HYBRID ACQUISITION PADA FORENSIK DIGITAL BERBASIS ISO/IEC 27037:2012 MENGGUNAKAN PORT MIRRORING DAN SINGLE BOARD COMPUTER

Dedy Hariyadi [1*], Muhammad Agung nugroho [2], Chanief Budi Setiawan [3], Arief Ikhwan Wicaksono [4]

[1,3,4] Teknologi Informasi Universitas Jendral Achmad Yani Yogyakarta
[2] Informatika Universitas Teknologi Digital Indonesia
email : dedy@unjaya.ac.id[1], m.agung.n@utdi.ac.id[2] , chanief.b.s@gmail.com[3], ariefikhwanwicaksono@gmail.com[4]

Abstraksi

Badan Siber dan Sandi Negara (BSSN) memaparkan bahwa Indonesia memiliki anomali lalu lintas sebesar 1,6 Miliar. Anomali lalu lintas terbesar berasal dari BotNet. Hal ini termasuk dalam kejahatan dunia maya dengan kategori kejahatan komputer karena pelaku dan korban berada dalam sistem dan jaringan komputer. Untuk menyelidiki kejahatan dunia maya, pendekatan forensik jaringan dapat digunakan dengan memperoleh bukti digital berupa lalu lintas jaringan. Tidak hanya lalu lintas jaringan yang diperoleh dengan menggunakan tangkapan lalu lintas jaringan, tetapi juga menggunakan perangkat berbiaya rendah seperti Raspberry Pi. Maka pada artikel ini diusulkan akuisisi hybrid yaitu melakukan akuisisi parsial pada sisi perangkat Router dalam hal ini Router Mikrotik dan akuisisi fisik pada kartu memori Raspberry Pi yang berfungsi untuk merekam sistem pendeteksi trafik berbahaya. Metode akuisisi hybrid sangat cocok diterapkan pada sistem komputer dan jaringan untuk menyelidiki kejahatan dunia maya, seperti anomali lalu lintas, cryptomining, pencuri malware, dan pembobolan data.

***Kata Kunci*:**

Cybercrime, Digital Forensics, Network Forensics, Hybrid Acquisition, Router

Abstract

Based on the records of the Badan Siber dan Sandi Negara (BSSN) that Indonesia has a traffic anomaly of 1.6 Billion. The largest traffic anomaly comes from BotNet. This is included in the cybercrime with the category of computer crime because the perpetrators and victims are located in computer systems and networks. To investigate cybercrimes, a network forensics approach can be used by acquiring digital evidence in the form of network traffic. Not only network traffic is acquired using network traffic capture, but also using low-cost devices such as the Raspberry Pi. So in this article a hybrid acquisition is proposed, which is to do a partial acquisition on the side of the Router device in this case the Mikrotik Router and physical acquisition on the Raspberry Pi memory card which functions to record the malicious traffic detection system. The hybrid acquisition method is very suitable to be applied to computer systems and networks to investigate cybercrime, such as traffic anomalies, cryptomining, malware stealer, and data.

***Keywords*:**
Cybercrime, Digital Forensics, Network Forensics, Hybrid Acquisition, Router

Pendahuluan

Peningkatan jumlah pengguna internet sebagai dampak dari perkembangan teknologi informasi memiliki potensi-pontensi bersifat negatif seperti kejahatan di ruang siber [1]. Berdasarkan survey di Indonesia oleh Asosiasi Penyelenggara Jasa Internet Indonesia menunjukan bahwa pengguna internet di Indonesia mengalami peningkatan dari tahun ke tahun [2]. Salah satu melakukan deteksi kejahatan di ruang siber, pada penelitian sebelumnya dilakuan dengan melakukan deteksi pada sisi sistem dan jaringan komputer yang disebut intrusion detection system (IDS). Pada IDS memiliki 2 model deteksi, yaitu *signature-based* dan *anomaly-based* [3].
Artikel yang ditulis peneliti dari American University bahwa seoerang Chief Executive Office, Chief Privacy Officer, dan Chief Information Officer harus memahami fase pada serangan siber atau cyber security seperti sebelum, saat kejadian dan setelah insiden terjadi [4]. Dengan terpasangnya IDS pada sistem dan jaringan komputer merupakan implementasi dari fase sebelum terjadi serangan siber [5]. Selain itu IDS dapat dimanfaatkan sebagai upaya pemantauan instrusi secara live sebagai implementasi dari fase saat kejadian serangan siber [6].

