IMPLEMENTASI METODE OSINT UNTUK MENGIDENTIFIKASI SERANGAN JUDI ONLINE PADA *WEBSITE*

Yusuf Raharja[1]

[1] Informatika, Sains dan Teknologi, Universitas Muhammadiyah Sidoarjo, Indonesia
[1]201080200017@umsida.ac.id

.

Abstrak

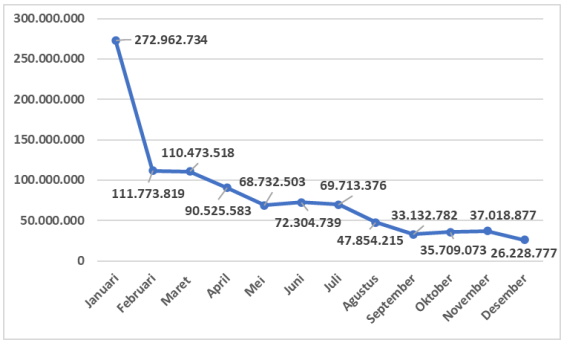
Serangan siber atau *cyber-attack* merupakan sebuah serangan yang dilakukan oleh suatu golongan untuk merusak, mencuri atau mengubah data dari suatu sistem komputer dengan cara memanfaatkan kerentanan sistem tersebut. *Web defacement* merupakan salah satu contoh dari serangan siber yang dilakukan dengan mengubah tampilan halaman dari *website* oleh oknum yang tidak memiliki wewenang. Serangan judi online pada *website* merupakan contoh dari *web defacement*. Judi online merupakan aktivitas taruhan yang dilakukan secara online dengan mempertaruhkan uang atau barang berharga. Serangan judi online semakin marak akibat dari perkembangan judi online yang semakin cepat. Dampak yang terjadi ketika sebuah *website* terkena *web defacement* judi online adalah situs tersebut menampilkan konten judi online. Serangan judi online sering dilakukan pada domain tingkat atas seperti .co.id, .edu, .or.id, dan .com. Penelitian ini menggunakan metode *Open Source Intelligence* (OSINT) dengan teknik google dork untuk mengidentifikasi serangan judi online pada *website* dengan domain .co.id, .edu, .or.id, dan .com. Hasil identifikasi menunjukkan bahwa sebanyak 511.000 situs web dengan domain .co.id, 61.700 situs web dengan domain .edu, 26.800 situs web dengan domain .or.id, dan 6.540.000 situs web dengan domain .com terkena serangan judi online, total 7.149.500 situs web terkena serangan judi online pada keempat domain tersebut.

Kata kunci: google dork, OSINT, serangan judi online, serangan siber, *web defacement*.

.

1. Pendahuluan

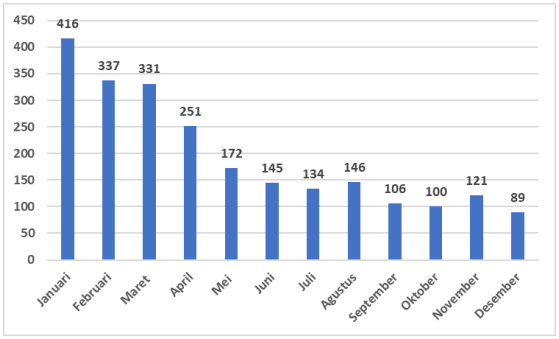
Serangan siber atau *cyber-attack* merupakan sebuah serangan yang dilakukan oleh suatu golongan untuk merusak, mencuri atau mengubah data dari suatu sistem komputer dengan cara memanfaatkan kerentanan sistem tersebut (Hidayatullah, 2023).



Gambar 1. Trafik Anomali Serangan Siber Tahun 2022 (Sumber: Badan Siber dan Sandi Negara)

Gambar 1 menunjukkan trafik anomali serangan siber tahun 2022 dengan jumlah trafik sebesar 976.429.996 jumlah tersebut mengalami penurunan yang cukup besar hingga 40% dari tahun sebelumnya. MyloBot Botnet menempati urutan 1 dalam top 10 trafik anomali dengan jumlah kasus sebanyak 254.260.339 kasus (Yusuf et al., 2022). Serangan siber dapat juga berupa *web defacement*.

Web defacement merupakan sebuah tindakan mengubah tampilan halaman dari *website* oleh orang yang tidak memiliki wewenang (Hariyadi, 2019). SQL *injection* merupakan teknik peretasan yang sering digunakan untuk melakukan *web defacement* dengan memanfaatkan celah keamanan pada sebuah sistem (Aji, 2023).



