

A garrafa que
me entregou



whoami

André Silva

Formado em Gestão de TI pela FIPP [Unoeste]

Consultor de Segurança da Informação pela PRIDE Security

Cursando Pós-Graduação em Inteligência e Investigação em Fontes Abertas [OSINT] pela WB Educação em parceria com a Faculdade Vinct

disclaimer

As informações e opiniões apresentadas nesta apresentação são de responsabilidade exclusiva do autor e não representam necessariamente as opiniões ou posições da PRIDE Security.

A graphic with a dark blue background. In the center is a glowing blue circle containing the text "OSINT". Surrounding this central circle are eight smaller circles, each containing a white icon: a globe, a cloud with a network symbol, a folder, a location pin, a speech bubble, a classical building, a padlock, and a cloud with a download symbol. A stylized, glowing blue hand is pointing its index finger at the central "OSINT" circle.

o que é OSINT?

- OSINT (*Open Source Intelligence*) é a coleta e análise de informações de fontes abertas disponíveis ao público.
- É usado em diferentes áreas para obter *insights* úteis a partir de dados acessíveis, como sites, redes sociais, documentos governamentais, periódicos, jornais, revistas e afins.

motivação

- Desafio proposto durante um Curso de Formação OSINT, ministrado pelo professor Romulo Carvalho, para coletar o máximo de informações disponíveis em fontes abertas sobre um fugitivo procurado pela justiça brasileira e também pela Interpol.



o que poderemos ter ao final?

- Algumas técnicas e *insights* valiosos utilizados durante a fase de coleta de informações.



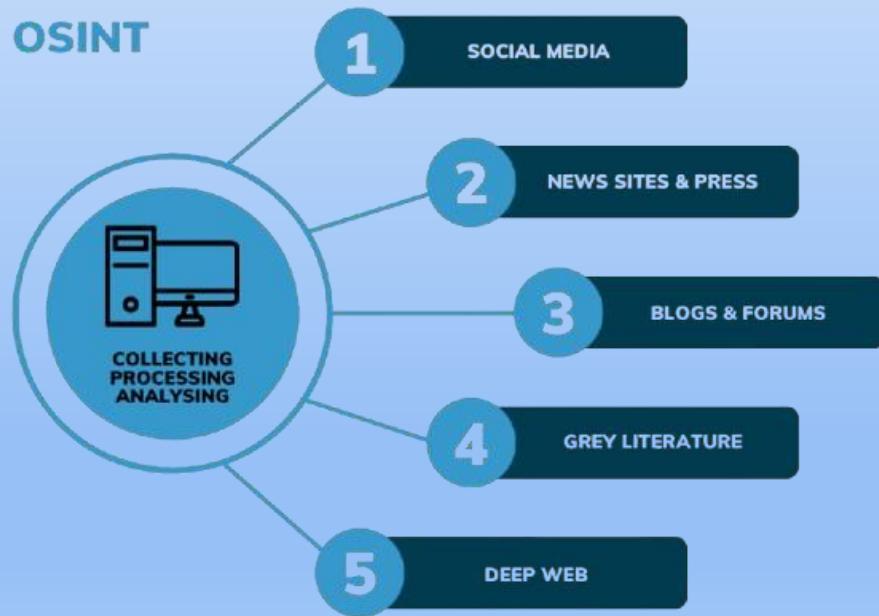
o caso



- Durante a execução do curso, foram apresentadas diversas técnicas e *insights* que podem ser usados para coleta de informações sobre pessoas nos mais diversos ambientes, sejam eles online ou offline.
- Algo que me ajudou nesse processo foi manter a mente aberta sobre todas as técnicas ali ensinadas, visto que, em algum momento, algo poderia ser útil durante a investigação.

a proposta

OSINT



- Ao final do curso fomos apresentados a uma lista de procurados pela justiça brasileira e em alguns casos, pela Interpol;
- A ideia era coletar o máximo de evidências e informações e até o final do curso, confeccionar um relatório e por fim apresentar o que foi possível com os ensinamentos obtidos durante o curso.

montando o caso

- Ao analisar as informações que foi possível durante o curso pude notar que muitas informações em processos [civis e criminais, pelo que observei] são bastante divulgadas, com informações até demais [isso é bom, continuem] nas várias fases dos processos.



era para ter finalizado, mas eu nunca parei

- Finalizado o curso eu continuei, em minhas horas vagas, buscando novas informações, avaliando o caso novamente por informações de processos disponíveis em fontes abertas, vídeos disponíveis sobre o caso, *podcasts* e mídias sociais [nesse caso].



infos, infos e mais infos...