Berbagai upaya dan penelitian telah dilakukan untuk deteksi terhadap kejahatan siber yang memanfaatkan sistem dan jaringan komputer. Pada penelitian sebelumnya IDS masih digunakan sebagai upaya mengetahui serangan siber pada fase-fase sebelum dan saat kejadian insiden siber [7]. Peneliti dari Telkom University melakukan implementasi

pencegahan serangan *malware* pada Dinas Komunikasi dan Informatika Pemerintah Kabupaten Subang dengan melakukan deteksi dan mengkombinasikan *fail2ban*. Teknik mendeteksi serangan malware dengan melakukan deteksi *malicious traffic* pada sistem dan jaringan komputer seluruh infrastruktur Pemerintah Kabupaten Subang [8][9]. Implementasi dari sistem deteksi *malicious traffic* juga dilakukan peneliti dari Institut Pertanian Bogor sebagai upaya pencegahan kejahatan siber berupa serangan malware pada sistem dan jaringan komputer. Bentuk implementasinya yaitu dengan pemasangan aplikasi berbasis *Open Source*, Maltrails pada sistem dan jaringan kompute. Pihak McAfee sebagai vendor layanan keamanan siber juga memanfaatkan Maltrails diintergrasikan dengan *Security Information and Event Management* (SIEM) sebagai langkah strategi dalam melakukan *Threat Hunting* [10].

Berdasarkan penelitian sebelumnya IDS menggunakan Maltrails masih dimanfaatkan sebagai upaya implementasi dari keamanan siber pada fase sebelum dan saat kejadian siber. Hal tersebut belum melakukan langkah-langkah mitigasi sebagai upaya tindak lanjut setelah kejadian siber, yaitu menggunakan pendekatan forensik digital. Sub-bidang forensik digital terkait dengan sistem dan jaringan komputer disebut forensik jaringan yang melakukan analisis terkait kejadian tidak wajar berupa serangan siber pada sistem dan jaringan komputer untuk penegakan hukum atau peraturan yang berlaku [11]. Maka pada artikel ini diusulkan analisis pada fase setelah kejadian siber menggunakan pendekatan forensik digital sesuai standar yang berlaku seperti ISO/IEC 27037:2012. Novelty dari artikel melakukan akuisisi barang bukti digital menggunakan dua teknik akuisisi, yaitu *live acquisition* dan *physical acquisition*.

Tinjauan Pustaka

Peneliti dari Universitas Islam Indonesia menyatakan bahwa teknik akuisisi juga bisa dilakukan secara langsung atau disebut live acquisition. Teknik live acquisition biasanya dilakukan pada perangkat elektronik atau barang bukti elektronik berupa perangkat jaringan atau pun yang terkait, seperti router, *smartphones*, server, dan sistem cctv [12] [13] [14] . Hal ini selaras dengan standar ISO/EIC 27037:2012 bahwa sistem yang besar dengan melibatkan sistem dan jaringan komputer dapat dilakukan akuisisi barang bukti digital secara langsung. Proses audit log digital juga dapat dilakukan dengan menggunakan basis dari CIS *Control* yang memiliki kaitan penting dalam implementasi ISO 27001. Dalam sistem security auditor ini dapat memberikan nilai pada setiap hasil audit yang dijalankan pada server testing dengan CIS *Benchmark* berdasarkan CIS *Control* [15].

Sistem dan jaringan komputer yang semakin komplek dituntut dapat dilakukan sebuah pengawasan yang terintegrasi. Hal ini sebagai upaya untuk menjaga peningkatan kualitas dan keamanan serta kenyamanan pengguna dalam menggunakan layanan dari sistem dan jaringan komputer. Berdasarkan laporan Badan Siber dan Sandi Negara bahwa pada tahun 2021 terdapat anomali trafik yang tercatat sebesar 1.6 Milyar. Anomali trafik ini bersumber dari BotNet, sebuah anomali yang disebabkan oleh komputer yang terhubung ke internet dan terinfeksi *malware* yang dikendalikan dari sebuah mesin pengendali (C2, *Command and Control*) [16].

