

The background of the slide is a dark blue circuit board. In the center-left, there is a glowing blue microchip with a bright white light emanating from its center, surrounded by smaller blue sparks. The word "SANS" is written in a large, white, serif font in the top right corner.

SANS

ゼロからはじめるOSINT Open Source Intelligence

SANS Institute
Technical Manager 上田 健吾
<https://www.sans.org>

SANS Institute

Technical Manager 上田 健吾 (Kengo UEDA)

2000年にセキュリティベンチャー起業後、文部科学省 21世紀COE研究員（慶應義塾大学大学院 後期博士課程）を経て、2007年に野村総合研究所に入社。NRIセキュアテクノロジーズに出向し、銀行、生損保、クレジットカード業界をはじめ、セキュリティ監査、ペネトレーションテスト、フォレンジック、事故対応支援やコンサルティングなど、数多くのセキュリティ関連プロジェクトに参加。東京工業大学にて特定准教授として情報セキュリティの講義も担当。2021年6月より現業。

GSEC、GCIH、GWEB、GWAPT、CISSP、CISA、CISM、QSA、ASV、情報セキュリティ主任監査人など、セキュリティ系の資格を多数取得。IT雑誌、学会誌への寄稿や、ニュースへの出演経験、登壇経験も多数。業務を通して得られる最新の情報を展開。

Agenda

01

OSINTの基礎

02

OSINTで用いられる技術例

検索・メタデータ・画像分析・SNSの活用

03

Dark Web

04

OSINT技術を身につけるために

Agenda

01

OSINTの基礎

02

OSINTで用いられる技術例

検索・メタデータ・画像分析・SNSの活用

03

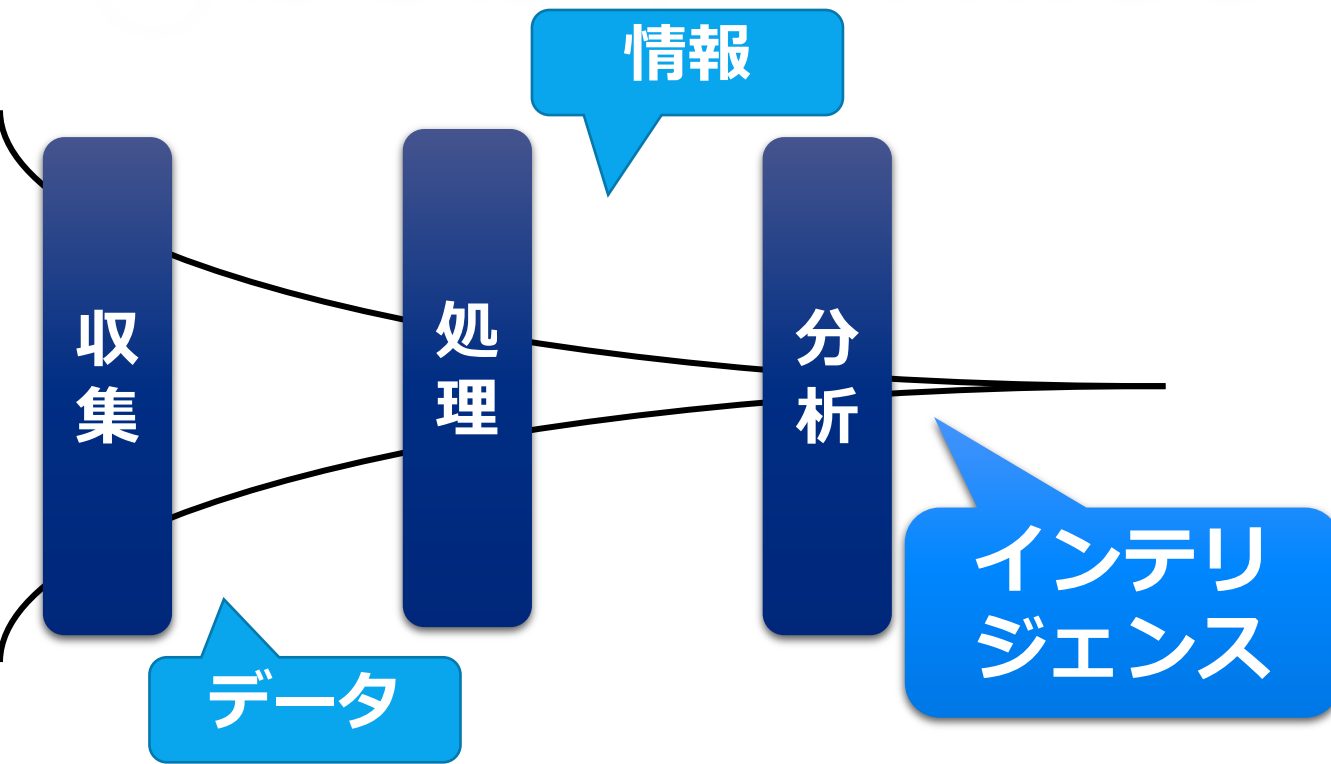
Dark Web

04

OSINT技術を身につけるために

What is OSINT?

