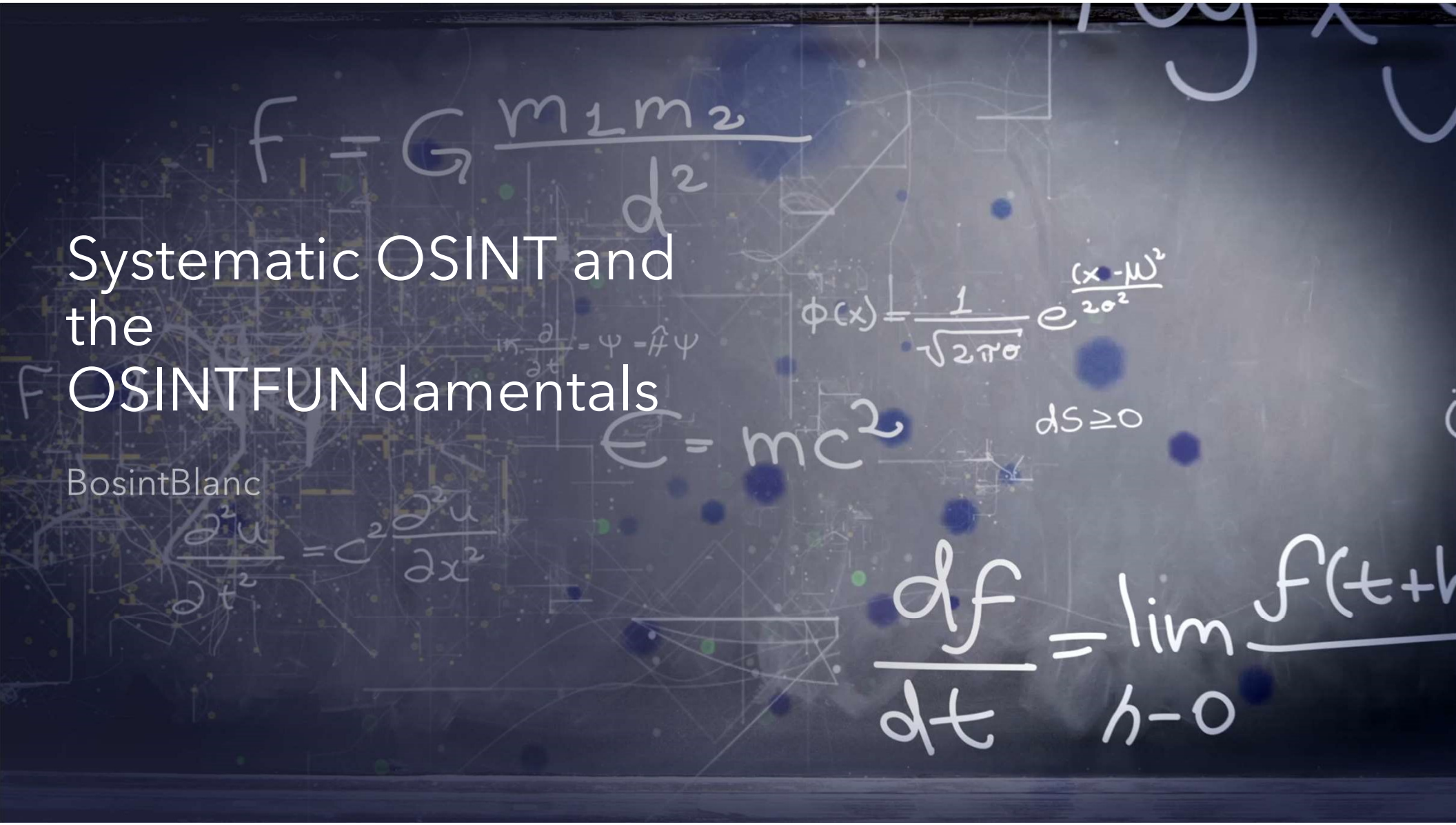


Systematic OSINT and the OSINTFUNdamentals

BosintBlanc

Whoaml?

- Background in Desktop Support, SOC/IR and lover of all things OSINT.
- Currently employed as a intelligence analyst team lead with threat intelligence firm DarkTower.
- 2nd place finish with team Dwayne “the sock” Johnson in Tracelabs Global Search Party.
- Case Tracking & Statistics Lead with NCPTF.

