Malware Hunting with Machine Learning

Malware Threat Intelligence using a framework for multiple ML models.

by

Saket Upadhyay

Feb 5, 2020

About Saket Upadhyay

- Independent Security Researcher

About Saket Upadhyay

- Independent Security Researcher
- Interested in Malware Analysis, R.E., M.L.

About Saket Upadhyay

- Independent Security Researcher
- Interested in Malware Analysis, R.E., M.L. and everything in between.

About Saket Upadhyay

- Independent Security Researcher
- Interested in Malware Analysis, R.E., M.L. and everything in between.
- Worked in some companies as PenTester and Vulnerability Analyst

About Saket Upadhyay

- Independent Security Researcher
- Interested in Malware Analysis, R.E., M.L. and everything in between.
- Worked in some companies as PenTester and Vulnerability Analyst
- 5 years in the field of cybersecurity. (learning and research)

About Saket Upadhyay

- Independent Security Researcher
- Interested in Malware Analysis, R.E., M.L. and everything in between.
- Worked in some companies as PenTester and Vulnerability Analyst
- 5 years in the field of cybersecurity. (learning and research)
- Currently persuing Bachelor’s: Cybersec. and Digital Forensics @ VIT Bhopal

Contents

Contents

Contents

1. What is a malware?

   How we define malware and what we understand from it.

2. Basic Detection Methods.

   Static, Dynamic and Hybrid Methods.

Contents

1. What is a malware?

   How we define malware and what we understand from it.

2. Basic Detection Methods.

   Static, Dynamic and Hybrid Methods.

3. Basic idea of Machine Learning in detection

   Why we need ML? What we get from ML in detection?

Contents

Contents

Contents

Contents

Contents

What is malware?

Textbook definition

Malware is any **software intentionally designed to cause damage** to a computer, server, client, or computer network (by contrast, software that causes *unintentional harm due to some deficiency is usually a software bug*).

Textbook definition

Malware is any **software intentionally designed to cause damage** to a computer, server, client, or computer network (by contrast, software that causes *unintentional harm due to some deficiency is usually a software bug*).
SOURCE : WIKIPEDIA

Textbook definition

A wide variety of types of malware exist, including

Textbook definition

A wide variety of types of malware exist, including

- Viruses ["Creeper system", 1971]

Textbook definition

A wide variety of types of malware exist, including

- Viruses ["Creeper system", 1971]
- Worms ["The Morris worm", 1988]

Textbook definition

A wide variety of types of malware exist, including

- Viruses ["Creeper system", 1971]
- Worms ["The Morris worm", 1988]
- Trojan horses ["ANIMAL", 1975]

Textbook definition

A wide variety of types of malware exist, including

- Viruses ["Creeper system", 1971]
- Worms ["The Morris worm", 1988]
- Trojan horses ["ANIMAL", 1975]
- Ransomware ["PC Cyborg", 1991]

Textbook definition

A wide variety of types of malware exist, including

- Viruses ["Creeper system", 1971]
- Worms ["The Morris worm", 1988]
- Trojan horses ["ANIMAL", 1975]
- Ransomware ["PC Cyborg", 1991]
- Spyware [around 2000]

Textbook definition

A wide variety of types of malware exist, including

- Viruses ["Creeper system", 1971]
- Worms ["The Morris worm", 1988]
- Trojan horses ["ANIMAL", 1975]
- Ransomware ["PC Cyborg", 1991]
- Spyware [around 2000]
- Adware [roughly in 1995]

Textbook definition

A wide variety of types of malware exist, including

- Viruses ["Creeper system", 1971]
- Worms ["The Morris worm", 1988]
- Trojan horses ["ANIMAL", 1975]
- Ransomware ["PC Cyborg", 1991]
- Spyware [around 2000]
- Adware [roughly in 1995]
- Scareware. [increase in activity since 2008]

Key behaviour observations

Key behaviour observations

- Stealing [copy, move and]

Key behaviour observations

- Stealing [copy, move and]
- Encrypting data [file modification calls]

Key behaviour observations

- Stealing [copy, move and]
- Encrypting data [file modification calls]
- Deleting sensitive data [file manipulation/mod.]

Key behaviour observations

- Stealing [copy, move and]
- Encrypting data [file modification calls]
- Deleting sensitive data [file manipulation/mod.]
- Altering or hijacking core computing funct. [system calls]

Key behaviour observations

- Stealing [copy, move and]
- Encrypting data [file modification calls]
- Deleting sensitive data [file manipulation/mod.]
- Altering or hijacking core computing funct. [system calls]
- Monitoring users [active processes, process hooks etc.]

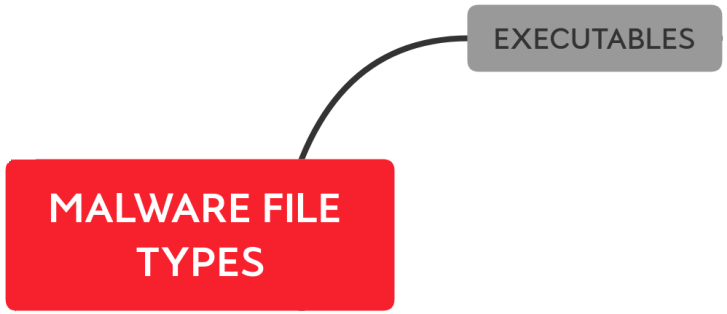
Key behaviour observations

- Stealing [copy, move and]
- Encrypting data [file modification calls]
- Deleting sensitive data [file manipulation/mod.]
- Altering or hijacking core computing funct. [system calls]
- Monitoring users [active processes, process hooks etc.]
- Process hijack[memory injection]
- Et Cetera

