ANT COLONY OPTIMIZATION ALGORITHM

Table of Contents:

- 1. Problem
- 2. Biological Phenomenon
- 3. Research Timeline
- 4. Application 1 – Antivirus Optimization
- 5. Application 2 – TSP
- 6. Statistical Data
- 7. Pros and Cons
- 8. Future Possibilities

1. Problem Statement

Current Antivirus Software are:

Signature Bound

Latency Reactive

Overhead Heavy

Weak Heuristics

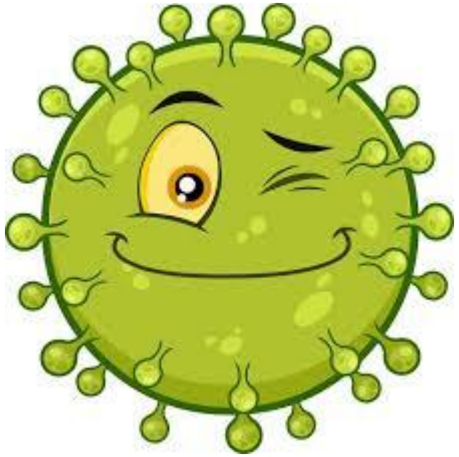
&

Deterministic Logic

Unoriginal Detection

Manual Dependency

Blind Heuristics



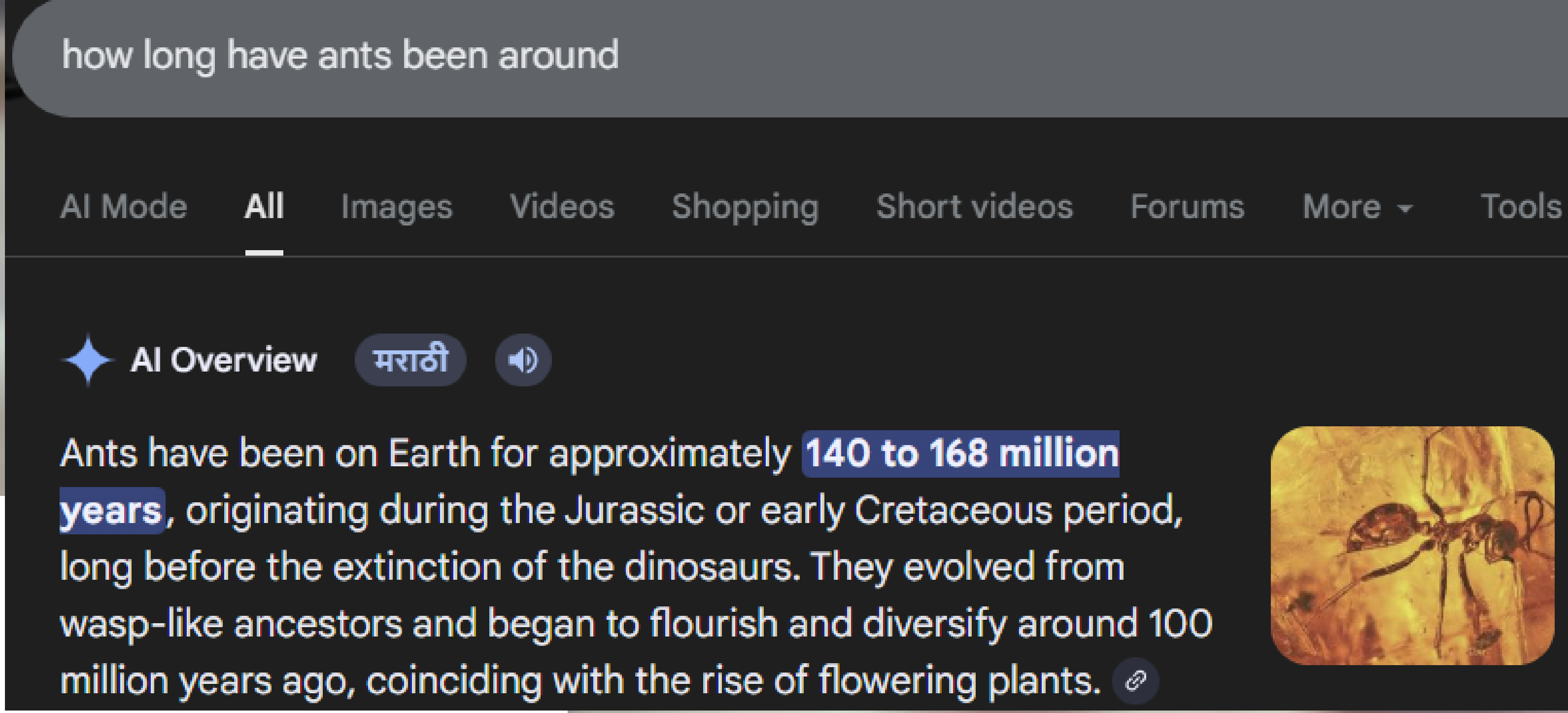
Computer Virus

A ZERO DAY VULNERABILITY

POLYMORPHIC VIRUS 💻🦠

SO WE HAVE

2. Biological Phenomenon



Ants have been on Earth for approximately **140 to 168 million years**, originating during the Jurassic or early Cretaceous period, long before the extinction of the dinosaurs. They evolved from wasp-like ancestors and began to flourish and diversify around 100 million years ago, coinciding with the rise of flowering plants.