- Apesar da grande quantidade de informações disponíveis, elas podem ser uma armadilha caso não sejam bem estruturadas e manipuladas, de forma que possam permitir a construção de uma narrativa sobre os fatos em questão.



de volta ao curso [agora outro]

- A história começou como uma proposta para aplicação das técnicas e ensinamentos de um curso em meados de 2022;
- Em 2025, bem no início do ano, adquiri mais um curso, dessa vez do professor Jézer Ferreira pela WB Educação.



novas técnicas, novas informações

- Algumas técnicas apresentadas eram conhecidas, outras eram totalmente novas;
- Essas novas técnicas me permitiram abrir o horizonte sobre como e o que buscar para obter novas informações sobre a localização desse foragido.



as pegadas digitais

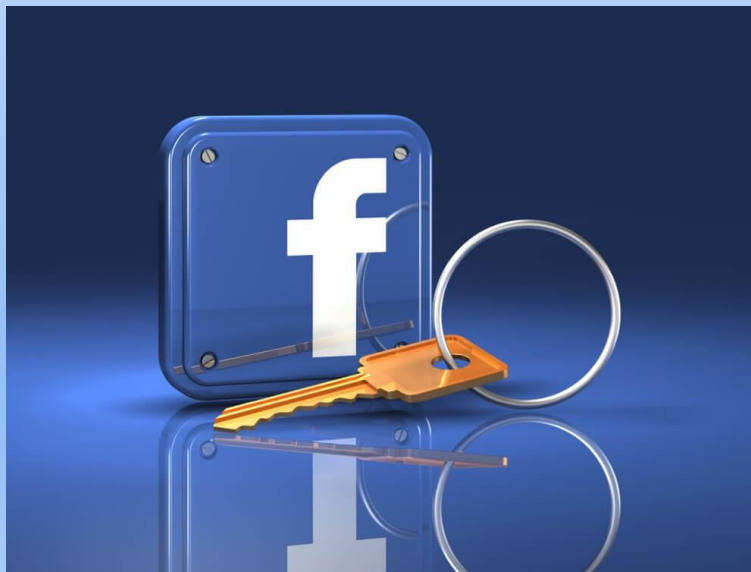


- É sabido que hoje temos acesso a muitas informações oriundas das mídias sociais e que algumas, apesar de esquecidas, ainda são muito relevantes e contem informações valiosas.