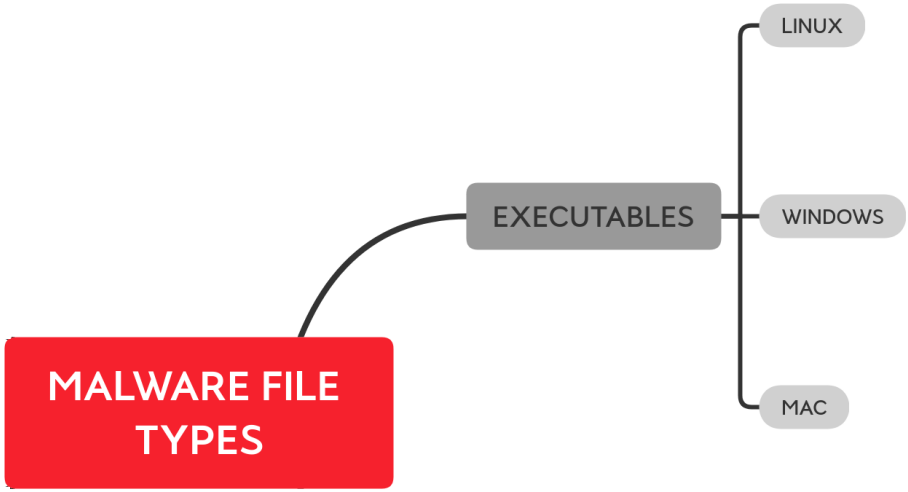
Malware Infection Vectors

MALWARE FILE TYPES

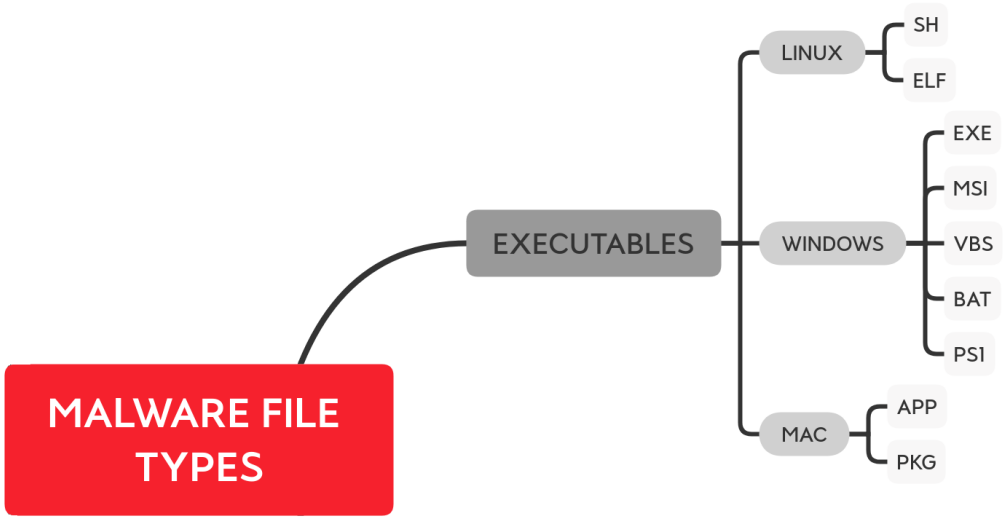
Malware Infection Vectors



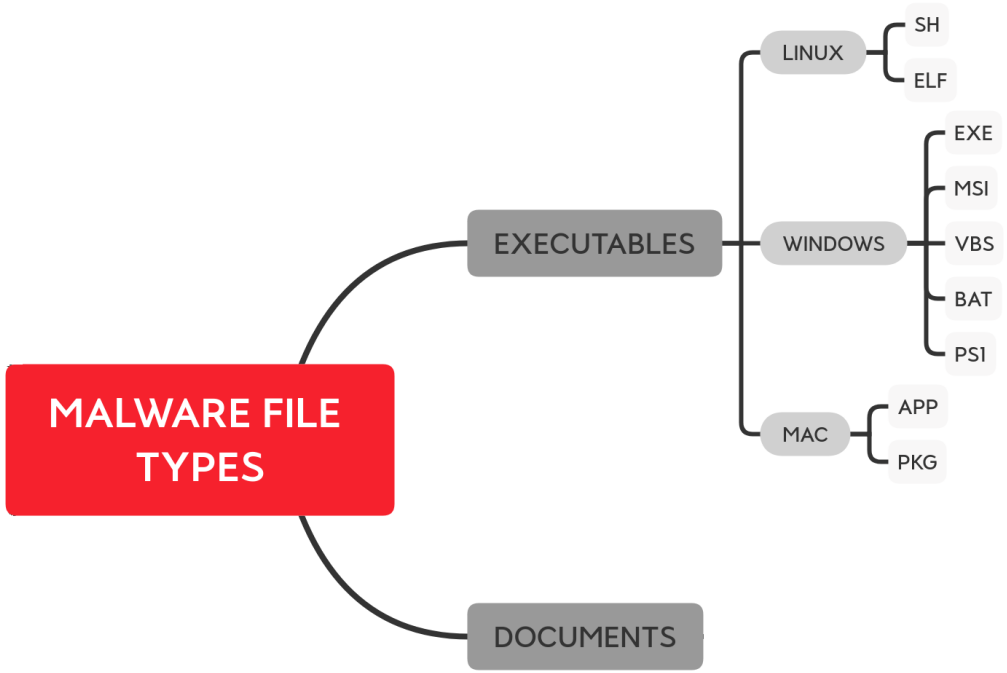
