JURNAL MAHAJANA INFORMASI
e-ISSN 2527 – 8290
Vol. 8 No. 2, Desember 2023, Hal. 80 - 88

Perbandingan Tools Forensik Dalam Analisis Bukti Digital Pada Aplikasi Skype Menggunakan Framework NIST

Muhammad Rizki Setyawan[1]*

[1]*Program Studi Teknik Informatika, Universitas Muhammadiyah Sorong*

*Penulis Korespondensi : rizki@um-sorong.ac.id

Article Info

Received : *03 Desember 2023*
Revised : *16 Desember 2023*
Accepted : *19 Desember 2023*

Abstract ***:*** *In the rapidly evolving digital era, human communication has undergone significant changes thanks to instant messaging. Instant messaging enables us to easily and quickly connect with people around the world through mobile devices or computers. However, the use of instant messaging applications can have negative impacts such as fraud, harassment, illegal transactions, and more. Therefore, proper handling of cybercrime cases is crucial, which is why mobile forensics has become significant. Mobile forensics is a branch of digital forensics that aims to collect, analyze, and interpret data from mobile devices. This research aims to evaluate the performance of three forensic tools: Oxygen Forensic Suite, Belkasoft Evidence Center, and MOBILedit Forensic Express. It focuses on finding digital evidence related to activity information in the Skype application using the framework provided by NIST. The research results indicate that Oxygen Forensic Suite achieved the highest index value (98%), followed by Belkasoft Evidence Center (88%) and MOBILedit Forensic Express (84%).*

Abstrak : Dalam perkembangan era digital yang pesat, komunikasi manusia telah mengalami perubahan signifikan berkat pesan instan atau Instant Messaging. Pesan instan memungkinkan kita untuk terhubung dengan orang-orang di seluruh dunia dengan mudah dan cepat melalui perangkat seluler atau komputer. Namun, dalam penggunaan aplikasi pesan instan ini dapat memiliki dampak negatif seperti penipuan, pelecehan, transaksi ilegal, dan masih banyak lagi. Sehingga penanganan yang tepat dalam kasus kejahatan siber sangat penting, dan inilah mengapa forensik mobile menjadi hal yang signifikan. Mobile forensic adalah cabang forensik digital yang bertujuan melakukan pengumpulan, analisis, dan interpretasi data dari perangkat mobile. Penelitian ini bertujuan untuk mengevaluasi kinerja tiga perangkat forensik, yaitu Oxygen Forensic Suite, Belkasoft Evidence Center dan MOBILedit Forensic Express. Dan, dalam menemukan bukti digital terkait informasi aktivitas pada aplikasi Skype dengan menggunakan framework dari NIST. Hasil penelitian menunjukkan bahwa tools forensik Oxygen Forensic Suite memiliki nilai indeks tertinggi (98%), diikuti oleh Belkasoft Evidence Center (88%) dan MOBILedit Forensic Express (84%).

Keyword *: Mobile Forensic, Skype, Digital Evidence, Cybercrime, NIST*

PENDAHULUAN

Dalam era digital yang terus berkembang, komunikasi manusia telah mengalami perubahan yang luar biasa. Dulu, kita mengandalkan surat pos yang lambat dan

telepon sebagai sarana utama berkomunikasi. Namun, dengan hadirnya teknologi modern, pesan instan atau *Instant Messaging* menjadi inovasi yang mempermudah dan mempercepat komunikasi (Nasirudin et al., 2020). Skype merupakan salah satu aplikasi pesan instan yang banyak digunakan di dunia. Pada tahun 2019, Skype memiliki lebih dari 300 juta pengguna, dan angka ini terus meningkat sejak pandemi COVID-19 pada tahun 2020 (Anton Yudhana et al., 2020). Meskipun pesan instan memiliki banyak manfaat tetapi aplikasi Skype juga dapat digunakan untuk tindakan yang negatif, termasuk penipuan, pelecehan, transaksi ilegal, dan kejahatan siber lainnya. Oleh karena itu, penanganan yang tepat diperlukan untuk menangani kasus-kasus kejahatan siber, mengingat bukti digital bisa berubah dan hilang (Rizki Setyawan et al., 2022).

