INVESTIGATION WITH OPEN SOURCE INTELLIGENCE (OSINT)

Presented By Rỉch | CyberFest 2022 #4

WHO AM I

- Security Consultant at Maxplus Anugerah
- Red Team & OSINT Enthusiast
- Oprekers & Researcher

:@enamnyatigakali

HISTORY

- OSINT has been around since World War 2 as an intelligence tool for many National Security Agencies.

- OSINT can be practiced for Due Diligence, Investigation, Observation and Cybersecurity.

- Today's, information sources can be collected from anywhere. Users just need to identify the targeted subject and search for it online.

OSINT, WHATS MEANING ?

It is called OpenSource because it collects data from publicly available sources for use in the context of intelligence about people or entities from a variety of sources including the Internet.

OSINT is one of many intelligence collection types.

The main categories are Human Intelligence (HUMINT), Social Media Inteligence (SOCMINT), Geospatial Intelligence (GEOINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), etc.

WHO USED

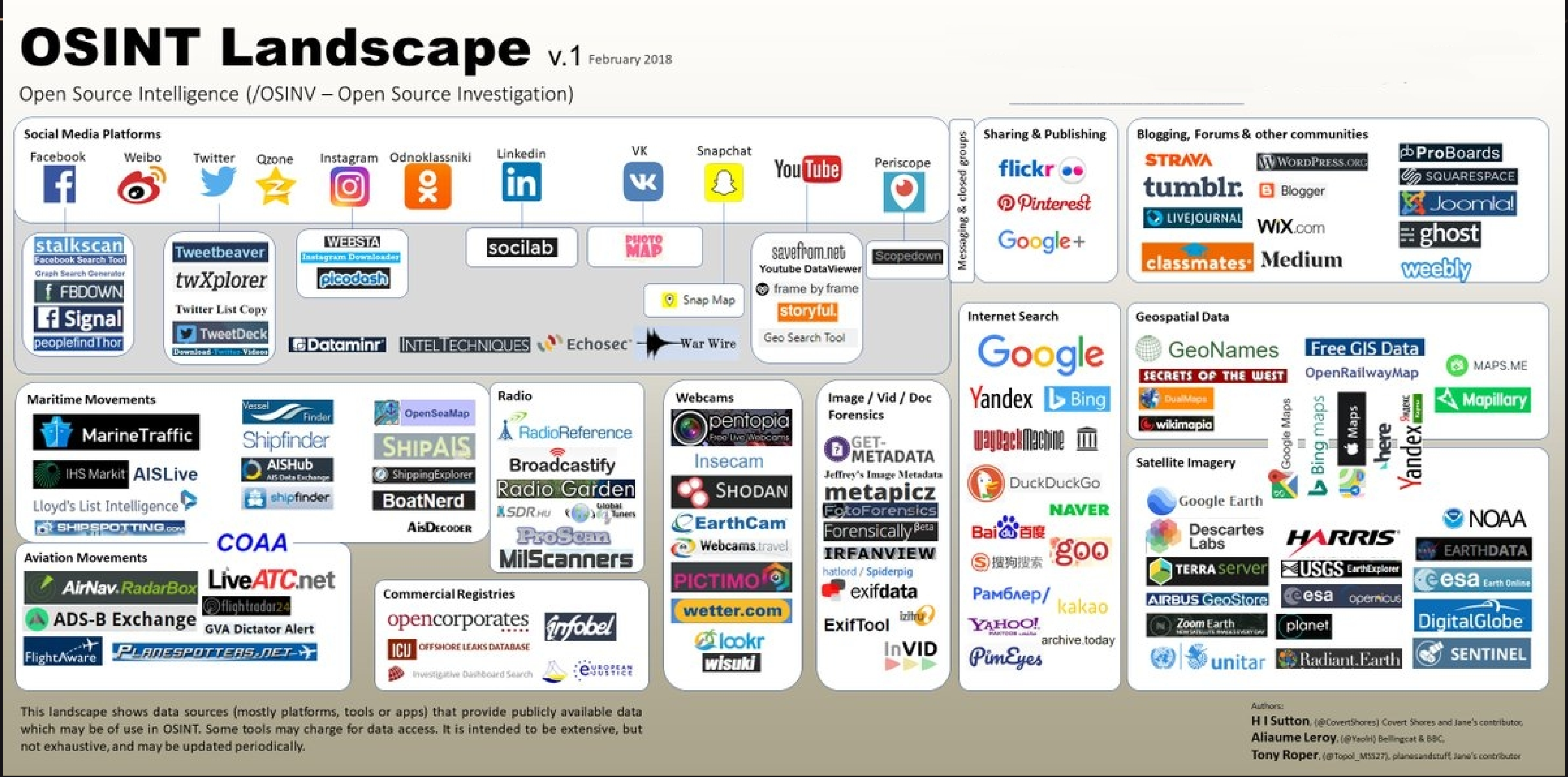
- Journalist.
- Cyber Security & Cyber Crime Groups
- Law Enforcement
- Private Investigator
- Bussines Corporate
- Terorist Groups