https://news.harvard.edu/gazette/story/2006/04/ants-are-surprisingly-ancient-arising-140-168-million-years-ago-2/

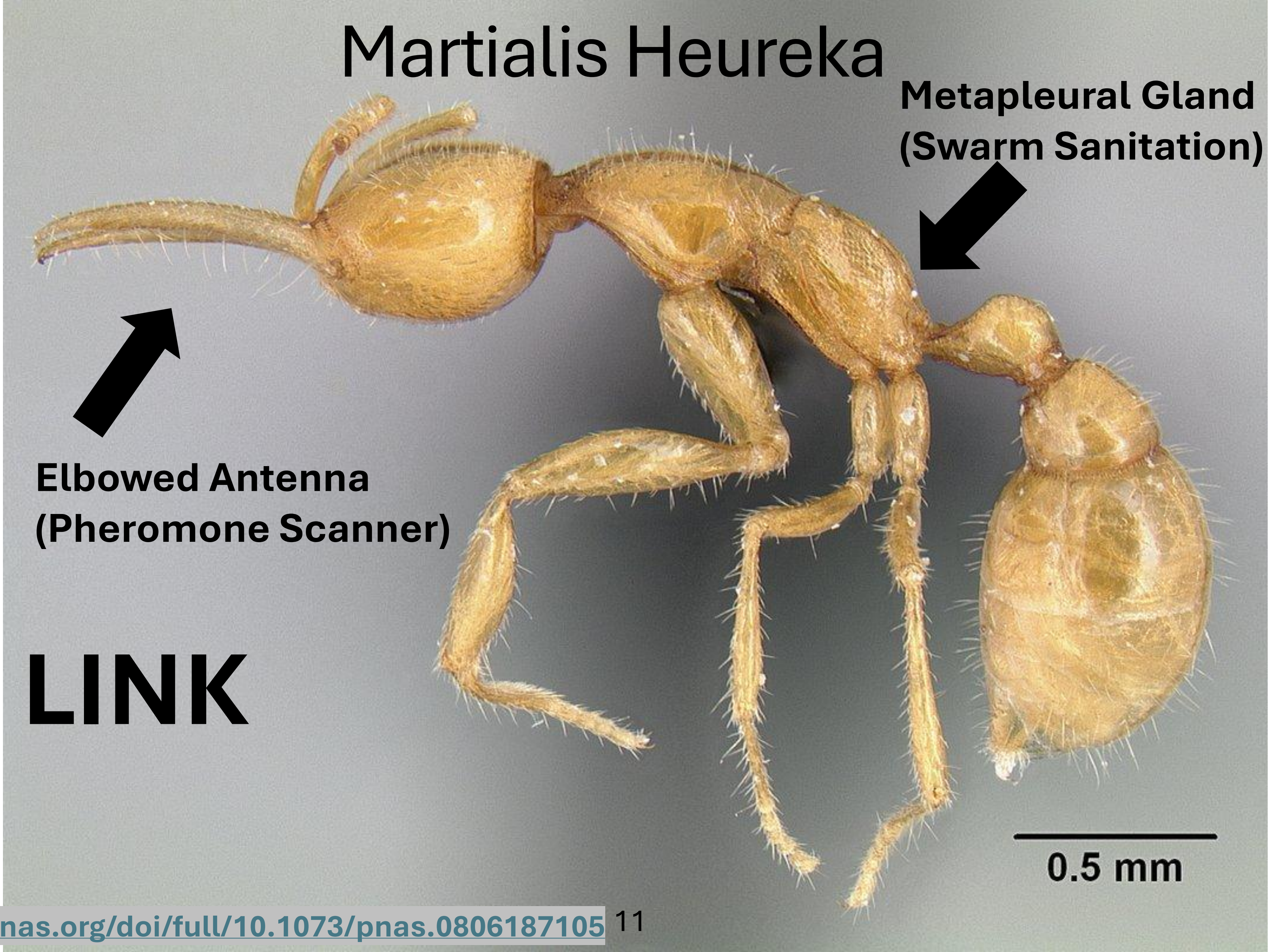
STEM ANTS

~~Introvert~~

Individualists

EXTINCT

Martialis Heureka



Metapleural Gland
(Swarm Sanitation)

Elbowed Antenna
(Pheromone Scanner)

THE LINK

https://www.pnas.org/doi/full/10.1073/pnas.0806187105

doi.org/10.1038/s41586-022-05120-w&authuser=2

Modern Ants (CROWN ANTs)

https://pmc.ncbi.nlm.nih.gov/articles/PMC11491779/

Advance Communication

Pheromones etc..

Evolutionary Stability

~120 Myo

Swarm Intelligence

Lack central control

Etc.

