



Peran Forensik *Smartphone* dalam Mengungkap Jejak Digital Transaksi Pencucian Uang Elektronik

Rafika Aprilia^{1*}, Yunan Prasetyo Kurniawan²

^{1,2}Fakultas Hukum, Universitas Pancasila, Indonesia

Email : rafikaap5223029@univpancasila.ac.id¹, yanprasetyo@univpancasila.ac.id²

Korespondensi penulis: rafikaap5223029@univpancasila.ac.id*

Abstract. Electronic money laundering has become a critical issue as a form of cybercrime. Advances in technology demonstrate that digital forensic applications, particularly those utilizing smartphones, can be employed to uncover digital traces of money laundering transactions. This study aims to analyze the relevance of existing legal frameworks, the effectiveness of smartphone forensic techniques, and the challenges faced in their implementation in Indonesia. Based on a review of the literature and regulatory analysis, it was found that legal frameworks such as UU No. 8 of 2010 on the Prevention and Eradication of Money Laundering (TPPU) and UU No. 19 of 2016 on Information and Electronic Transactions (ITE) provide an adequate legal foundation. However, gaps in implementation, such as limited human and technological resources, remain significant obstacles. Forensic techniques, including metadata analysis and device extraction, have shown great potential in identifying the flow of illicit funds. Nonetheless, their application is hindered by data confidentiality and the lack of uniform technical standards. Given the increasing complexity of digital crimes, an integrated approach is required, combining regulatory strengthening with technological capacity building, to enhance the effectiveness of smartphone forensics in addressing electronic money laundering.

Keywords: digital transaction, electronic money laundering, smartphone forensic.

Abstrak. Pencucian uang elektronik menjadi permasalahan yang krusial sebagai salah satu bentuk kejahatan siber. Perkembangan teknologi menunjukkan bahwa aplikasi digital forensik terutama menggunakan smartphone dapat digunakan untuk mengungkap jejak digital transaksi pencucian dana tersebut. Studi ini bertujuan menganalisis relevansi kerangka hukum yang ada, efektivitas teknik forensik smartphone, serta kendala yang dihadapi dalam penerapan teknik tersebut di Indonesia. Berdasarkan kajian literatur dan analisis regulasi, ditemukan bahwa kerangka hukum seperti UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU) dan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) telah menyediakan dasar hukum yang memadai. Namun, celah dalam implementasi, seperti keterbatasan sumber daya manusia dan teknologi, menjadi hambatan utama. Teknik forensik seperti analisis metadata dan ekstraksi perangkat telah menunjukkan potensi besar dalam mengidentifikasi alur dana ilegal, tetapi penerapannya terbatas oleh kerahasiaan data dan kurangnya standar teknis yang seragam. Dengan meningkatnya kompleksitas kejahatan digital, dibutuhkan pendekatan yang terintegrasi antara penguatan regulasi dan pengembangan kapasitas teknologi untuk meningkatkan efektivitas forensik smartphone dalam penanganan pencucian uang elektronik.

Kata Kunci: transaksi digital, pencucian uang elektronik, forensik smartphone.

I. PENDAHULUAN

Kemajuan teknologi digital telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk sektor keuangan. Salah satu inovasi yang terus berkembang pesat adalah uang elektronik (*e-money*), yang memungkinkan masyarakat melakukan transaksi dengan mudah dan cepat melalui perangkat digital, seperti *smartphone*. Indonesia, sebagai salah satu negara dengan tingkat adopsi teknologi tinggi, mencatat pertumbuhan signifikan dalam penggunaan uang elektronik. Data Bank Indonesia menunjukkan bahwa nilai transaksi uang

elektronik di Indonesia meningkat secara eksponensial selama beberapa tahun terakhir, mencerminkan transformasi masyarakat ke arah digitalisasi keuangan.

Namun, di balik kemudahan yang ditawarkan, perkembangan ini juga membuka celah bagi aktivitas kejahatan finansial, seperti pencucian uang. Dalam praktiknya, pencucian uang menggunakan uang elektronik sering kali melibatkan transfer dana melalui aplikasi digital yang dirancang untuk menyembunyikan identitas pelaku dan asal-usul dana ilegal. Beberapa faktor, seperti anonimitas yang diberikan oleh platform digital, lemahnya implementasi prosedur *Know Your Customer* (KYC), serta kurangnya pengawasan yang komprehensif, telah dimanfaatkan oleh pelaku untuk menjalankan aksi kejahatan. Tantangan ini semakin kompleks dengan meningkatnya volume dan variasi transaksi digital.