OSINT SOURCE’S ?

Open Data Source Category :

- Search Engine (Google, Yahoo, Bing, Shodan)
- Social Media (Facebook, Twitter, Instagram, Tiktok)
- Publishing Media (Blog, Website, Wikileak, Panama Papers, Forum Data Leak)
- Internet Address Databases (Whois, DNS)
- Maps And Commercial Imagery (Google Maps, Bing Map)
- Government Reports / Document.
- Photo, Images, Video
- The Dark Web

OSINT RESOURCES



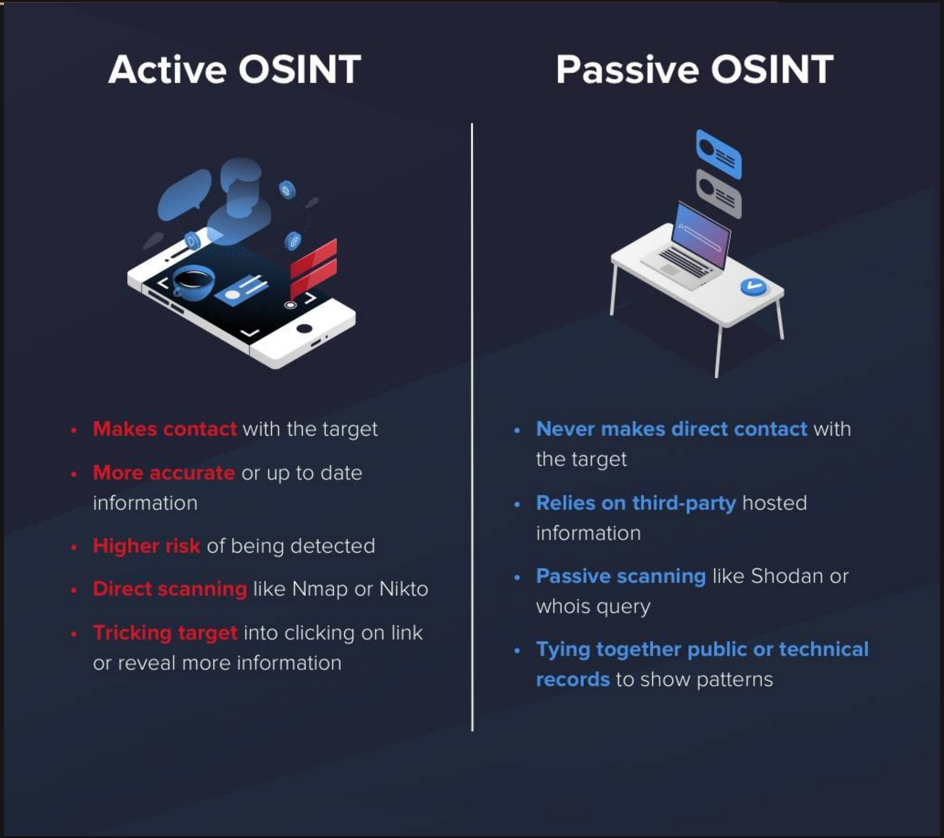
OSINT Landscape v.1 February 2018

Open Source Intelligence (/OSINV – Open Source Investigation)

This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.