Open Source INTelligence



インターネットをはじめとする多くの情報源からデータを収集し、分析・精査・取捨選択を行い、特定の個人やシステム、組織などについての調査を行う手法

- ・テキスト（文書、ブログなど）
- ・メディア（音声、ビデオ、写真など）
- ・位置情報（マップ、GPSなど）

OSINT Process

計画

- OSINTの目的とゴールを策定

収集

- 必要な情報を検索・収集

処理

- 複数の言語・フォーマットの情報をノーマライズ

分析

- 収集した情報の分析



Inaccurate Data

意図せず不正確なデータ

- OCRの誤認識、誤植など

古すぎるデータ

- 更新されていないwhois情報など

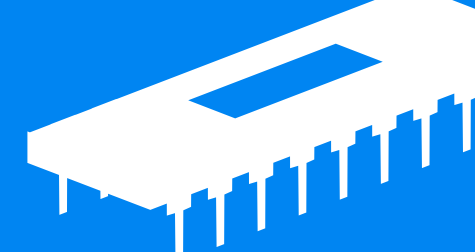
ターゲットに似た人物のデータ

- 同姓同名の人物など

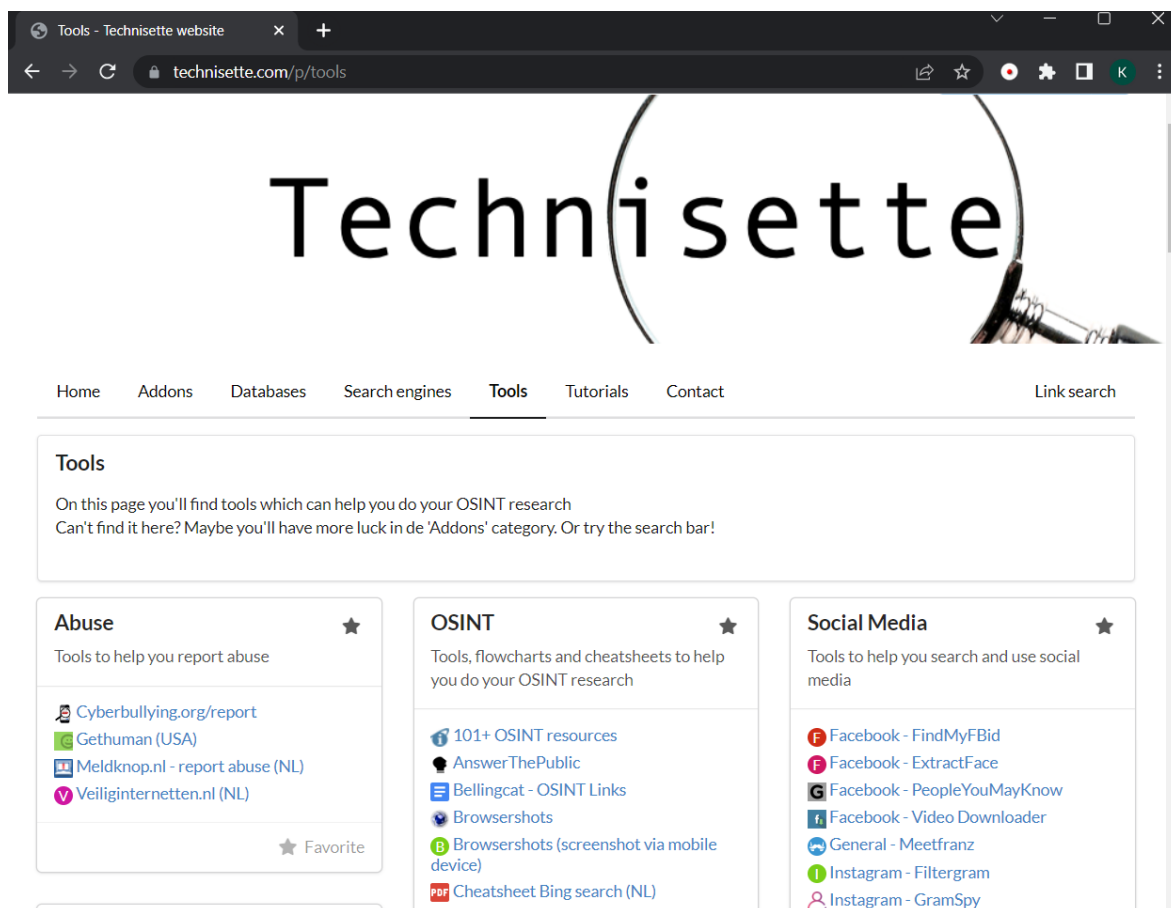
偽情報

- 自慢や偽りの情報、捜査攪乱情報など





<https://technisette.com>



OSINTに活用できるリンク集

- 世界各国の検索エンジン
- ブラウザのアドオン
- 世界各国のWhoisデータベース
- 世界各国の電話番号リスト
- 写真データベース
- 政府情報
- SNS
- OSINTので利用できるツール集
- OSINTチュートリアルビデオ

Agenda

01

OSINTの基礎

02

OSINTで用いられる技術例

検索・メタデータ・画像分析・SNSの活用

03

Dark Web

04

OSINT技術を身につけるために

Google Cheat Sheet

<https://www.sans.org/posters/google-hacking-and-defense-cheat-sheet/>

Operator Examples	
Operator Example	Finds Pages Containing
<i>sailboat chesapeake bay</i>	the words sailboat , Chesapeake and Bay
<i>sloop OR yawl</i>	either the word sloop or the word yawl
<i>"To each his own"</i>	the exact phrase to each his own
<i>virus -computer</i>	the word virus but NOT the word computer
<i>Star Wars Episode +III</i>	This movie title, including the roman numeral III
<i>~boat loan</i>	loan info for both the word boat and its synonyms: canoe , ferry , etc.
<i>define:sarcastic</i>	definitions of the word sarcastic from the Web
<i>mac * x</i>	the words Mac and X separated by exactly one word
<i>I'm Feeling Lucky (Google link)</i>	Takes you directly to first web page returned for your query

Search Parameters		
Search Parameters	Value	Description of Use in Google Search URLs
q	the search term	The search term
filter	0 or 1	If filter is set to 0, show potentially duplicate results.
as_epq	a search phrase	The value submitted is as an exact phrase. No need to surround with quotes.
as_ft	i = include e = exclude	The file type indicated by as_filetype is included or excluded in the search.
as_filetype	a file extension	The file type is included or excluded in the search indicated by as_ft .
as_occt	any = anywhere title = page title body = text of page url = in the page URL links = in links to the page	Find the search term in the specified location.
as_dt	i = include e = exclude	The site or domain indicated by as_sitesearch is included or excluded in the search.
as_sitesearch	site or domain	The file type is included or excluded in the search indicated by as_dt .
as_qdr	m3 = three months m6 = six months y = past year	Locate pages updated with in the specified time frame.



Purpose

This document aims to be a quick reference outlining all Google operators, their meaning, and examples of their usage.

What to use this sheet for

Use this sheet as a handy reference that outlines the various Google searches that you can perform. It is meant to support you throughout the Google Hacking and Defense course and can be used as a quick reference guide and refresher on all Google advanced operators used in this course. The student could also use this sheet as guidance in building innovative operator combinations and new search techniques.

This sheet is split into these sections:

- Operator Examples
- Advanced Operators
- Number Searching
- Calculator Operators
- Search Parameters

Google Hacking DB

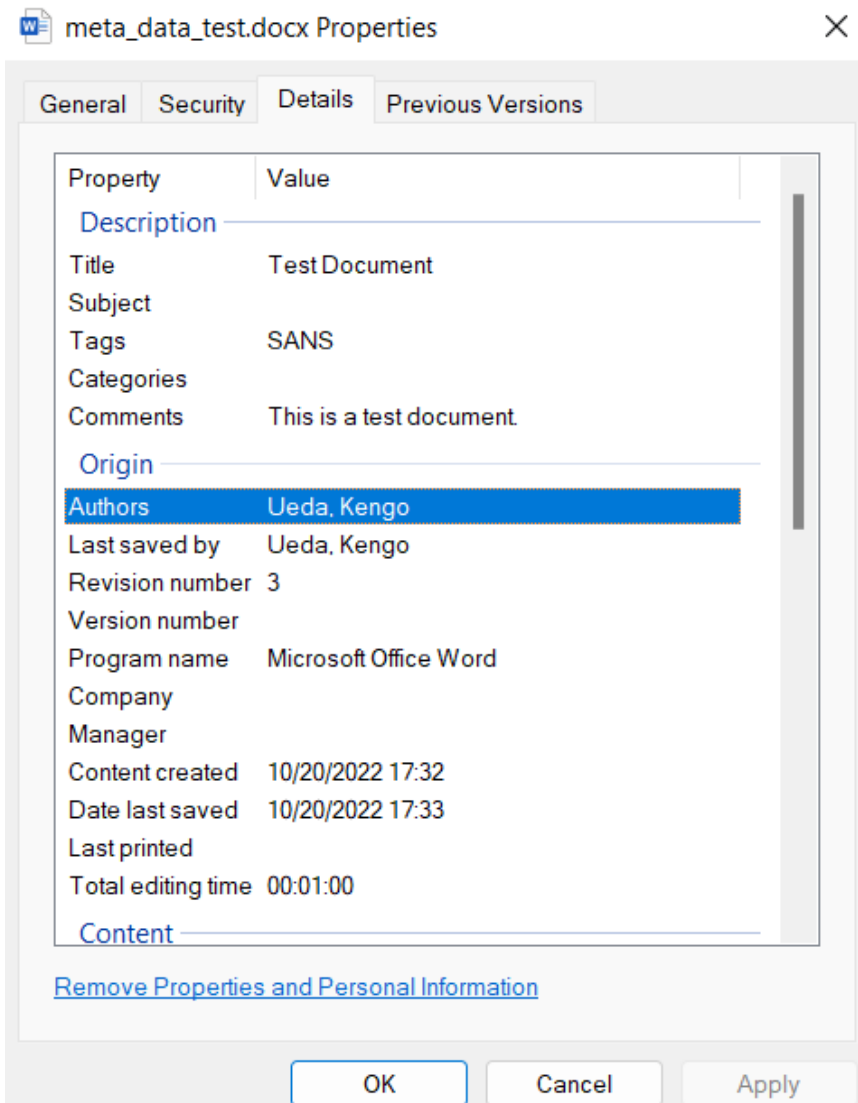
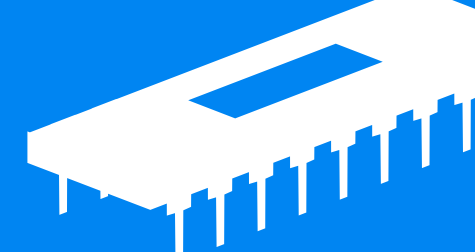
<https://www.exploit-db.com/google-hacking-database>



The screenshot shows the 'Google Hacking Database' section of the Exploit Database website. The header includes the 'EXPLOIT DATABASE' logo and navigation icons. The main content area has a title 'Google Hacking Database', a 'Filters' button, a 'Reset All' button, and a 'Quick Search' input field. A 'Show 15' dropdown menu is also present. Below the search bar, there is a table with columns for 'Date Added', 'Dork', 'Category', and 'Author'. The table lists several search queries and their corresponding categories and authors.