Dalam konteks ini, teknologi forensik, khususnya forensik *smartphone*, memainkan peran yang sangat krusial dalam membantu otoritas hukum mengungkap jejak digital yang ditinggalkan oleh pelaku. Forensik *smartphone* adalah cabang dari digital forensik yang berfokus pada pengumpulan, analisis, dan interpretasi data yang tersimpan di perangkat *mobile*, seperti komunikasi melalui pesan instan, log transaksi keuangan, hingga penggunaan aplikasi. Dengan menggunakan teknik analisis data yang canggih, forensik *smartphone* mampu mengidentifikasi pola transaksi yang mencurigakan dan menghubungkannya dengan aktivitas ilegal.

Studi kasus di Indonesia menunjukkan relevansi dan pentingnya penerapan forensik *smartphone* dalam menangani kasus pencucian uang elektronik. Pada 2021, Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) mengungkap modus pencucian uang menggunakan mata uang kripto, seperti Bitcoin. Modus ini digunakan dalam berbagai tindak pidana, termasuk korupsi dan kejahatan siber seperti *scamming* dan *ransomware*. PPATK menyebutkan bahwa penggunaan aset kripto sebagai media pencucian uang telah menjadi ancaman yang terus berkembang di Indonesia sejak 2015.

Selain itu, modus pencucian uang dengan teknik *smurfing* dan *structuring* telah menjadi perhatian utama otoritas keuangan. *Smurfing* melibatkan pemecahan transaksi keuangan dalam jumlah kecil untuk menghindari deteksi, sedangkan *structuring* adalah pengaturan sistematis transaksi agar terlihat normal dalam sistem keuangan. Modus ini sering memanfaatkan platform digital seperti dompet elektronik (*e-wallet*) atau rekening mule dengan identitas palsu untuk memindahkan dana secara terkoordinasi, sehingga menyulitkan pelacakan. Laporan PPATK menunjukkan peningkatan tren ini, terutama dalam konteks kejahatan berbasis teknologi, yang memperkuat kebutuhan akan kerangka regulasi dan teknologi anti-pencucian uang yang lebih efektif.

Dengan latar belakang tersebut, penelitian ini bertujuan untuk mengkaji peran forensik *smartphone* dalam mengungkap jejak digital pada kasus pencucian uang elektronik di Indonesia. Fokus penelitian akan mencakup teknik forensik yang digunakan, tantangan yang dihadapi dalam pengumpulan dan analisis data digital, serta implikasi hukum dalam penanganan kasus semacam ini. Harapannya, penelitian ini tidak hanya memberikan wawasan akademis tetapi juga kontribusi praktis bagi penegakan hukum di era digital yang terus berkembang.

2. METODE PENELITIAN

Penelitian ini dikaji berdasarkan studi literatur dan bersifat normatif dengan mengacu pada sumber hukum undang-undang. Metode penelitian ini dilakukan untuk membangun landasan teoretis dan memahami konteks hukum serta teknis terkait penerapan forensik *smartphone* dalam investigasi kasus pencucian uang elektronik. Penelitian ini dimulai dengan mengidentifikasi dan menganalisis sumber hukum primer, seperti kajian undang-undang terkait permasalahan tersebut serta peraturan mengenai sistem pembayaran yang dikeluarkan oleh Bank Indonesia. Literatur sekunder, termasuk artikel jurnal, laporan dari Satgas Waspada Investasi, dan panduan teknis forensik digital, digunakan untuk melengkapi pemahaman terhadap tantangan praktis dan metode yang digunakan. Studi literatur ini juga diarahkan untuk mengidentifikasi celah penelitian yang ada, seperti keterbatasan regulasi dan hambatan teknis, guna memberikan kontribusi ilmiah dan praktis dalam pengembangan forensik digital sebagai alat investigasi hukum.