Research Timeline

Stimergy

Pierre Paul Grassé

GOD

∞

1959

Double Bridge Experiment

www.shutterstock.com

Jean Louis Deneubourg

Herodotus

5th centaury BC

1989

Pheromone Transition Rule

Marco Dorigo

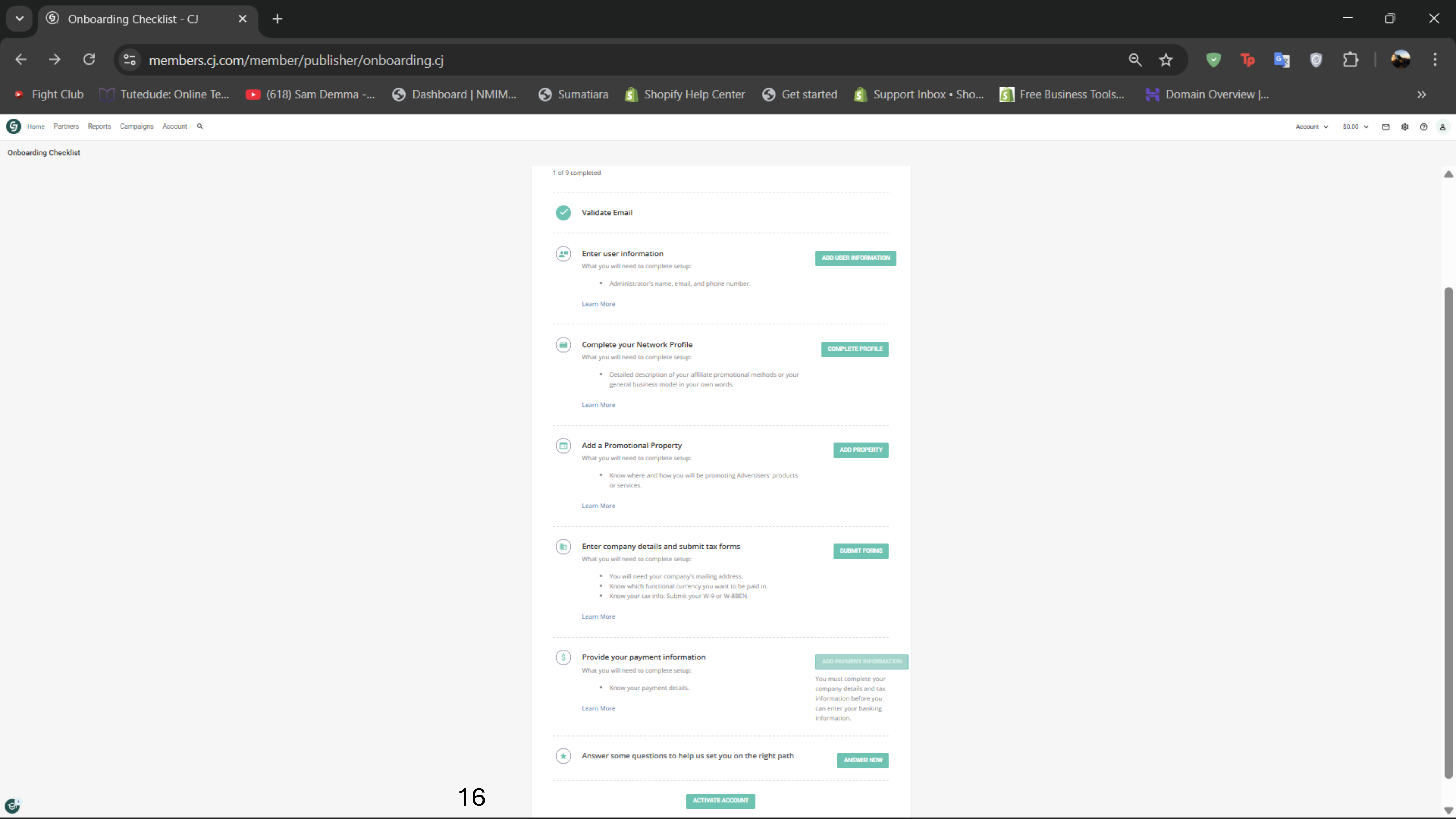
1991

Antivirus using ACO

kaspersky

SARANG-18

2010



Onboarding Checklist

1 of 9 completed

✓ Validate Email

Enter user information

What you will need to complete setup:

- Administrator's name, email, and phone number.

Learn More

ADD USER INFORMATION

Complete your Network Profile

What you will need to complete setup:

- Detailed description of your affiliate promotional methods or your general business model in your own words.

Learn More

COMPLETE PROFILE

Add a Promotional Property

What you will need to complete setup:

- Know where and how you will be promoting Advertisers' products or services.

Learn More

ADD PROPERTY

Enter company details and submit tax forms

What you will need to complete setup:

- You will need your company's mailing address.
- Know which functional currency you want to be paid in.
- Know your tax info: Submit your W-9 or W-8BEN.

Learn More

SUBMIT FORMS

Provide your payment information

What you will need to complete setup:

- Know your payment details.