Date Added	Dork	Category	Author
2022-09-19	intext:"index of" ".sql"	Files Containing Juicy Info	Gopalsamy Rajendran
2022-09-19	intitle:"index of" inurl:superadmin	Files Containing Juicy Info	Mahedi Hassan
2022-09-19	intitle:"WAMPSEVER Homepage"	Files Containing Juicy Info	HackerFrenzy
2022-09-19	inurl: json beautifier online	Files Containing Juicy Info	Nyein Chan Aung
2022-09-19	intitle:"IIS Windows Server"	Files Containing Juicy Info	HackerFrenzy
2022-09-19	intitle:"index of" inurl:SUID	Files Containing Juicy Info	Mahedi Hassan
2022-09-19	intitle:"index of" intext:"Apache/2.2.3"	Files Containing Juicy Info	Wagner Farias
2022-08-18	inurl:"index.php?page=news.php"	Advisories and Vulnerabilities	Omar Shash
2022-08-18	inurl:/sym404/root	Files Containing Juicy Info	Numen Blog

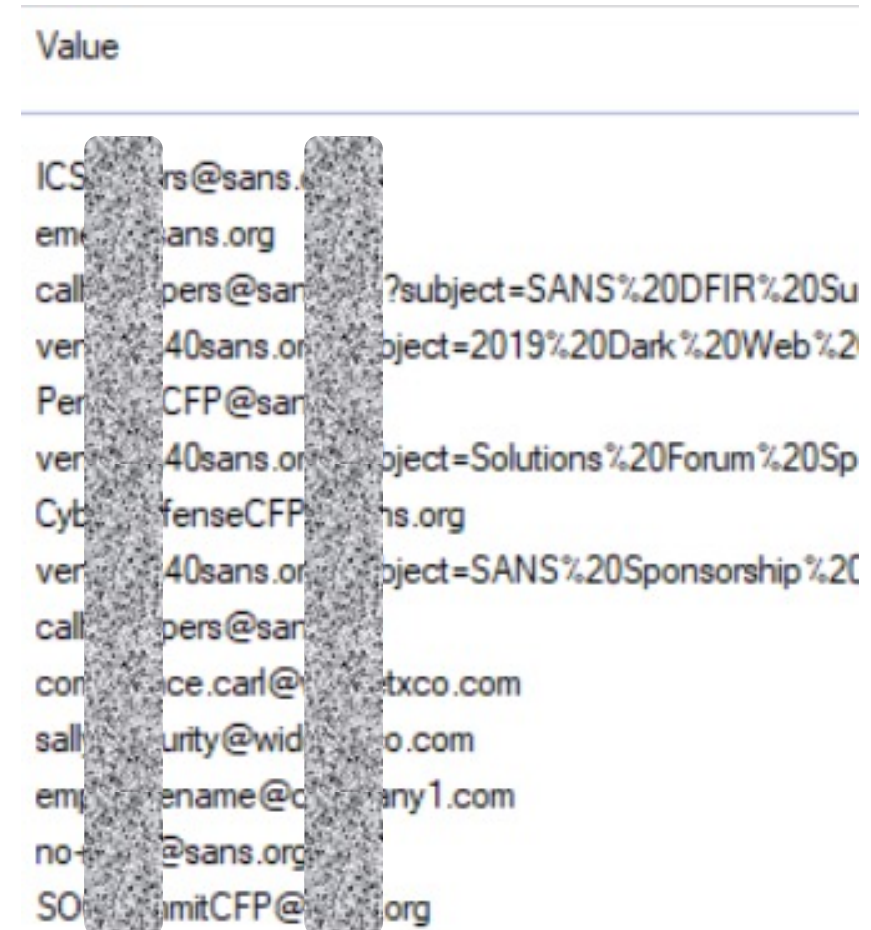
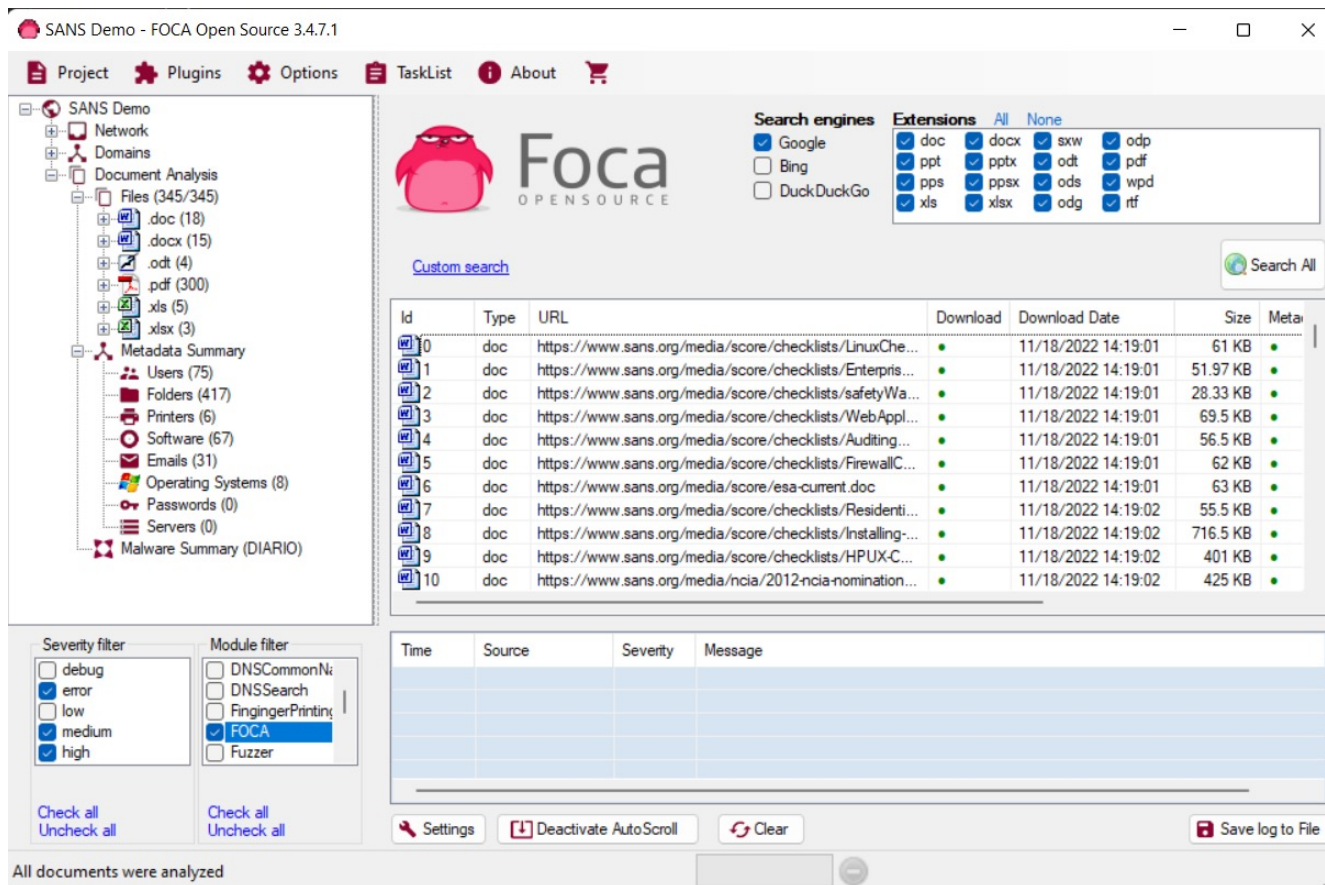
Meta Data



- ユーザ名
- 作成者 / 編集者の氏名
- 会社名
- 部署名 / 属性など
- ソフトウェア名
- GPS位置情報
- 写真を撮影した日付や時刻
- 利用しているカメラ / 電話など
- PC上の場所
- PC上のタイムスタンプ などなど