Untuk melakukan investigasi dan analisis serangan siber [17] pada sistem dan jaringan komputer dengan kasus anomali atau *malicious traffic* dapat menggunakan pendekatan forensik jaringan [18]. Tahapan dalam melakukan akuisisi barang bukti digital pada perangkat jaringan seperti switch menggunakan pendekatan forensik jaringan dapat menggunakan teknik *Port Mirroring*. Isitlah lain dari *Port Mirroring* adalah SPAN (*Switched Port Analyzer*), suatu teknik penyalinan trafik ke media lain dari sebuah port yang dilalui oleh trafik utama [19][20]. Pada umumnya menyalin trafik pada teknik port mirroring dieksport ke dalam berkas berformat pcap sebagai barang bukti digital [21].

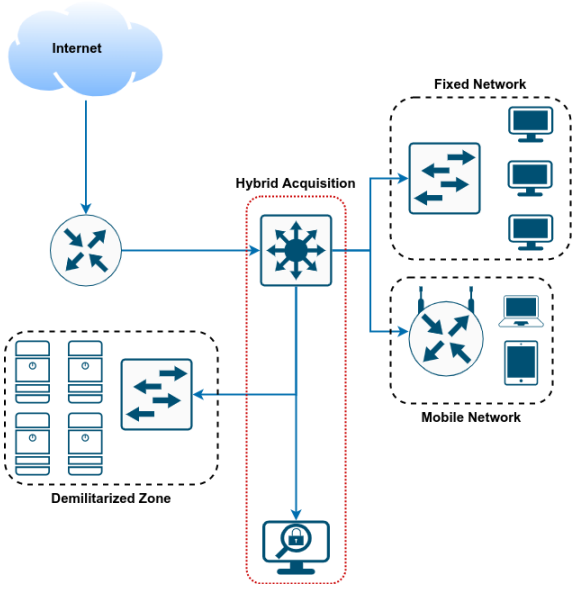
Metode Penelitian

Standarisasi forensik digital yang digunakan secara global diantaranya ISO/IEC 27037:2012. Adapun proses melakukan forensik digital berdasarkan ISO/IEC 27037:2012 terdapat 4 tahapan, yaitu *identification*, *collection*, *acquisition*, dan *preservation* [22]. Pada artikel ini fokus pada tahapan *acquisition*, yaitu tahapan melakukan proses penyalinan barang bukti digital dari barang bukti elektronik dengan menyertakan dokumentasi teknik dan aktivitas yang dilakukan selama proses. Teknik acquisition pada forensik digital secara umum terbagi menjadi 3 [23]:

a) *Manual Acquisition*, teknik yang dilakukan oleh *Digital Evidence First Responder* dengan melakukan pembacaan dan pencarian barang bukti digital secara langsung pada barang bukti elektronik dengan kondisi keterbatasan waktu dan teknologi akuisisi terhadap barang bukti elektronik. Teknik ini bersifat low priority karena tingkat intergrity cukup lemah pada barang bukti digital.
b) *Physical Acquisition*, teknik yang dilakukan *Digital Evidence First Responder* dalam mendapatkan barang bukti digital dengan melakukan penyalin secara indentik dengan barang bukti elektronik. Teknik ini biasa disebut juga teknik cloning.

c) *Logical Acquisition*, teknik yang dilakukan *Digital Evidence First Responder* dengan melakukan penyalinan barang bukti digital sesuai dengan obyek atau berkas yang terindikasi terkait dengan tindak kejahatan. Hal ini dilakukan karena berbagai kondisi diantaranya sistem dengan kapasitas yang besar, sistem terkait dengan sistem lainnya yang tidak boleh mati, dan ruang lingkup terhadap sistem yang akan diakuisisi.

Pada penelitian ini tahapan live acquisition menggunakan teknik port mirroring dikombinasikan *Single Board Computer* (SBC), Raspberry Pi. Fungsi dari Raspberry Pi sebagai media atau barang bukti elektronik tambahan dalam menyimpan hasil salinan trafik berdasarkan *port mirroring*. Sehingga berkas yang tersimpan dalam memory card Raspberry Pi dapat dikategorikan sebagai barang bukti digital, selayaknya *memory card* pada *smartphone* [24]. Penelitian ini mengusulkan model *Hybrid Acquisition* yang menggabungkan *live acquisition* pada sisi perangkat jaringan dan *physical acquisition* pada sisi media penyimpanan di Raspberry Pi dimana divisualisasikan pada gambar 1.