Malware Infection Vectors



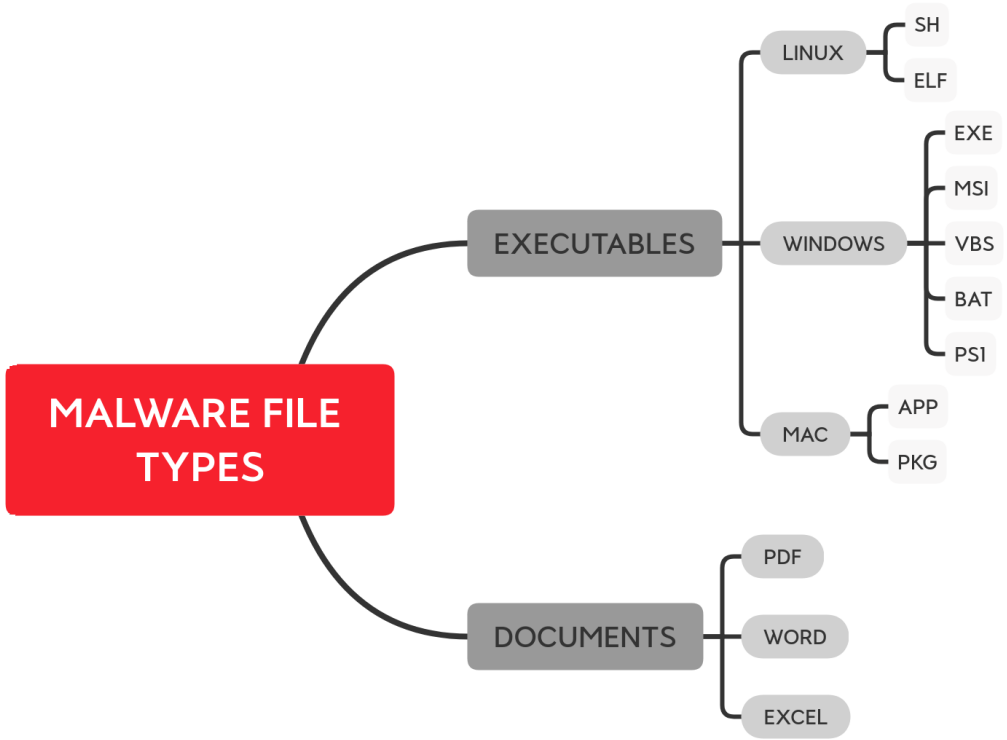
Malware Infection Vectors



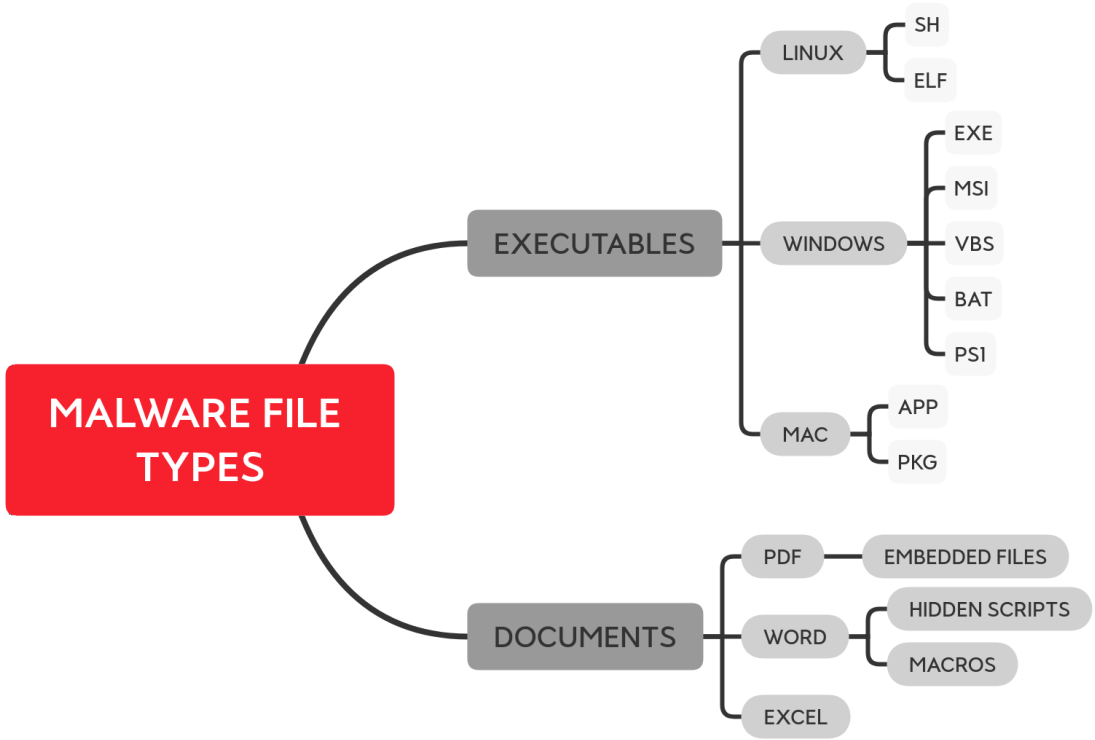
Malware Infection Vectors



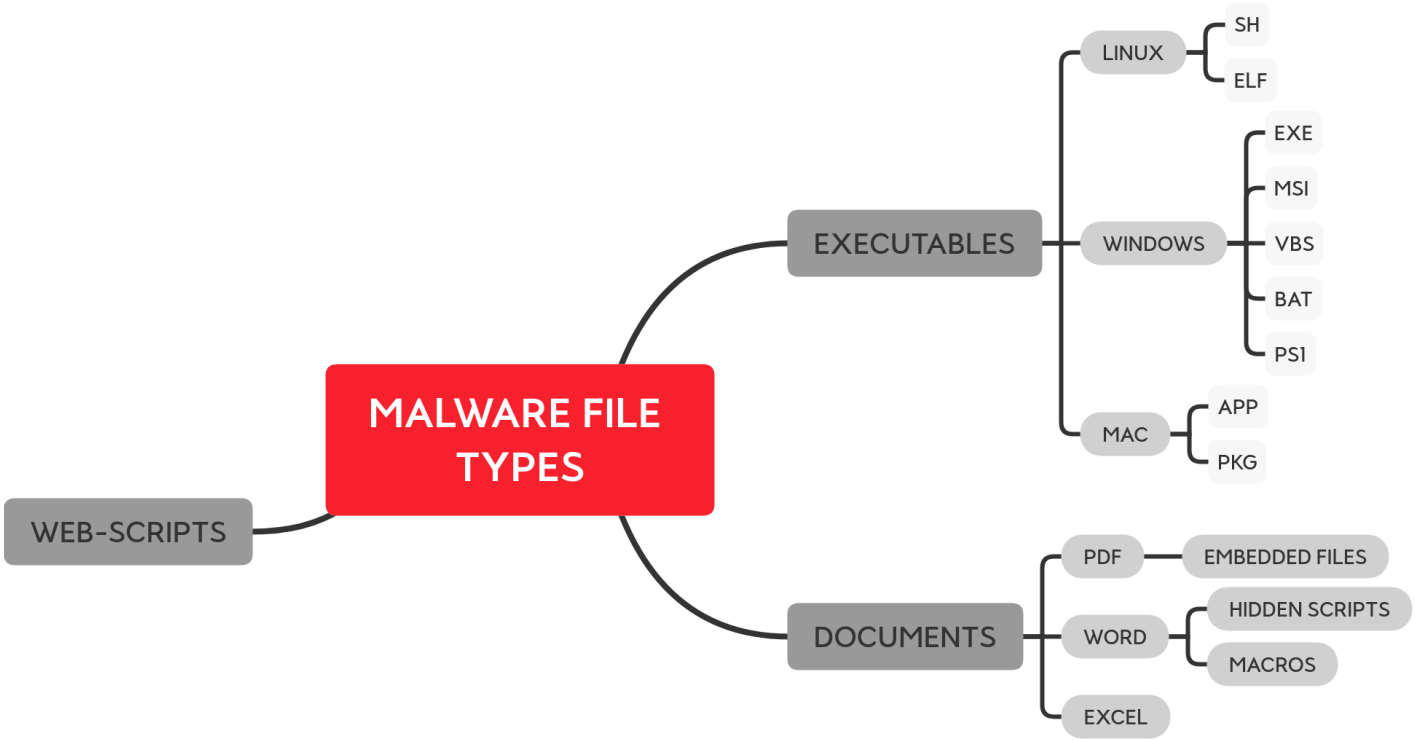