Mobile forensic merupakan cabang *forensik digital* yang khusus mempelajari pengumpulan, analisis, dan interpretasi data yang terkait dengan perangkat *mobile*, seperti ponsel pintar, tablet, dan perangkat wearables. (Hikmatyar & Sugiantoro, 2019). *Mobile forensic* melibatkan penggunaan metode dan tools khusus untuk memperoleh data dari perangkat *mobile*. Beberapa jenis data yang biasanya dianalisis dalam mobile forensik meliputi pesan teks, panggilan telepon, kontak, email, media sosial, foto, video, data lokasi, data sensor, dan data aplikasi. (Zuhriyanto et al., 2020).

Terdapat dua metode yang umum digunakan saat melakukan *mobile forensic*, yang pertama dengan metode *live forensic*, merujuk pada proses pengumpulan dan analisis data dari perangkat mobile yang masih aktif atau hidup. Dalam metode ini, analisis forensik bekerja pada perangkat yang sedang berjalan dan berinteraksi langsung dengan sistem operasi, aplikasi, dan data yang ada di dalamnya. Metode yang kedua adalah *Static Forensic* melibatkan proses pengumpulan dan analisis data dari perangkat mobile yang tidak aktif atau mati (Yudhana et al., 2019).

Beberapa *framework* umum yang digunakan termasuk *National Institute of Standards and Technology* (NIST) (Riadi & Nasrulloh, 2019), *National Institute of Justice* (NIJ) (Setyawan et al., 2019), *Digital Forensik Research Workshop* (DFRWS) (Fadillah et al., 2022), *The Association of Chief Police Officers* (ACPO) (Riadi et al., 2019), dan lainnya. Dengan menggunakan *framework*, para analis forensik dapat memastikan bahwa prosedur yang dilakukan sesuai dengan standar yang berlaku dan dapat diterima sebagai bukti yang sah dalam proses hokum (Riadi et al., 2020).

Penelitian serupa dilakukan oleh (Fanani et al., 2022), dimana penelitian ini melakukan investigasi dan menganalisis bukti digital yang terkait pada aplikasi Michat. Penelitian lain yang terkait dengan subjek yang sama dilakukan oleh (Nafila & Prayudi, 2022) dimana penelitian ini mencari jejak digital yang dapat digunakan sebagai bukti dalam kasus kejahatan pada aplikasi Signal. Penelitian lainnya oleh (Mualfah et al., 2021), bertujuan untuk menemukan bukti digital yang telah dihapus dari aplikasi TamTam Messenger menggunakan tools forensik MobileEdit dan metode NIJ.

Pada penelitian ini bertujuan untuk melakukan investigasi bukti digital terkait kejahatan siber yaitu perdagangan vape narkoba melalui penggunaan aplikasi pesan instan Skype berbasis Android. Penelitian ini juga membandingkan kemampuan tiga tools forensik yaitu Belkasoft Evidence Center, MobilEdit Forensic Express, dan Oxygen Forensic Suite dalam menganalisis barang bukti yang terkait dengan kasus tersebut,

JURNAL MAHAJANA INFORMASI
e-ISSN 2527 – 8290
Vol. 8 No. 2, Desember 2023, Hal. 80 - 88

seperti gambar, video, informasi akun, kontak person, dan percakapan yang dapat ditemukan dalam aplikasi Skype dengan menggunakan *framework* dari *National Institute of Standards and Technology* (NIST).

METODE

Tahapan Penelitian

Penelitian ini mengikuti tahapan yang disusun berdasarkan *framework* yang dikembangkan oleh *National Institute of Standards and Technology* (NIST). Framework ini terdiri dari empat tahapan utama, sebagaimana dijelaskan dalam Gambar 1.

Gambar 1. Tahapan NIST

Adapun penjelasan dari tahapan *National Institute of Standards and Technology* (NIST) adalah sebagai berikut:

1. *Collection*

Pada tahap ini yang dilakukan pertama pengumpulan barang bukti, mempersiapan tools dan bahan serta melakukan rooting pada smartphone. Selanjutnya membuatan *backup* atau *cloning* dari smartphone yang ditemukan. Tujuannya untuk memastikan bahwa data asli pada smartphone tetap utuh dan tidak terpengaruh pada saat dilakukan analisis forensik digital pada tahap selanjutnya.

2. *Examination*

Tahap ini melakukan pemeriksaan dan pengambilan bukti digital yang terlihat maupun yang sudah terhapus pada file *backup* atau *cloning* yang telah dibuat sebelumnya menggunakan metode yang dibenarkan secara hukum.