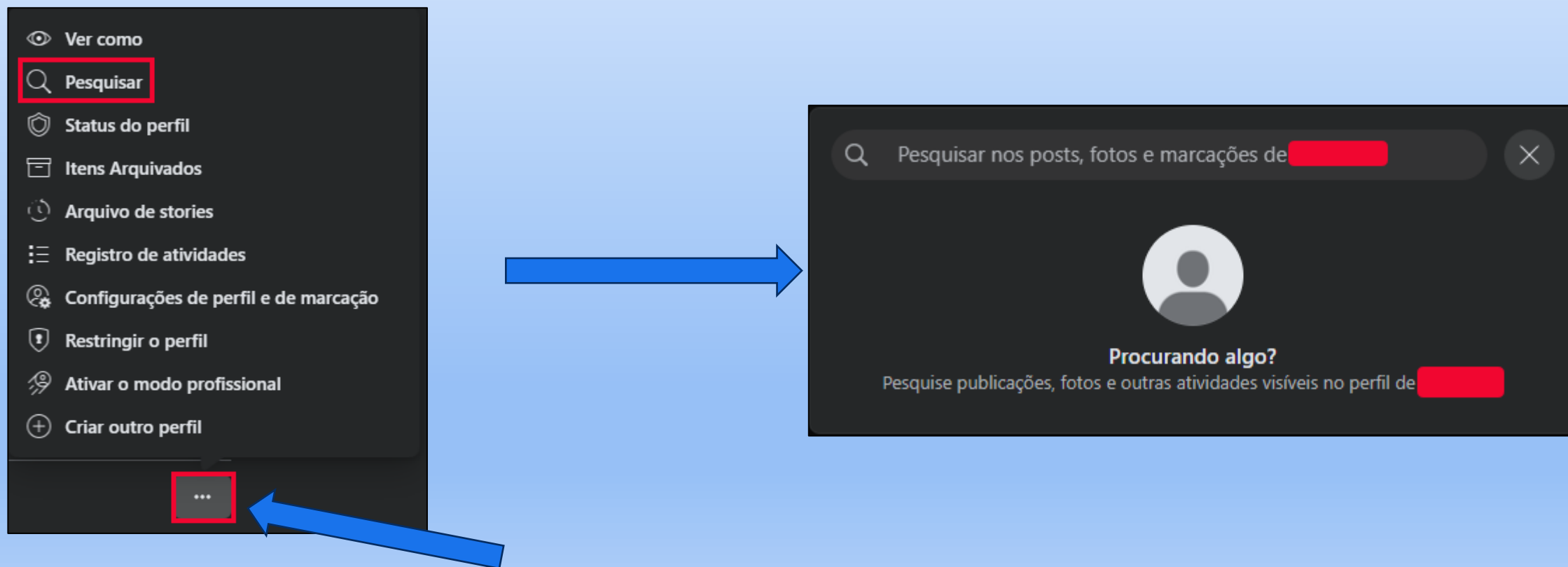


meus perfis são fechados será?

- Uma das técnicas ensinadas foi que, ao entrar em um perfil fechado no Facebook, é possível verificar se a opção de busca dentro do perfil está ativa e caso esteja, pesquisar pelo nome do usuário do perfil.



busca no perfil do Facebook



a garrafa

- Dentre as várias informações novas obtidas, foi possível identificar uma foto, utilizando a técnica da pesquisa no perfil do Facebook que revelou algo muito importante 🎯
- Ok, uma garrafa ... e?



além da montanha

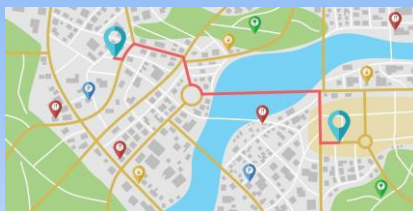
- Junto a imagem identificada no passo anterior, haviam outros elementos que foram corroborados com informações obtidas em vídeos e *podcasts* disponíveis sobre o caso.



a busca continua



- Busca por nomes;
- Busca por processos [civis ou criminais], podem conter muitas informações importantes;
- Busca por familiares;
- Busca por postagens utilizando *dorks* [não se limite ao Google, existem outros buscadores];
- Busca por vídeos, reportagens, *podcasts* e etc sobre o caso [caso haja];
- Ao identificar alguma imagem, tente colocá-la na narrativa para verificar onde ela pode se encaixar.



e não para por aí

- É preciso levar em consideração todas informações disponíveis e descartar o que não se encaixa [é difícil, mas importante];
- As reportagens e declarações de advogados e familiares podem revelar muitas informações interessantes, coisas que podem ser ditas sem intenção, podem, muitas vezes ajudar a montar o caso.

...estava com alguém e já tinham um bebê.



IMAGEM MERAMENTE ILUSTRATIVA

alguns fatos relevantes sobre esse caso

- Ao buscar informações sobre a família não foi possível identificar muitas coisas sobre o pai do foragido, mas sobre a mãe sim, então foquei nessa estratégia [e deu certo];
- Eu havia coletado muitas informações sobre o pai e até inseri no relatório, mas percebi que deveria mudar o foco e abrir os horizontes.
- Comecei a corroborar as declarações dos advogados e ao buscar informações da mãe do foragido, foi possível ligar tais evidências a essas declarações.



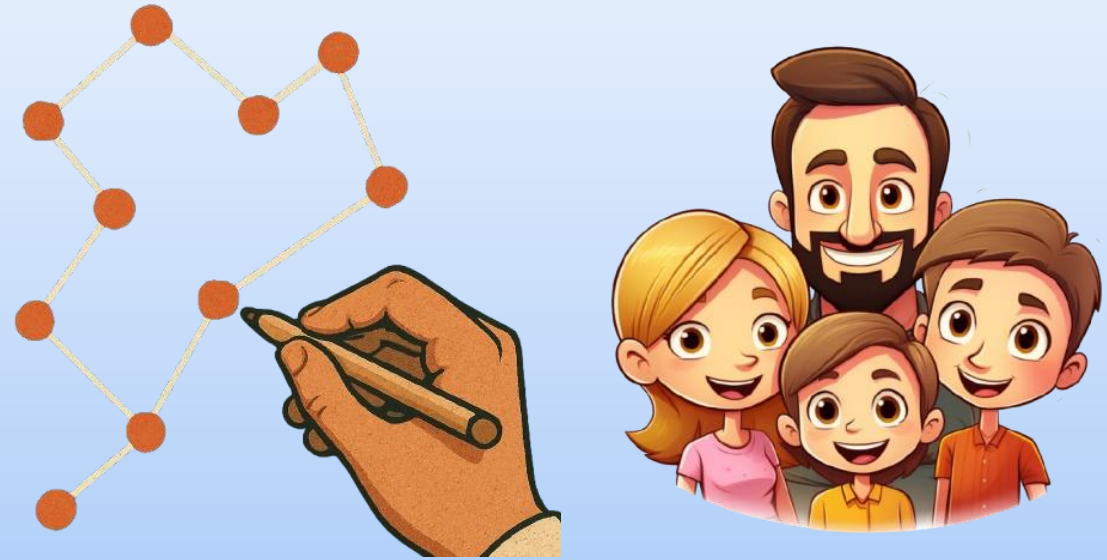
mas eu busco o que então? *dorks*?

