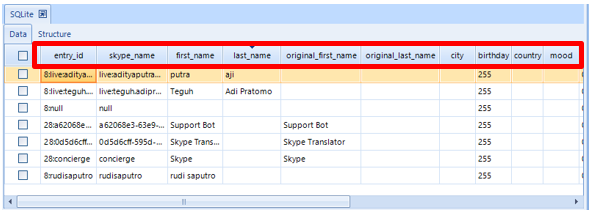
Dari Gambar 13 (b) informasi yang bisa didapatkan dari bukti digital kontak berupa *skype name, first name, last name, original first name, original last name, city, birthday*, dan informasi lainnya.

Dari Gambar 13 (c) informasi yang bisa didapatkan dari bukti digital file gambar berupa *name, size*, SHA-2-Hash dan informasi lainnya.

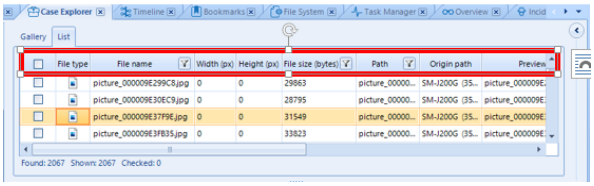
Sedangkan proses analisis pada tool Belkasoft melakukan pencarian informasi untuk mendapatkan informasi bukti digital seperti yang disajikan pada Gambar 14 (a) pesan, Gambar 14 (b) kontak, dan Gambar 14 (c) file gambar



(a) Pesan



(b) Kontak



(c) File Gambar

Gambar 14 Contoh proses analisis menggunakan Belkasoft

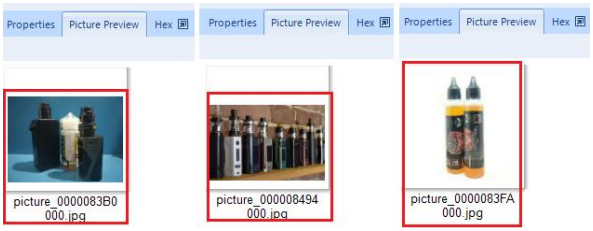
Dari Gambar 14 (a) informasi yang bisa didapatkan dari bukti digital pesan berupa *direction, from, to, message, time, type, origin path* dan informasi lainnya.

Dari Gambar 14 (b) informasi yang bisa didapatkan dari bukti digital kontak berupa *entry id, skype name, first name, last name, original first name, original last name, city, birthday*, dan informasi lainnya.

Dari Gambar 14 (c) informasi yang bisa didapatkan dari bukti digital file gambar berupa *file type, file name, width, height, path, file size* dan informasi lainnya.

Proses analisis pertama yaitu mencari informasi data dari barang bukti A yang berhasil diekstraksi pada setelah melakukan metode penghapusan sesi 1 dan sesi 2.

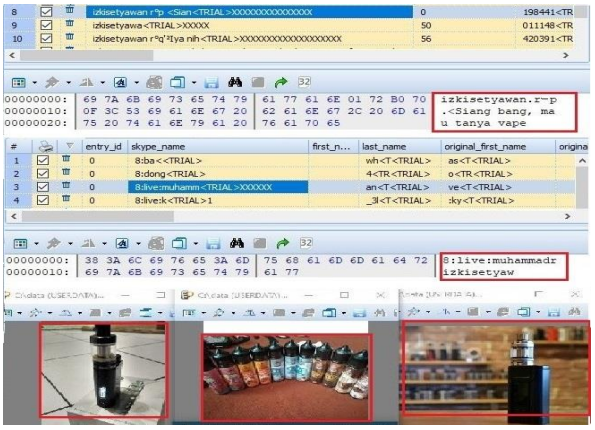
Analisis bukti digital dari barang bukti A pada skenario sesi 1 menggunakan Oxygen tidak dilakukan karena pada proses ekstraksi tidak berhasil mengembalikan data yang terhapus. Sedangkan hasil analisis bukti digital dari proses ekstraksi menggunakan belkasoft seperti yang disajikan pada Gambar 15.



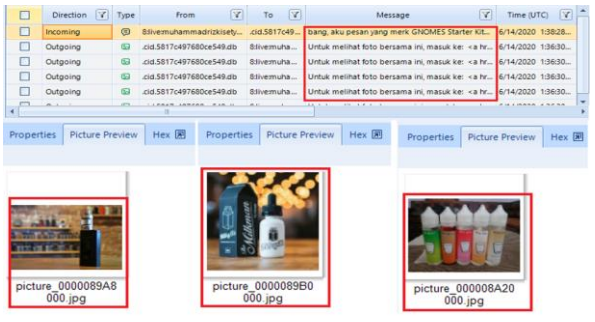
Gambar 15. Contoh hasil analisis barang bukti A pada Sesi 1 menggunakan Belksoft

Hasil analisis barang bukti A pada skenario sesi 1 menggunakan Belkasoft hanya berhasil menemukan bukti digital berupa 13 file gambar yang valid, sementara bukti digital berupa kontak dan pesan tidak berhasil di kembalikan.