Malware Infection Vectors



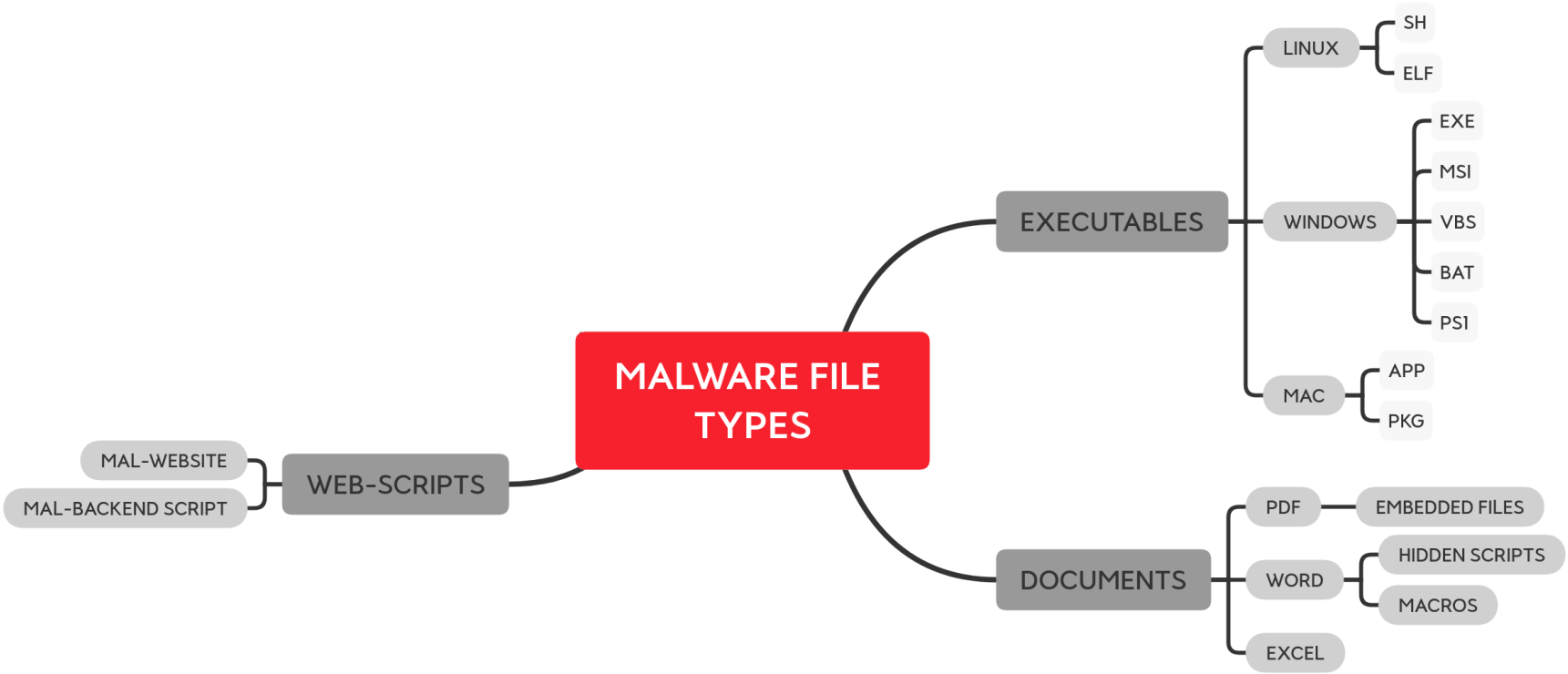
Malware Infection Vectors



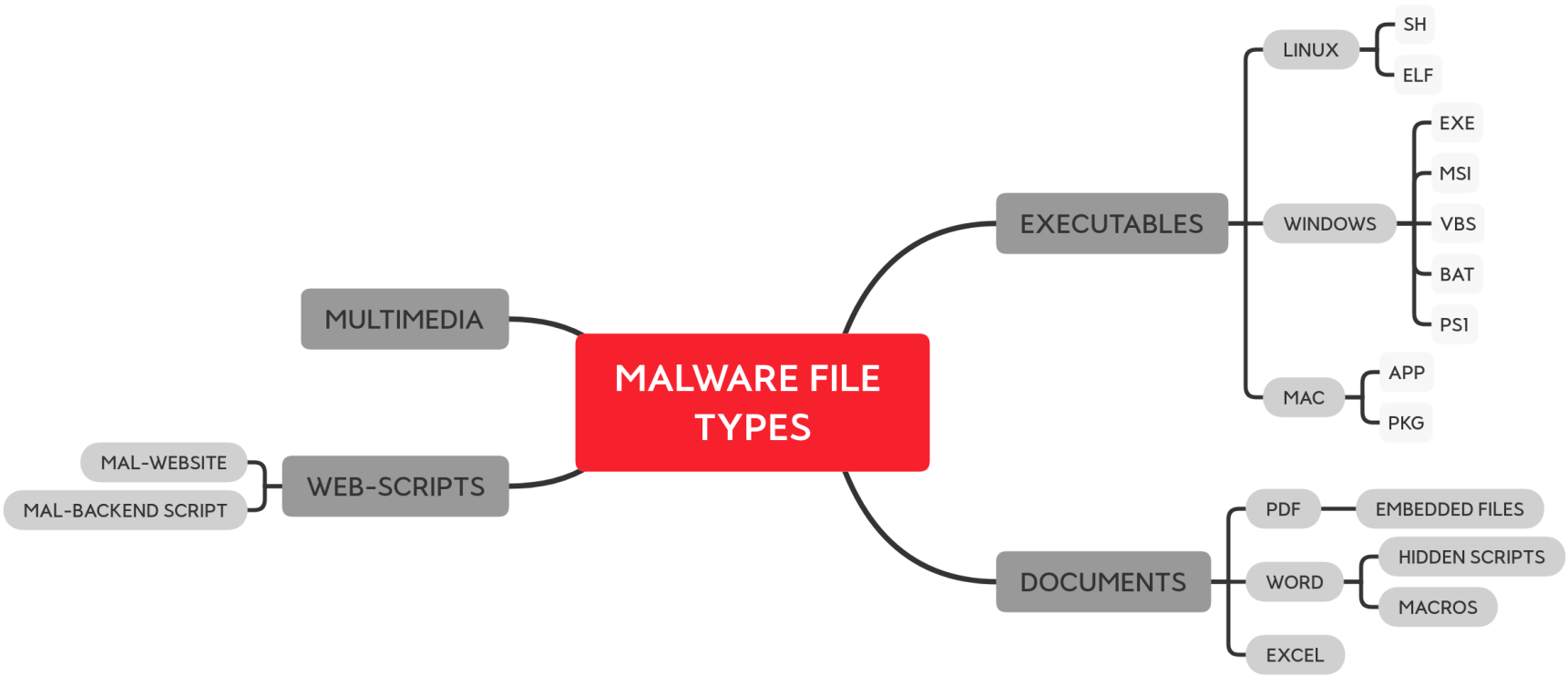
Malware Infection Vectors



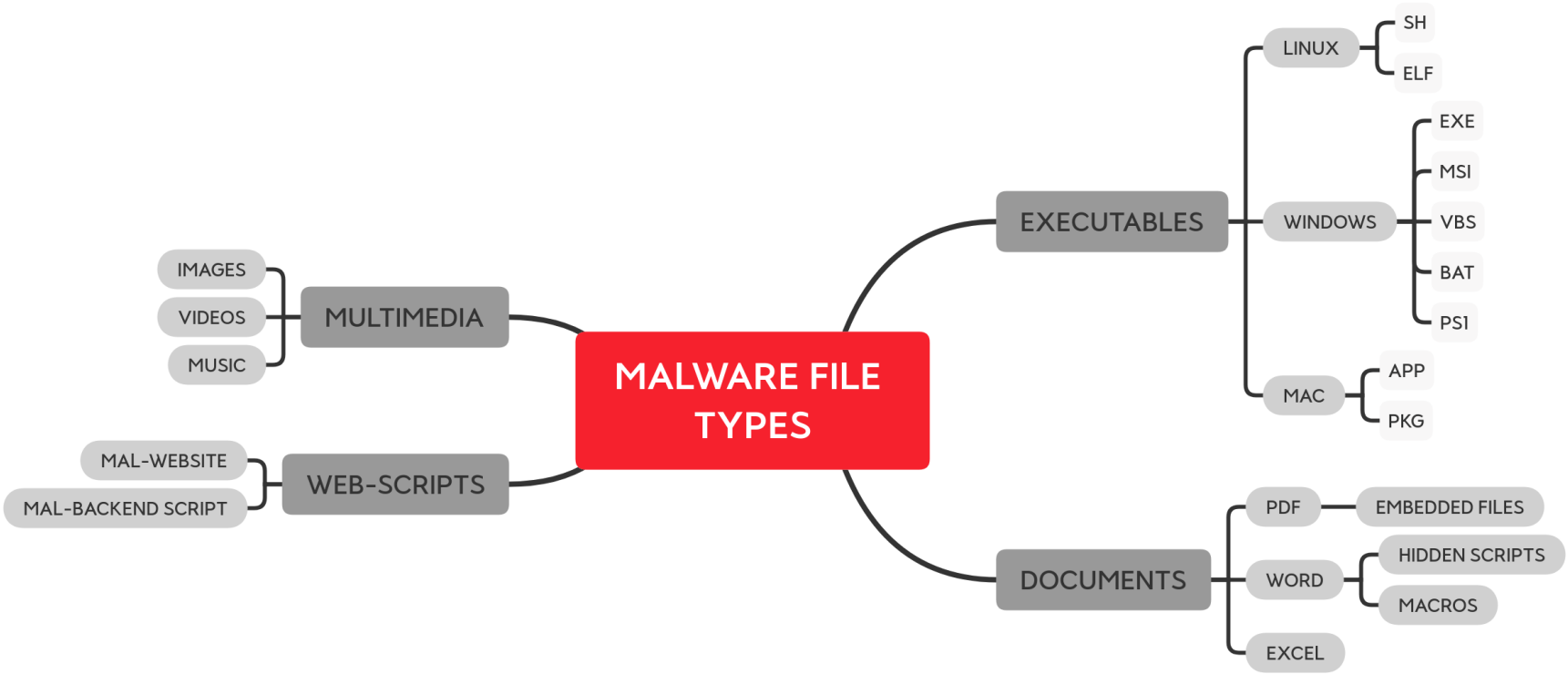