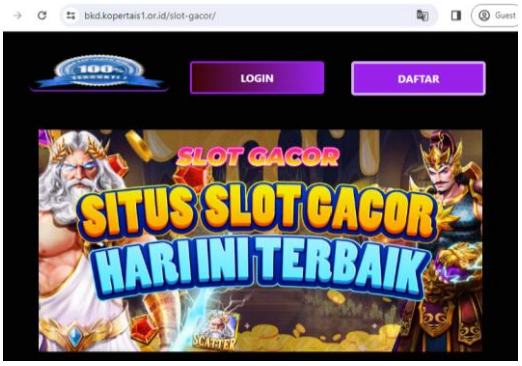
Gambar 2. Data Kasus *Web Defacement* Tahun 2022 (Sumber : Badan Siber dan Sandi Negara)

Gambar 2 menunjukkan data kasus *web defacement* tahun 2022 dengan jumlah kasus sebanyak 2348 kasus, dengan jumlah kasus tertinggi pada bulan Januari dengan total kasus sebesar 416 kasus (Yusuf et al., 2022). Serangan *web defacement*

sering kali dilakukan pada domain yang memiliki level tertinggi yaitu *top level domain* (TLD) atau yang dapat disebut domain tingkat atas.

Top Level Domain (TLD) adalah domain tingkat teratas dalam hirarki *domain name system* (DNS) (Sirait & Simangungsong, 2020). *Top Level Domain* (TLD) yaitu bagian akhir dari nama domain yang berfungsi untuk menunjukkan kategori dari situs web yang terletak pada setelah tanda titik, contoh dari *Top Level Domain* (TLD) antara lain .com, .org, .net, .gov, .edu, .ac.id, .go.id, sch.id, dan .co.id (Iqbal Kurniansyah & Sinurat, 2020). *Top Level Domain* (TLD) terdiri dari beberapa jenis seperti *Generic Top Level Domain* (GTLD), *Premium Top Level Domain* (PTLD), *Country Code Top Level Domains* (CCTLD) (Yesputra et al., 2022). *Top Level Domain* (TLD) tidak luput dari serangan *web defacement* judi online.

Judi online merupakan aktivitas taruhan yang dilakukan secara online dengan mempertaruhkan uang atau barang berharga (Yanuar Vernanda Saputra & Pranoto, 2023). Judi online memiliki berbagai macam jenis seperti slot, judi bola, domino, poker (Sitanggang et al., 2023). Judi online dikategorikan sebagai kejahatan siber atau *cybercrime* (Irawan et al., 2023). Serangan judi online pada *website* merupakan contoh dari *web defacement*, serangan judi online semakin marak akibat dari perkembangan judi online yang semakin cepat. Serangan judi online sering dilakukan pada domain tingkat atas. Dampak yang terjadi ketika sebuah *website* terkena *web defacement* judi online adalah situs tersebut menampilkan konten judi online.



Gambar 3. Web Yang Terkena Serangan Judi Online (Sumber : bkd.kopertais1.or.id)

Gambar 3 menunjukkan akibat dari *web defacement* judi online, tampilan pada *website* tersebut berubah menampilkan konten judi online. Tujuan dari serangan tersebut adalah mempromosikan situs judi tersebut. Metode *Open Source Intelligence* (OSINT) dapat digunakan untuk mengidentifikasi situs web yang terkena serangan judi online.

Open Source Intelligence (OSINT) adalah proses mengumpulkan dan menganalisis informasi yang tersedia untuk umum untuk menghasilkan informasi yang dapat dimanfaatkan dalam pengambilan keputusan (Prasetyo et al., 2023). Menurut Undang-Undang Publik Amerika Serikat, *Open Source Intelligence* adalah informasi yang dikumpulkan dari publik. Informasi ini kemudian dikumpulkan, dianalisis, dan disebarluaskan kepada khalayak yang membutuhkan (Andria, 2021). *Open Source Intelligence* memiliki keuntungan dalam penggunaannya yaitu informasi yang dikumpulkan dari sumber publik yang tidak mengganggu hukum yang berarti legal (Aplikasi et al., 2023). Google dork merupakan salah satu teknik dalam metode *Open Source Intelligence* (OSINT yang memanfaatkan *search engine* google untuk menemukan informasi sensitif dan kerentanan dalam situs web (Abasi et al., 2020).

