Modul 2 – Search Intelligence & Digital Footprint

Kuasai teknik pencarian lanjutan dan analisis jejak digital untuk menemukan informasi yang tersembunyi dari pencarian biasa. Modul ini dirancang untuk membekali Anda dengan kemampuan investigasi digital yang sistematis dan profesional.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Gambaran Umum Modul

Apa yang Akan Anda Pelajari?

Modul ini mencakup enam topik utama yang membawa Anda dari teknik pencarian dasar hingga investigasi domain dan infrastruktur digital secara mendalam.

01

Teknik Pencarian Lanjutan

Operator dan strategi pencarian yang melampaui kemampuan Google biasa

02

Google Dorking

Menemukan data sensitif yang terekspos secara tidak sengaja di internet

03

Analisis Jejak Digital

Memahami dan memetakan jejak yang ditinggalkan individu atau organisasi

04

Investigasi Domain & WHOIS

Mengungkap informasi kepemilikan dan infrastruktur sebuah website

Teknik Pencarian Lanjutan

Mesin pencari seperti Google menyimpan jauh lebih banyak informasi daripada yang muncul di halaman pertama. Dengan memahami operator pencarian lanjutan, investigator dapat menyaring hasil secara presisi dan menemukan konten yang tidak terindeks secara langsung.

site:

Membatasi hasil hanya dari domain tertentu. Contoh: `site:kemenkeu.go.id laporan`

filetype:

Mencari jenis file tertentu seperti PDF, XLS, atau DOCX yang dipublikasikan secara online

intitle:

Mencari kata kunci spesifik yang muncul dalam judul halaman web

inurl:

Menyaring halaman berdasarkan kata kunci yang terdapat dalam URL

Teknik Investigasi

Google Dorking Dasar

Google Dorking adalah teknik menggunakan operator pencarian khusus (Google Dorks) untuk menemukan informasi sensitif yang tidak sengaja terekspos ke publik. Teknik ini digunakan secara legal oleh peneliti keamanan dan investigator untuk mengidentifikasi kerentanan dan data yang bocor.

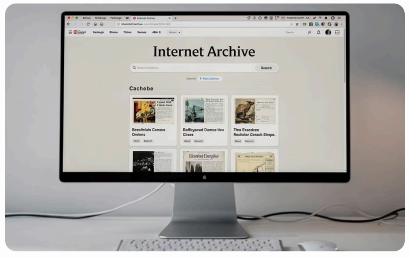
⚠ Gunakan Google Dorking hanya untuk tujuan investigasi yang sah dan etis. Mengakses sistem tanpa izin adalah tindakan ilegal.

Contoh Dork Populer

```
intitle:"index of" password

filetype:xls "username" "password"

site:.go.id filetype:pdf "rahasia"

inurl:admin intitle:login

intitle:"webcam" inurl:view
```

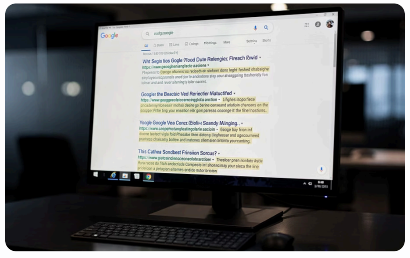
Mencari Informasi Tersembunyi

Informasi yang tampaknya sudah dihapus atau tidak dipublikasikan seringkali masih dapat ditemukan melalui berbagai teknik dan layanan khusus. Investigator digital perlu memahami tempat-tempat digital di mana data tersebut dapat bertahan.



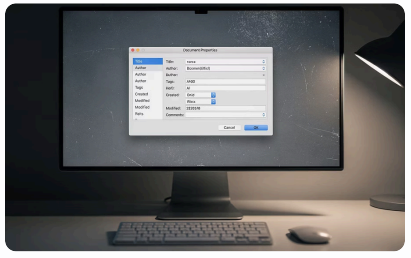
Wayback Machine

Mengakses snapshot historis sebuah website dari masa lalu melalui **web.archive.org**, bahkan setelah konten dihapus



Cache Google

Melihat versi tersimpan halaman web yang diindeks Google, berguna ketika halaman asli sudah tidak dapat diakses



Metadata Dokumen

Dokumen PDF dan Office menyimpan metadata seperti nama penulis, tanggal edit, dan perangkat yang digunakan

Analisis Jejak Digital

Setiap aktivitas online meninggalkan jejak — disebut **Digital Footprint**. Memahami dan memetakan jejak ini adalah inti dari investigasi OSINT modern.

Jejak Aktif

Informasi yang sengaja dipublikasikan: postingan media sosial, profil publik, komentar forum, dan data registrasi website

Jejak Pasif

Data yang dikumpulkan tanpa disadari: log akses, cookies, alamat IP, dan data lokasi dari perangkat

Jejak Organisasi

Infrastruktur digital organisasi: domain, subdomain, alamat IP server, email karyawan, dan dokumen publik

Investigasi Domain

WHOIS & DNS Lookup

Dua alat fundamental dalam investigasi domain yang membantu mengungkap identitas pemilik dan struktur infrastruktur sebuah website.