3. HASIL DAN PEMBAHASAN

Dasar Hukum Penerapan Forensik *Smartphone*

Analisis terhadap kerangka regulasi di Indonesia menunjukkan bahwa penggunaan forensik *smartphone* dalam investigasi kasus pencucian uang elektronik memiliki dasar hukum yang kuat, meskipun tantangan teknis dan implementasi masih memerlukan perhatian lebih lanjut. Beberapa undang-undang yang relevan telah mendukung upaya ini, baik dari aspek pengakuan alat bukti elektronik maupun prosedur penegakan hukum yang melibatkan data digital.

- a. Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU)

UU ini memberikan landasan hukum yang komprehensif untuk memberantas tindak pidana pencucian uang, termasuk transaksi berbasis uang elektronik. Pasal 3 hingga Pasal 5 menegaskan bahwa upaya penyamaran atau penyembunyian dana hasil tindak pidana dapat

dikenakan sanksi pidana berat. Dalam konteks teknologi forensik, penggunaan *smartphone* sebagai sumber data transaksi mencurigakan memberikan peluang signifikan untuk mengungkap pola aktivitas keuangan yang sulit dilacak secara manual. Regulasi ini memberikan legitimasi kepada otoritas penegak hukum untuk mengakses dan menganalisis data transaksi elektronik sebagai bagian dari upaya investigasi.

b. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya (UU Nomor 19 Tahun 2016)

UU ITE menegaskan pentingnya dokumen elektronik sebagai alat bukti yang sah di pengadilan (Pasal 5), sehingga hasil analisis forensik digital dari *smartphone* dapat diakui secara hukum. Selain itu, Pasal 44 memberikan kewenangan kepada aparat penegak hukum untuk mengakses data elektronik yang relevan dengan tindak pidana, termasuk perangkat digital seperti *smartphone*. Aspek ini sangat penting dalam mengintegrasikan temuan forensik ke dalam sistem peradilan pidana, sekaligus memberikan kerangka hukum yang memastikan data digital diproses sesuai prosedur yang berlaku.

c. Undang-Undang Nomor 18 Tahun 2017 Tentang Perlindungan Data Pribadi (UU PDP)

UU ini berperan dalam mengatur penggunaan data pribadi selama proses investigasi. Pasal 58 memperbolehkan akses data oleh penegak hukum dengan syarat mematuhi prinsip transparansi, akuntabilitas, dan keamanan. Meskipun memberikan perlindungan terhadap privasi individu, regulasi ini tetap memungkinkan penegak hukum untuk memanfaatkan data digital dari perangkat *smartphone* yang terkait dengan tindak pidana pencucian uang, dengan catatan bahwa proses pengambilan data dilakukan secara sah dan bertanggung jawab.

d. Undang-Undang Nomor 3 Tahun 2011 Tentang Transfer Dana

UU tersebut melengkapi upaya investigasi dengan mewajibkan penyelenggara sistem pembayaran untuk melaporkan transaksi mencurigakan ke Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) sesuai Pasal 7. Selain itu, Pasal 18 memberikan kewenangan kepada otoritas untuk memeriksa catatan transaksi yang relevan. Data yang diperoleh dari sistem pembayaran elektronik ini dapat diintegrasikan dengan hasil analisis forensik *smartphone*, memberikan gambaran lebih lengkap tentang pola transaksi yang mencurigakan.

Hasil analisis tersebut menunjukkan bahwa kerangka hukum di Indonesia telah mengakomodasi kebutuhan untuk mengintegrasikan teknologi forensik dalam investigasi kejahatan finansial, khususnya pencucian uang elektronik. Namun, keberhasilan implementasi sangat bergantung pada pemahaman mendalam tentang prosedur hukum oleh penyidik serta kesiapan teknologi yang digunakan dalam analisis forensik. Selain itu, peningkatan kapasitas

sumber daya manusia dan infrastruktur teknologi menjadi langkah strategis untuk mendukung optimalisasi penerapan forensik *smartphone*.