Penelitian terdahulu yang dilakukan oleh Miftahul Fadli Mutaqin untuk mengidentifikasi serangan judi online menggunakan metode *Open Source Intelligence* (OSINT) dengan teknik google dork. Penelitian tersebut melakukan identifikasi pada 3 domain antara lain .sch.id, .ac.id, dan .go.id, dengan menggunakan operator google dork "site" dan kata kunci "slot". Hasilnya menunjukan bahwa 313.000 situs web dengan domain .sch.id, 1.650.000 situs web dengan domain .ac.id, dan 2.090.000 situs web dengan domain .go.id terkena serangan judi online (Fadli Mutaqin & Ferdiansyah, 2022).

Penelitian ini bertujuan untuk melengkapi gap dari penelitian sebelumnya dengan melakukan identifikasi serangan judi online menggunakan metode *Open Source Intelligence* (OSINT) dengan teknik google dork pada situs web dengan domain .co.id, .edu, .or.id, .com dan menggunakan operator google dork "site" dan "intext" serta kata kunci yang digunakan identik dengan situs judi yaitu "slot gacor" atau "maxwin".

2. Metode

Penelitian ini menggunakan metode *Open Source Intelligence* (OSINT) sebagai metode untuk mengumpulkan informasi terkait situs web yang terkena serangan judi online.

Gambar 4. Alur Pencarian Situs Web Yang Diserang Judi Online.

Gambar 4 menunjukkan alur pencarian situs web yang terserang judi online, berikut adalah penjelasan rinci dari setiap langkah yang ditunjukan pada gambar.

2.1 Kata kunci

Kata kunci digunakan untuk melakukan pencarian, judi online identik dengan kata seperti slot gacor, maxwin. Kata kunci yang akan digunakan dalam pencarian yaitu “slot gacor” atau “maxwin”.

2.2 Operator Khusus

Google dork memiliki beberapa operator khusus untuk menemukan informasi sensitif pada situs web.

Tabel 1 Operator Google Dork

Operator	Penjelasan
Cache	Menunjukkan versi cache dari halaman web yang dicari
Filetype	Mencari jenis file tertentu pada halaman web
Intext	Mencari halaman web yang berisi kata atau frasa tertentu di dalam *body* halaman
Intitle	Menemukan halaman web yang judulnya memiliki frasa atau kata tertentu
Inurl	Mencari halaman web yang URL-nya berisi kata atau frasa tertentu
Link	Mencari halaman web web yang tertaut ke URL tertentu
Site	Mencari secara spesifik suatu halaman web seperti mencari halaman web dengan domain tertentu

Tabel 1 menunjukkan beberapa operator yang umum digunakan pada google dork untuk mencari informasi yang sensitif pada situs web. Operator site digunakan dalam penelitian ini untuk mencari situs web secara spesifik pada domain .co.id, .edu, or.id, dan .com.

2.3 Pencarian

Pencarian dilakukan setelah menentukan kata kunci serta operator yang digunakan. Query yang digunakan pada penelitian ini seperti berikut :

- site:.co.id intext:"slot gacor" | intext:"maxwin"
- site:.edu intext:"slot gacor" | intext:"maxwin"
- site:.or.id intext:"slot gacor" | intext:"maxwin"
- site:.com intext:"slot gacor" | intext:"maxwin"

Query tersebut berarti bahwa pencarian dilakukan pada halaman situs web yang mengandung kata “slot gacor” atau “maxwin” pada bagian *body* halaman web, dengan pencarian dibatasi pada domain .co.id, .edu, .or.id dan .com.

2.4 Hasil Pencarian

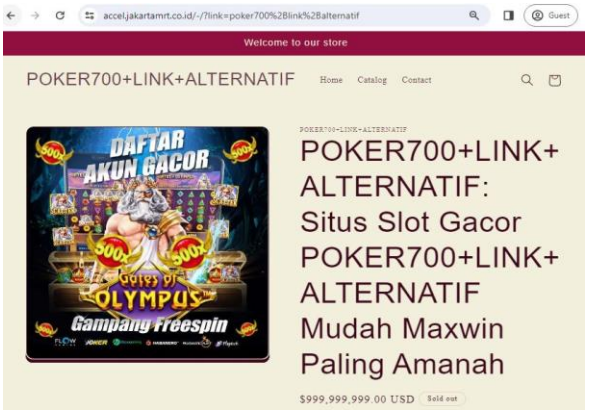
Hasil pencarian diperoleh dari proses pencarian. Hasil tersebut berupa jumlah situs pada domain .co.id, .edu, .or.id dan .com yang terkena serangan judi online.