Malware Infection Vectors



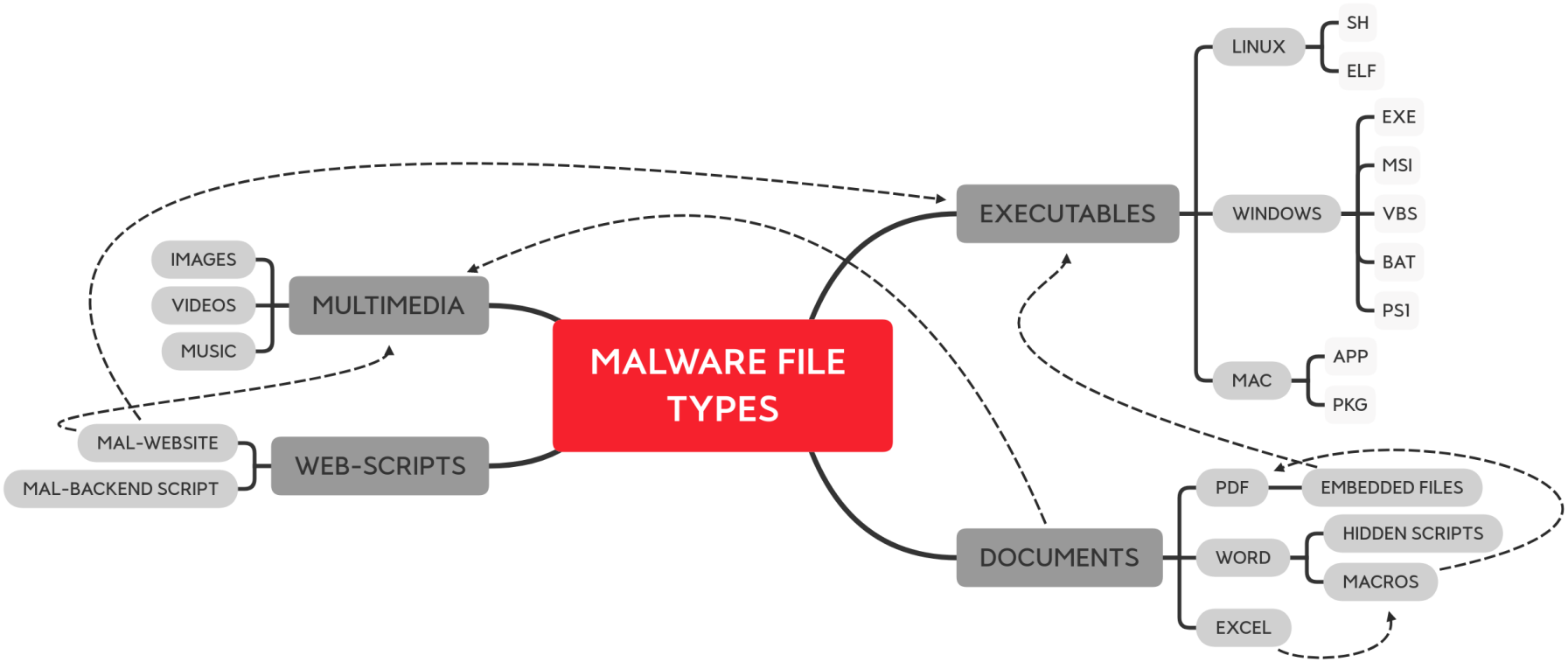
Malware Infection Vectors



Malware Infection Vectors

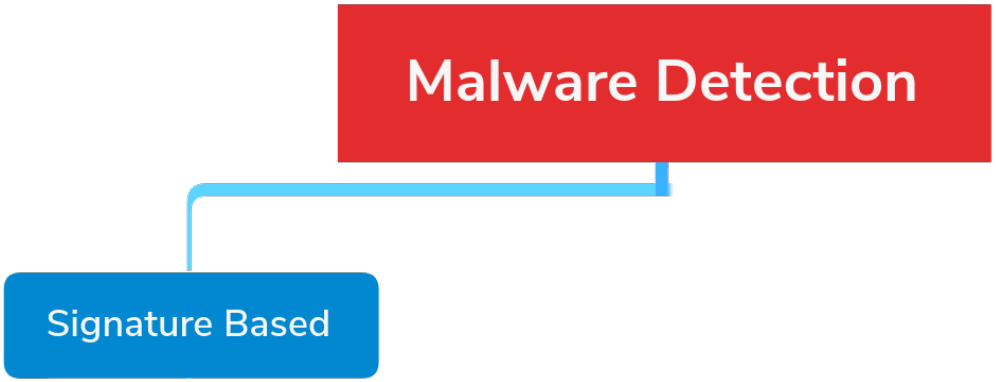


Malware Infection Vectors

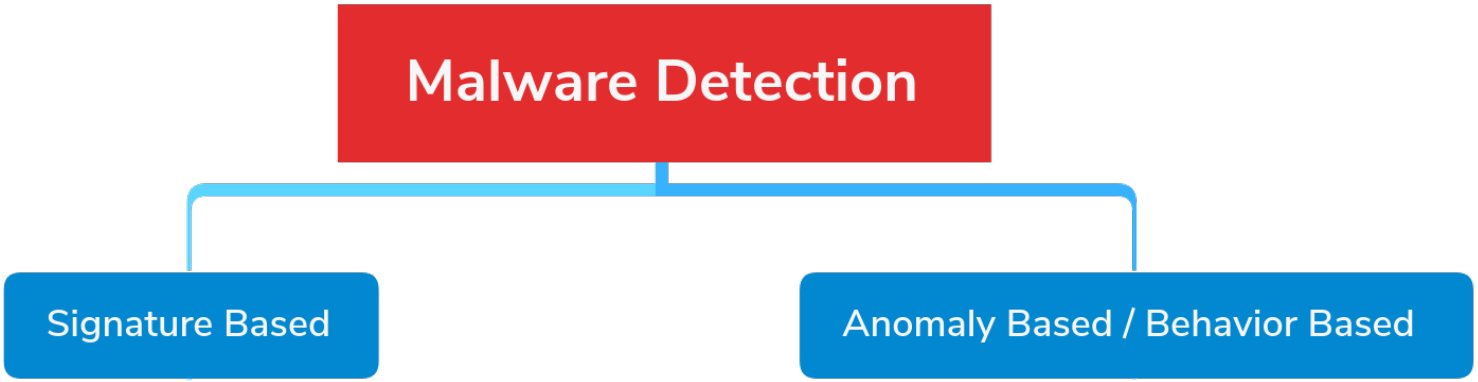