FOCA

ドメインを指定するとGoogleからそのドメインで公開されているファイル類を検索してダウンロードし、それらのファイルに含まれるメタデータを解析する。



Reverse Image Search

画像検索エンジンを用いて入手した画像に関するデータを収集

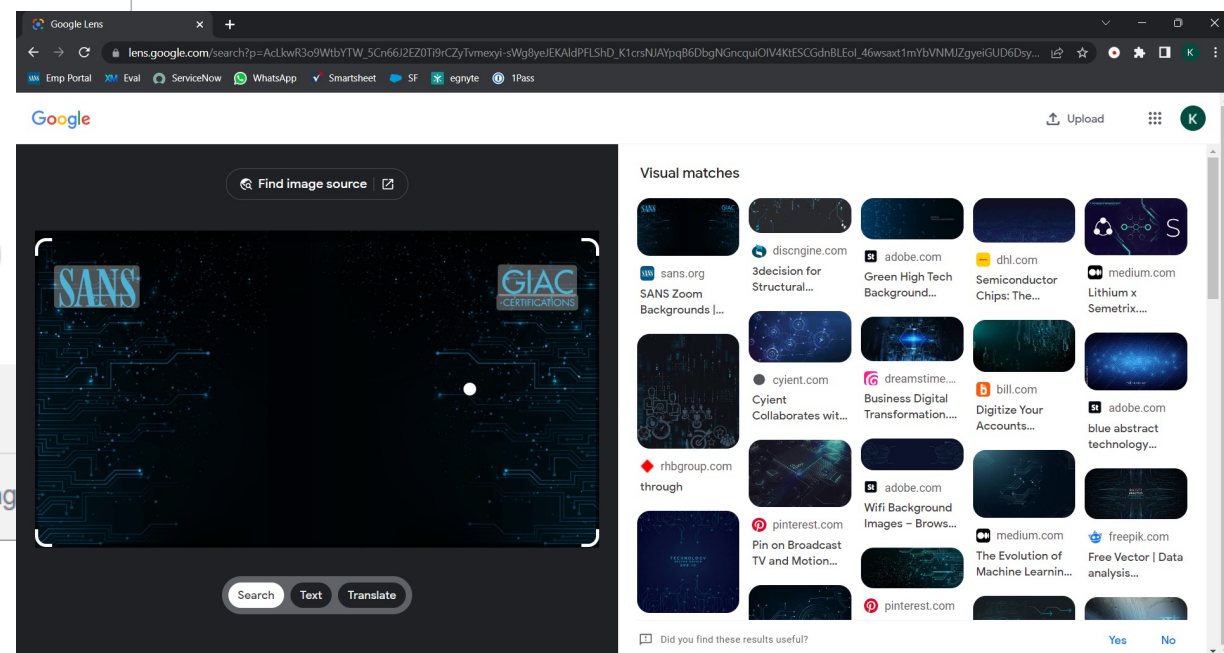
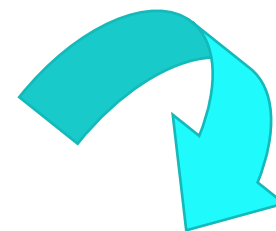
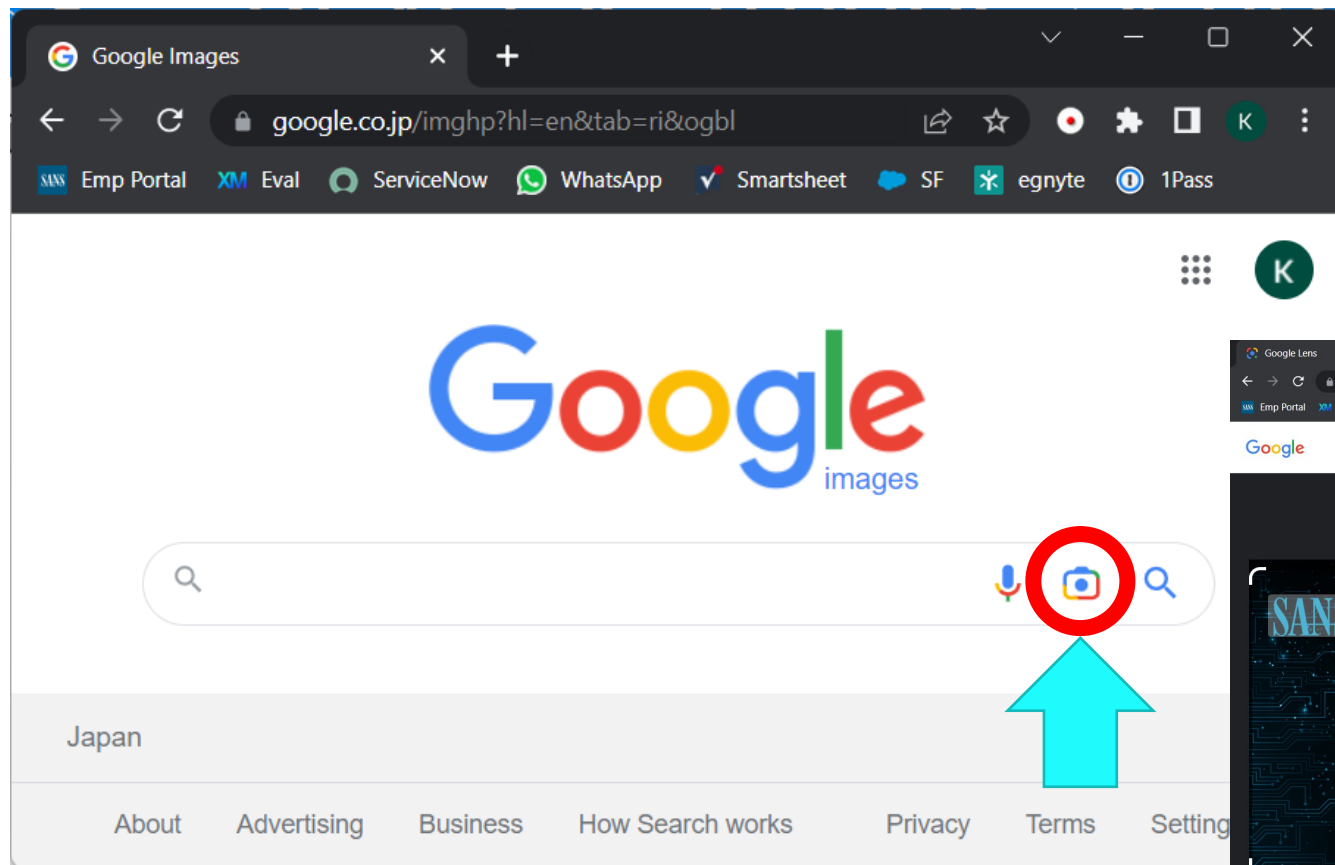