3. Hasil dan Pembahasan

Metode *Open Source Intelligence* (OSINT) dapat digunakan untuk mengumpulkan informasi terkait serangan judi online secara efektif dengan menggunakan teknik google dork. Penelitian ini menggunakan operator google dork “site” dan “intext” serta kata kunci “slot gacor” atau “maxwin”.

Gambar 5. Pencarian Situs Web Pada Domain .co.id

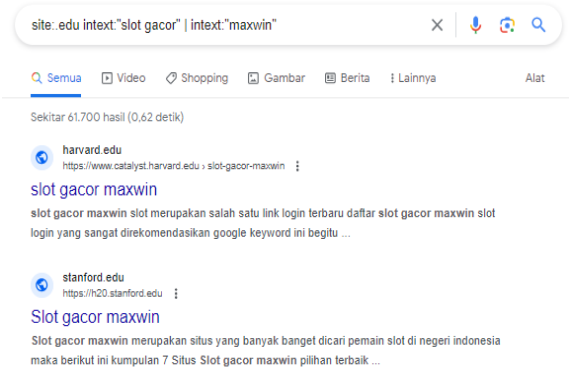
Gambar 5 menunjukkan pencarian situs web dengan domain .co.id yang dilakukan pada tanggal 15 Desember 2023. Hasilnya menunjukkan sebanyak 511.000 situs web yang terkena serangan judi online.



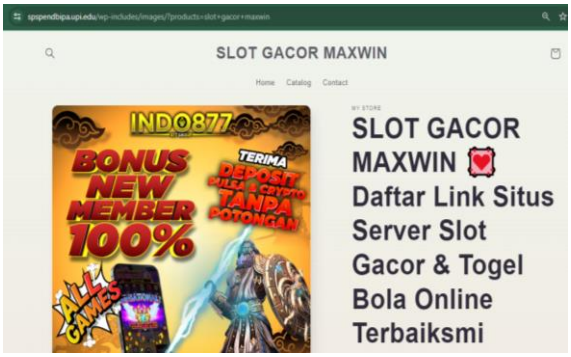
Gambar 6. Konten Judi Online Muncul Pada Situs Web Dengan Domain co.id (Sumber : accel.jakartamrt.co.id)

Gambar 6 menunjukkan salah satu tampilan halaman situs web pada domain co.id yang menampilkan konten judi online akibat dari serangan judi online, dapat dilihat bahwa situs web tersebut terdapat kata yang identik dengan judi online yaitu “slot gacor” atau “maxwin”. Situs web tersebut diakses pada tanggal 15 Desember 2023.

Gambar 7 menunjukkan pencarian situs web dengan domain .edu yang dilakukan pada tanggal 15 Desember 2023. Hasilnya menunjukkan sebanyak 61.700 situs web yang terkena serangan judi online.

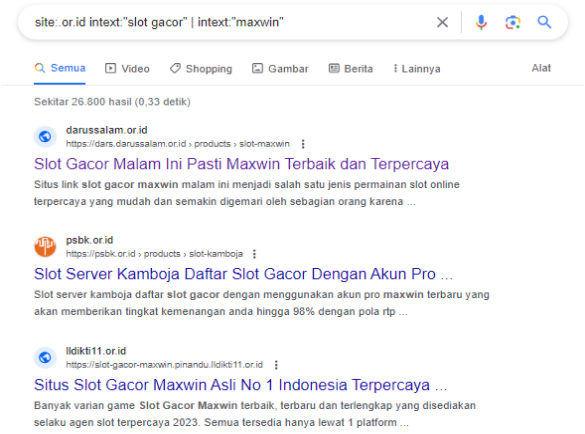


Gambar 7. Pencarian Situs Web Pada Domain .edu



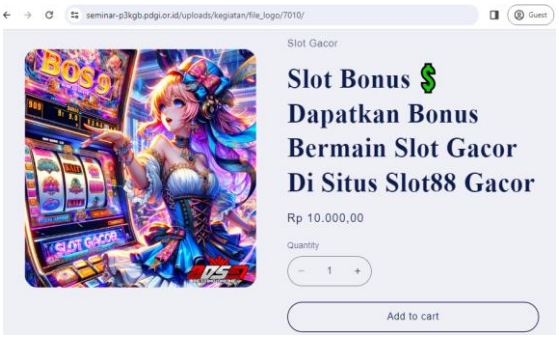
Gambar 8. Konten Judi Online Muncul Pada Situs Web Dengan Domain .edu (Sumber : spspendbipa.upi.edu)

