JURNAL AHLI MUDA INDONESIA

journal homepage: https://journal.akb.ac.id/

FORENSIK DIGITAL SISTEM INFORMASI BERBASIS WEB

Andria[1], Sekreningsih Nita[2]

[1,2] Sistem Informasi, Fakultas Teknik, Universitas PGRI Madiun
e-mail : andria@unipma.ac.id[1], nita@unipma.ac.id[2]

Penulis Korespondensi Andria, Sistem Informasi, Fakultas Teknik, Universitas PGRI Madiun.
e-mail: andria@unipma.ac.id

ARTIKEL INFO

Artikel History:
Menerima 25 Mei 2021
Revisi 1 Juni 2021
Diterima 6 Agustus 2021
Tersedia Online 31 Desember 2021

Kata kunci :
Digital, Forensik, Maltego, Sistem Informasi, Web

ABSTRAK

Objektif. Pengungkapan suatu kejahatan siber seperti peretasan situs web diperlukan adanya forensik digital yang bertujuan untuk mengidentifikasi, menganalisa dan memetakan jaringan komunikasi pada suatu sistem informasi berbasis web.
Material dan Metode. Forensik digital dalam penelitian ini menggunakan aplikasi Maltego yang dapat melakukan footprinting yaitu mengumpulkan informasi sebanyak mungkin dari situs web yang dilakukan forensik digital. Sistem operasi yang digunakan untuk menjalankan aplikasi Maltego yaitu Linux yang merupakan sistem operasi open source.
Hasil. Hasil peneltian ini dapat digunakan sebagai solusi dalam menangani sebuah kasus yang membutuhkan barang bukti digital. Informasi yang didapatkan dapat divisualisasikan dalam bentuk pemetaan jaringan komunikasi dan informasi yang mudah dipahami.
Kesimpulan. Forensik digital sangat diperlukan dalam mendapatkan barang bukti digital dari pengungkapan suatu kasus kejahatan siber. Saran untuk penelitian selanjutnya yaitu melakukan komparasi penggunaan aplikasi forensik digital untuk dapat melihat perbandingan hasil yang lebih lengkap dan akurat.

ARTICLE INFO

Artikel History:
Received 25th May 2021
Revision 6th June 2021
Accepted 6th August 2021
Available Online 31st December 2021

Keywords :
Digital, Forensic, Information System, Maltego, Web

ABSTRACT

Objective. Disclosure of a cybercrime such as hacking a website requires digital forensics, which aims to identify, analyze and map communication networks on a web-based information system.
Material and Methods. Digital forensics in this study uses the Maltego application, which can do footprinting, which is to collect as much information as possible from websites that are carried out by digital forensics. The operating system used to run Maltego applications is Linux which is an open-source operating system.
Result. The results of this research can be used as a solution in handling a case that requires digital evidence. The information obtained can be visualized in the form of a mapping of communication networks and information that is easy to understand.
Conclusion. Digital forensics is indispensable in obtaining digital evidence from disclosing a cybercrime case. Suggestions for further research are to compare the use of digital forensic applications to be able to see a more complete and accurate comparison of results.

Doi : 10.46510/jami.v2i2.73
ISSN 2722-4406 (p)/2722-4414(e)

1. PENDAHULUAN

Pemanfaatan teknologi informasi, media dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi telah pula menyebabkan hubungan dunia menjadi tanpa batas dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat.Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum (Riskawati, 2016) Teknologi informasi yang semakin berkembang pesat dapat menjadi suatu ancaman ketika disalahgunakan seperti untuk aktivitas peretasan yang tentunya dapat merugikan. Berdasarkan data Pusopkamsinas BSSN, terdapat 149 Juta serangan cyber Semester I 2020. Tujuan penelitian ini yaitu melakukan forensik digital untuk mengidentifikasi, menganalisa dan memetakan jaringan komunikasi pada suatu sistem informasi berbasis web.