Image Analysis

投稿前後の文脈を分析

- 写真を投稿する前後の投稿を分析

写真の前景を分析

- 撮影対象と撮影者の間のオブジェクトを分析

写真の背景を分析

- 山や建物などの地理的特徴を分析

場所に関する目印を検出

- 看板や標識、ロゴや像などの目印を検出・分析

～ 試行錯誤 ～



Image Analysis Sample

ここはいったいどこでしょう？



Image Analysis Sample

Reverse Image Searchで川沿いのレールや建物のイメージが近い写真を発見

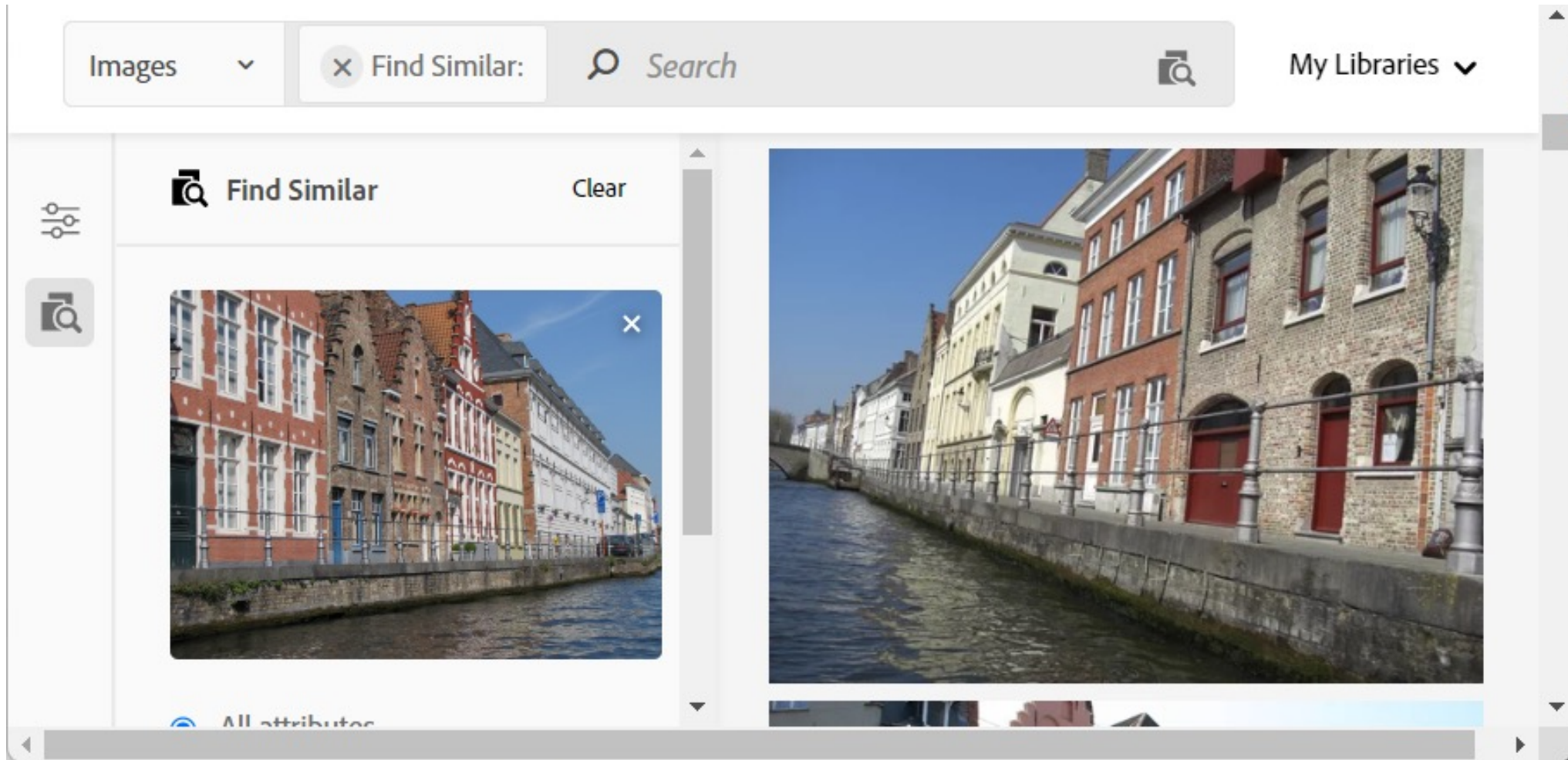


Image Analysis Sample

Reverse Image Searchで川沿いのレールや建物のイメージが近い写真を発見



Bruges

Save to Library

Download Preview

☒ Standard license (Free with trial) ⓘ

☐ Extended license (US\$79.99) ⓘ

Download free with trial

Image Analysis Sample

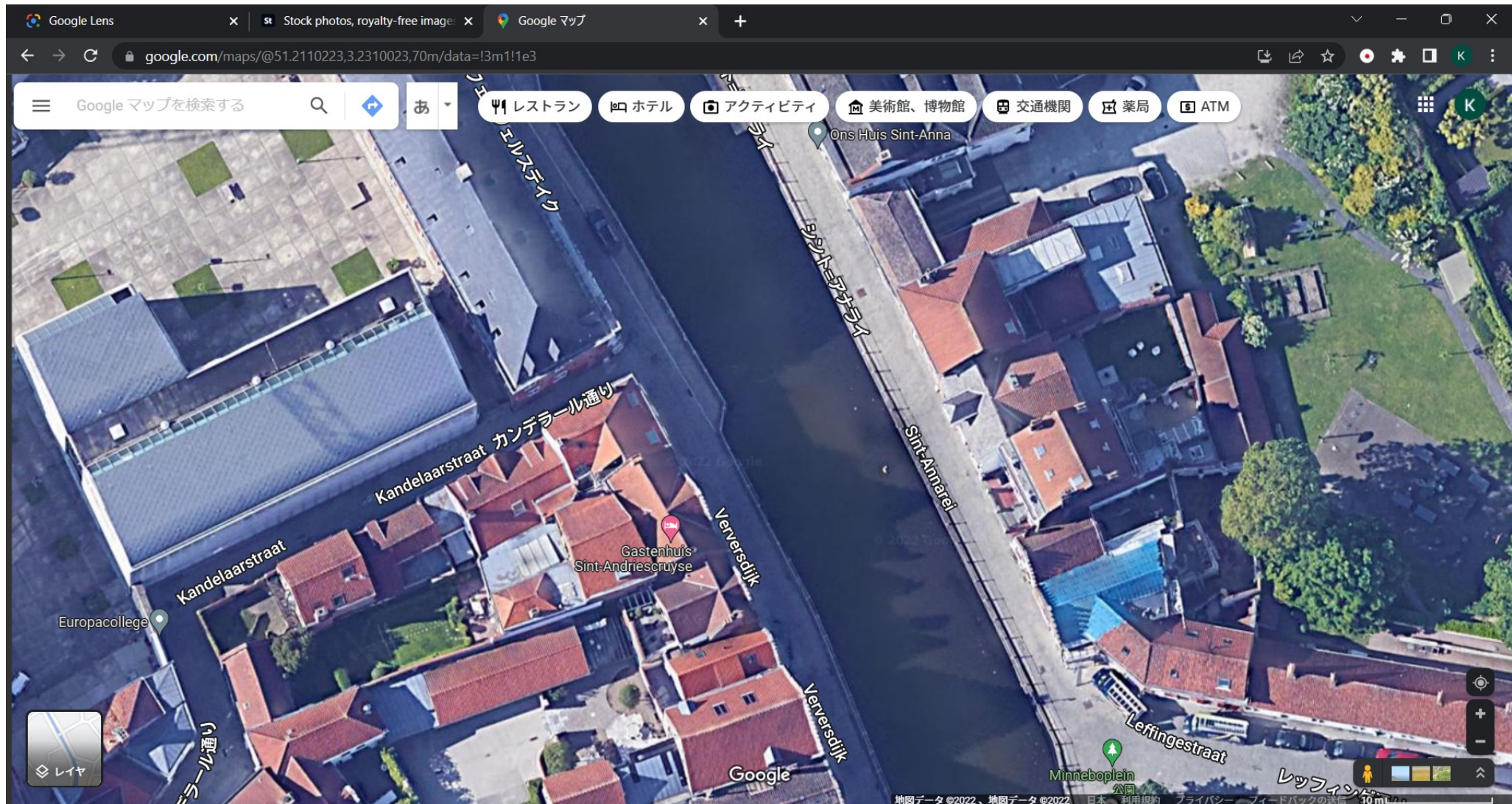
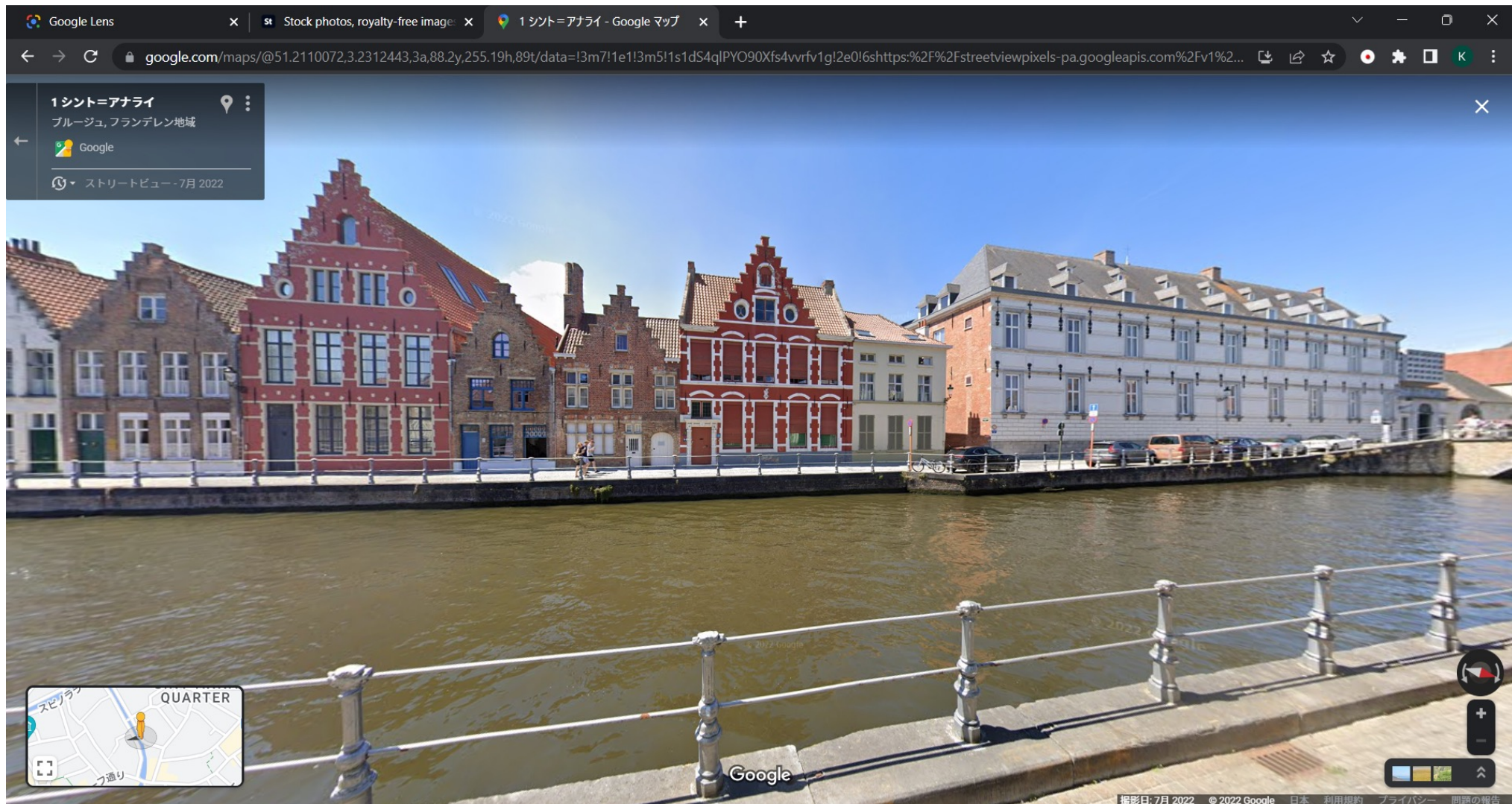