3. *Analysis*

Pada tahap ini, data yang telah berhasil diambil dari file *backup* dari smartphone akan dianalisis secara lebih detail dan teliti untuk mencari bukti potensial yang mungkin ada. Analisis ini bertujuan untuk mengungkap informasi yang tersembunyi dalam data yang telah diambil.

4. *Reporting*

Pada tahap ini, dilakukan pelaporan mengenai perbandingan kinerja tiga *tools* forensik yang digunakan dalam menemukan bukti digital.

Alat dan Bahan

Pada penelitian ini dibutuhkan alat dan bahan dalam membantu proses pencarian dan analisis barang bukti digital terlihat pada Tabel 1.

Tabel 1. Alat dan Bahan

No	Alat dan Bahan	Keterangan
1	Laptop	Merek Asus A46CB
2	*Smartphone*	Samsung Galaxy J2
3	Kabel Data USB	USB Tipe C
4	Aplikasi Skype	Versi
6	Oxygen Forensic Suite	Versi 2014
7	Belkasoft Evidence Center	Versi 9.6
8	MOBILedit Forensic Express	Versi 7.0.2.16723
9	SQLite Database Browser Portable	Versi 8.15.0.440

Skenario Kasus

Skenario kasus pada penelitian ini disesuaikan dengan kasus-kasus kejahatan digital yang terjadi pada smartphone android. Skenario kasus ini mengangkat kasus tentang adanya kemungkinan perdagangan barang ilegal berupa narkoba dalam bentuk vape dan liquid vape. Dalam percakapan pada aplikasi Skype Messenger disimulasikan sebagai perdagangan vape dan liquid vape. Barang bukti yang digunakan sebuah Smartphone Android berupa Samsung J2 yang telah terinstall aplikasi Skype. Aktivitas yang dilakukan pada aplikasi Skype adalah

JURNAL MAHAJANA INFORMASI
e-ISSN 2527 – 8290
Vol. 8 No. 2, Desember 2023, Hal. 80 - 88

mengirim dan menerima Percakapan, gambar, dan video.

Rumus perhitungan Akurasi

Pada penelitian ini untuk mengukur indeks akurasi yang dihitung dengan menggunakan rumus berikut (Umar et al., 2022):

$$Po = \frac{Px}{Pn} x\ 100\% \quad (1)$$

Keterangan:
Po : Angka index
Px : jumlah yang terdeteksi *tools* forensik
Pn : jumlah total keseluruhan data

HASIL DAN PEMBAHASAN

Collection

Pada tahap ini yang dilakukan adalah mengumpulkan dan mengamankan barang bukti elektronik yang ditemukan pada tempat kejadian perkara (TKP) dengan kasus perdagangan narkoba dalam bentuk liquid vape. Proses pengumpulan barang bukti berhasil menemukan barang bukti berupa sebuah Smartphone dengan merk Samsung Galaxy J2 seperti yang dipaparkan pada Gambar 3.

Gambar 3. Samsung Galaxy J2

Setelah berhasil menemukan barang bukti, langkah selanjutnya adalah melakukan pengamanan dengan mengaktifkan *Airplane Mode*, mengaktifkan *USB Debugging* serta melakukan rooting pada smartphone agar saat mengangkat data menjadi lebih mudah. Proses selanjutnya adalah melakukan *perservasi* atau pengamanan data dengan membuat *backup data* atau *physical image* menggunakan *MOBILedit Forensic Express* terlihat pada Gambar 4.

Gambar 4. Pembuatan backup atau cloning

Waktu yang dibutuhkan dalam melakukan proses membuat *backup* atau *cloning* tergantung dari kapasitas penyimpanan pada *smartphone* yang digunakan. Hasil dari *backup* atau *cloning* data seperti yang dipaparkan pada Gambar 5.

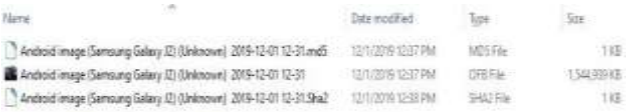
Gambar 5. Hasil backup

Examination

Pada tahap ini melakukan pemeriksaan atau examination dari data yang sudah di backup sebelumnya menggunakan tools forensik untuk menemukan bukti digital. Proses pemeriksaan dilakukan menggunakan tiga tools forensik berupa Oxygen Forensic Suite, MOBILedit Forensic Express, dan Belkasoft Evidence Center.