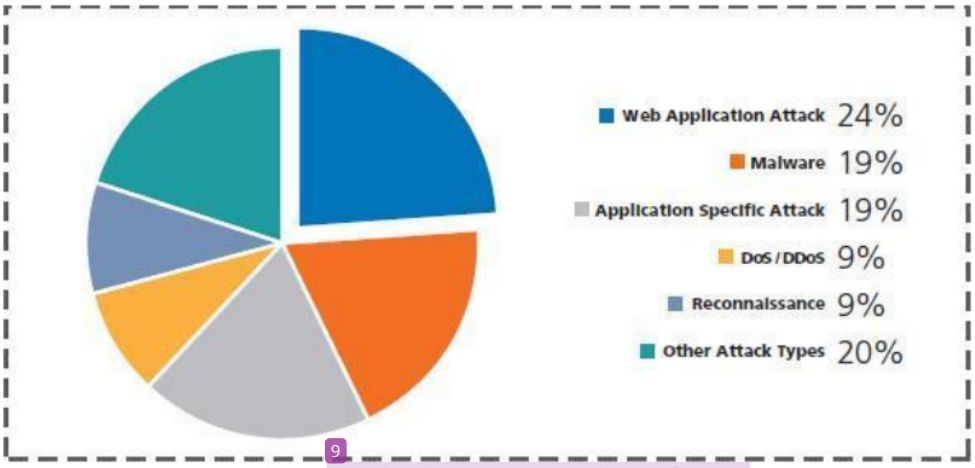
Gambar 1. Ilustrasi | Data Pusopkamsinas BSSN
(BSSN, n.d.)

Seperti pada gambar 1 yang dikutip dari situs cyberthread.id dapat dijelaskan bahwa Pusat Operasi Keamanan Siber Nasional (Pusopkamsinas) Badan Siber dan Sandi Negara (BSSN) berhasil mendeteksi 149.783.617 serangan siber yang terjadi di Indonesia pada semester pertama tahun 2020. Data dihimpun BSSN dari bulan Januari hingga Juni 2020.

Kejahatan siber atau yang dikenal dengan istilah cybercrime tentu menjadi suatu ancaman serius yang perlu diantisipasi dan ditangani dengan tepat, sebagai contoh dalam penerapan sistem informasi berbasis web tidak sedikit ditemukan kasus peretasan sehingga dari hal tersebut tentu perlu adanya suatu tindakan pengungkapan pelaku yaitu dengan dilakukannya forensik digital atau digital forensic yang merupakan suatu ilmu pengetahuan dan keahlian dalam melakukan

identifikasi, analisa dan pemetaan jaringan komunikasi pada suatu sistem informasi serta mengumpulkan bukti-bukti digital yang terkait dengan tindakan cybercrime tersebut.

Banyaknya kasus peretasan data menjadi suatu ancaman dalam penerapan dan pemanfaatan suatu sistem informasi berbasis web (Andria, 2021). Berdasarkan data yang dikutip pada situs calyptix.com dijelaskan bahwa terdapat 5 jenis serangan siber teratas seperti ditampilkan pada gambar 2 sebagai berikut.



Gambar 2. Top 5 Cyber Attack Types in 2016 So Far
(Calyptix Security, 2016)

Seperti ditunjukkan pada gambar 2, dijelaskan bahwa dari kelima serangan siber teratas tersebut serangan pada web aplikasi menempati urutan pertama yang artinya jenis serangan siber tersebut mentargetkan paling banyak situs web. Hal ini menjadi tantangan bagi Forensika teknologi informasi dan penegak hukum untuk melakukan penyelidikan terhadap barang bukti dari tersangka dalam kasus kejahatan karena bukti digital yang akan dijadikan sebagai barang telah dihapus oleh pelaku sehingga untuk mendapatkan kembali bukti digital, Forensika teknologi informasi dan penegak hukum dituntut untuk melakukan analisis forensik recovery data dalam mengembalikan data yang telah dihapus tersebut (Riadi et al., 2019)

Digital forensik merupakan bagian ilmu forensik yang digunakan untuk penyelidikan dan penyidikan suatu perkara dalam investigasi materi (data) yang dan penemuan konten perangkat digital (Rachmie, 2020). Sehingga dalam pengungkapan suatu kejahatan siber seperti peretasan situs web tersebut diperlukan adanya forensik digital yang bertujuan untuk mengidentifikasi, menganalisa dan memetakan jaringan komunikasi pada suatu sistem informasi berbasis web.