Disclaimer:

Nothing in this presentation represents the views of my employers or organizations I am associated with past, present or future.

7 Fundamental Skills

- OSINT is an amazingly broad discipline. There are so many facets to learn that it can feel quite overwhelming. That's why when learning it we should break in to fundamental and digestible parts.

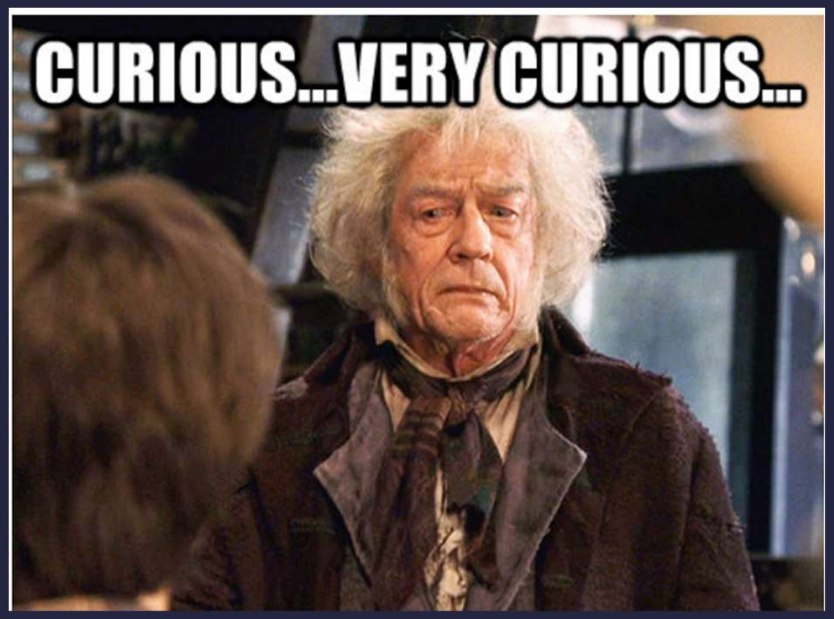
- Your fundamental skills may be different than mine depending on your background and training. This list is not meant to be exhaustive.

7 Fundamental Skills

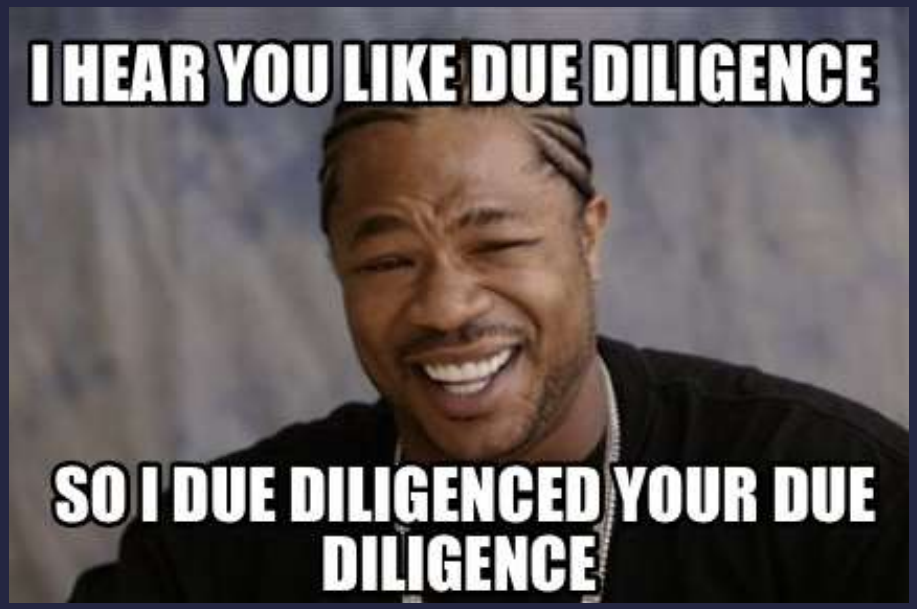
- Curiosity.
- Diligence
- Analytic and Intelligence Technique
- Networking
- Technique and Tools
- Ethics
- Communication

Fundamental 1: Curiosity

- OSINT is about uncovering answers.
- Chase rabbit trails.
    - Any time spent learning is time well spent.