Selanjutnya melakukan analisis data hasil ekstraksi dari barang bukti A pada skenario sesi 2. Hasil analisis yang dilakukan seperti yang disajikan pada Gambar 16 (a) menggunakan Oxygen dan 16 (b) menggunakan Belkasoft.



(a) Menggunakan Oxygen



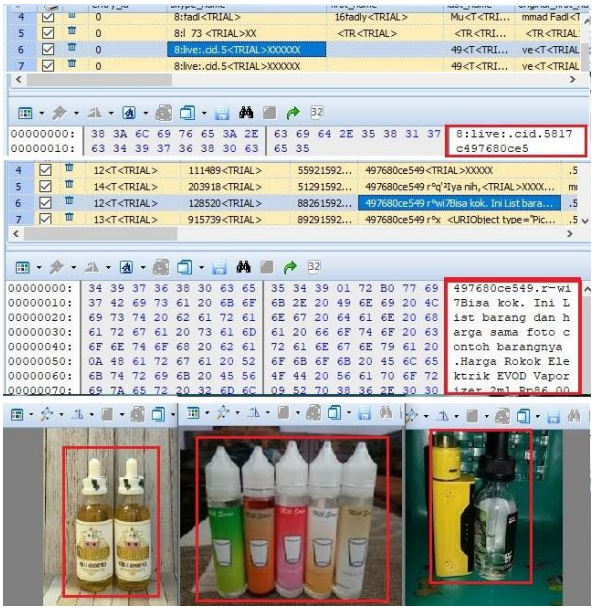
(b) Menggunakan Belkasoft

Gambar 16. Contoh hasil analisis barang bukti A pada Sesi 2

Hasil analisis data ekstraksi dari barang bukti A pada skenario sesi 2 menggunakan Oxygen berhasil menemukan bukti digital yang terdiri dari 11 kontak yang valid dan 1 kontak yang sama dari data kontak berjumah 12 yang berhasil dikembalikan. Bukti digital berupa data pesan hanya berhasil menemukan 7 pesan yang valid dan 20 pesan yang sama dari data pesan berjumah 27 yang berhasil dikembalikan. Barang bukti file gambar berhasil menemukan 13 file gambar yang valid. Sedangkan hasil analisis menggunakan Belkasoft hanya berhasil menemukan bukti digital yang terdiri dari 9 data pesan yang valid. Bukti digital berupa file gambar berhasil menemukan 13 file gambar yang valid. Sementara untuk bukti digital kontak tidak berhasil di dikembalikan.

Proses analisis kedua yaitu mencari informasi data dari barang bukti B yang berhasil diekstraksi pada metode penghapusan sesi 1 dan sesi 2. Analisis bukti digital dari ekstrasksi barang bukti B pada skenario sesi 1 menggunakan Oxygen dan belkasoft tidak dilakukan karena pada proses ekstraksi data dari barang bukti B tidak berhasil mengembalikan data yang terhapus.

Selanjutnya melakukan analisis data ekstraksi dari barang bukti B pada metode penghapusan sesi 2. Hasil analisis bukti digital yang dilakukan menggunakan Oxygen seperti yang disajikan pada Gambar 17. Sedangkan analisis data menggunakan belkasoft tidak dilakukan karena tidak berhasil mengembalikan data yang terhapus.



Gambar 17. Contoh hasil analisis barang bukti B pada Sesi 2 menggunakan Oxygen

Hasil analisis data dari barang bukti B pada metode penghapusan sesi 2 menggunakan Oxygen berhasil menemukan 10 data kontak yang valid dan 5 data kontak yang sama dari data kontak berjumah 15 yang berhasil *recovery*. Bukti digital berupa data pesan hanya berhasil menemukan 6 pesan yang valid dan 21 pesan yang sama dari data pesan berjumah 27 yang berhasil *recovery*.

Barang bukti file gambar berhasil menemukan 10 file gambar yang valid.

Perbandingan hasil analisis *recovery* bukti digital yang valid dari barang bukti A menggunakan *tool* forensik sesuai dengan metode penghapusan sesi 1 dan sesi 2 menggunakan Oxygen dan Belkasoft seperti yang disajikan pada Tabel 4.