Adapun penelitian sebelumnya yang berjudul "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ)", penelitian ini membahas

perbandingan terkait tool Forensik yang digunakan untuk proses eksaminasi dan analisa. Pengambilan salinan bukti digital dilakukan dengan metode forensik statik, sedangkan tahapan penelitian dan analisa mengadaptasi dan mengimplementasikan metode forensik dari National Institute of Justice (NIJ) untuk mendapatkan bukti digital. Software pembeku drive seperti Shadow Defender terbukti berpengaruh terhadap praktik eksaminasi forensik digital terhadap didapatkannya bukti-bukti digital, dengan kondisi tersebut prosentase keberhasilannya merestorasi file hanya 28,7% sehingga dapat menjadi hambatan dalam proses forensik digital (Riadi et al., 2018)

Adapula penelitian dengan judul ""Investigasi Forensik Pada E-Mail Spoofing Menggunakan Metode Header Analysis", menjelaskan bahwa Email merupakan salah satu fasilitas internet yang banyak digunakan untuk komunikasi dan bertukar informasi. Hal ini memungkinkan pihak ketiga menyalahgunakan email untuk mendapatkan informasi secara ilegal dengan mengubah identitas pengirim email dan menjadikannya seperti email yang berasal dari email yang sah (legitimate email), aktivitas tersebut biasa dikenal dengan istilah email spoofing. Untuk dapat mendeteksi adanya email spoofing, maka perlu adanya investigasi forensik email terhadap email spoofing. Salah satu teknik investigasi forensik email adalah menggunakan analisis header email (header analysis method) (Hoiriyah et al., 2016)

Penelitian lainnya dengan judul "Perbandingan Kinerja Perangkat Lunak Forensik untuk File Carving dengan Metode NIST", penelitian ini melakukan perbandingan performansi perangkat lunak forensik open source untuk mengembalikan data, yaitu Scalpel, Foremost dan Autopsy, menggunakan metode forensik National Institute of Standards Technology (NIST). Proses pengujian yang dilakukan menggunakan teknik file carving. Hasil file carving dianalisis dengan melihat tingkat keberhasilan (akurasi) alat forensik yang digunakan dalam pengembalian data. Scalpel menunjukkan akurasi file carving tertinggi dengan keberhasilan sebesar 100% untuk 20 file dokumen dalam format pdf dan Docx, dan 90% untuk file gambar dalam format png dan jpeg (Yuwono et al., 2019)

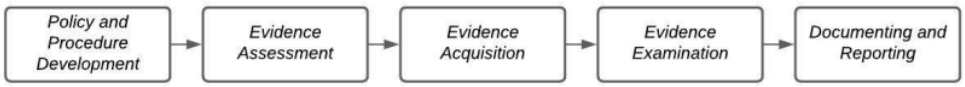
Adapun forensik digital dalam penelitian ini menggunakan aplikasi Maltego. Dilansir dari situs resmi Maltego.com, dijelaskan bahwa Maltego merupakan aplikasi open source intelligence (OSINT) dan alat analisis tautan grafis untuk mengumpulkan dan menghubungkan informasi untuk tugas-tugas investigasi (Maltego, n.d.). Menurut Departemen Angkatan Darat Amerika Serikat, dijelaskan bahwa Open-source intelligence (OSINT) adalah disiplin intelijen yang berkaitan dengan kecerdasan yang dihasilkan dari informasi yang tersedia secara publik yang dikumpulkan, dieksploitasi, dan disebarluaskan pada waktu yang tepat kepada khalayak yang tepat

untuk tujuan pengalamatan kebutuhan informasi dan intelijen khusus (Army, 2012). Aplikasi Maltego dapat melakukan footprinting yaitu mengumpulkan informasi sebanyak mungkin dari situs web yang dilakukan forensik digital. Sistem operasi yang digunakan untuk menjalankan aplikasi Maltego yaitu Parrot OS yang merupakan sistem operasi open source.

2. MATERIAL DAN METODE

Bahan dan alat yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Satu unit PC/laptop bersistem operasi Linux, adapun secara spesifik Linux yang digunakan adalah Parrot OS yang merupakan sistem operasi open source dari distribusi Linux berbasis Debian dengan fokus pada keamanan, privasi, dan pengembangan.
2. Aplikasi Maltego untuk melakukan footprinting yaitu mengumpulkan informasi sebanyak mungkin dari situs web yang dilakukan forensik digital.
3. Koneksi internet
4. Situs web, dalam penelitian menggunakan contoh situs web yang dirancang khusus untuk keperluan simulasi beralamatkan di http://vulnweb.com (Acunetix, n.d.)
5. Penelitian ini menggunakan metode analisa forensik dari National Institute of Justice (NIJ). Metode ini untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat diketahui alur dan langkah-langkah penelitian secara sistematis sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada (Riadi et al., 2018)
6. Berdasarkan dokumen National Institute of Justice (NIJ), terdapat 5 tahapan dalam menangani dan mengidentifikasi bukti digital terkait dengan aktivitas forensik digital (digital forensic), seperti yang ditunjukkan pada gambar 1 sebagai berikut:



Gambar 1. Tahapan forensik digital

Pada gambar 1 dapat dijelaskan bahwa 5 tahapan forensik digital tersebut masing-masing dapat dirinci berdasarkan pada studi kasus pada penelitian ini. Lebih jelasnya sebagai berikut:

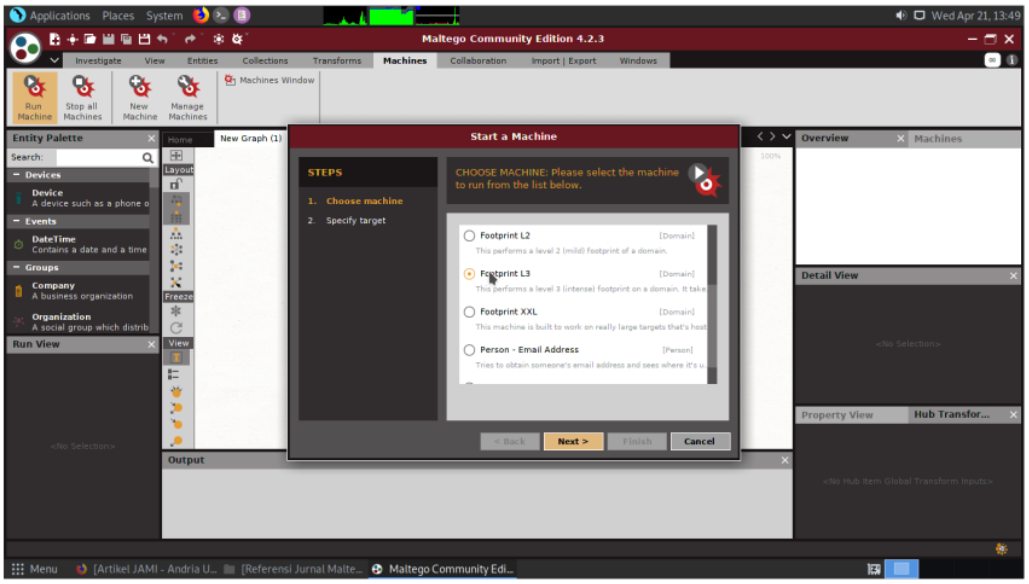
1. *Policy and Procedure Development*
   Memahami prosedur dan kebijakan pengembangan terkait dengan aturan atau regulasi pada objek yang akan dilakukan forensik digital, pada penelitian ini web yang digunakan sebagai objek forensik digital merupakan situs web yang dirancang khusus untuk keperluan simulasi pengujian.

2. *Evidence Assessment*
   Penilaian barang bukti yang dapat berupa data, informasi rekam jejak, alur dan lain sebagainya yang terkait dengan konten digital sebagai barang bukti.
3. *Evidence Acquisition*
   Pengumpulan barang bukti dari hasil penilaian barang bukti yang dianggap relevan sesuai dengan yang akan dilakukan forensik digital.
4. *Evidence Examination*
   Pemeriksaan barang bukti dari hasil pengumpulan barang bukti.
5. *Documenting and Reporting*
   Dokumentasi dan pelaporan dari hasil forensik digital

3. HASIL DAN PEMBAHASAN

Pada penelitian ini, objek yang digunakan yaitu sebuah situs web yang dirancang khusus untuk keperluan simulasi pengujian yang akan dilakukan forensik digital untuk mengumpulkan informasi dan memetakan jaringan komunikasi guna memudahkan dalam proses identifikasi, analisa dan pengumpulan barang bukti digital dalam mengungkap kejahatan siber seperti peretasan situs web misalnya, sehingga pihak terkait yang berwenang dapat mengambil keputusan yang tepat berdasarkan barang bukti digital yang diperoleh.