***Examination* menggunakan Oxygen Forensic Suite**

Hasil examination physical image menggunakan Oxygen Forensic Suite seperti yang dipaparkan pada Gambar 6.

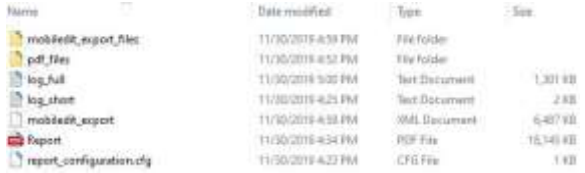


Gambar 6. Hasil *examination* menggunakan *Oxygen Forensic Suite*

JURNAL MAHAJANA INFORMASI
e-ISSN 2527 – 8290
Vol. 8 No. 2, Desember 2023, Hal. 80 - 88

***Examination* menggunakan Oxygen Forensic Suite**

Hasil examination physical image menggunakan menggunakan MOBILedit Forensic Express seperti yang dipaparkan pada Gambar 7.



Gambar 7. Hasil *examination* menggunakan MOBILedit Forensic Express

***Examination* menggunakan Oxygen Forensic Suite**

Hasil examination physical image menggunakan *Belkasoft Evidence Center* seperti yang dipaparkan pada Gambar 8.

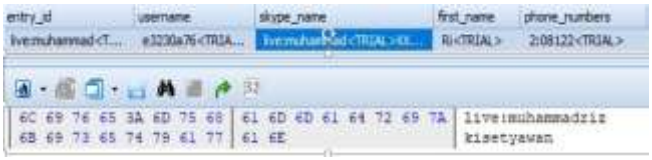
Gambar 8. Hasil examination menggunakan Belkasoft Evidence Center

Analysis

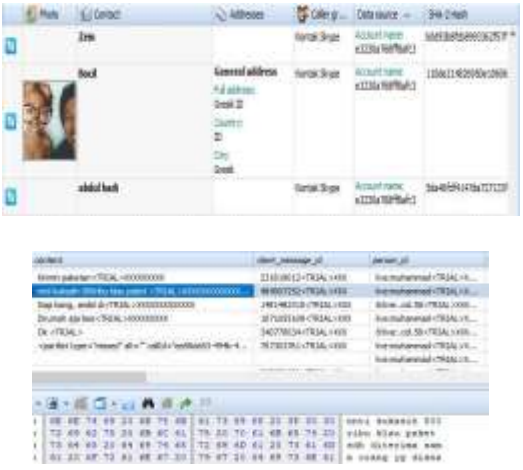
Tahap Analysis merupakan tahap selanjutnya dari tahap examination yaitu untuk mencari secara detail barang bukti potensial menggunakan tools forensik yang digunakan dan membatasi proses pencarian tentang bukti digital yang berhubungan dengan aplikasi Skype Messenger. Hasil analisis dari *tools* forensik yang digunakan pada penelitian ini adalah sebagai berikut:

***Analysis* menggunakan Oxygen Forensic Suite**

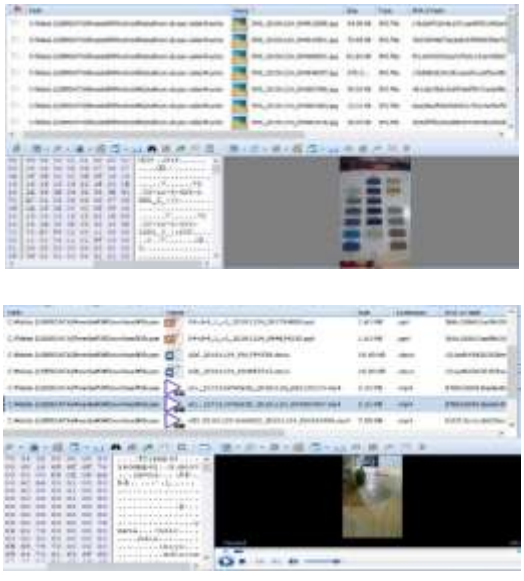
Hasil analisis data menggunakan Oxygen Forensic Suite berhasil menemukan bukti digital berupa informasi akun, kontak person, percakapan, gambar dan video. Adapun tampilan hasil bukti digital menggunakan Oxygen Forensic Suite yang ditemukan seperti yang dipaparkan pada Gambar 9, Gambar 10, Gambar 11, dan Gambar 12.