Learn More

ADD PAYMENT INFORMATION

You must complete your company details and tax information before you can enter your banking information.

Answer some questions to help us set you on the right path

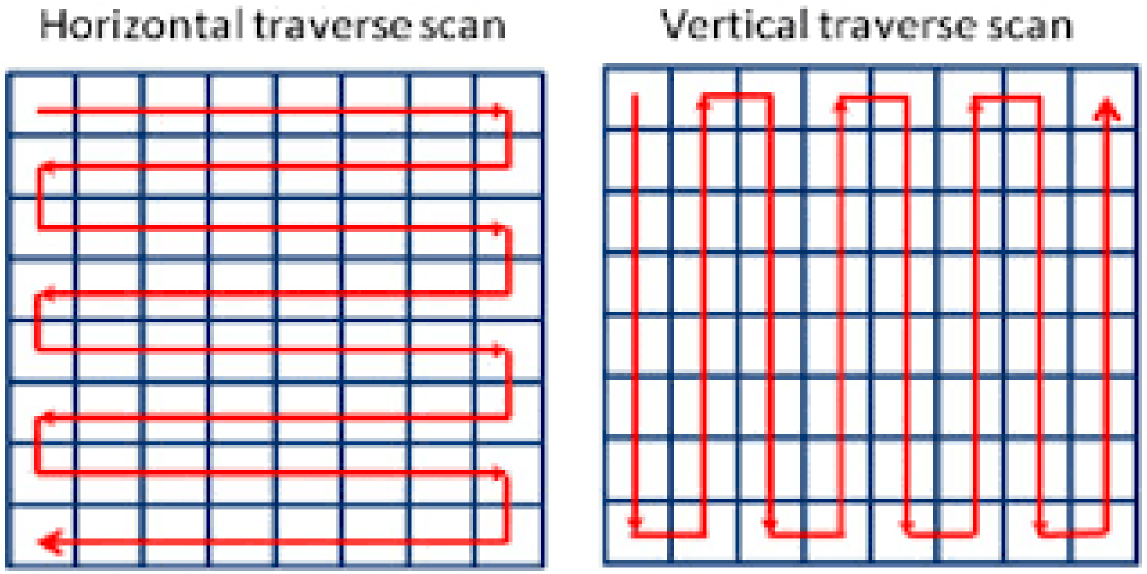
ANSWER NOW

ACTIVATE ACCOUNT

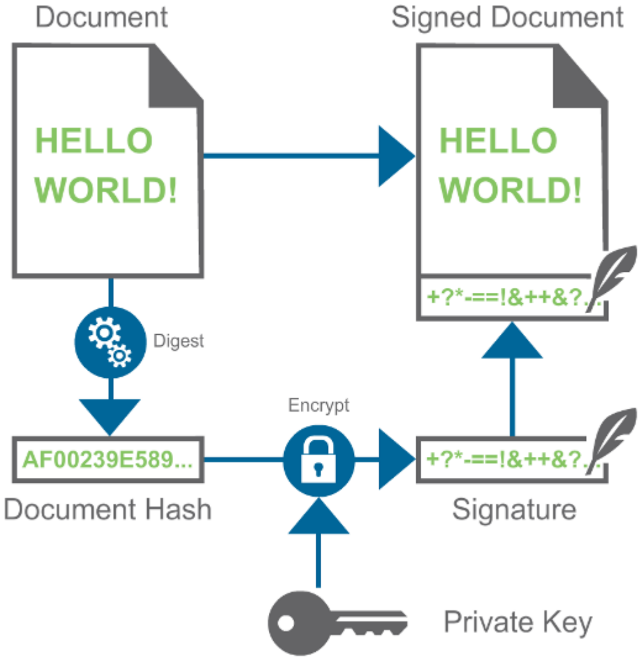
Application 1- Antivirus Optimization

1. Traverse Scanning

2. Signature Matching

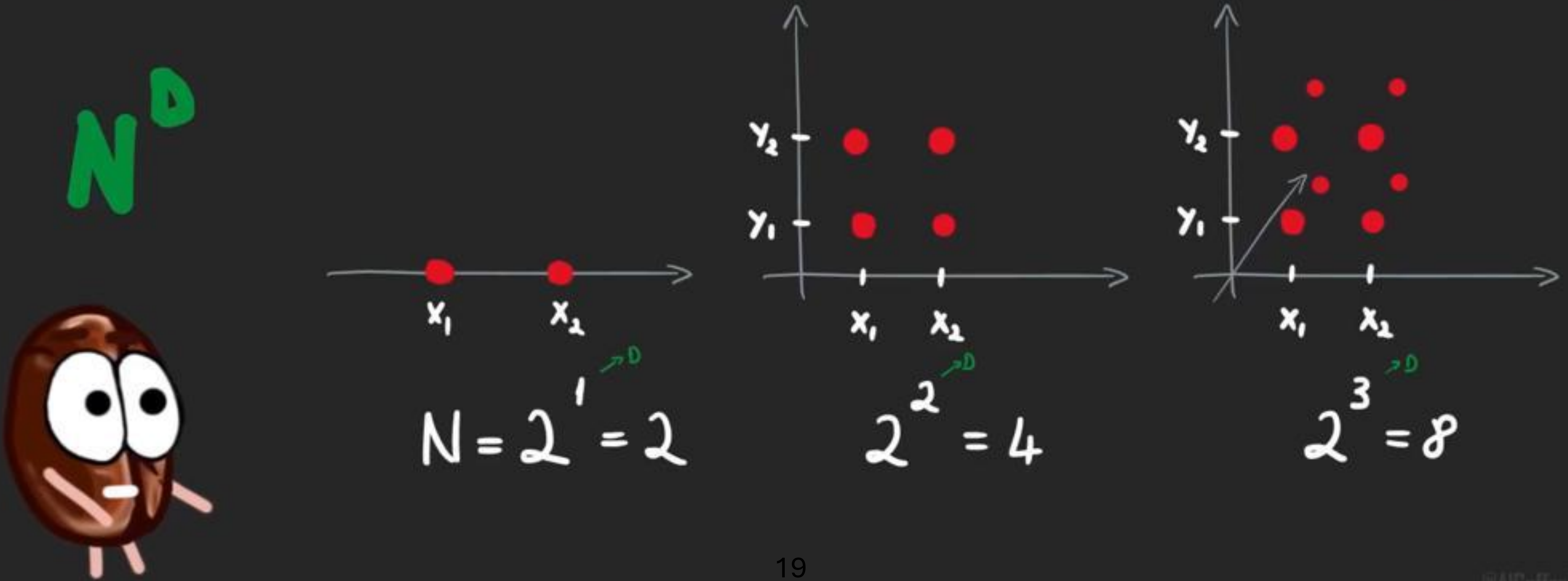