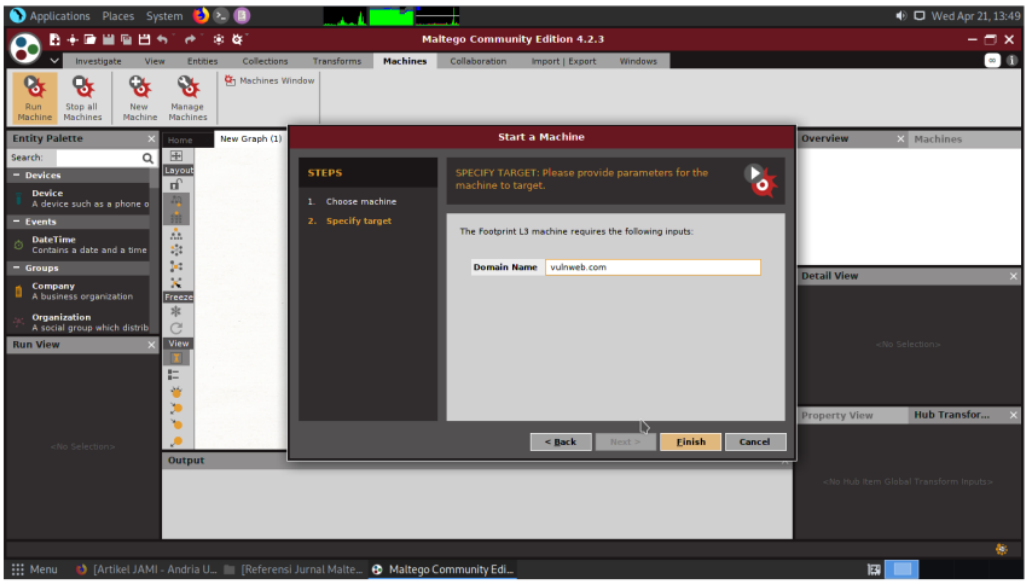
Langkah pertama yaitu membuka aplikasi Maltego kemudian login ke akun yang sudah pernah dibuat sebelumnya, namun apabila baru pertama kali menggunakan aplikasi Maltego maka langkah awal yang perlu dilakukan yaitu dengan registrasi terlebih dahulu. Setelah aplikasi Maltego terbuka, kemudian memilih jenis Machine. Lebih jelasnya seperti ditunjukkan pada gambar 2 sebagai berikut.



Gambar 2. Pemilihan *Machine* di Maltego

Seperti yang ditunjukkan pada gambar 2, pada penelitian ini machine yang dipilih yaitu Footprint L3 untuk mendapatkan informasi yang intens dan lengkap dalam melakukan Footprinting. Footprinting merupakan teknik pengumpulan informasi sebanyak mungkin dari situs web yang akan dilakukan forensik digital.

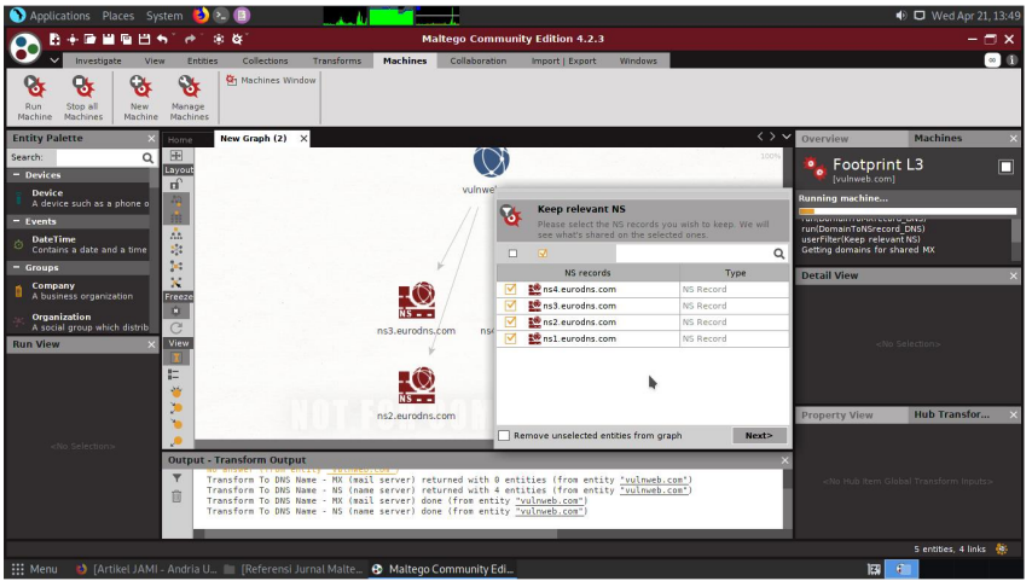
Selanjutnya memasukkan alamat situs web pada kolom Domain Name seperti yang ditunjukkan pada gambar 3 sebagai berikut.