Image Analysis Sample



Connection on SNS



利点

- 迅速に、かつ大量の情報を入手可能

欠点

- 対象に気づかれる可能性

調査対象の配偶者や子ども、親族や友人、同僚などにつながることも可能

Twitter for OSINT

アカウントのBio/URL/Location

フォロー/フォロワーなどのつながり

行動パターン

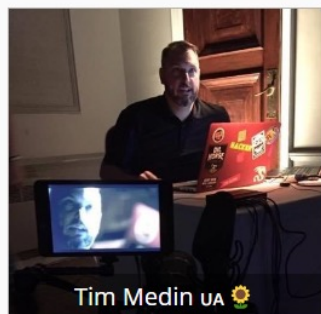
写真やビデオ

場所の情報

トピックに関する感情



Social Bearing



Tim Medin ua

Kerberoast Guy • @RedSiege CEO •
SANS 560 Author, Senior Instructor
• Hater of Mac N Cheese • Packers
owner • Work Req:
<https://t.co/ALJldLMDfZ>

Created on: 5/1/2008
TUQI Score: 11.08
Website: redsiege.com
Location: Longview, TX
Tweets: 17953
Tweets/day: 3.38
Followers: 16233
Following: 558
Frnd/Fllw ratio: 29.09
Twt/Fllw ratio: 0.9
Favourited: 43328
In lists: 307
Last tweet: 5h ago
Last tweet via: Twitter for iPhone
Language: English

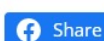
@TimMedin on Twitter

Supporting Social Bearing
will help develop new
features, cover running
costs and keep this site free

FILTERS

User search & analytics for '@TimMedin'

Showing the user timeline for @TimMedin. Twitter limits number of tweets returned to 3,200



TWEETS

198

LOAD MORE

TIMEFRAME

53 days

REACH

16,340

IMPRESSIONS

1,575,284

TOTAL RT'S

62,851

@0

TOTAL FAVES

478,044

@0

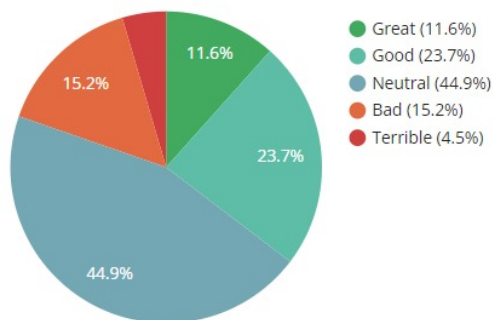
REPLIES

101

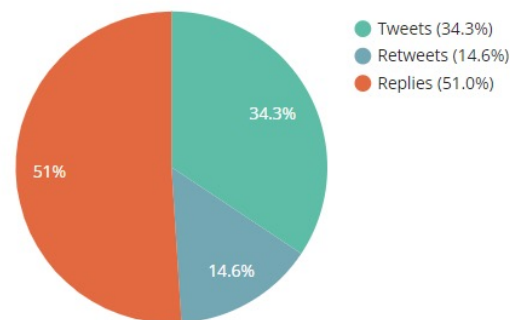
HIDDEN

0

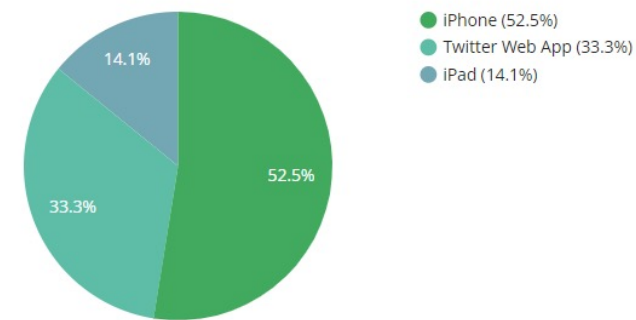
TWEETS BY SENTIMENT



TWEETS BY TYPE



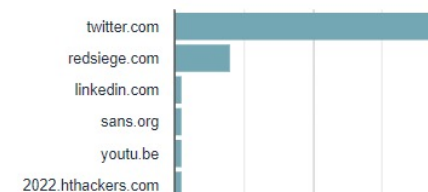
TWEETS BY SOURCE



TWEETS BY LANGUAGE



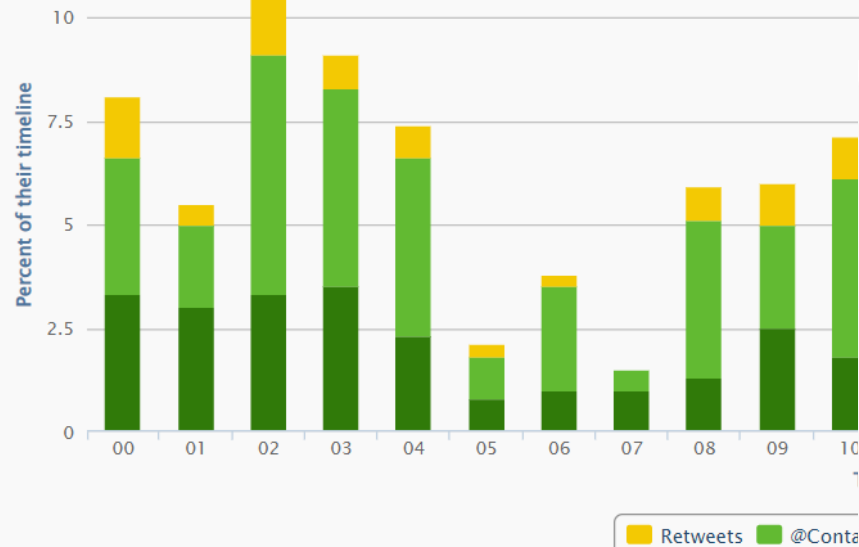
TOP DOMAINS SHARED



Followerwonk

Most active hours for TimMedin

This chart details TimMedin's Twitter activity. Using up to 400 of their most recent actions, we chart when they tweet, @contact tweet (ones that begin with someone's name), and retweet. Compare to the above chart to see how their activity compares to their friends.



Bio word cloud of users TimMedin follows

To help make sense of the "biography" field of each Twitter user, we've assembled this word cloud which shows you the most frequently occurring words.

security — sans — instructor — author — hacker — own — infosec — hehim — cyber — cybersecurity — opinions — founder — tweets — team — researcher — director — red — research — former — husband — consultant — mastodon — views — father — things

Two word bio cloud

sans instructor — information security — red team — cyber security — incident response

Location word cloud of users TimMedin follows

Similar to the above word cloud, here we show you the relative frequency of words used in the "location" field of users TimMedin follows.