Gambar 9. Bukti digital informasi akun dari Oxygen Forensic Suite



Gambar 10. Bukti digital Kontak Persondan percakapan dari Oxygen Forensic Suite



Gambar 11 Bukti digital Gambar dan Video

JURNAL MAHAJANA INFORMASI
e-ISSN 2527 – 8290
Vol. 8 No. 2, Desember 2023, Hal. 80 - 88

dari Oxygen Forensic Suite

***Analysis* menggunakan MOBILedit Forensic Express**

Hasil analisis data menggunakan MOBILedit Forensic Express dan SQLite Database Browser Portable untuk membaca file database yang ditemukan telah berhasil menemukan bukti digital berupa informasi akun, kontak person, percakapan, dan gambar. Adapun tampilan hasil bukti digital menggunakan MOBILedit Forensic yang ditemukan seperti yang dipaparkan pada Gambar 12, Gambar 13, dan Gambar 14.

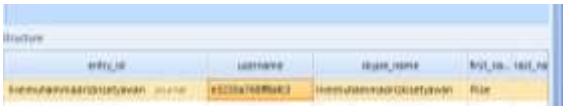
Gambar 12. Bukti digital informasi akun menggunakan SQLite Database Browser

Gambar 13. Bukti digital kontak person dari MOBILedit Forensic Express

Gambar 14. Bukti digital percakapan dan gambar dari MOBILedit Forensic Express

***Analysis* menggunakan Belkasoft Evidence Center**

Hasil analisis data menggunakan Belkasoft Evidence Center berhasil menemukan bukti digital berupa informasi akun, kontak person, percakapan, gambar dan video. Adapun tampilan bukti digital yang ditemukan menggunakan MOBILedit Forensic yang ditemukan seperti yang dipaparkan pada Gambar 15, Gambar 16, fsm Gambar 17.



Gambar 15 Bukti digital informasi akun dari Belkasoft Evidence Center

Gambar 16 Bukti digital kontak person dan percakapan dari Belkasoft Evidence Center

JURNAL MAHAJANA INFORMASI
e-ISSN 2527 – 8290
Vol. 8 No. 2, Desember 2023, Hal. 80 - 88

Gambar 17 Bukti digital Gambar dan Video dari Belkasoft Evidence Center

Reporting

Pada tahap ini, dilakukan penyusunan laporan dan presentasi hasil laporan yang mencakup hasil analisis tools forensik dalam menemukan bukti digital. Perbandingan hasil analisis dari masing-masing tools forensik disajikan dalam Tabel 3.

Tabel 3. Perbandingan hasil analisis dari ketiga tool forensik

Bukti Digital	Data Asli	Tools Forensik: Oxygen Forensic Suite	Tools Forensik: MOBILedit Forensic Express	Tools Forensik: Belkasoft Evidence Center
Informasi Akun	1	1	1	1
Kontak Person	19	19	19	19
Percakapan	52	42	42	42
Gambar	9	9	9	9
Video	3	0	0	3
Total	**84**	**71**	**71**	**74**

Selanjutnya dilakukan pengukuran kemampuan setiap tools forensik dalam menemukan bukti digital. Untuk mengukur ini, digunakan indeks akurasi yang dihitung dengan menggunakan rumus berikut (Umar et al., 2022) :

a. Perhitungan indeks akurasi Oxygen Forensic Suite:

$$Po = \frac{84}{81} \text{x } 100\% = 98\%$$

b. Perhitungan indeks akurasi Belkasoft Evidence Center:

$$Po = \frac{84}{74} \text{x } 100\% = 88\%$$

c. Perhitungan indeks akurasi MOBILedit Forensic Express:

$$Po = \frac{84}{71} x\ 100\% = 84\%$$

Berdasarkan perhitungan indeks akurasi, ditemukan bahwa Oxygen Forensic Suite memiliki kemampuan yang berhasil dalam mendapatkan bukti digital dengan nilai indeks sebesar 98%. Belkasoft Evidence Center mendapatkan bukti digital dengan nilai indeks 88%, sedangkan MOBILedit Forensic Express berhasil mendapatkan bukti digital dengan nilai indeks 84%.