Authors:
H I Sutton, (@CovertShores) Covert Shores and Jane's contributor,
Aliaume Leroy, (@Yaolt) Bellingcat & BBC,
Tony Roper, (@Topol_MSS27), planesandstuff, Jane's contributor

DIFERENT OSINT GATHERING



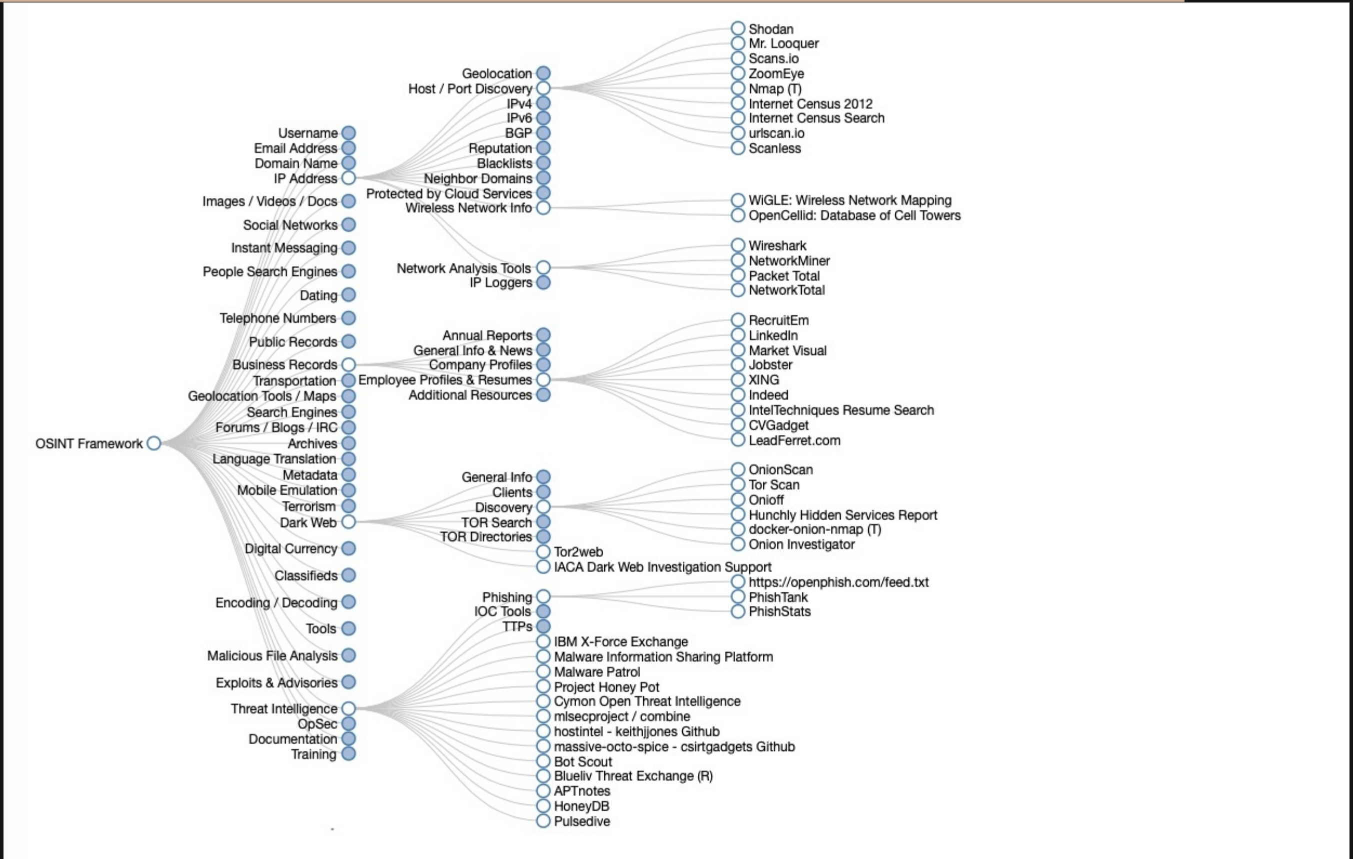
Active OSINT

- **Makes contact** with the target
- **More accurate** or up to date information
- **Higher risk** of being detected
- **Direct scanning** like Nmap or Nikto
- **Tricking target** into clicking on link or reveal more information

Passive OSINT

- **Never makes direct contact** with the target
- **Relies on third-party** hosted information
- **Passive scanning** like Shodan or whois query
- **Tying together public or technical records** to show patterns