Gambar 1. *Hybrid acquisition*

Hasil dan Pembahasan

Dalam melakukan investigasi *cybercrime* pada ekosistem sistem dan jaringan komputer yang kompleks maka perlu dilakukan mencatat dan memantau lalu lintas jaringan pada router. Hasil pencatatan dan pemantauan lalu lintas jaringan dapat dicatat pada suatu media untuk mempermudah analisis. Tahapan ini merupakan bagian dari *identification*, *collection*, *acquisition*, dan preservation sesuai dengan SNI ISO/IEC 27037:2014. Router yang telah teridentifikasi pada artikel ini adalah Mikrotik RB1100HX2 yang telah mendukung Switched Port Analyzer untuk melakukan pencatatan dan pemantauan lalu lintas jaringan [25]. Fitur *Switched Port Analyzer* pada router Mikrotik RB1100HX2 terimplementasi dalam fitur *Port Mirroring*. Teknik *Port Mirroring* dimanfaatkan sebagai *live acquisition* pada sistem dan jaringan komputer dalam proses pencatatan lalu lintas jaringan [26].

Router Mikrotik RB1100HX2 memiliki chipset yang yang mendukung *switching*. Adapun chipset yang digunakan RB1100HX2 adalah Atheros 8327. Dua chipset Atheros 8327 terpasang pada port, ethernet 1 – ethernet 5 (switch1) dan ethernet 6 – ethernet 10 (switch2). Tahapan melakukan *port mirroring* pada Mikrotik sebagai berikut:

- Masuk ke menu Switch menggunakan perintah /interface ethernet switch
- Setup port 1 (ethernet1) disalin ke port 2 (ethernet2) menggunakan perintah set mirror-source=ether1 mirror-target=ether2 0

Proses dari *live acquisition* dilanjutkan dengan menyiapkan sebuah perangkat, dalam hal ini Raspberry Pi yang berfungsi untuk mengolah data-data lalu lintas jaringan hasil dari *Port Mirroring*. Raspberry Pi sebelumnya sudah terinstall aplikasi *malicious traffic detection system* menggunakan Maltrail. Dengan menggunakan Maltrail mencatat semua lalu lintas jaringan yang berada pada Layer 3 terkait aktivitas-aktivitas abnormal pada jaringan. Adapun aktivitas abnormal pada jaringan yang dicatat dan diolah Maltrail bersumber dari beberapa penyedia informasi keamanan siber publik seperti *urlhaus*, *alienvault*, *ransomwaretrackerurl*, *malc0de*, *ransomwaretrackerdns*, *cobaltstrike*, dan sebagainya [26].

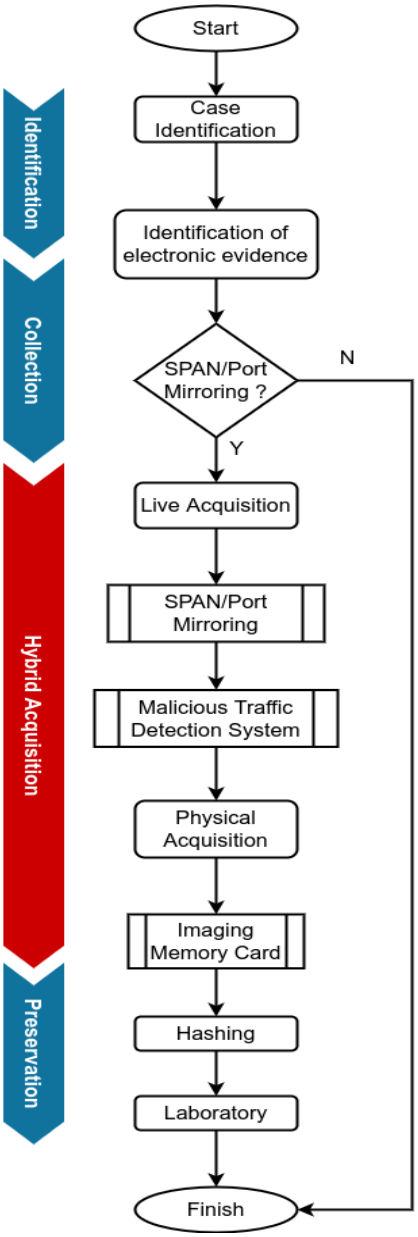
Tabel 1. Hasil *malicous traffic detection system* dengan mailtrail dari proses *acquisition*