https://www.researchgate.net/figure/Horizontal-and-vertical-traverse-scans_fig5_282175661



https://library.mosse-institute.com/articles/2023/08/digital-signatures.html blessing curse

The blurse of dimensionality



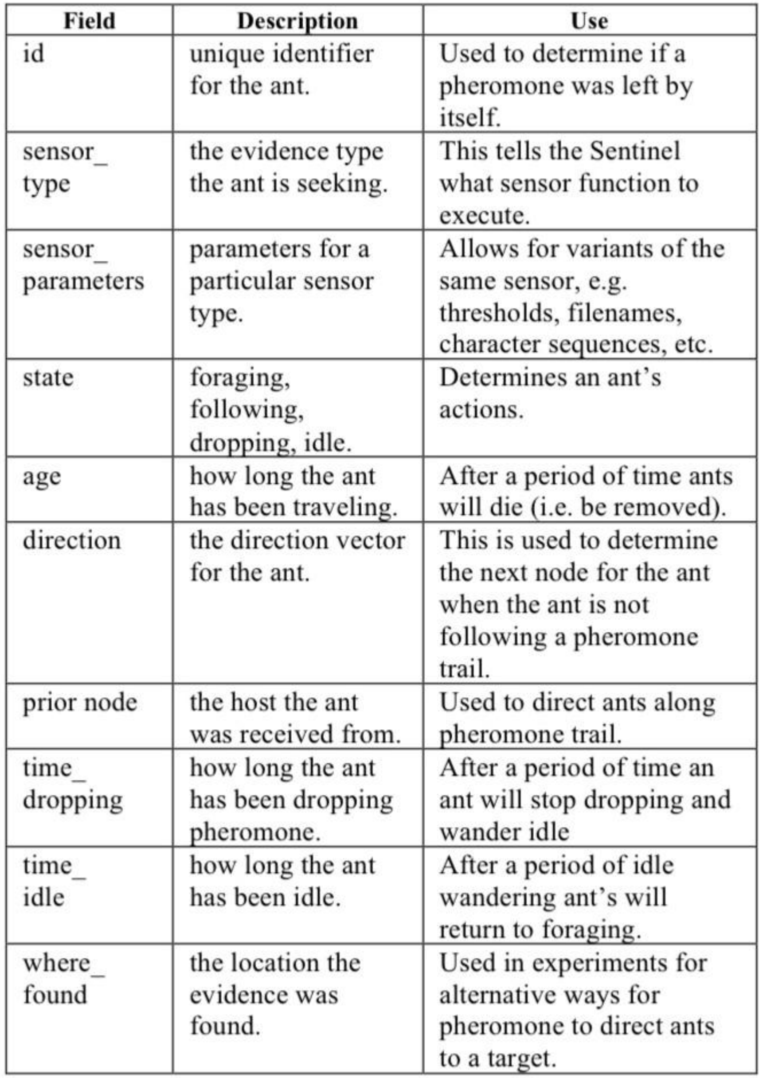
Here’s How ACO solves it…

Mathematical Abstraction

Biological Model	Computational Equivalent
Ant	Independent computational agent
Colony	Multi-agent system
Pheromone	Weighted probability
Environment	search space
Evaporation	decay mechanism
Foraging path	traversal path