KESIMPULAN DAN SARAN

Dari hasil diatas dapat disimpulkan bahwa dengan menggunakan framework NIST dan 3 tools forensik berupa Oxygen Forensic Suite, Belkasoft Evidence Center, MOBILedit Forensic Express berhasil menemukan bukti digital terkait informasi aktivitas pada aplikasi Skype. Bukti digital tersebut meliputi akun pengguna, daftar kontak, percakapan, gambar, dan video yang terkait dengan penggunaan aplikasi Skype. Kemudian dari hasil perhitungan indeks akurasi didapatkan Oxygen Forensic Suite memiliki kinerja terbaik dalam menemukan bukti digital dengan nilai indeks sebesar 98%., diikuti oleh Belkasoft Evidence Center dengan nilai indeks 88%, dan MOBILedit Forensic Express dengan nilai indeks 84%.

DAFTAR PUSTAKA

Anton Yudhana, Abdul Fadlil, & Setyawan, M. R. (2020). Analysis of Skype Digital Evidence Recovery based on Android Smartphones Using the NIST Framework. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(4), 682–690. https://doi.org/10.29207/resti.v4i4.2093

Fadillah, M. N., Rusydi, U., & Yudhana, A. (2022). Analisis Forensik Aplikasi Dompet Digital Pada Smartphone Android Menggunakan Metode DFRWS. *Kumpulan JurnaL Ilmu Komputer (KLIK)*, *09*(02), 265–278.

Fanani, G., Riadi, I., & Yudhana, A. (2022). Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop. *Jurnal Media Informatika Budidarma*, *6*(2), 1263. https://doi.org/10.30865/mib.v6i2.3946

Hikmatyar, F. G., & Sugiantoro, B. (2019). Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases. *International Journal on Informatics for Development (IJID)*, *7*(2), 19. https://doi.org/10.14421/ijid.2018.07204

Mualfah, D., Viransa, A., & Amran, H. F. (2021). Akuisisi Bukti Digital Pada Aplikasi Tamtam Messenger Menggunakan Metode National Institute of Justice. *Journal of Software Engineering and Information Systems*, *3*(1). https://doi.org/10.37859/seis.v3i1.4548

Nafila, F. L., & Prayudi, Y. (2022). Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android Menggunakan metode NIST. *Jurnal Sains Komputer & Informatika (J-SAKTI)*, *6*(1), 532–543. http://ejurnal.tunasbangsa.ac.id/index.php/jsakti/article/view/466

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

Riadi, I., & Nasrulloh, I. M. (2019). 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)*, *6*(5), 509–518. https://doi.org/10.25126/jtiik.201961516

Riadi, I., Sunardi, S., & Sahiruddin. (2020). Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *7*(1), 197–204. https://doi.org/10.25126/jtiik.202071921

Riadi, I., Umar, R., & Aziz, M. A. (2019). Forensik Web Layanan Instant Messaging Menggunakan Metode Association of Chief Police Officers (ACPO). *Mobile and Forensics*, *1*(1), 30. https://doi.org/10.12928/mf.v1i1.705

Rizki Setyawan, M., Hermansa, H., & Fadli Hasa, M. (2022). Analisis Forensik Digital Pada Skype Berbasis Windows 10 Menggunakan Framework ACPO. *Jurnal Ilmiah Betrik*, *13*(2), 111–119. https://doi.org/10.36050/betrik.v13i2.469

Setyawan, M. R., Yudhana, A., & Fadlil, A. (2019). Akuisisi Data Pada Skype Messenger Menggunakan Metode National Institute Of Justice. *SYSTEMIC : Information System and Informatics*

Journal., *5*(2), 13–18. https://doi.org/10.29080/systemic.v5i2.724

Umar, R., Yudhana, A., & Fadillah, M. N. (2022). Perbandingan Tools Forensik Pada Aplikasi Dompet Digital. *JIKO (Jurnal Informatika Dan Komputer)*, *6*(2), 242. https://doi.org/10.26798/jiko.v6i2.621

Yudhana, A., Riadi, I., & Zuhriyanto, I. (2019). Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS). *TECHNO*, *20*(2), 125–130. https://doi.org/10.30595/techno.v20i2.4594

Zuhriyanto, I., Yudhana, A., & Riadi, I. (2020). Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop. *JURNAL RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(5), 829–836. https://doi.org/10.29207/resti.v4i5.2152