OSINT RESOURCES



OSINT Framework

Username
Email Address
Domain Name
IP Address
Images / Videos / Docs
Social Networks
Instant Messaging
People Search Engines
Dating
Telephone Numbers
Public Records
Business Records
Transportation
Geolocation Tools / Maps
Search Engines
Forums / Blogs / IRC
Archives
Language Translation
Metadata
Mobile Emulation
Terrorism
Dark Web
Digital Currency
Classifieds
Encoding / Decoding
Tools
Malicious File Analysis
Exploits & Advisories
Threat Intelligence
OpSec
Documentation
Training

Geolocation
Host / Port Discovery
IPv4
IPv6
BGP
Reputation
Blacklists
Neighbor Domains
Protected by Cloud Services
Wireless Network Info
Network Analysis Tools
IP Loggers
Annual Reports
General Info & News
Company Profiles
Employee Profiles & Resumes
Additional Resources
General Info
Clients
Discovery
TOR Search
TOR Directories
Tor2web
IACA Dark Web Investigation Support
Phishing
IOC Tools
TTPs
IBM X-Force Exchange
Malware Information Sharing Platform
Malware Patrol
Project Honey Pot
Cymon Open Threat Intelligence
mlsecproject / combine
hostintel - keithjjones Github
massive-octo-spice - csirtgadgets Github
Bot Scout
Blueliv Threat Exchange (R)
APTnotes
HoneyDB
Pulsedive

Shodan
Mr. Looquer
Scans.io
ZoomEye
Nmap (T)
Internet Census 2012
Internet Census Search
urlscan.io
Scanless
WiGLE: Wireless Network Mapping
OpenCellid: Database of Cell Towers
Wireshark
NetworkMiner
Packet Total
NetworkTotal
RecruitEm
LinkedIn
Market Visual
Jobster
XING
Indeed
IntelTechniques Resume Search
CVGadget
LeadFerret.com
OnionScan
Tor Scan
Onioff
Hunchly Hidden Services Report
docker-onion-nmap (T)
Onion Investigator
https://openphish.com/feed.txt
PhishTank
PhishStats

WHY ?

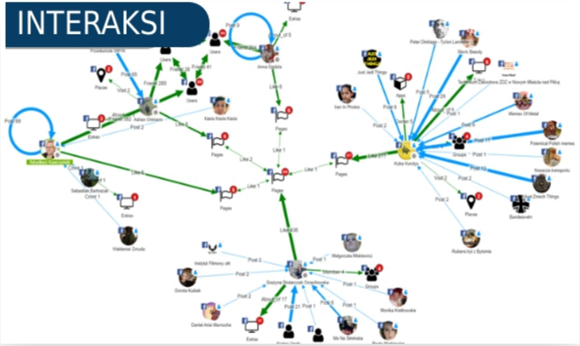
Due to the rapidly increasing number of open sources of information available, it is imperative that intelligence and law enforcement agencies around the world collect information effectively and efficiently

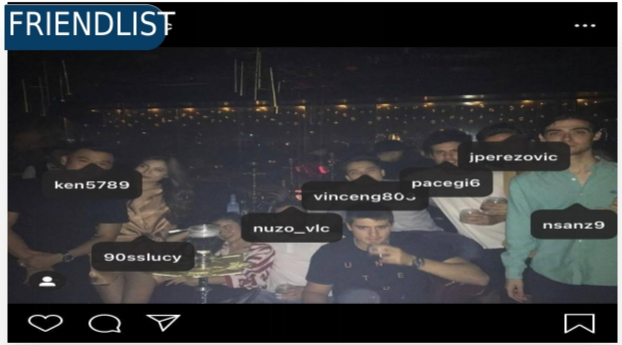
OSINT is not only limited to searching for information, but at this time use investigation for :

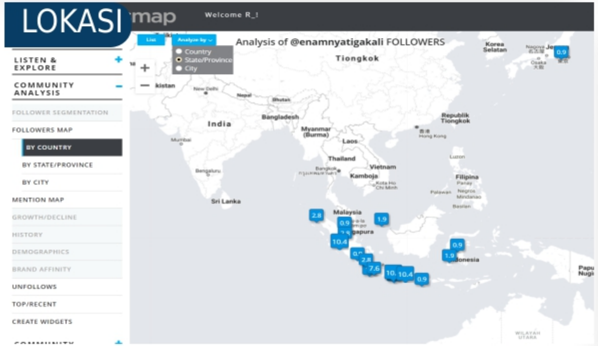
- Fraud
- Cyber Crime (Hacking, Defacing, Carding)
- Human Trafficking
- Cyber Espionage
- etc