Parameter	Meaning	Mathematical Role
α	Pheromone influence	Controls exploitation
β	Heuristic influence	Controls exploration
ρ	Evaporation rate	Controls memory decay
m	Number of ants	Affects convergence speed

TABLE I. ANT PACKET DEFINITION



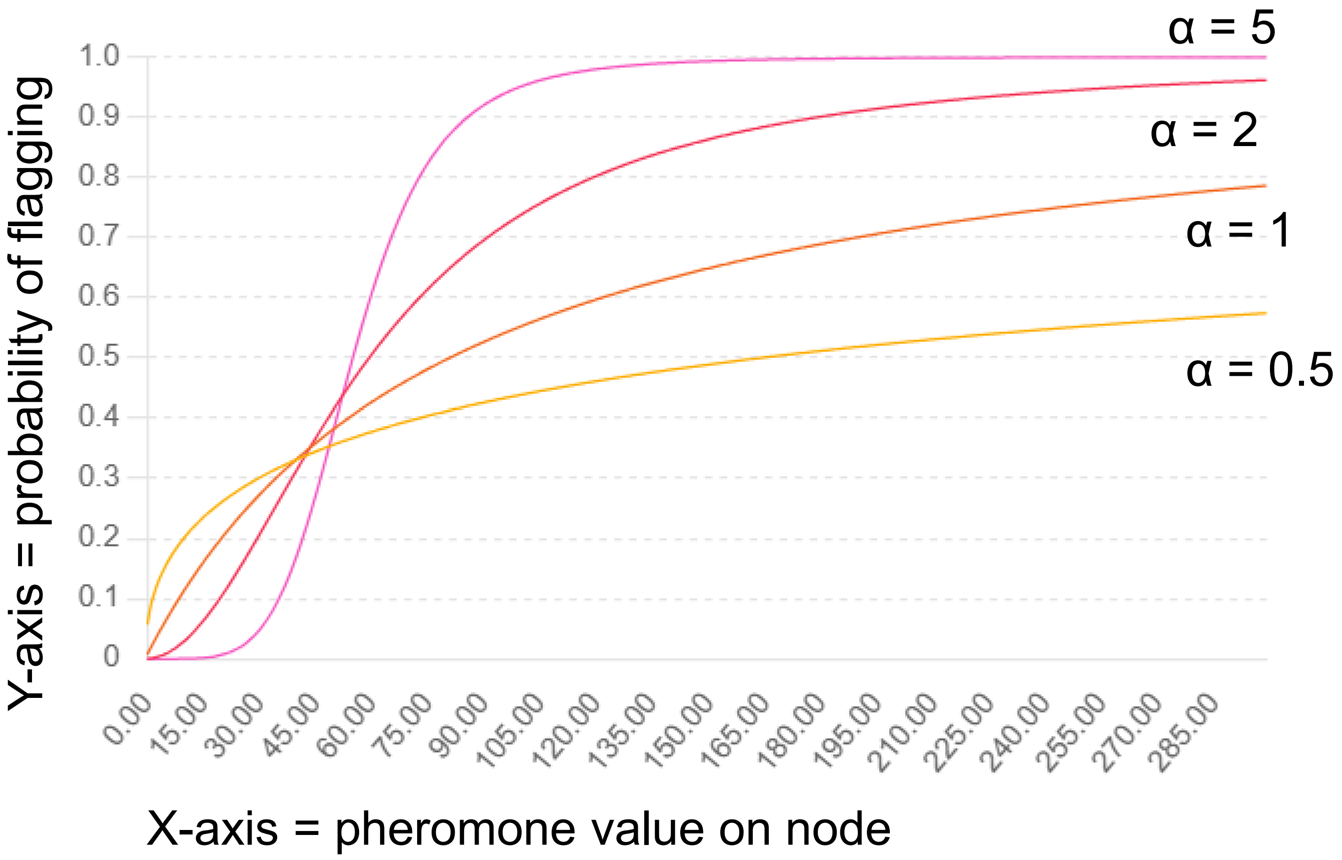
Field	Description	Use
id	unique identifier for the ant.	Used to determine if a pheromone was left by itself.
sensor_ type	the evidence type the ant is seeking.	This tells the Sentinel what sensor function to execute.
sensor_ parameters	parameters for a particular sensor type.	Allows for variants of the same sensor, e.g. thresholds, filenames, character sequences, etc.
state	foraging, following, dropping, idle.	Determines an ant's actions.
age	how long the ant has been traveling.	After a period of time ants will die (i.e. be removed).
direction	the direction vector for the ant.	This is used to determine the next node for the ant when the ant is not following a pheromone trail.
prior node	the host the ant was received from.	Used to direct ants along pheromone trail.
time_ dropping	how long the ant has been dropping pheromone.	After a period of time an ant will stop dropping and wander idle
time_ idle	how long the ant has been idle.	After a period of idle wandering ant's will return to foraging.
where_ found	the location the evidence was found.	Used in experiments for alternative ways for pheromone to direct ants to a target.