Gambar 8 menunjukkan tampilan salah satu situs web pada domain .edu yang menampilkan konten judi online akibat dari serangan judi online. Situs web yang ada pada gambar merupakan situs web milik salah satu universitas yang ada di Indonesia, pada situs tersebut terdapat kata yang identik dengan judi online yaitu "slot gacor" atau "maxwin". Situs web tersebut diakses pada tanggal 15 Desember 2023



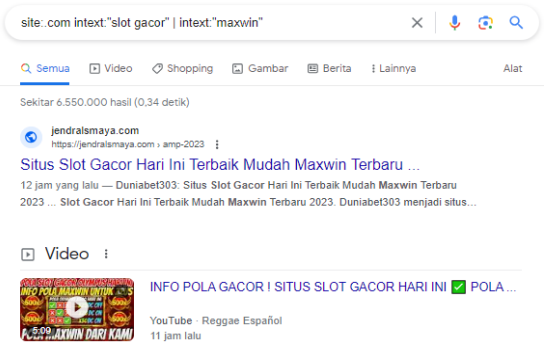
Gambar 9. Pencarian Situs Web Pada Domain .or.id

Gambar 9 menunjukkan pencarian situs web pada domain .or.id yang dilakukan pada tanggal 15 Desember 2023. Hasilnya menunjukkan sebanyak 26.800 situs web yang terkena serangan judi online.



Gambar 10. Konten Judi Online Muncul Pada Situs Web Dengan Domain .or.id (Sumber : seminar-p3kgb.pdgi.or.id)

Gambar 10 menunjukkan tampilan salah satu situs web pada domain .or.id yang menampilkan konten judi online akibat terkena serangan judi online, dapat dilihat bahwa situs web tersebut terdapat kata yang identik dengan judi online yaitu "slot gacor". Situs web tersebut diakses pada tanggal 15 Desember 2023



Gambar 11. Pencarian Situs Web Pada Domain .com

Gambar 11 menunjukkan pencarian situs web pada domain .com yang dilakukan pada tanggal 15 Desember 2023. Hasilnya menunjukkan sebanyak sebanyak 6.550.000 situs web yang terkena serangan judi online.

Gambar 12. Konten Judi Online Muncul Pada Situs Web Dengan Domain .com (Sumber : rsxor.com)

Gambar 12 menunjukkan tampilan salah satu situs web pada domain .com yang menampilkan

konten judi online akibat terkena serangan judi online, tampilan situs web tersebut berisi kata-kata yang identik dengan judi online yaitu "slot gacor". Situs web tersebut diakses pada tanggal 15 Desember 2023

Tabel 2 Hasil Pencarian Situs Web

Domain	Jumlah Situs Web Yang Terkena Serangan Judi Online
.co.id	511.000
.edu	61.700
.or.id	26.800
.com	6.550.000

Tabel 2 menunjukkan hasil pencarian situs web yang terkena serangan judi menggunakan metode *Open Source Intelligence* (OSINT) dengan teknik google dork, yang mencapai total 7.149.500 situs web. Domain .com merupakan domain yang paling banyak terserang judi online dengan total 6.550.000 situs web, menyusul domain .co.id pada urutan kedua dengan total 511.000 situs web, diikuti domain .edu pada urutan ketiga dengan total 61.700 situs web dan pada pada urutan terakhir yaitu domain .or.id dengan total 26.800 situs web.

4. Kesimpulan

Kesimpulan dari penelitian ini adalah bahwa identifikasi serangan judi online pada situs web pada domain .co.id, .edu, .com, dan or.id. dapat menggunakan metode *Open Source Intelligence* (OSINT) dengan teknik google dork. Proses pencarian situs web yang terkena serangan judi online menggunakan metode *Open Source Intelligence* (OSINT) dengan teknik google dork dilakukan pada tanggal 15 Desember 2023. Hasil identifikasi menunjukkan bahwa sebanyak 511.000 situs web dengan domain .co.id, 61.700 situs web dengan domain .edu, 26.800 situs web dengan domain .or.id, dan 6.540.000 situs web dengan domain .com terkena serangan judi online, total 7.149.500 situs web terkena serangan judi online pada keempat domain tersebut.

Saran untuk penelitian selanjutnya yaitu dapat menggunakan metode lain untuk mengidentifikasi serangan judi online pada situs web. Saran untuk pengelola situs web adalah untuk meningkatkan keamanan situs webnya dari serangan judi online dan serangan lainnya yang dilakukan oleh oknum yang tidak bertanggung jawab.