Gambar 3. Pengisian *Domain Name*

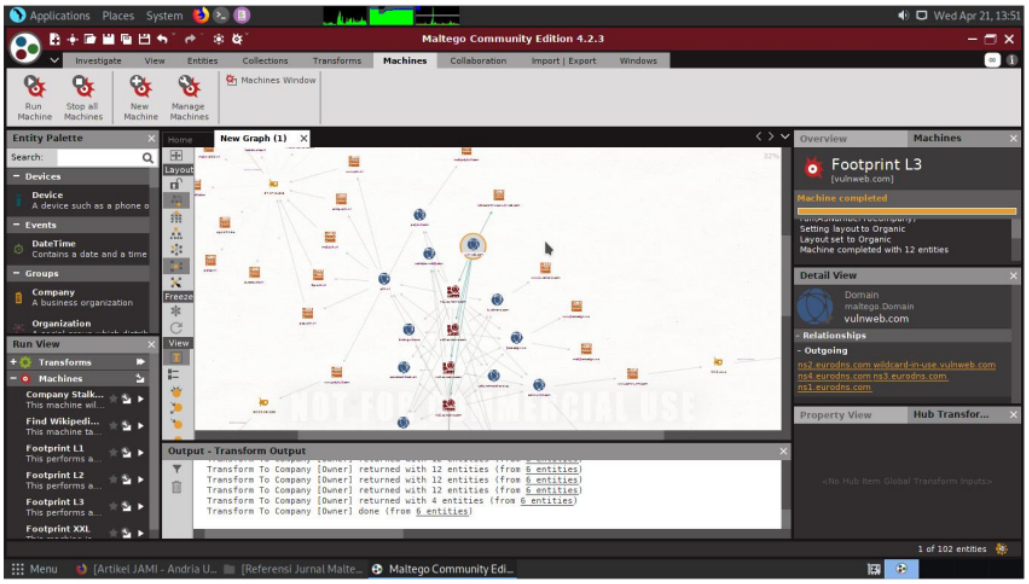
Pada gambar 3 dapat dijelaskan bahwa diperlukan pengisian alamat situs web pada kolom domain name di aplikasi Maltego. Situs web yang dimaksud merupakan situs web target yang akan dilakukan forensik digital. Pada penelitian ini situs web yang digunakan yaitu situs web yang dirancang khusus untuk keperluan simulasi pengujian yang beralamatkan di http://vulnweb.com.

Selanjutnya aplikasi Maltego akan menjalankan prosesnya dengan melakukan footprinting terhadap situs web tersebut. Lebih jelasnya seperti yang terlihat pada gambar 4 sebagai berikut.



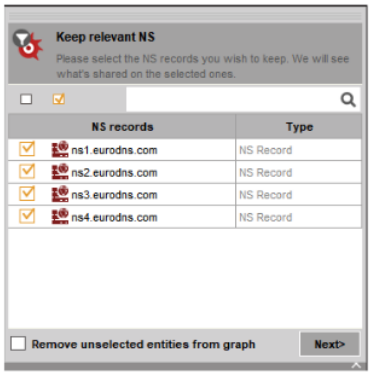
Gambar 4. Proses *Footprinting*

Pada gambar 4 dapat dijelaskan bahwa proses footprinting tersebut meliputi scanning terhadap berbagai macam informasi yang berkaitan dengan situs web yang dilakukan forensik digital, seperti: IP Address, name server, domain, jaringan yang terkoneksi dan lain sebagainya. Berikutnya, pemetaan jaringan komunikasi dan informasi secara lebih detail ditunjukkan pada gambar 5 sebagai berikut.