Tabel 4 Perbandingan hasil analisis *recovery* bukti digital dari barang bukti A (Samsung J2)

Tool Forensik	Bukti Digital	Data Awal	Sesi 1	Sesi 2
Oxygen	Kontak	11	0	11
	Pesan	25	0	7
	Gambar	13	0	13
Belkasoft	Kontak	11	0	0
	Pesan	25	0	9
	Gambar	13	13	13

Kinerja hasil analisis *recovery* data dari barang bukti A pada metode penghapusan sesi 1, menggunakan Oxygen tidak dapat mengembalikan data, dan prosentase keberhasilan menggunakan Belkasoft sebesar 26%. Sedangkan kinerja hasil analisis *recovery* data pada metode penghapusan sesi 2, prosentase keberhasilan menggunakan Oxygen sebesar 63% dan Belkasft sebesar 44%.

Perbandingan hasil analisis *recovery* bukti digital yang valid dari barang bukti B menggunakan *tool* forensik sesuai dengan metode penghapusan sesi 1 dan sesi 2 menggunakan Oxygen dan Belkasoft seperti yang disajikan pada Tabel 5.

Tabel 5 Perbandingan hasil analisis *recovery* bukti digital dari barang bukti B (Andromax A)

Tool Forensik	Bukti Digital	Data Awal	Sesi 1	Sesi 2
Oxygen	Kontak	10	0	10
	Pesan	22	0	6
	Gambar	10	0	10
Belkasoft	Kontak	10	0	0
	Pesan	22	0	0
	Gambar	10	0	0

Kinerja hasil analisis *recovery* data dari barang bukti B pada metode penghapusan sesi 1, Oxygen dan Belkasoft tidak dapat mengembalikan data. Sedangkan kinerja hasil analisis *recovery* pada metode penghapusan sesi 2, prosentase keberhasilan menggunakan Oxygen sebesar 61% dan Belkasoft tidak dapat mengembalikan data.

Hasil evaluasi analisis *recovery* menggunakan tools Oxygen dan Belkasoft pada kedua barang bukti berupa Samsung J2 dan Andromax A menggunakan metode penghapusan sesi 1 dan sesi 2 seperti yang disajikan pada Tabel 6 dan Tabel 7.

Tabel 6 Hasil analisis *recovery* bukti digital menggunakan tool Oxygen pada kedua barang bukti

Oxygen Forensic Suite			
Barang Bukti	Bukti Digital	Sesi 1	Sesi 2
Samsung J2	Kontak	-	✓
	Pesan	-	✓
	Gambar	-	✓
Andromax A	Kontak	-	✓
	Pesan	-	✓
	Gambar	-	✓

Tabel 7 Hasil analisis *recovery* bukti digital menggunakan tool Belkasoft pada kedua barang bukti

Belkasoft Evidence Center			
Barang Bukti	Bukti Digital	Sesi 1	Sesi 2
Samsung J2	Kontak	-	-
	Pesan	-	✓
	Gambar	✓	✓
Andromax A	Kontak	-	-
	Pesan	-	-
	Gambar	-	-

4. Kesimpulan

Penelitian tentang analisis *recovery* bukti digital Skype berbasis *Smartphone Android* Menggunakan *Framework* NIST berhasil dilakukan. Hasil *recovery* bukti digital dari *smartphone* Samsung J2 pada metode penghapusan melalui aplikasi manager, tool Oxygen tidak dapat mengembalikan data yang terhapus dan prosentase keberhasilan menggunakan belkasoft sebesar 26%. Sedangkan hasil *recovery* data dengan metode penghapusan secara manual prosentase keberhasilan menggunakan Oxygen sebesar 63% dan Belkasoft sebesar 44%. Hasil *recovery* bukti digital dari *smartphone* Andromax A pada skenario penghapusan melalui aplikasi manager, *tool* Oxygen dan Belkasoft tidak dapat mengembalikan data yang terhapus. Sedangkan penghapusan secara manual Oxygen sebesar 61% dan Oxygen tidak dapat mengembalikan data.

Dapat disimpulkan hasil *recovery* data dari kedua *smartphone* yang digunakan sesuai metode penghapusan melalui aplikasi manager *tool* Belkasoft memiliki kinerja lebih baik dari Oxygen, dan *recovery* data penghapusan secara manual *tool* Oxygen memiliki kinerja lebih baik dari Belkasoft. Perbedaan merek *smartphone* yang digunakan juga dapat memberikan hasil yang berbeda saat mengembalikan data yang terhapus. Beberapa saran untuk penelitian selanjutnya terdapat berbagai macam jenis sistem operasi, *tools* forensik, dan jenis *smartphone* yang berbeda serta metode lainnya yang dapat digunakan untuk melakukan analisis forensik.

Daftar Rujukan

[1] R. Umar, I. Riadi, dan G. M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 3, hal. 949, Jun 2018, doi: 10.18517/ijaseit.8.3.3591.