https://doi.org/10.1109/ITNG.2011.159

Mathematical Functions

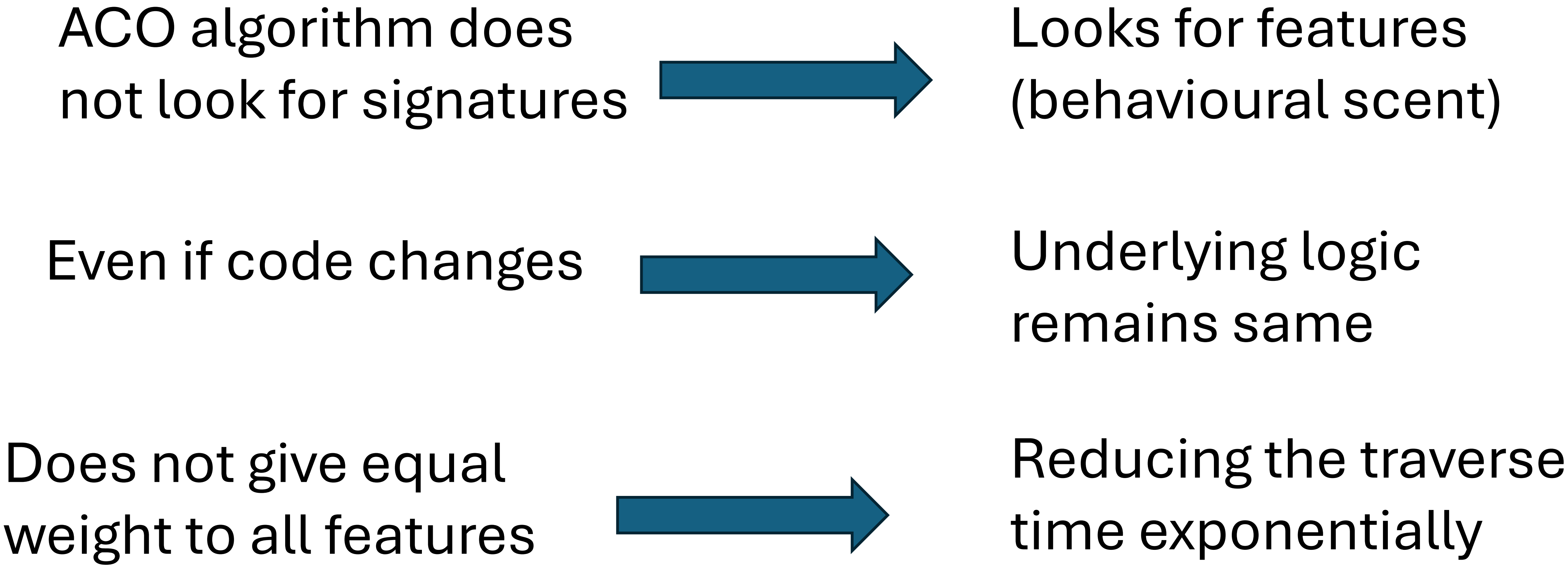
$$p_{ij}^{k}(t) = \begin{cases} \dfrac{[\tau_{ij}(t)]^{\alpha}[\eta_{ij}]^{\beta}}{\sum\limits_{k \in allowed_k} [\tau_{ik}(t)]^{\alpha}[\eta_{ik}]^{\beta}} & j \in allowed_k \\ 0 & \text{else} \end{cases}$$

α = pheromone influence (sensitivity)
β= heuristic influence
N^{k}_{i} = feasible neighbors for ant k
Ϯ$_{ij}$ (t)= collective memory
Π_{ij} = local heuristic



https://www.academia.edu/24860312/ANT_COLONY_OPTIMIZATION_METHODS_AND_APPLICATIONS

How ACO solves these problems…



ACO algorithm does not look for signatures → Looks for features (behavioural scent)

Even if code changes → Underlying logic remains same

Does not give equal weight to all features → Reducing the traverse time exponentially