Sensor	**Event**	**Severity**	**Attack mode**
raspberrypi	1	Low	Known attacker
raspberrypi	4	High	Malware
raspberrypi	1	Low	Mass scanner
raspberrypi	1	Low	Mass scanner
raspberrypi	1	Low	Mass scanner
raspberrypi	2	Low	Mass scanner
raspberrypi	1	Low	Mass scanner
raspberrypi	1	Low	Mass scanner
raspberrypi	1	Low	Known attacker
raspberrypi	1	Low	Mass scanner

Sensor	Event	Severity	Attack mode
raspberrypi	1	Low	Mass scanner
raspberrypi	1	Low	Known attacker
raspberrypi	1	Low	Mass scanner
raspberrypi	1	Low	Known attacker
raspberrypi	1	Low	Mass scanner
raspberrypi	2	Medium	Domain suspicious
raspberrypi	1	Low	Mass scanner
raspberrypi	3	Medium	Site suspicious

Berdasarkan pencatatan lalu lintas jaringan menggunakan 2 teknik, port mirroring pada Mikrotik dan *malicous traffic detection system* menggunakan Maltrail, maka barang buktinya tidak sekadar barang bukti digital berupa berkas .pcap semisal menggunakan *Wireshark* [27]. Namun, perangkat elektronik pencatat dan pemantau lalu lintas jaringan dapat dijadikan barang bukti elektronik. Pada penelitian ini menunjukan bahwa barang bukti elektronik yang dapat dikumpulkan berdasarkan SNI ISO/IEC 27037:2014 adalah Router, Raspberry Pi, dan *Memory Card*. Sehubungan Router pada ekosistem kritikal maka tidak bisa diamankan secara fisik, hanya dicatat identifikasi perangkatnya dan melakukan teknik *port mirroring*. Untuk Raspberry Pi pengumpulan atau penyitaan perangkat elektronik sebagai barang bukti elektronik sesuai prosedur diantaranya dicatat identifikasi perangkat, dimasukan dalam tas khusus barang bukti, pelabelan, dana pencatatat *Chain of Custody*. Sedangkan pada barang bukti elektronik berupa Memory Card dilakukan cloning atau imaging terhadap barang bukti digital tersimpan berupa informasi-informasi dari *malicous traffic detection system*.

Setelah dilakukan *cloning* atau *imaging*, *Memory card* diberlakukan sama seperti Raspberry Pi sebagai barang bukti elektronik. Hanya perlu tambahan informasi hash dari *Memory Card* sebagai wujud tahapan presevasi. Tahap terakhir semua barang bukti berupa, Raspberry Pi, *Memory Card*, dan Hasil *cloning*/*imaging* dibawa ke laboratorium untuk dianalisis selayaknya penanganan lanjutan terkait barang buki elektronik dan/digital. Adapun alur penanganan tindak kejahatan siber yang teridentifikasi dari *malicious traffic* dapat dilihat pada Gambar 2.



Gambar 2. Alur *hybrid acquisition*

Kesimpulan dan Saran

Kejadian tindak kejahatan siber pada sistem dan jaringan komputer suatu institusi yang memiliki jaringan komplek perlu penanganan barang bukti secara hati-hati supaya tidak mengganggu proses bisnis institusi tersebut. Sesuai SNI ISO/IEC 27037:2014 diperkenankan melakukan akuisisi secara parsial atau logikal pada sebuah sistem dan jaringan komputer yang komplek karena sistem yang berjalan tidak boleh terhenti. Pada artikel ini disimpulkan bahwa untuk mengakuisisi lalu lintas jaringan menggunakan teknik port mirroring atau SPAN. Selanjutnya informasi lalu lintas jaringan disimpan menggunakan Raspberry Pi yang terinstall Maltrail. Teknik-teknik sebelumnya menggunakan

wireshark yang barang bukti digitalnya berupa berkas pcap. Maka di artikel ini dilakukan akuisisi secara fisikal dari Raspberry Pi yang menyimpan informasi dari lalu lintas jaringan.