Gambar 5. Tampilan hasil *footprinting*

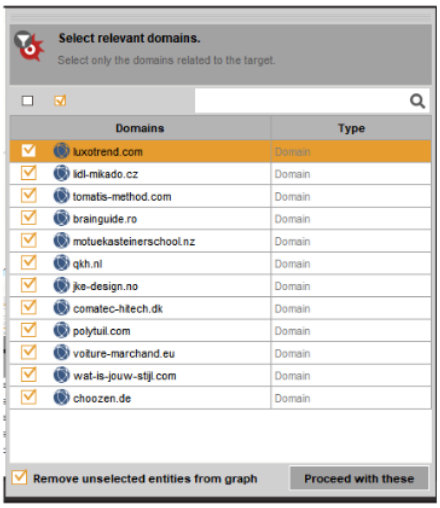
Pada gambar 5 dapat dijelaskan bahwa hasil footprinting menampilkan pemetaan jaringan komunikasi dan informasi secara lebih rinci dari proses forensik digital pada situs web target. Apabila ingin melihat informasi lebih jauh dan lebih dalam lagi, kita bisa melakukan dengan cara menyorot objek yang dimaksud dan mengklik kanan kemudian memilih berbagai macam sumberdaya informasi yang kita perlukan dan kemudian Maltego akan menampilkan hasilnya sesuai dengan request. Berikut ini hasil forensik digital pada situs vulnweb.com yang ditunjukkan pada gambar 6 hingga gambar 9 sebagai berikut.



Gambar 6. Forensik Digital *NS Records*

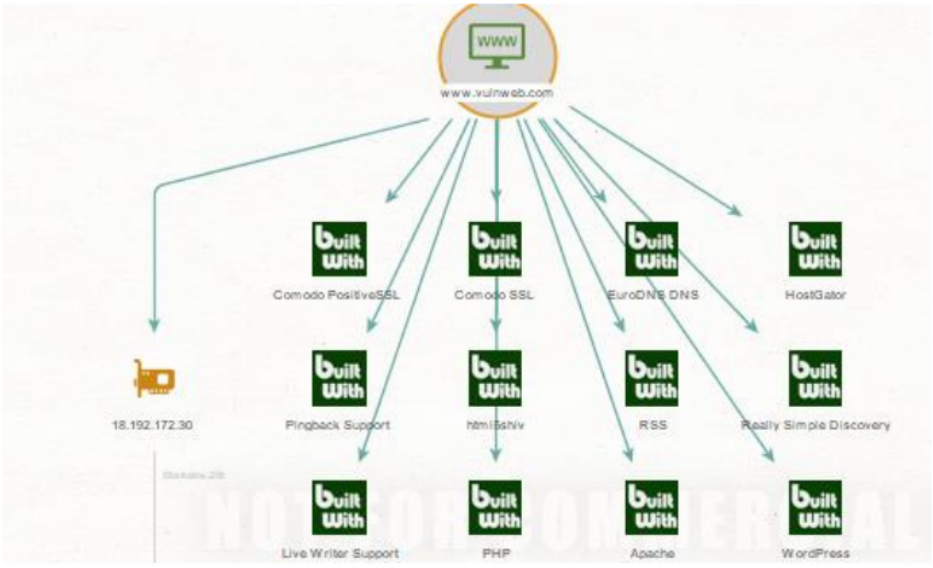
Pada gambar 6 dapat dijelaskan bahwa terdapat informasi NS Records yang terdiri dari 4 ns pada situs web target. NS merupakan singkatan dari nameserver yaitu suatu database atau server dan didalamnya terdapat domain name s IP Address.

Selanjutnya pada gambar 7 dibawah ini dapat dijelaskan bahwa pada situs web target memiliki relevansi dan keterkaitan dengan 12 domain lainnya.



Gambar 7. Forensi`k Digital *Domains* terkait

Pada gambar 8 dibawah ini dapat dijelaskan bahwa pada situs web target menggunakan backend technology seperti bahasa pemrograman PHP, Webserver Apache dan informasi lainnya yang berkaitan dengan teknologi dibalik layar pada situs web tersebut.



Gambar 8. Forensik Digital *Backend Web Technologies*

Berikutnya pada gambar 9 menunjukkan hasil forensik digital pada IP Address yang memuat situs web tersebut berada pada suatu jaringan mana dan berlokasi dimana. Sehingga dari informasi IP Address tersebut bisa didapatkan bukti digital yang konkrit berdasarkan dari hasil yang ditampilkan.