[2] S. Kemp, "Digital 2019: Global Internet Use Accelerates," *Hootsuite and We Are Social*, 2019. https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates (diakses Mei 17, 2020).

[3] S. Ikhsani dan B. C. Hidayanto, "Analisa Forensik Whatsapp dan LINE Messenger Pada Smartphone Android Sebagai Rujukan Dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia," *Jurnal Teknik ITS*, vol. 5, no. 2, 2016, doi: 10.12962/j23373539.v5i2.17271.

[4] A. Yudhana, I. Riadi, dan F. Ridho, "DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 9, no. 11, hal. 177–183, 2018.

[5] F. G. Hikmatyar dan B. Sugiantoro, "Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases," *International Journal on Informatics for Development (IJID)*, vol. 7, no. 2, hal. 19, Jan 2019, doi: 10.14421/ijid.2018.07204.

[6] D. T. Yuwono, A. Fadlil, dan Sunardi, "Perbandingan Kinerja Perangkat Lunak Forensik untuk File Carving dengan Metode NIST," *Jurnal Teknologi dan Sistem Komputer*, vol. 7, no. July, hal. 89–92, 2019, doi: 10.14710/jtsiskom.7.3.2019.89-92.

[7] M. N. Faiz, R. Umar, dan A. Yudhana, "Analisis Live Forensics untuk Perbandingan Kemananan Email pada Sistem Operasi Proprietary," *ILKOM Jurnal Ilmiah*, vol. 8, no. 3, hal. 242–247, Des 2016, doi: 10.33096/ilkom.v8i3.79.242-247.

[8] Sunardi, I. Riadi, dan M. H. Akbar, "Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi," *Rekayasa Sistem dan Teknologi Informasi (RESTI)*, vol. 4, no. 3, hal. 576–583, 2020.

[9] I. Riadi, S. Sunardi, dan S. Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *Jurnal Rekayasa Teknologi Informasi (JURTI)*, vol. 3, no. 1, hal. 87–95, 2019, doi: 10.30872/JURTI.V3I1.2292.

[10] B. C. Ogazi-Onyemaechi, A. Dehghantanha, dan K. K. R. Choo, "Performance of Android Forensics Data Recovery Tools," in *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, no. March, 2017, hal. 91–110.

[11] N. R. Roy, A. K. Khanna, dan L. Aneja, "Android phone forensic: Tools and techniques," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Apr 2016, hal. 605–610, doi: 10.1109/CCAA.2016.7813792.

[12] S. Ningsih, "Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 3, hal. 294–304, 2018, doi: 10.17781/P002463.

[13] I. Riadi, R. Umar, dan M. A. Aziz, "Forensik Web Layanan Instant Messaging Menggunakan Metode Association of Chief Police Officers (ACPO)," *Mobile and Forensics*, vol. 1, no. 1, hal. 30, 2019, doi: 10.12928/mf.v1i1.705.

[14] M. R. Setyawan, A. Yudhana, dan A. Fadlil, "Akuisisi Data Pada Skype Messenger Menggunakan Metode National Institute Of Justice," *SYSTEMIC : Information System and Informatics Journal.*, vol. 5, no. 2, hal. 13–18, 2019, doi: 10.29080/systemic.v5i2.724.

[15] A. Yudhana, I. Riadi, I. Zuhriyanto, dan K. Kunci, "Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," *TECHNO*, vol. 20, no. 2, hal. 125–130, 2019, doi: 10.30595/techno.v20i2.4594.

[16] A. Yudhana, R. Umar, dan A. Ahmadi, "Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method," *Scientific Journal of Informatics*, vol. 6, no. 1, hal. 54–63, 2019.

[17] I. Riadi, A. Yudhana, dan M. C. F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," *Scientific Journal of Informatics*, vol. 5, no. 2, hal. 235–247, 2018.

[18] I. Riadi, S. Sunardi, dan Sahiruddin, "Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. x, no. 30, hal. 1–8, 2020, doi: 10.25126/jtiik.202071921.

[19] I. Riadi dan I. M. Nasrulloh, "Analisis Forensik Solid State Drive (Ssd) Menggunakan Framework Grr Rapid Response Forensic Analysis Of Solid State Drives (Ssd) Using The Grr Rapid Response Framework," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 6, no. 5, hal. 509–518, 2019, doi: 10.25126/jtiik.201961516.

[20] I. Riadi, S. Sunardi, dan A. Hadi, "Analisis Bukti Digital TRIM Enable SSD NVMe Menggunakan Metode Static Forensics," *JUITA: Jurnal Informatika*, vol. 8, no. 1, hal. 65, 2020, doi: 10.30595/juita.v8i1.6584.