Maka dari proses dua metode akuisisi tersebut dapat disimpulkan sebagai metode *hybrid acquisition* dengan menggabungkan *partial acquisition* dan *physical acquisition*. Hal ini sebagai upaya mengikuti prinsip forensik digital pada SNI ISO/IEC 27037:2014, yaitu meminimalisir penanganan barang bukti secara langsung. Dengan metode *hybrid acquisition* perlu koordinasi dengan berbagai pihak yang memiliki kewenangan terkait pengelolaan sistem dan jaringan komputer. Penelitian selanjutnya dapat dikombinasikan dengan metode-metode kesiapan forensik digital (*forensic readiness*) pada institusi untuk mempermudah proses identifikasi dan investigasi jika terjadi kejahatan siber atau tindak kejahatan lainnya yang terkait dengan sistem dan jaringan komputer.

Daftar Pustaka

[1] R. Raodia, "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)," *Jurisprud. Jur. Ilmu Huk. Fak. Syariah Dan Huk.*, vol. 6, no. 2, pp. 230–239, 2019.

[2] D. P. I. Kusuma, N. H. Maulida, and D. Hariyadi, "Evaluasi Potensi Celah Keamanan SQL Injection Menggunakan Nearest Neighbor pada Security-Software Development Life Cycle," *J. Repos.*, vol. 2, no. 9, pp. 1273–1280, 2020.

[3] D. A. Effendy, K. Kusrini, and S. Sudarmawan, "Classification of intrusion detection system (IDS) based on computer network," in *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, IEEE, 2017, pp. 90–94.

[4] G. Dhillon, "What to do before and after a cybersecurity breach," *Am. Univ. Wash. DC Kogod Cybersecurity Gov. Cent.*, 2015.

[5] P. Satam, "A methodology to design intrusion detection systems (IDS) for IoT/networking protocols," PhD Thesis, The University of Arizona, 2019.

[6] P. I. Priyadarsini and G. Anuradha, "A novel ensemble modeling for intrusion detection system," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 2, p. 1963, 2020.

[7] D. Hariyadi, C. B. Setiawan, and B. Setiyadi, "Pengembangan Sistem Pemantauan dan Deteksi Serangan pada Ekosistem Rumah Cerdas," *J. Komtika Komputasi Dan Inform.*, vol. 5, no. 2, pp. 132–139, 2021.

[8] H. Hudzaifah, A. Sularsa, and D. R. Suchendra, "Membangun Sistem Monitoring Malicious Traffic Di Jaringan Dengan Maltrail," *EProceedings Appl. Sci.*, vol. 4, no. 3, 2018.

[9] R. W. Shiddiq, *Implementasi Sensor Maltrail dan Fail2Ban Untuk Mendeteksi dan Mencegah Serangan Malware Pada Jaringan Server Diskominfo Sumedang Dengan Push Notifikasi*. Universitas Telkom, D3 Teknologi Telekomunikasi, 2021. Accessed: Apr. 23, 2023. [Online]. Available: https://repository.telkomuniversity.ac.id/pustaka/174726/implementasi-sensor-maltrail-dan-fail2ban-untuk-mendeteksi-dan-mencegah-serangan-malware-pada-jaringan-server-diskominfo-sumedang-dengan-push-notifikasi.html

[10] McAfee, "Integrating SIEM into Your Threat Hunting Strategy," *TechRepublic*, Apr. 20, 2023. https://www.techrepublic.com/resource-library/whitepapers/integrating-siem-into-your-threat-hunting-strategy/ (accessed Apr. 23, 2023).

[11] D. Hariyadi, H. Wijayanto, and I. D. Sari, "Analisis Barang Bukti Digital Aplikasi Paziim pada Ponsel Cerdas Android dengan Pendekatan Logical Acquisition," *Cyber Secur. Dan Forensik Digit.*, vol. 2, no. 2, pp. 52–56, 2019.