Basic Detection Methods

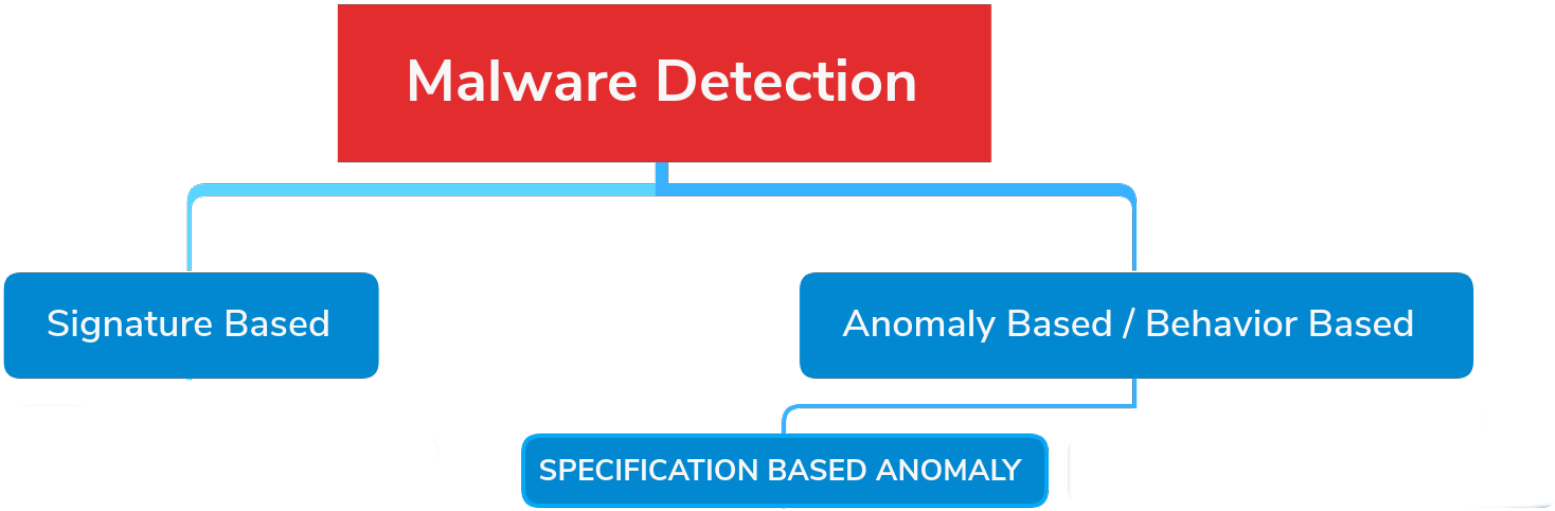
Detection Strategies



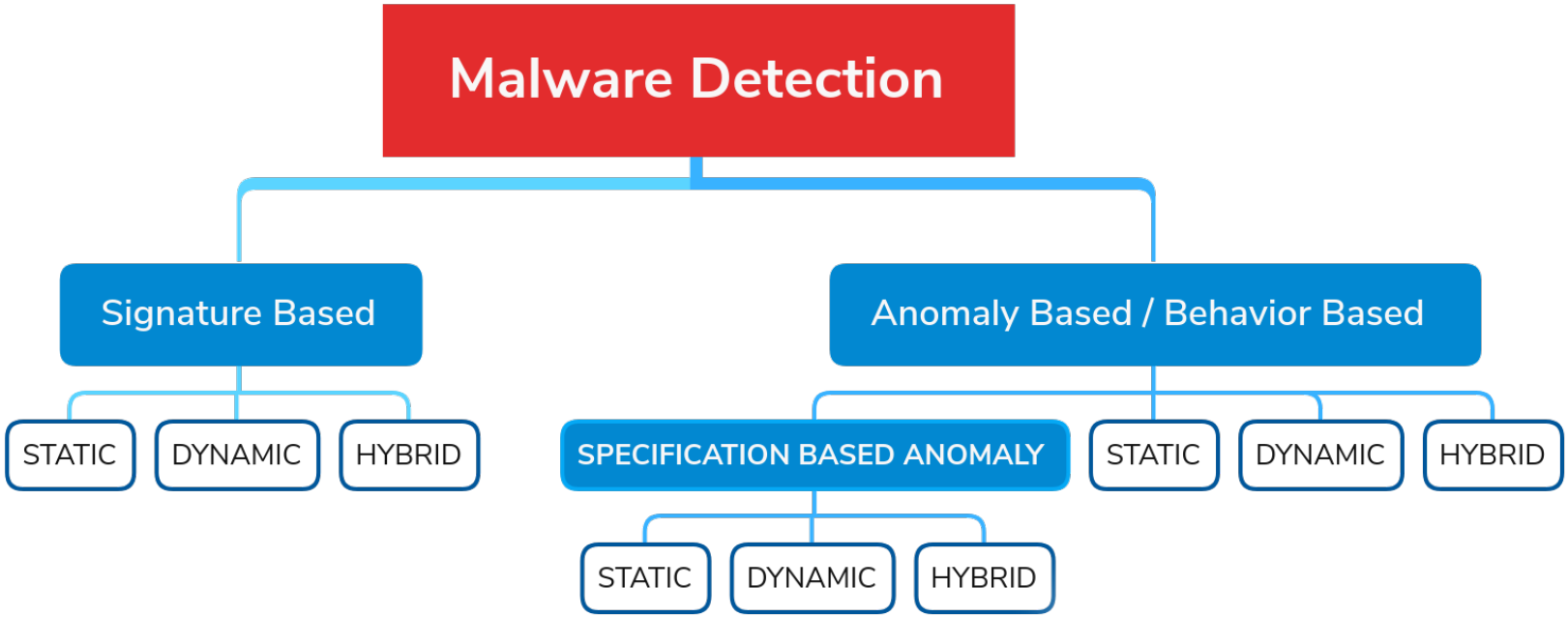
Detection Strategies



Detection Strategies