Penerapan Teknik Forensik *Smartphone* di Indonesia

Perkembangan teknologi forensik digital di Indonesia telah membuka peluang signifikan dalam penanganan tindak pidana pencucian uang elektronik. Forensik *smartphone* menjadi salah satu alat utama yang digunakan oleh aparat penegak hukum untuk menganalisis jejak digital yang tersimpan dalam perangkat pelaku. Teknik ini memanfaatkan berbagai metode, mulai dari ekstraksi data hingga rekonstruksi aktivitas digital, untuk mendukung pembuktian hukum.

a. Ekstraksi Data *Smartphone*

Ekstraksi data adalah langkah awal dalam proses forensik *smartphone*, yang bertujuan untuk memperoleh salinan lengkap data dari perangkat. Di Indonesia, alat seperti *Cellebrite UFED* dan *Oxygen Forensic Suite* telah digunakan secara luas oleh aparat penegak hukum, termasuk Direktorat Tindak Pidana Siber Bareskrim Polri. Melalui perangkat ini, data seperti log panggilan, pesan teks, riwayat penelusuran, serta informasi aplikasi keuangan dapat diekstraksi untuk dianalisis lebih lanjut. Sebagai contoh, dalam sebuah kasus pencucian uang yang melibatkan aplikasi dompet elektronik pada tahun 2022, ekstraksi data memungkinkan PPATK melacak transaksi mencurigakan yang sebelumnya tidak terdeteksi melalui laporan perbankan reguler.

b. Analisis Metadata dan Geolokasi

Metadata dari perangkat *smartphone*, seperti waktu, lokasi, dan identitas perangkat, memainkan peran penting dalam investigasi pencucian uang elektronik. Metadata ini dapat digunakan untuk melacak pola transaksi mencurigakan yang sering kali melibatkan berbagai lokasi geografis sebagai upaya untuk menyamarkan jejak dana. Sebagai contoh, metadata menjadi alat kunci dalam mengidentifikasi sindikat internasional yang menggunakan beberapa perangkat dan lokasi untuk mentransfer dana secara ilegal. Penggunaan metadata juga diterapkan dalam investigasi yang melibatkan aplikasi dompet elektronik, di mana lokasi transaksi yang terekam membantu mengungkap jaringan kejahatan yang tersebar di berbagai wilayah di Indonesia.

c. Analisis Aplikasi Keuangan dan Jejak Digital

Aplikasi keuangan seperti dompet elektronik dan layanan perbankan digital menjadi target utama dalam analisis forensik *smartphone*. Analisis ini mencakup identifikasi transaksi mencurigakan, seperti transfer dana ke rekening anonim, penggunaan akun palsu, atau pola aktivitas yang tidak wajar. Dalam sebuah studi kasus, PPATK berhasil mengidentifikasi

transaksi mencurigakan senilai miliaran rupiah yang melibatkan beberapa aplikasi dompet elektronik populer melalui teknik ini. Analisis jejak digital juga melibatkan penelusuran data log dari aplikasi tersebut untuk menentukan frekuensi transaksi, jumlah dana, dan penerima, yang menjadi dasar pembuktian hukum.

d. Rekonstruksi Jejak Digital

Rekonstruksi jejak digital dilakukan untuk menyusun kembali urutan aktivitas digital yang telah dihapus atau disembunyikan oleh pelaku. Teknik ini menggunakan perangkat lunak canggih yang dapat memulihkan data yang hilang, termasuk riwayat pesan terenkripsi dan file yang telah dihapus. Di Indonesia, teknik ini diterapkan dalam kasus pencucian uang yang melibatkan aplikasi *peer-to-peer lending ilegal*, dimana data yang telah dihapus oleh pelaku berhasil direkonstruksi untuk mengungkap aliran dana yang digunakan dalam aktivitas pencucian uang.

Tantangan Penerapan Forensik Smartphone pada Pencucian Uang Elektronik

Forensik *smartphone* telah menjadi salah satu pendekatan krusial dalam investigasi kejahatan siber, termasuk pencucian uang elektronik. Namun, implementasinya di Indonesia menghadapi berbagai tantangan multidimensional yang melibatkan aspek teknologi, sumber daya manusia, regulasi, serta kompleksitas modus operandi kejahatan.

a. Keterbatasan Teknologi dan Infrastruktur

Teknologi forensik yang digunakan untuk menganalisis data *smartphone* sering kali bersifat kompleks dan memerlukan alat canggih. Sebagian besar teknologi ini, seperti perangkat *Cellebrite UFED* atau *Magnet AXIOM*, merupakan produk impor dengan biaya tinggi, yang membatasi penggunaannya pada lembaga tertentu. Selain itu, enkripsi perangkat dan aplikasi modern semakin kompleks, sehingga memerlukan perangkat lunak dekripsi yang lebih canggih untuk mendapatkan data yang relevan. Di Indonesia, akses terhadap teknologi ini masih terbatas pada beberapa lembaga penegak hukum, yang menyebabkan kesenjangan dalam efektivitas investigasi antarwilayah.