WHOIS Lookup

Database publik yang menyimpan informasi registrasi domain, termasuk:

- Nama dan kontak pemilik domain
- Tanggal pendaftaran dan kedaluwarsa
- Registrar yang digunakan
- Nameserver yang terdaftar

DNS Lookup

Memetakan infrastruktur teknis sebuah domain, antara lain:

- Record A – alamat IP server utama
- Record MX – server email yang digunakan
- Record CNAME – alias atau subdomain
- Record TXT – verifikasi dan kebijakan SPF

Tools yang direkomendasikan: **who.is**, **whois.domaintools.com**, **dnschecker.org**, dan **MXToolbox**

Tools yang Digunakan

Berikut adalah toolkit utama yang akan digunakan dalam modul ini. Setiap tool memiliki keunggulan dan kasus penggunaan yang berbeda dalam investigasi digital.

Google Advanced Search

Antarmuka visual untuk membangun query pencarian kompleks tanpa harus menghafal operator. Tersedia di **google.com/advanced_search**. Ideal untuk pemula yang baru memulai investigasi berbasis pencarian.

WHOIS Lookup

Layanan seperti **who.is** dan **DomainTools** memungkinkan pencarian data registrasi domain secara instan. Berguna untuk mengidentifikasi pemilik domain dan riwayat kepemilikan.

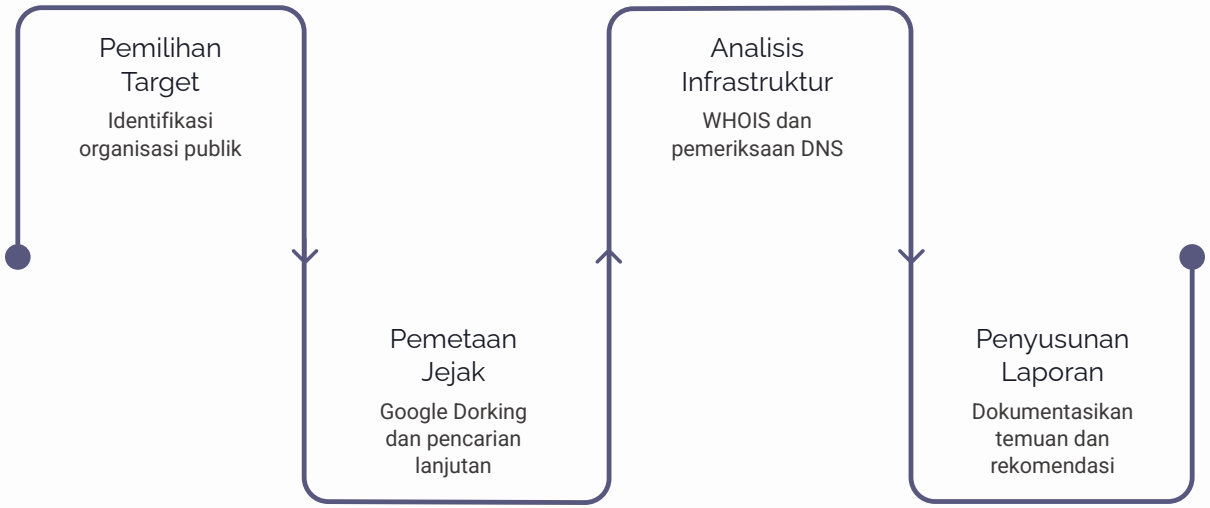
DNS Lookup

Tools seperti **dnschecker.org** dan **nslookup** membantu memetakan record DNS sebuah domain dan mengungkap infrastruktur server yang ada di balik sebuah website.

Sesi Praktik

Investigasi Jejak Digital Organisasi Publik

Pada sesi praktik ini, peserta akan melakukan investigasi nyata terhadap sebuah organisasi publik menggunakan teknik dan tools yang telah dipelajari.



Setiap peserta akan mendokumentasikan temuan mereka secara sistematis — mulai dari identifikasi target, pemetaan jejak digital, hingga analisis infrastruktur domain. Praktik ini mensimulasikan alur kerja investigator digital profesional.

Ringkasan Modul 2

Capaian & Outcome Pembelajaran

Setelah menyelesaikan Modul 2, peserta diharapkan memiliki kemampuan praktis berikut:

Pencarian Presisi

Mampu menggunakan operator Google dan Google Dorks untuk menemukan informasi spesifik secara efisien

Analisis Footprint

Mampu mengidentifikasi dan memetakan jejak digital aktif maupun pasif milik individu atau organisasi

Investigasi Domain

Mampu menggunakan WHOIS dan DNS Lookup untuk mengungkap kepemilikan dan infrastruktur website

Dokumentasi Temuan

Mampu menyusun laporan investigasi digital yang sistematis dan dapat dipertanggungjawabkan

Peserta yang menguasai modul ini mampu menemukan informasi yang tidak mudah ditemukan melalui pencarian biasa — fondasi dari setiap investigasi OSINT yang efektif.