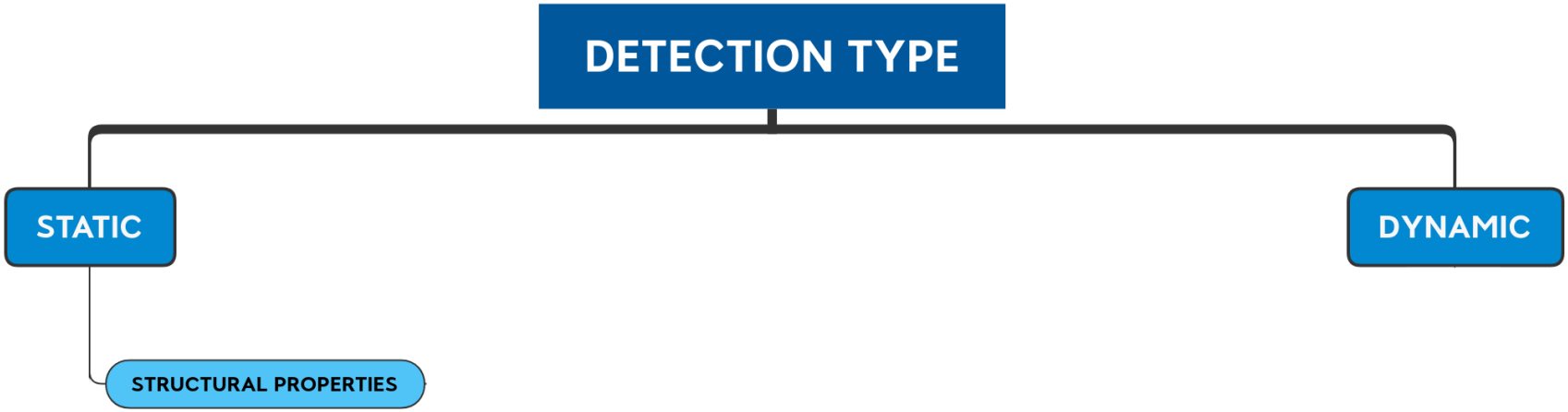
Detection Strategies



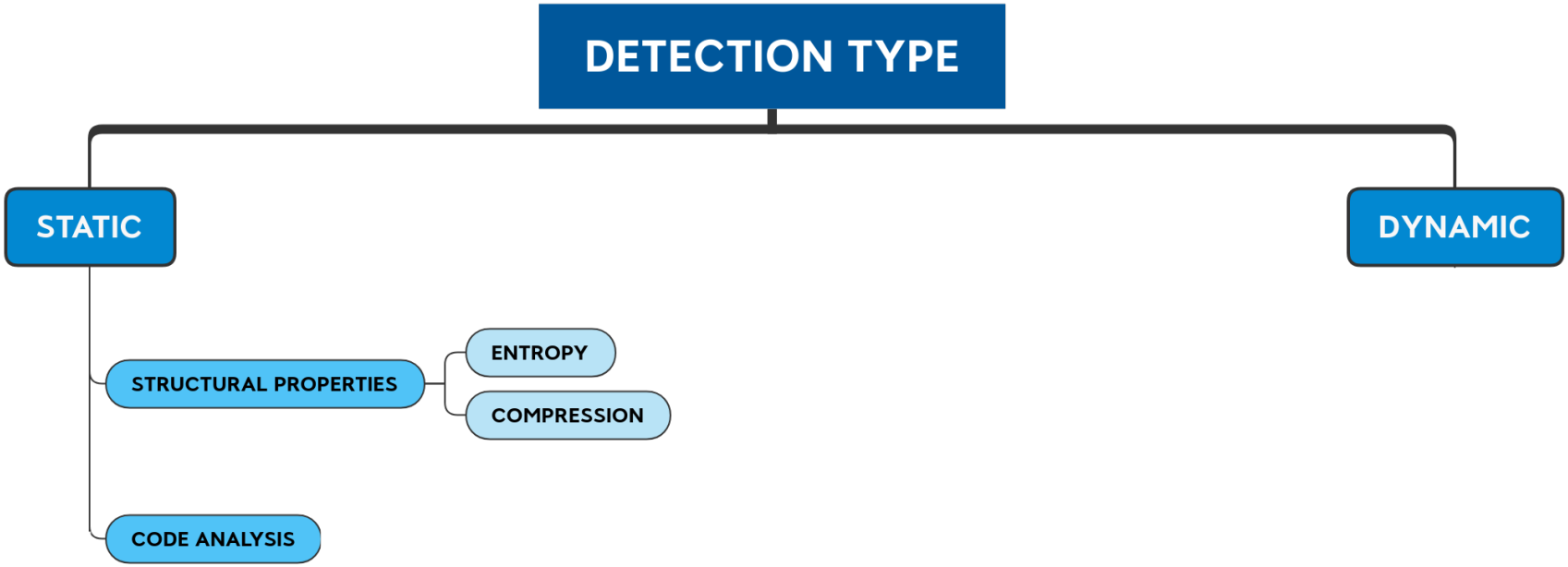
STATIC & DYNAMIC Analysis

STATIC & DYNAMIC Analysis

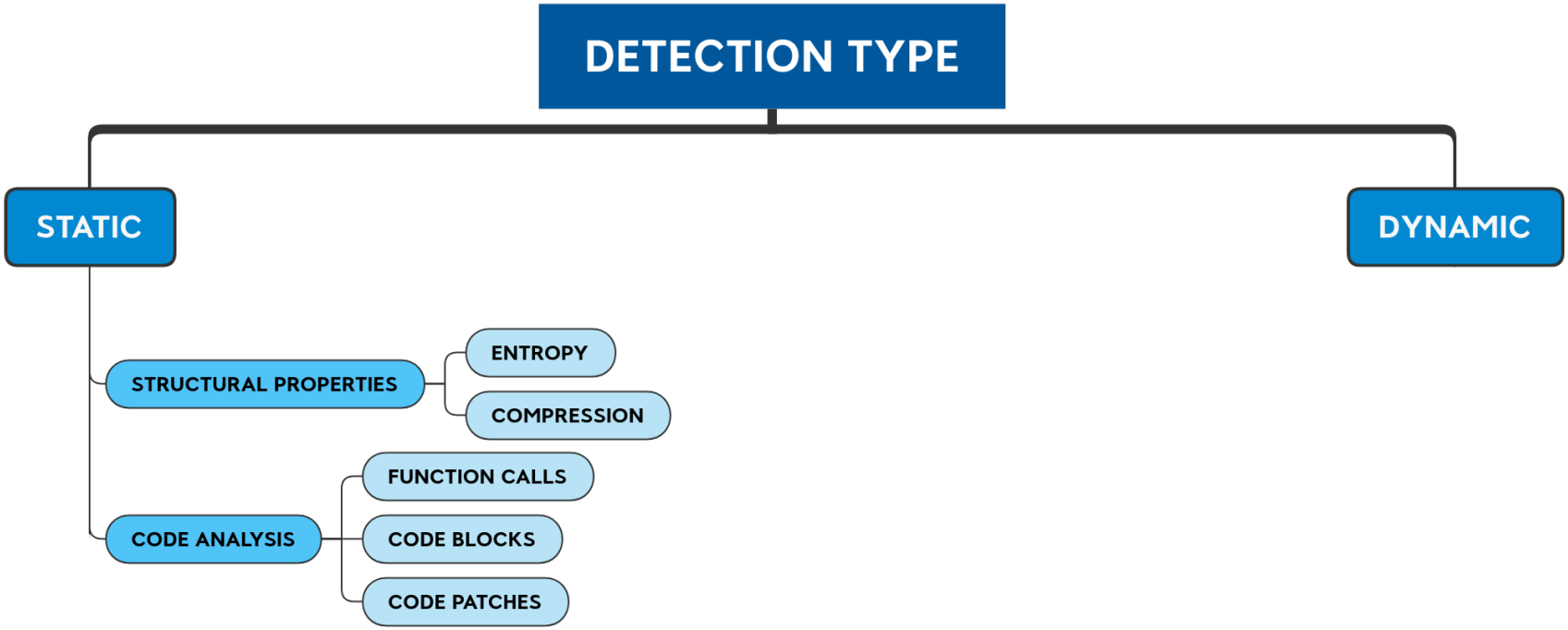
STATIC & DYNAMIC Analysis