Fundamental 2: Diligence



- So you've hit the wall. When you don't know where to take an investigation it's important not to give up.
- Adapt to what information you DO have. Find novel pivot points.

Fundamental 3: Analytic & Intelligence Technique

- Analytic and intelligence technique is what separates good OSINT from the worst kind of OSINT.

Fundamental 3: The Good, the bad, and the OSINT.

- Good OSINT
  - Belingcat, Tracelabs, ILF , NCPTF (and many more).
- Bad OSINT
  - Reddit and the Boston bomber.
  - Multiple people falsely accused during the US capitol riots.

Fundamental 3: Technique is key.

- For your next OSINT investigation try this simple method to add deeper analysis to your hypothesis.

- Do you have high, medium , or low certainty about the hypothesis?

Fundamental 3: Technique is key.

- Set a threshold for each certainty level for example you might use:
  - High – 5 points of verification with zero pieces of evidence against my conclusion.
  - Medium – 5 points of verification with some evidence against my conclusion OR 3 points of verification with zero evidence against my conclusion.
  - Low – A small amount of supporting evidence or a medium amount of evidence against my conclusion.

Fundamental 3: Baby Got Bias

- Three common types of bias
  - Dunning-Kruger Effect
    - People perceive a concept or event to be simplistic because they lack knowledge on it.
    - EX: “Gelocation is pretty easy right. You just reverse image search stuff”

Fundamental 3: Baby Got Bias

- Availability Bias
  - Sometimes called ‘availability heuristic’. This is the tendency to use information we can recall quickly when evaluating a topic.
  - EX: You read a news story about people who have won the lottery. As time passes you begin to buy more and more lottery tickets overestimating your chances of winning.

Fundamental 3: Baby Got Bias

- Fundamental Attribution Error
  - The tendency to attribute someone's behavior to existing and unfounded stereotypes while attributing our own behavior to external factors.
  - EX: You get cut off on the highway and yell "what a maniac" attributing the action to poor character when it's possible they have a very good reason to be in a hurry.

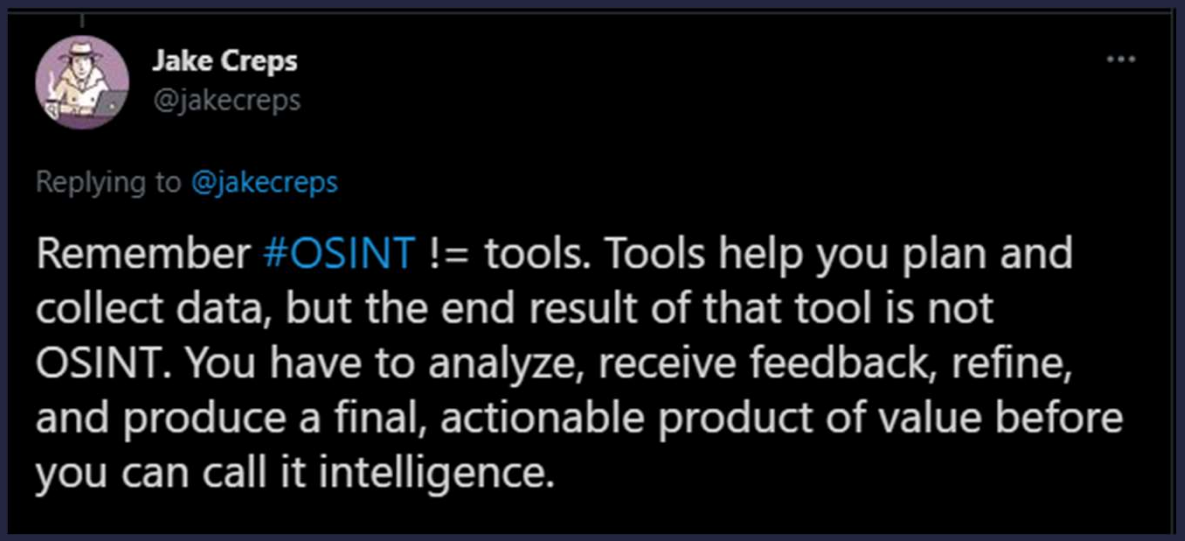
Fundamental 4: Community & Networking

- Networking is a requirement and not just a good idea.
- Infosec at large requires you get involved to continue to grow as both a person and a professional.