- `intext:"nome completo" inurl:"instagram.com"`
- "nome completo" "processo"
- "nome completo" @outlook.com
- Em dado momento foi dito pelos advogados que o fugitivo poderia estar em outro país. Dessa forma, realizei a busca pelo nome da mãe na tentativa de identificar alguma informação.
- "nome da mãe" "país"
- Talvez para corroborar essa fala, a mãe tenha ido para outro país, visto que foi informado que o foragido havia fugido com a mãe 😁



a família pode ser um ponto importante

- Foi informado ainda que um familiar havia se mudado para outra cidade no Brasil e que o foragido poderia ter ido junto [informação obtida em um vídeo disponível no YouTube];
- “nome do familiar” “cidade”
- “nome do familiar” “processo”



Google
Dorks

ainda na família

- Foi possível identificar, pelas postagens da mãe, que ela havia realizado algumas coisas que corroboravam com as declarações dos advogados, além da busca por informações nas imediações onde a famigerada **garrafa** foi identificada 😁
- Cada interação, cada menção de @ em alguma publicação é válida;
- As publicações de terceiros e comentários também contam 😊
- Identifiquei ainda que havia uma procura por um certo tipo de *kitnet* nas imediações da localização da **garrafa**

Hidratem-se 👉



a comunidade

- Nessa apresentação minha intenção foi tentar devolver para a comunidade um pouco do que aprendi nesse curto período de tempo e sei que ainda há muito o que ser aprendido;
- Percebi que há diversas pessoas dispostas a ensinar e compartilhar conhecimento;
- Tive contato com pessoas muito boas e que atuam a bastante tempo nesses cenários e que me ajudaram a construir esse caso;
- Se você tem dúvidas? Pergunte 😁



enfim, relatório entregue

- Eu procurei utilizar diversas técnicas aprendidas ao longo do tempo, que me permitiram conhecer diversas ferramentas [pagas e gratuitas];
- O que aprendi é que as ferramentas nascem e morrem quase que na mesma velocidade e é preciso manter as técnicas e *insights* aprendidos para que as buscas não sejam impactadas;
- Sua maior ferramenta é você mesmo, nunca pare de estudar;
- Esse relatório foi encaminhado à Polícia Civil e também para dois delegados [Dr. Emerson Wendt e Dr. Alesando Barreto].



novidades sobre o caso



- Ao que tudo indica, o relatório foi recebido e novas investigações foram iniciadas na tentativa de validar as informações presentes no relatório;
- É importante ter seriedade, pois o trabalho pode mexer com vidas inocentes, caso alguma informação não tenha sido validada mais de uma vez [ISSO É EXTREMAMENTE IMPORTANTE];
- Foi possível observar que ainda é um processo lento um órgão policial receber um relatório de uma pessoa comum informando que identificou o paradeiro de alguém oriundas de fontes abertas, mídias sociais e afins. Contudo, vale insistir, procurar pessoas mais próximas a tais órgãos e mostrar o que foi identificado e pedir uma avaliação, uma crítica.

disclaimer final

- Eu gostaria mesmo era de mostrar tudo o que fiz e com quem foi, porém fui instruído a manter sob sigilo, visto que poderia atrapalhar as investigações e até mesmo ter minha integridade física ameaçada [já que se trata de um caso policial, nunca se sabe] 😁
- Fiquei feliz de poder colocar o que aprendi em prática e utilizar esses conhecimentos para o bem.





the end