SCOPE ANALYSIS

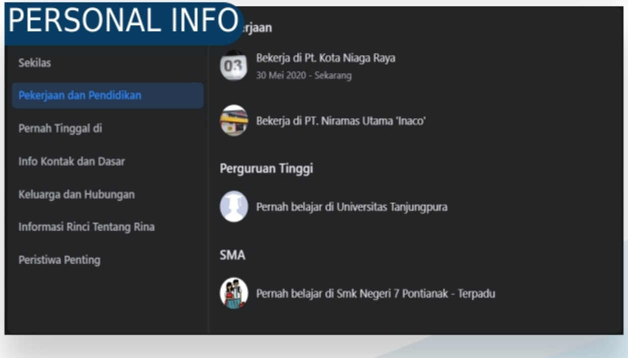
- Publik / Private Post
- Related Friend
- Personal Info
- Hashtag
- Geolocation
- Friendlist
- Photo / Video
- E-mail
- Document
- Phone Number
- dll


INTERAKSI


FRIENDLIST


LOKASI

Analysis of @enamnyatigakali FOLLOWERS


PERSONAL INFO

…rjaan

Bekerja di Pt. Kota Niaga Raya
30 Mei 2020 - Sekarang

Bekerja di PT. Niramas Utama 'Inaco'

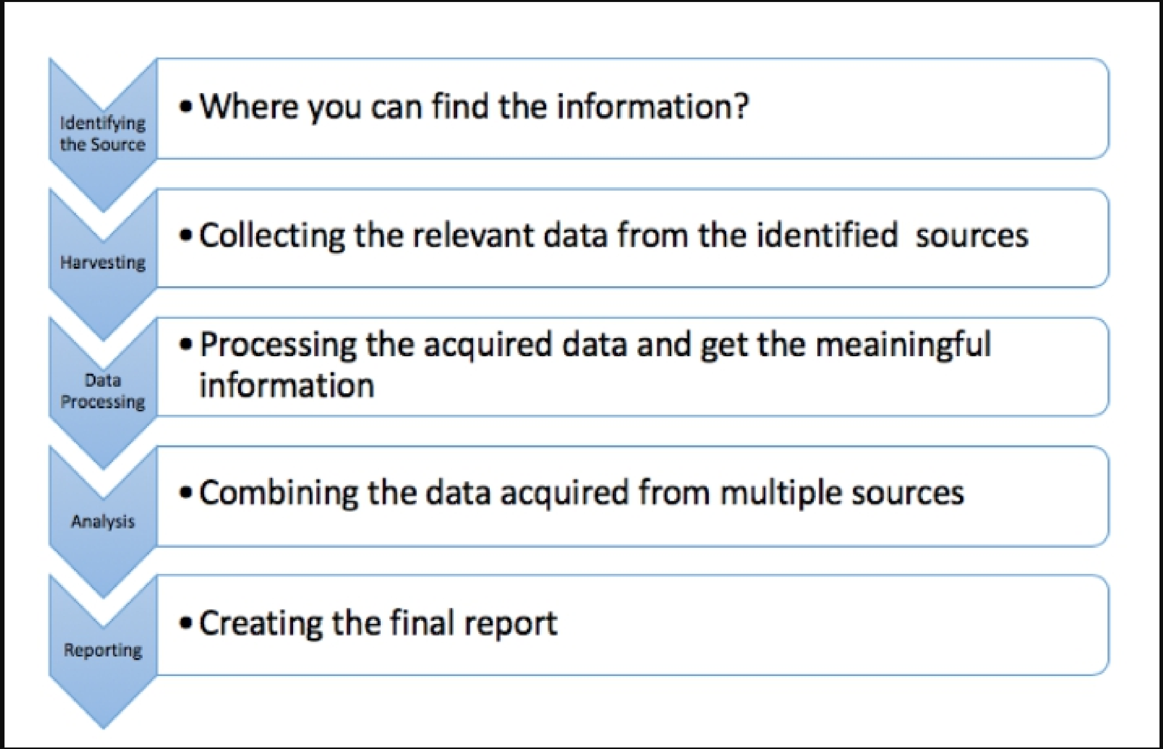
Perguruan Tinggi

Pernah belajar di Universitas Tanjungpura

SMA

Pernah belajar di Smk Negeri 7 Pontianak - Terpadu

OSINT PROCESS



Identifying the Source
- Where you can find the information?