Fundamental 4: Mind The Gap

- To solve complex problems you need diversity of experience, expertise and knowledge.
- Networking isn't just about getting a new job it's about finding the holes in your knowledge.
- I've been most successful through joining a volunteer organization whose cause excites me and by being active and engaging the OSINT and Infosec Twitter communities.

Fundamental 5: Tools and Technique



Fundamental 5: A Tool By Any Other Name

- Getting used to mastering tools quickly is pivotal to success in OSINT as they often go as quickly as they come.
- 3 question to ask to learn a tool quickly:
  - What's the goal?
  - What's the method?
  - Do I need to find an expert to learn from?

Fundamental 6: Ethics and Verification

- DON'T DO CRIMES

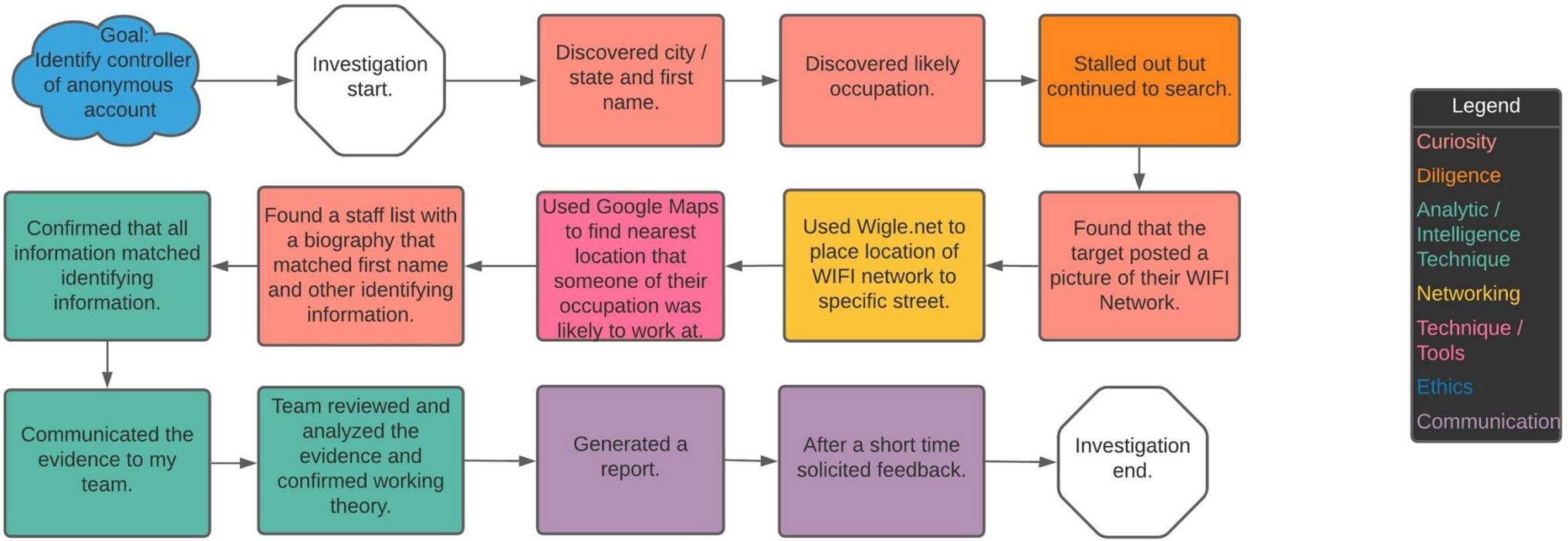
Fundamental 6: How Does One Ethic?

- Three questions for ethics.
  - Is it legal? I.e. does it follow all National, state and local ordinances
  - Is it approved? I.e. does it follow my organizational policies and code of conduct.
  - Is it moral? I.e. does it follow my personal internal compass or values of what is right and wrong.

Fundamental 7: Communication

- Information not conveyed in a comprehendible way is meaningless.
- How I communicate depends on my audience.
  - C-Suite = Cost, Return on Investment, high level.
  - Marketing = Brand and Reputation.
  - Technical team = Scope, evidence, process.

Let's Put It All Together:



Q & A

Contact:

Twitter :
@bosintblanc
Email:
osintholmes@protonmail.com
Discord:
BosintBlanc