Daftar Pustaka:

Abasi, R., Farooq, A., & Hakkala, A. (2020). *Google dorks: Use cases and Adaption study Reza Abasi: Google dorks: Use cases and adaption study*.

Aji, B. B. (2023). Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website. *Cyber Security Dan Forensik Digital*, *6*(1), 25–29. https://doi.org/10.14421/csecurity.2023.6.1.40

Andria, A. (2021). Forensik Digital Sistem Informasi Berbasis Web. *JAMI: Jurnal Ahli Muda Indonesia*, *2*(2), 33–44. https://doi.org/10.46510/jami.v2i2.73

Aplikasi, A. K., Darnita, Y., Febriansyah, M., Wijaya, A., Apridiansyah, Y., Toyib, R., & Bali, J. (2023). Analisis Komparatif Aplikasi Open Source Intelligence Berbasis Website Dengan Tools Osint Command Line Kominfo Bengkulu. *Jurnal Media Infotama*, *19*(2), 256.

Fadli Mutaqin, M., & Ferdiansyah, D. (2022). Identifikasi Kerentanan Terhadap Serangan Slot Backdoor Pada Website di Indonesia Dengan Menggunakan Metode OSINT. *Pasinformatik*, *1*(2), 1–8. https://doi.org/10.29322/IJSRP.X.X.2018.pXXXX

Hariyadi, D. (2019). Analisis Serangan Web Defacement pada Situs Web Pemerintah Menggunakan ELK Stack | Hariyadi | JISKA (Jurnal Informatika Sunan Kalijaga). *JISKA Research Centre*, *4*(1), 1–8. http://202.0.92.5/saintek/JISKA/article/view/1439

Hidayatullah, C. (2023). Jenis dan Dampak Cyber Crime. *Prosiding SAINTEK: Sains Dan Teknologi*, *2*(1), 216–221. https://www.jurnal.pelitabangsa.ac.id/index.php/SAINTEK/article/view/2159

Iqbal Kurniansyah, M., & Sinurat, S. (2020). Sistem Pendukung Keputusan Pemilihan Server Hosting dan Domain Terbaik untuk WEB Server Menerapkan Metode VIKOR. *JSON (Jurnal Sistem Komputer Dan Informatika)*, *2*(1), 14–24. https://doi.org/10.30865/json.v2i1.2450

Irawan, G., Ramadhan, A., & Raja Ali Haji, M. (2023). *Strategi Badan Siber dan Sandi Negara dalam Mengatasi Permasalahan Judi Online Berdasarkan Perspektif Cyber Crime di Indonesia (National Cyber and Encryption Agency Strategy in Overcoming Online Gambling Problems Based on Cyber Crime Perspective in Indone*. *1*(4), 854–867.

Prasetyo, D., Sebayang, N., & Dillianto, B. (2023). Pemanfaatan Open Source Intelligence dalam Membantu Tugas TNI untuk Melindungi Pertahanan Negara. *JIIP - Jurnal Ilmiah Ilmu Pendidikan*, *6*(10), 7963–7966. https://doi.org/10.54371/jiip.v6i10.3016

Sirait, T. N., & Simangungsong, J. B. (2020). Analisis Yuridis Pelaksanaan Tugas Pokok Pengelola Domain Internet Indonesia. *Nommensen Journal of Legal Opinion*, *1*(01), 52–62. https://doi.org/10.51622/njlo.v1i01.38

Sitanggang, A., Sari, B. P., Sidabutar, E. D., Cahya, M., Nababan, R. Y., & Medan, U. N. (2023). Penegakan Undang-Undang ITE Terhadap Kasus Judi Online. *Mediation : Journal of Law*,

2, 16–22.

Yanuar Vernanda Saputra, M., & Pranoto, E. (2023). Pencegahan Tindak Pidana Perjudian Online. *PLEDOI (Jurnal Hukum Dan Keadilan)*, *2*(1), 20–30. https://doi.org/10.56721/pledoi.v2i1.171

Yesputra, R., Efendi Hutagalung, J., & Saputra, E. (2022). Workshop Pemahaman Search Engine Optimization Untuk Optimalisasi Website Desa Di Kabupaten Batubara. *Jurnal Bangun Abdimas*, *1*(1), 29–39. https://doi.org/10.56854/ba.v1i1.8

Yusuf, A., Ariyanto, T., & Amanda, C. D. (2022). Keamanan siber indonesia 2022. *Badan Siber Dan Sandi Negara*.