Gambar 9. Forensik Digital *IP Address*

4. KESIMPULAN

Berdasarkan hasil dan pembahasan, maka didapatkan kesimpulan bahwa aplikasi Maltego dapat digunakan untuk keperluan forensik digital pada suatu situs web dalam upaya mengumpulkan informasi dan memetakan jaringan komunikasi apa saja yang tekait didalamnya dengan melakukan teknik footprinting yang dapat ditentukan sesuai dengan kebutuhan. Adapun beberapa informasi yang dapat ditampilkan Maltego diantaranya seperti: nameserver, domain, block IP hosting, backend technology dan peta jaringan situs web.

Hasil peneltian ini dapat digunakan sebagai solusi dalam menangani sebuah kasus yang membutuhkan barang bukti digital. Informasi yang didapatkan dapat divisualisasikan dalam bentuk pemetaan jaringan komunikasi dan informasi yang mudah dipahami.

UCAPAN TERIMAKASIH

Penulis menyampaikan terimakasih yang sebanyak-banyaknya kepada Universitas PGRI Madiun melalui UPT Komputer yang telah menyediakan fasilitas komputer dan koneksi internet guna mendukung terlaksananya penelitian ini. Penulis juga menyampaikan banyak terimakasih kepada komunitas siber atas dukungan literatur yang tersedia di situs web guna menunjang dari penelitian ini.

DAFTAR PUSTAKA

Andria;Ningrum, W. A., & Mubarok, I. (2021). PENGUJIAN KEAMANAN BASIS DATA SISTEM INFORMASI BERBASIS WEB. *PROSIDING SNAST*, 66–74.

Army, U. S. . D. (2012). U.S.A. Department of the Army, "Open-Source Intelligence ATP 2-22.9," vol. 2–22.9, no. July, p. 91, 2012. *Open-Source Intelligence ATP 2-22.9*, *2*, *22.9*.

BSSN, P. (n.d.). *NEWS : Pusopkamsinas BSSN: 149 Juta Serangan Cyber Semester I 2020, Naik Lima Kali Lipat*. Retrieved April 17, 2021, from https://cyberthreat.id/read/7687/Pusopkamsinas-BSSN-149-Juta-Serangan-Cyber-Semester-I-2020-Naik-Lima-Kali-Lipat

Calyptix Security. (2016). *Top 5 Cyber Attack Types in 2016 So Far*. Web Page. https://www.calyptix.com/top-threats/top-5-cyber-attack-types-in-2016-so-far/

Hoiriyah, H., Sugiantoro, B., & Prayudi, Y. (2016). Investigasi Forensik pada E-mail Spoofing menggunakan Metode Header Analysis. *Data Manajemen Dan Teknologi Informasi*, *17*(4), 20–25.

Maltego. (n.d.). *Homepage - Maltego*. Retrieved 22nd April 2021, from https://www.maltego.com/

Rachmie, S. (2020). PERANAN ILMU DIGITAL FORENSIK TERHADAP PENYIDIKAN KASUS PERETASAN WEBSITE. *JURNAL LITIGASI (e-Journal)*, *21*(1), 104–127.

Riadi, I., Sunardi, S., & Sahiruddin, S. (2019). Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ). *Jurnal Rekayasa Teknologi Informasi (JURTI)*, *3*(1), 87–95.

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij). *Evo (Electronics, Informatics, and Vocational Education)*, *3*(1), 70–82.

Riskawati, Riskawati; Tahir, H. (2016). PENANGANAN KASUS CYBER CRIME DI KOTA MAKASSAR (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). *Jurnal Tomalebbi*, *2*, 93–103.

Yuwono, D. T., Fadlil, A., & Sunardi, S. (2019). Perbandingan Kinerja Perangkat Lunak Forensik untuk File Carving dengan Metode NIST. *Jurnal Teknologi Dan Sistem Komputer*, *7*(3), 89–92.

FORENSIK DIGITAL SISTEM INFORMASI BERBASIS WEB

ORIGINALITY REPORT

10%	%	%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to STMIK STIKOM Bali Student Paper	3%
2	Submitted to President University Student Paper	2%
3	Submitted to Universitas Mercu Buana Student Paper	2%
4	Submitted to Universitas Esa Unggul Student Paper	1%
5	Submitted to Universitas Hasanuddin Student Paper	1%
6	Submitted to Universitas Islam Riau Student Paper	1%
7	Submitted to Universitas Sebelas Maret Student Paper	1%
8	Submitted to Sriwijaya University Student Paper	<1%
9	Submitted to University of Maryland, University College Student Paper	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		