GAME TIME

solo

1	A	3	N	@
2	5	7	#	P
3	E	3	L	@
4	6	!	N	S
5	8	$	E	K
6	I	9	T	&

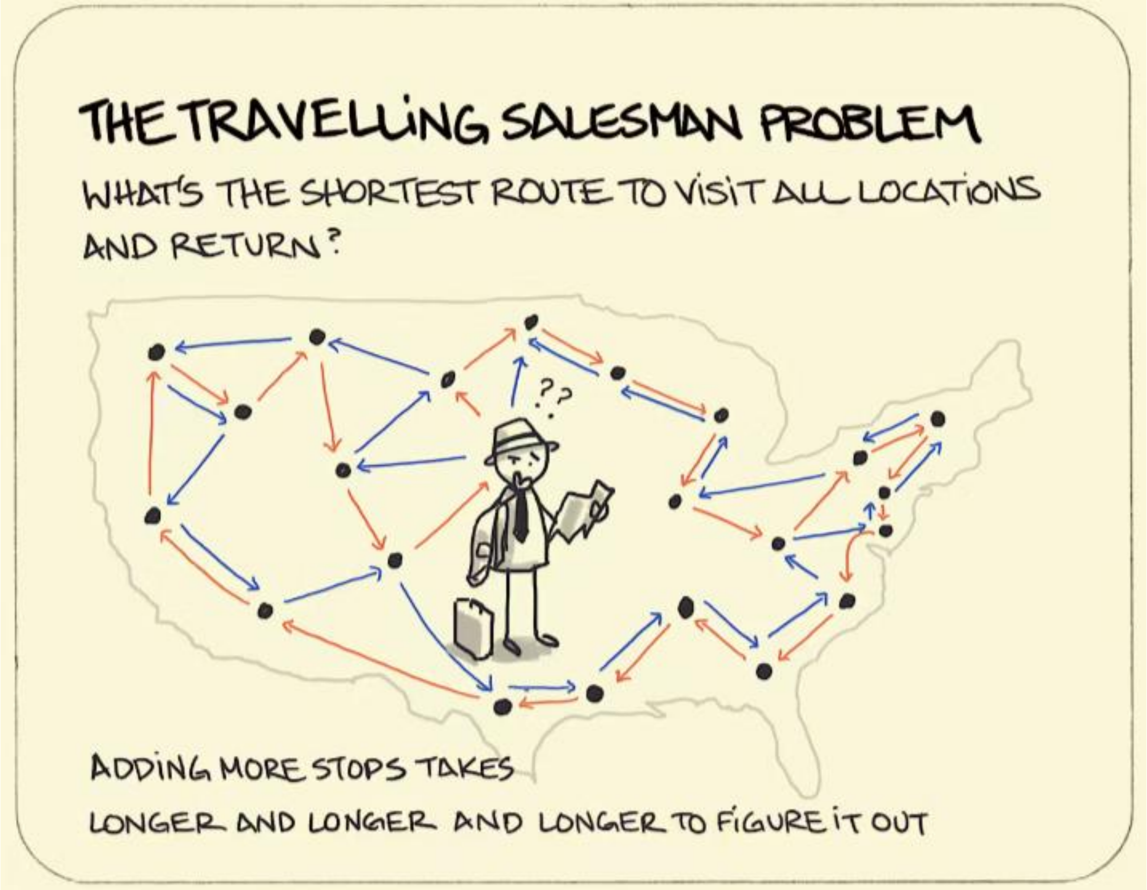
Team

1	6	&	A	G
2	U	7	L	-
3	7	$	I	T
4	8	#	U	V
5	E	2	K	-
6	9	)	O	M

Application 2- Travelling Salesman Problem(TSP)

WHAT EXACTLY IS TSP ?

TSP stands for **Travelling Salesman Problem**.


THE TRAVELLING SALESMAN PROBLEM
WHAT'S THE SHORTEST ROUTE TO VISIT ALL LOCATIONS AND RETURN?
??
ADDING MORE STOPS TAKES LONGER AND LONGER AND LONGER TO FIGURE IT OUT

Mathematical Representation

Let:

- n= number of cities
- d_{ij} =distance from city $i$to city

$$\min \sum n \; d_{i,\pi(i)}$$

What is

THE TRAVELING SALESMAN PROBLEM?

Statistical Data

Study / Experiment	Dataset	Metric	Traditional Method	ACO-Based Method	% Improvement
Malware Clustering Study (IJACSA, 2023)	Virus Dataset	Detection Accuracy	72%	88%	+22% relative improvement
Malware Clustering Study (IJACSA, 2023)	Worm Dataset	Detection Accuracy	68%	87%	+28% relative improvement
ACO Feature Selection Study	Malware Features (High-dimensional)	Feature Reduction	120 features used	75 optimal features selected	~37% reduction
Hybrid ACO + ML Model	Malware Classification	False Positive Rate	12%	7%	~41% reduction
ACO-based Intrusion Detection	Network Traffic Dataset	Detection Efficiency	81%	92%	+11% absolute improvement

Pros

Excellent for combinatorial optimization

Positive feedback accelerates learning

Flexible and hybrid-friendly

Capable of escaping local minima (with proper tuning)

Intuitive mathematical and biological foundation.

Cons

Can get stuck too early

Needs careful tuning

Uses a lot of memory

Not ideal for continuous problems

No guarantee of best possible answer

Too much randomness sometimes

May need many iterations to stabilize

Future Propositions

- AI-driven self-learning systems for detecting zero-day and unknown malware
- Ant Colony Optimization (ACO) for faster and smarter threat path detection
- Real-time behavior-based monitoring instead of only signature-based scanning
- Cloud-integrated threat intelligence for faster global updates
- Lightweight antivirus engines optimized for IoT and smart devices
- Automated threat isolation and autonomous response systems
- Reduced CPU and RAM usage through advanced optimization algorithms
- Adaptive security models that evolve with emerging cyber threats

NOT SURE IF YOU'RE CLAPPING
BECAUSE THE PRESENTATION WAS GOOD
OR BECAUSE ITS OVER
mgflip.com

THANK YOU

ANY QUESTIONS?