Harvesting
- Collecting the relevant data from the identified sources

Data Processing
- Processing the acquired data and get the meainingful information

Analysis
- Combining the data acquired from multiple sources

Reporting
- Creating the final report

Problem With Data ?

- *No data found Cause “Fake Person”.*
- *There is a similarity of target data about Names / Aliases*
- *Some of the data you get may not seem to "match" your description of the event or target*
- *Some people will throw out seemingly irrelevant data and not report it*
- *Hanya karena berbeda, jika dipercaya dapat relevan dengan data atau analisis lebih lanjut*

Hide Your Profile.

- Sock Puppet

  - Full Profile Identity : *fakenamegenerator.com.*

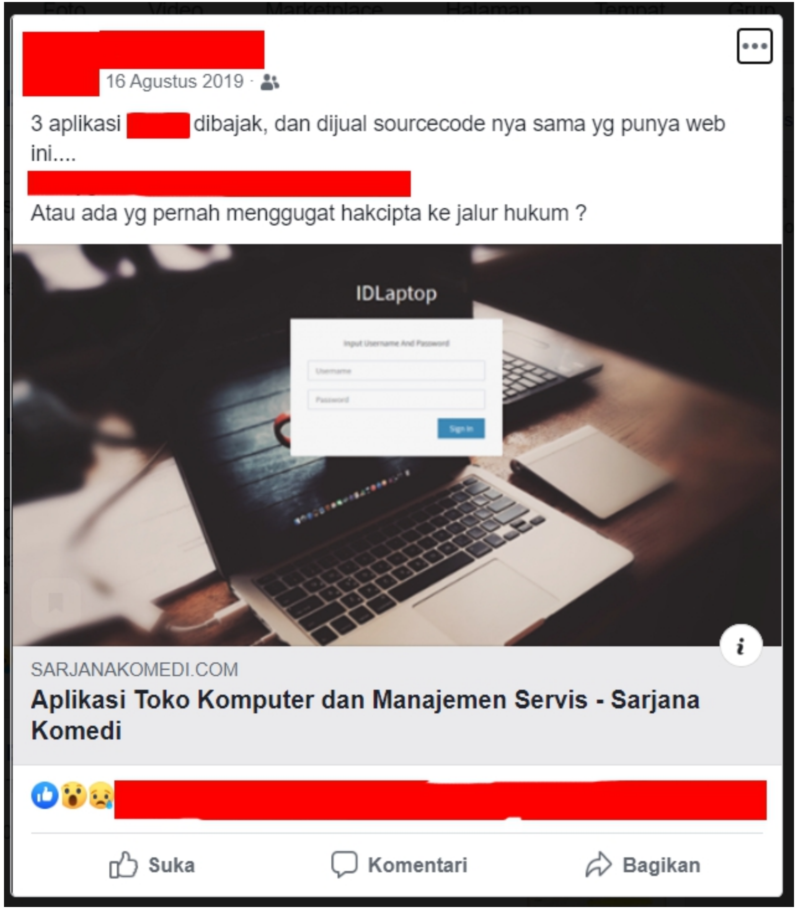
  - Encrypted E-mail / Temporary Email
  (ex : Proton Mail / CryptoGmail.Com)

  - Temporary Phone Number (Free / Paid)

  - Social Media Profile With Morphing Photo
  (ex: morphthing.com / thispersondoesnotexist.com)

  - VPN.

SAMPLE CASE



[redacted]

16 Agustus 2019 ·

3 aplikasi [redacted] dibajak, dan dijual sourcecode nya sama yg punya web ini....

[redacted]

Atau ada yg pernah menggugat hakcipta ke jalur hukum ?

SARJANAKOMEDI.COM

Aplikasi Toko Komputer dan Manajemen Servis - Sarjana Komedi

[redacted]

Indonesian OSINT Discuss

: https://t.me/OSINT_ID

THANK YOU