b. Keterbatasan Keahlian Sumber Daya Manusia

Penerapan forensik digital membutuhkan tenaga ahli dengan keterampilan tinggi dalam menangani perangkat lunak dan perangkat keras forensik. Indonesia masih menghadapi keterbatasan tenaga ahli di bidang ini. Pelatihan forensik digital di tingkat nasional masih belum merata, terutama untuk personel di luar pusat-pusat metropolitan. Hal ini menjadi hambatan signifikan, mengingat kejahatan pencucian uang sering kali melibatkan transaksi lintas wilayah yang memerlukan investigasi koordinatif.

c. Regulasi dan Privasi Data

Regulasi yang berkaitan dengan pengumpulan dan analisis data digital sering kali menjadi tantangan dalam proses penyelidikan. Di satu sisi, investigasi forensik membutuhkan akses penuh terhadap data pribadi pengguna *smartphone*, tetapi di sisi lain, regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) mengatur batasan yang ketat terhadap akses tersebut. Batasan ini, jika tidak diimbangi dengan prosedur pengambilan data yang tepat, dapat menyebabkan bukti yang diperoleh dianggap tidak sah di pengadilan.

d. Kompleksitas Teknologi Keuangan Modern

Pencucian uang elektronik memanfaatkan kemajuan teknologi keuangan, seperti dompet elektronik, *peer-to-peer lending*, dan mata uang kripto, yang dirancang untuk menyembunyikan aliran dana secara efektif. Transaksi berbasis mata uang kripto, misalnya, menggunakan sifatnya yang pseudonim untuk menyulitkan pelacakan forensik. Selain itu, transaksi mikro dengan frekuensi tinggi yang melibatkan beberapa perangkat di lokasi berbeda memperumit proses analisis data digital.

e. Kurangnya Integrasi Antarinstansi

Investigasi yang melibatkan forensik *smartphone* memerlukan koordinasi antarinstansi, seperti kepolisian, otoritas keuangan, dan regulator teknologi informasi. Namun, kurangnya integrasi sistem dan komunikasi antarinstansi sering kali menyebabkan fragmentasi data investigasi, yang menghambat proses penyelesaian kasus. Integrasi antarinstansi mampu mempercepat dan mempermudah proses forensik *smartphone*, sehingga kasus-kasus pencucian uang elektronik dapat teratasi dengan lebih efektif.

Tantangan penerapan forensik *smartphone* pada pencucian uang elektronik di Indonesia menunjukkan perlunya pendekatan multidimensional untuk meningkatkan efektivitasnya. Diperlukan investasi dalam pengembangan teknologi lokal, pelatihan intensif untuk sumber daya manusia, dan penguatan kerangka kerja kolaborasi antarinstansi. Selain itu, revisi regulasi yang memungkinkan pengumpulan data forensik dengan tetap memperhatikan aspek privasi pengguna dapat memberikan keseimbangan antara efektivitas investigasi dan perlindungan hak asasi manusia.

4. KESIMPULAN

Berdasarkan hasil kajian literatur dalam studi ini, forensik *smartphone* memainkan peran yang sangat vital dalam upaya pengungkapan tindak pidana pencucian uang elektronik di Indonesia. Dengan meningkatnya penggunaan teknologi digital dan platform keuangan elektronik, perangkat *smartphone* sering kali menjadi sumber bukti yang krusial dalam proses investigasi. Teknik-teknik forensik digital, seperti ekstraksi data dari perangkat, analisis

metadata, dan rekonstruksi jejak transaksi, memungkinkan pihak berwenang untuk mengidentifikasi aliran dana yang terkait dengan aktivitas ilegal. Meskipun demikian, penerapan forensik *smartphone* di Indonesia menghadapi beberapa kendala, termasuk terbatasnya infrastruktur teknologi dan sumber daya manusia yang terlatih di bidang ini. Selain itu, meskipun sudah ada regulasi yang mengatur tindak pidana pencucian uang, seperti UU No. 8 Tahun 2010 dan UU No. 19 Tahun 2016, implementasi regulasi tersebut masih sering terkendala oleh kurangnya pemahaman teknis di lapangan dan tantangan dalam pengelolaan data elektronik yang sangat terdistribusi. Selain itu, investigasi forensik juga memiliki keterbatasan akses terhadap data pengguna karena dilindungi oleh UU PDP. Oleh karena itu, untuk memperkuat upaya pemberantasan pencucian uang elektronik, diperlukan peningkatan kapasitas teknologi forensik digital, penguatan kerjasama lintas lembaga, serta penyesuaian regulasi agar lebih responsif terhadap perkembangan teknologi keuangan dan kejahatan digital yang terus berkembang.