usa — tx — texas — washington — dallas — fl — austin — dc — ca

Agenda

01

OSINTの基礎

02

OSINTで用いられる技術例

検索・メタデータ・画像分析・SNSの活用

03

Dark Web

04

OSINT技術を身につけるために

Dark Web

Surface Web

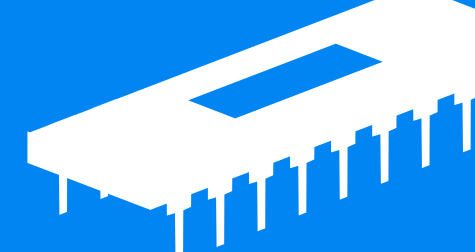
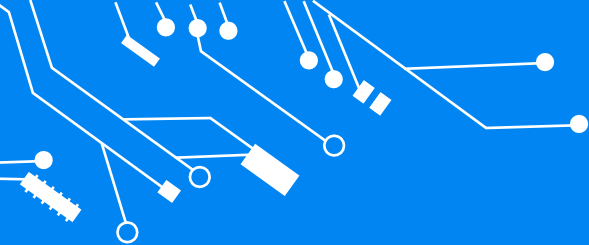
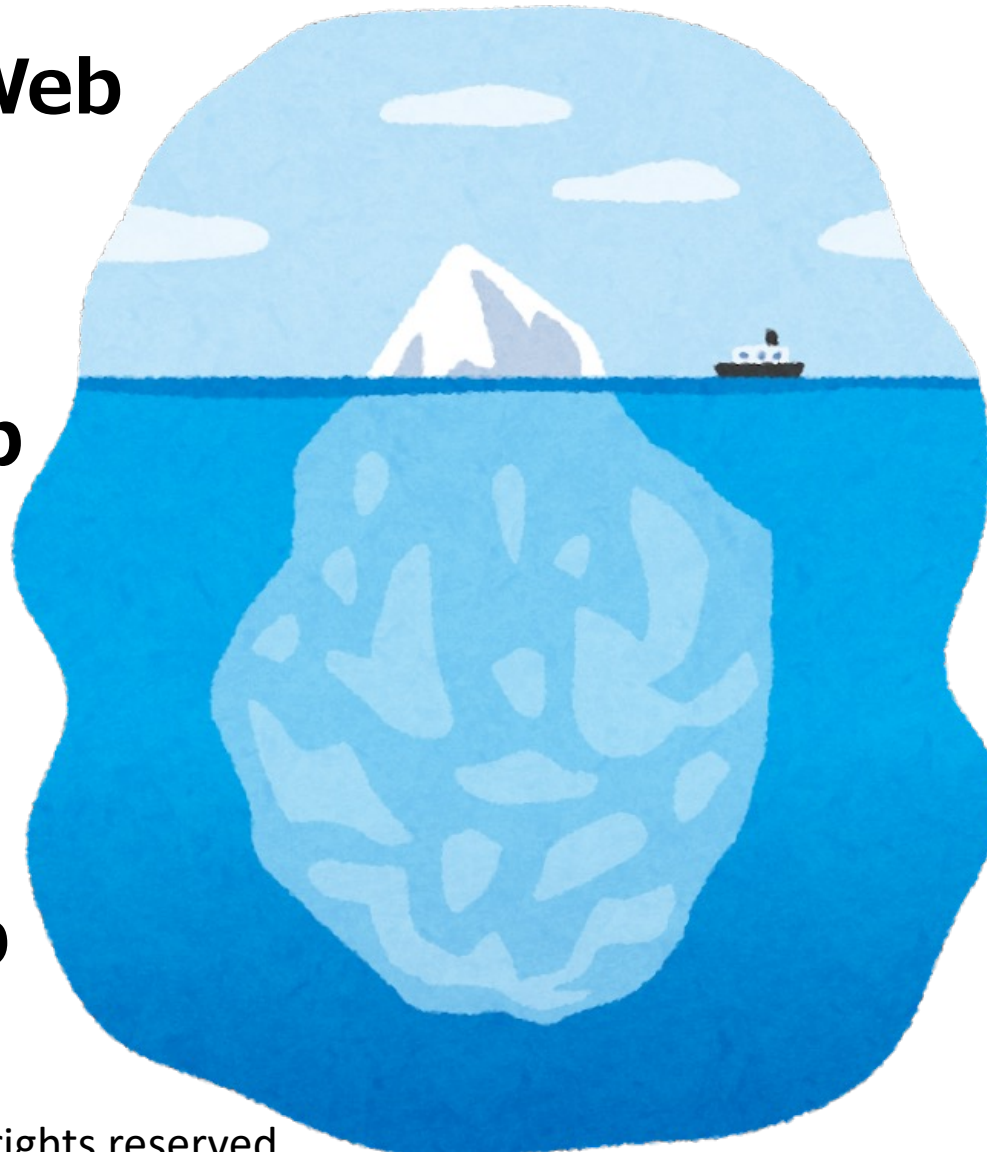
Google
Wikipedia
Twitter

Deep Web

法的ドキュメント
医療情報
金融情報
学術情報
政策情報

Dark Web

非合法情報
プライベートな通信
密輸・禁制品販売



Dark Web



利用者

- 犯罪者
- 政府・法的機関
- 内部告発者
- プライバシーを気にするユーザ

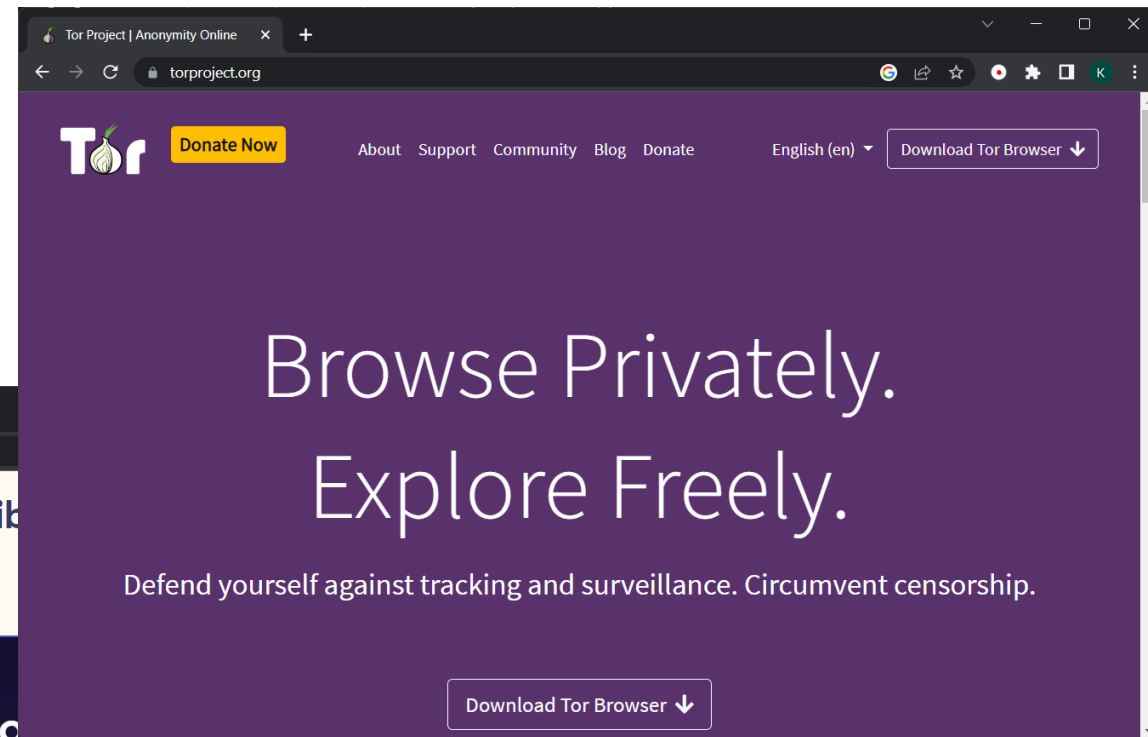
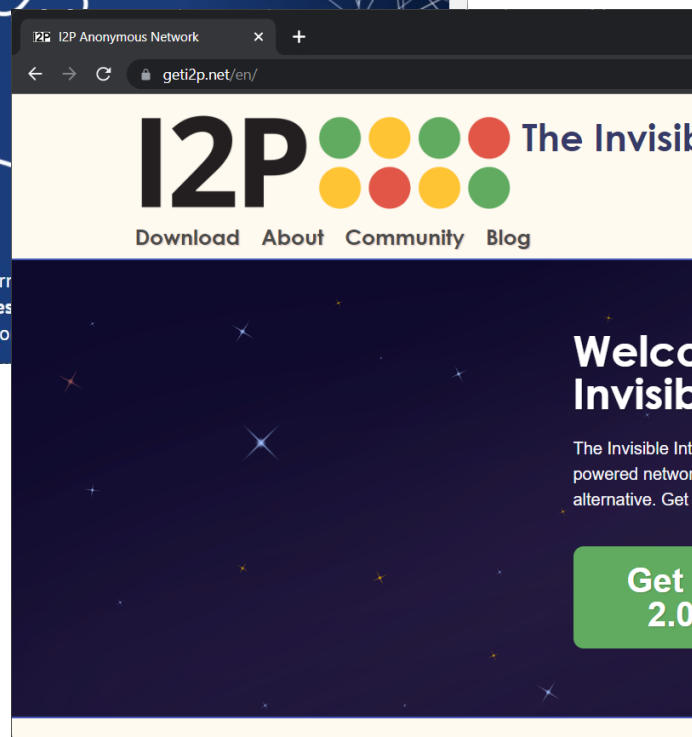
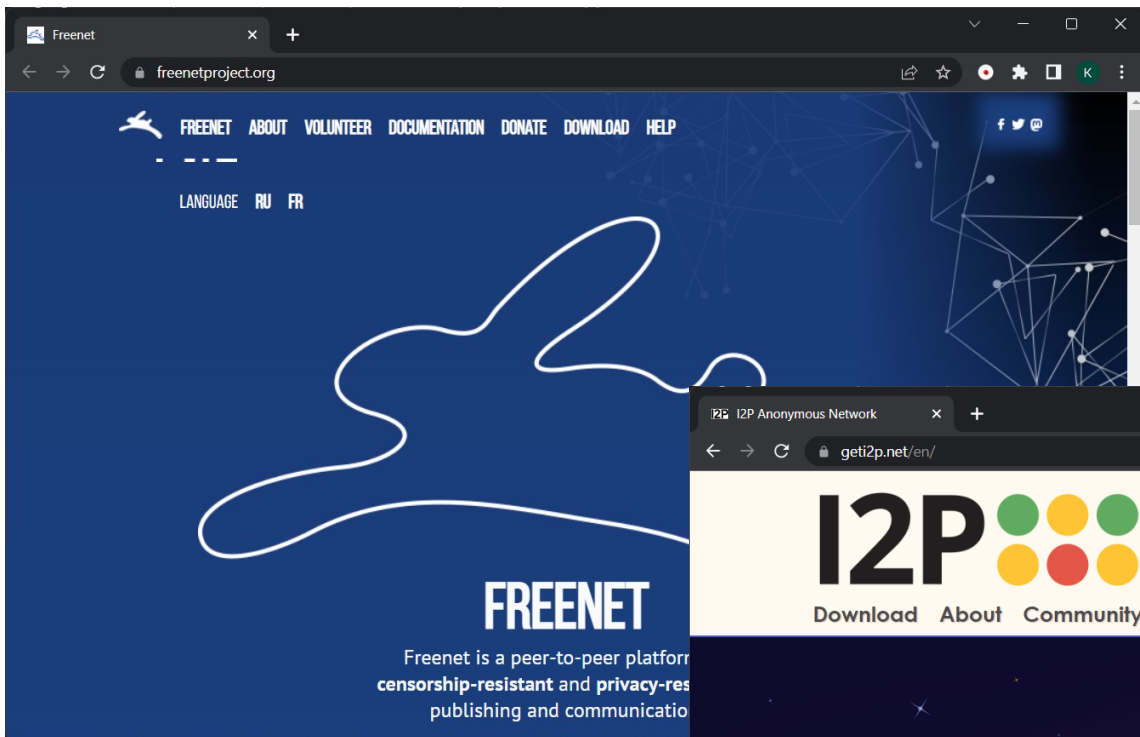
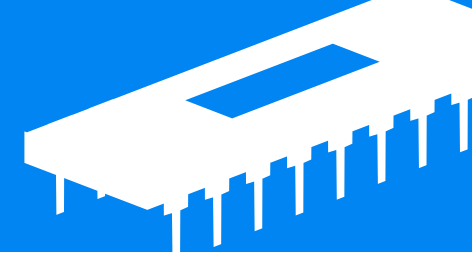
サービス例