[12] D. Hariyadi, F. E. Nastiti, and F. N. Aini, "Framework for acquisition of cctv evidence based on acpo and sni iso/iec 27037: 2014," in *Int. Conf. Informatics Dev*, 2018.

[13] D. Hariyadi, M. Kusuma, and A. Sholeh, "Digital Forensics Investigation on Xiaomi Smart Router Using SNI ISO/IEC 27037: 2014 and NIST SP 800-86 Framework," in *International Conference on Science and Engineering (ICSE-UIN-SUKA 2021)*, Atlantis Press, 2021, pp. 143–147.

[14] A. R. Supriyono, B. Sugiantoro, and Y. Prayudi, "Eksplorasi Bukti Digital Pada Smart Router Menggunakan Metode Live Forensics," *J. Infotekmesin*, vol. 10, no. 2, pp. 38–45, 2019.

[15] M. Najib, B. Purnomosidi D.P, and M. A. Nugroho, "IMPLEMENTASI SECURITY AUDITOR UNTUK STANDARDISASI INSTALASI SERVER PADA LAYANAN SAAS MENGGUNAKAN CIS BENCHMARK," *Cyber Secur. Dan Forensik Digit.*, vol. 5, no. 2, pp. 83–88, Jan. 2023, doi: 10.14421/csecurity.2022.5.2.3929.

[16] BSSN, "Laporan Tahunan Monitoring Keamanan Siber Tahun 2021 | bssn.go.id," 2021. https://bssn.go.id/laporan-tahunan-monitoring-keamanan-siber-tahun-2021/ (accessed Apr. 23, 2023).

[17] R. Sahtyawan, "PENERAPAN ZERO ENTRY HACKING DIDALAM SECURITY MISCONFIGURATION PADA VAPT (VULNERABILITY ASSESSMENT AND PENETRATION TESTING)," *J. Inf. Syst. Manag. JOISM*, vol. 1, no. 1, Art. no. 1, Jul. 2019, doi: 10.24076/joism.2019v1i1.18.

[18] European Union Agency for Cybersecurity., *Introduction to network forensics: analysis of an airport third party VPN connection compromise toolset : document for students.* LU: Publications Office, 2019. Accessed: Apr. 23, 2023. [Online]. Available: https://data.europa.eu/doi/10.2824/995110

[19] J. Bullock and J. T. Parker, *Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework*. John Wiley & Sons, 2017.

[20] Sudarshan, "Malicious Traffic Detection System using Publicly Available Blacklist's," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 6S, pp. 356–361, Sep. 2019, doi: 10.35940/ijeat.F1075.0886S19.

[21] H. Alamsyah and A. Al Akbar, "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System," *JOINTECS J. Inf. Technol. Comput. Sci.*, vol. 5, no. 1, pp. 17–24, 2020.

[22] R. A. Ramadhan, P. R. Setiawan, and D. Hariyadi, "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037: 2012 and NIST SP800-86 Framework," *IT J. Res. Dev.*, vol. 6, no. 2, pp. 162–168, 2022.

[23] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," *Int J Electr Comput Eng*, vol. 8, no. 5, pp. 3991–4003, 2018.

[24] S. C. Sathe and N. M. Dongre, "Data acquisition techniques in mobile forensics," in *2018 2nd international conference on inventive systems and control (icisc)*, IEEE, 2018, pp. 280–286.

[25] A. Sa`di, R. Andriani, and T. Taufikurrahman, "PERANCANGAN SISTEM AUTENTIKASI WIRELLESS HOTSPOT BERBASIS RADIUS MENGGUNAKAN MIKROTIK," *J. Inf. Syst. Manag. JOISM*, vol. 4, no. 2, Art. no. 2, Jan. 2023, doi: 10.24076/joism.2023v4i2.953.

[26] F. Daryabar, A. Dehghantanha, B. Eterovic-Soric, and K.-K. R. Choo, "Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices," *Aust. J. Forensic Sci.*, vol. 48, no. 6, pp. 615–642, 2016.

[27] B. Actoriano and I. Riadi, "Forensic Investigation on WhatsApp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2," *Int. J. Cyber-Secur. Digit. Forensics IJCSDF*, vol. 7, no. 4, pp. 410–419, 2018.