DAFTAR PUSTAKA

Buku

Sulistiyani, E., & Mardiansyah (Ed.). (2022). *Laporan tahunan: Budaya Indonesia mendunia, menyambut keanggotaan FATF*. Jakarta: Pusat Pelaporan dan Analisis Transaksi Keuangan.

Jurnal

Lee, S. Y. (2022). Mobile digital forensics framework to increase security level of for smartphone user. *Journal of Logistics, Informatics and Service Science*, 9(1), 68–84. <https://doi.org/10.33168/LISS.2022.0106>

Pandey, A. K., Tripathi, A. K., Kapil, G., Singh, V., Khan, M. W., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Current challenges of digital forensics in cyber security. In *Critical Concepts, Standards, and Techniques in Cyber Forensics* (pp. 31–46). <https://doi.org/10.4018/978-1-7998-1558-7.ch003>

Pongpaichet, S., Sukosit, B., Duangtanawat, C., Jamjongdamrongkit, J., Mahacharoensuk, C., Matangkarat, K., Singhajan, P., Noraset, T., & Tuarob, S. (2016). CAMELON: A system for crime metadata extraction and spatiotemporal visualization from online news articles. *IEEE Access*, 4, 1–27. <https://doi.org/10.1109/ACCESS.2024.3363879>

Prendi, L., Borakaj, D., & Prendi, K. (2023). The new money laundering machine through cryptocurrency: Current and future public governance challenges. *Corporate Law and Governance Review*, 5(2), 84–91. <https://doi.org/10.22495/clgrv5i2p9>

Tara, H., & Mishra, A. (2021). A comparative study of digital forensic tools for data extraction from electronic devices. *Journal of Punjab Academy of Forensic Medicine and Toxicology*, 21(1), 97–104. <https://doi.org/10.5958/0974-083X.2021.00016.9>

Makalah

Ginting, Y. P., & Indradewi, A. A. (2021). Transaksi keuangan mencurigakan dari uang elektronik pada masa pandemi Covid-19. Dalam *Seminar Nasional Hukum Universitas Negeri Semarang*, Semarang, 27 Juli 2021. <https://doi.org/10.15294/snunes.v7i2.724>

Regulasi

Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana.

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, beserta perubahannya (UU No. 19 Tahun 2016).

Undang-Undang Nomor 18 Tahun 2017 tentang Perlindungan Data Pribadi.

Website

Aditya, N. R., & Hakim, R. N. (2021, April 22). Penjelasan lengkap PPATK soal modus cuci uang lewat Bitcoin. *Kompas.com*.
<https://nasional.kompas.com/read/2021/04/22/16410731/penjelasan-lengkap-ppatk-soal-modus-cuci-uang-lewat-bitcoin>

Jannah, F. Z. (2023). Kejahatan keuangan dalam pembayaran digital. *Bank Indonesia*.
<https://www.bi.go.id/bi-institute/BI-Epsilon/Pages/Kejahatan-Keuangan-Dalam-Pembayaran-Digital.aspx>

Rahayu, R. (2023). 5 tindak pidana pencucian uang terbesar di Indonesia, PPATK duga capai Rp 183,88 T. *Tempo.co*. <https://www.tempo.co/ekonomi/5-tindak-pidana-pencucian-uang-terbesar-di-indonesia-ppatk-duga-capai-rp-183-88-t-218736>

Tobing, T. L. (2019). Satgas Waspada Investasi apresiasi upaya penegakan hukum fintech ilegal. *OJK*. <https://www.ojk.go.id/waspada-investasi/id/siaran-pers/Pages/Satgas-Waspada-Investasi-Apresiasi-Upaya-Penegakan-Hukum-Fintech-Ilegal.aspx>