- 匿名ブラウズ
- 匿名メッセージング
- 匿名ファイル共有
- 非公開Webサイト
- 掲示板
- 非合法販売

WARNING!

Dark Webには非合法、倫理的でない、不穏な情報が含まれているため、アクセスをする際には十分にリスクを考慮してください。

3 Dark Networks



Tor Browser

Download Tor Browser

Protect yourself against tracking, surveillance, and censorship.



Download for Windows

[Signature](#) ?



Download for macOS

[Signature](#) ?



Download for Linux

[Signature](#) ?



Download for Android

Dark Web Search



Random Onions

Fresh Onions

Search and Find .onion websites ...

Search what you mind...

Search

Are you "Adventurous?" :) Try Visit a Random .Onion website. Check this feature. [/random](#)

Promoted sites ⓘ

A banner displaying several promoted sites. From top to bottom: 'SHOP card CLONE CARD' with a yellow logo; 'CC KINGDOM CREDIT CARDS PAYPAL ACC' with a crown icon and the URL 'CCKINGDOMTMF7W7L.ONION'; 'Tor HIDDEN WIKI 2019' with a purple onion icon; a Chinese text banner '中文高端担保市场 安全 你想要的都在这里 大赚'; 'DeepMarket MULTISIG ESCROW MARKETPLACE' with a red 'POPULAR 70+ SELLERS' badge; and a partially visible 'SUBPRICE' banner at the bottom.

- Torch
- Phobos
- Onion Land Search
- Deep Search
- TOR66
- Visitor
- Hoodle

Agenda

01

OSINTの基礎

02

OSINTで用いられる技術例

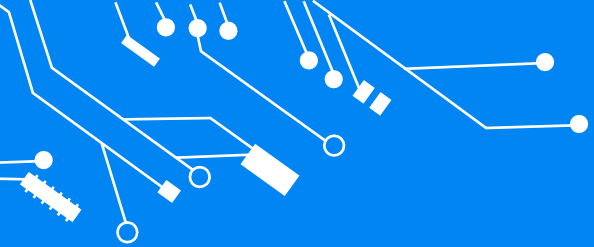
検索・メタデータ・画像分析・SNSの活用

03

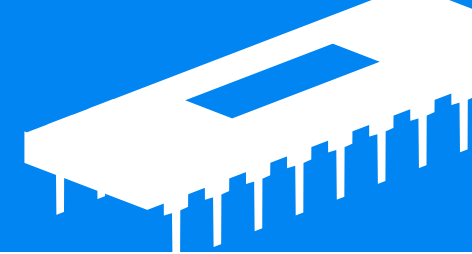
Dark Web

04

OSINT技術を身につけるために



OSINT Training



OSINT技術者の人材育成が必要とされている



Select Training

業務に適合した内容であること

体系立った内容であること

実践的な内容であること

復習可能な教材があること

定評、実績あるトレーニングであること

身につけた能力を評価・測定できること



SANS Tokyo
January 2023
23-28 January

09:30 - 17:00 JST
6 Courses

In-Person & Live Online

[View Courses](#)

SANS Institute (SysAdmin, Audit, Network, Security)

SANS

SANS本部：米国メリーランド州

情報セキュリティトレーニング、認定資格、調査研究におけるグローバルリーダー

第一線の専門家による講義・高品質のマテリアル


単なる知識の習得ではなく実務的なスキルを習得

多様なラーニングフォーマット（オンライン、対面、プライベート開催等）

Coming Soon : SEC497

[Train and Certify](#)[Manage Your Team](#)[Security Awareness](#)[Resources](#)[Get Involved](#)[About](#)[Home](#) > [Courses](#) > SEC497: Practical Open-Source Intelligence (OSINT)**Beta**

SEC497: Practical Open-Source Intelligence (OSINT)

[Register Now](#) **Online****36 CPEs**

SEC497 is based on two decades of experience with open-source intelligence (OSINT) research and investigations supporting law enforcement, intelligence operations, and a variety of private sector businesses ranging from small start-ups to Fortune 100 companies. The goal is to provide practical, real-world tools and techniques to help individuals perform OSINT research safely and effectively. One of the most dynamic aspects of working with professionals from different industries worldwide is getting to see their problems and working with them to help solve those problems. SEC497 draws on lessons learned over the years in OSINT to help others. The course not only covers critical OSINT tools and techniques, it also provides real-world examples of how they have been used to solve a problem or further an investigation. Hands-on labs based on actual scenarios provide students with the opportunity to practice the skills they learn and understand how those skills can help in their research. 29 Hands-on Labs + Capstone CTF

Course Authors:



Matt Edmondson
Certified Instructor

2023年6月26日～7月1日
開催予定

SANS

THANK YOU

上田 健吾 (Kengo Ueda)
japan@sans.org / <https://www.sans.org>



@sansinstitute.japan



@SANS_JAPAN