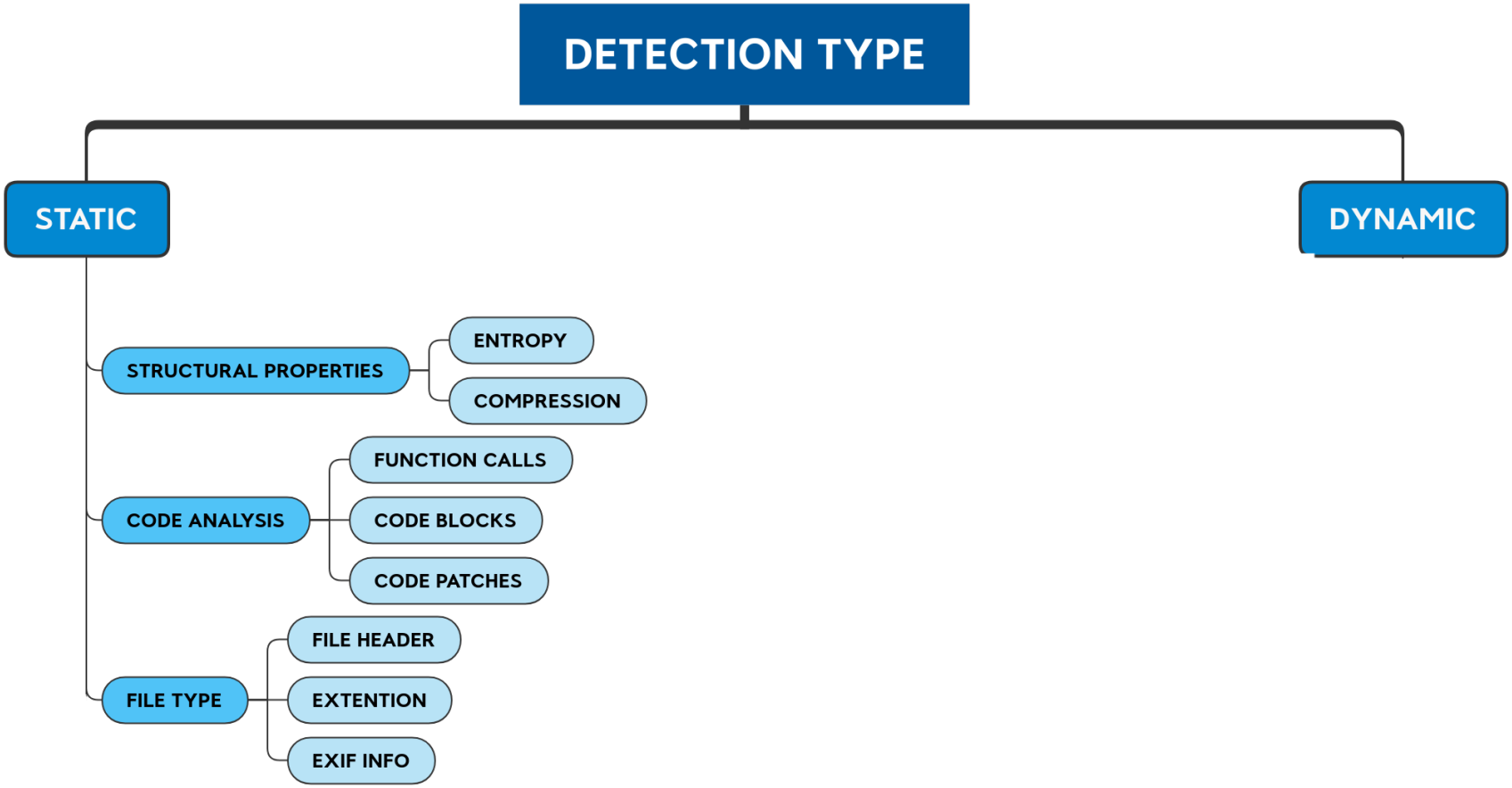
STATIC & DYNAMIC Analysis



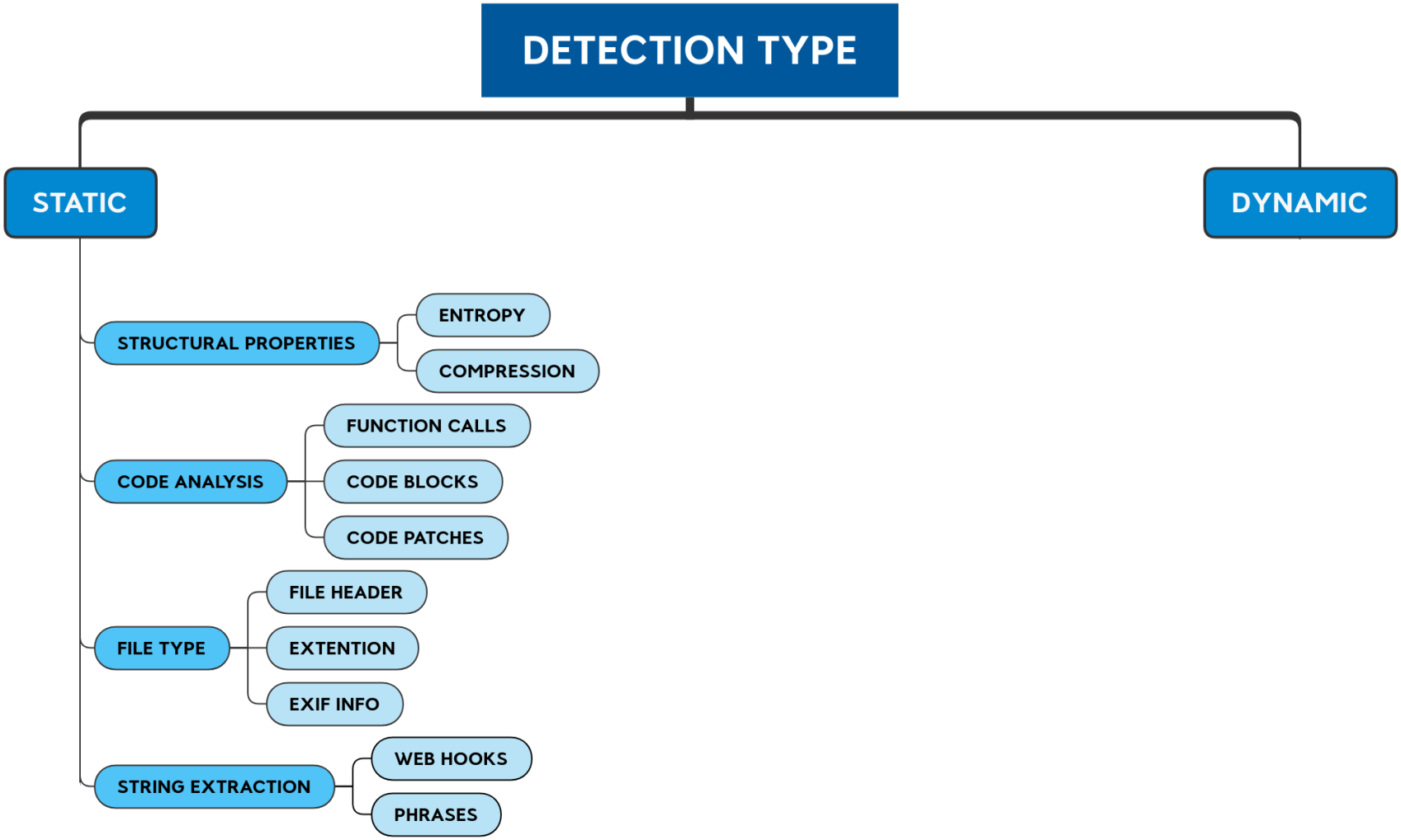
STATIC & DYNAMIC Analysis



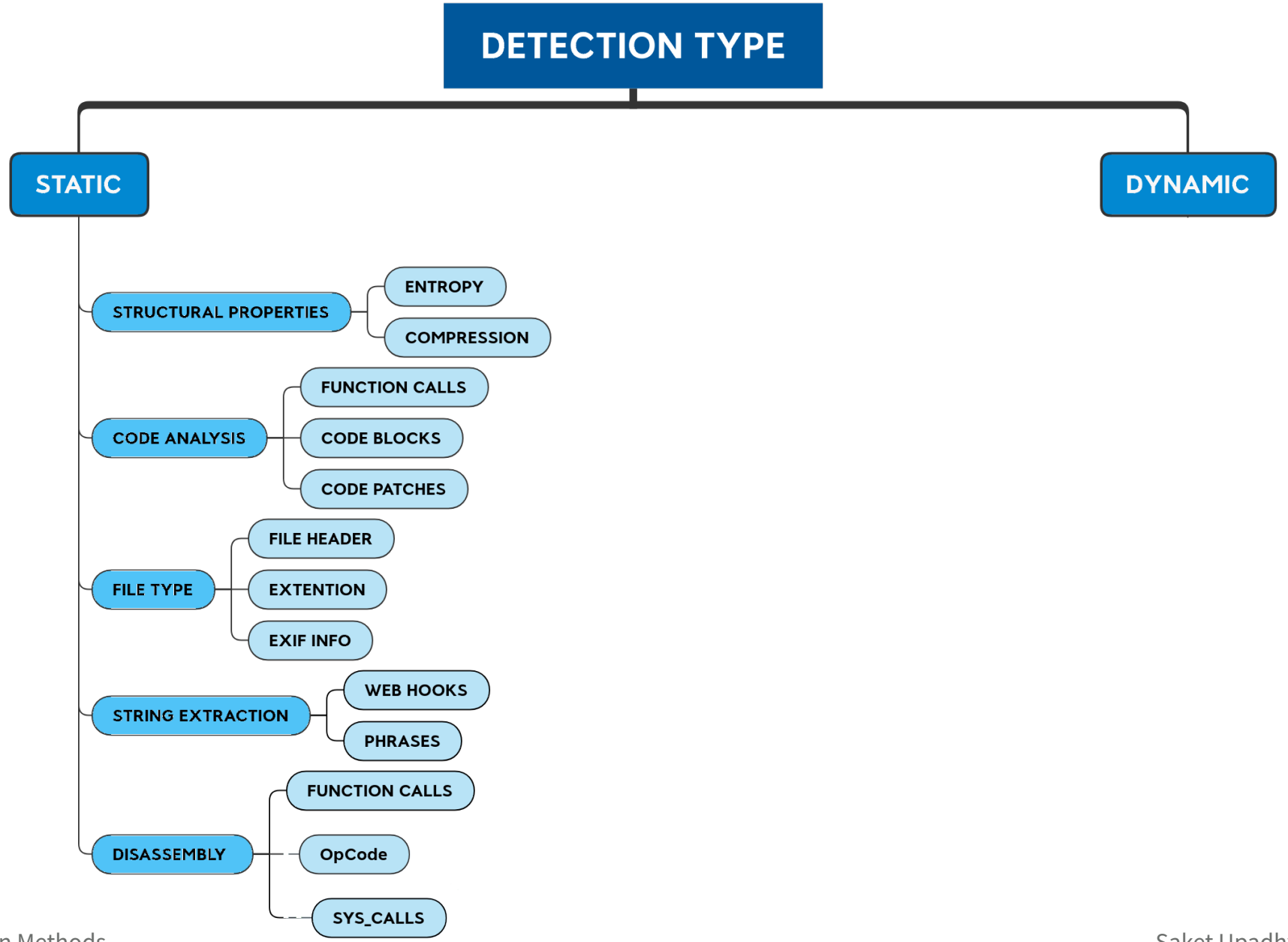
STATIC & DYNAMIC Analysis



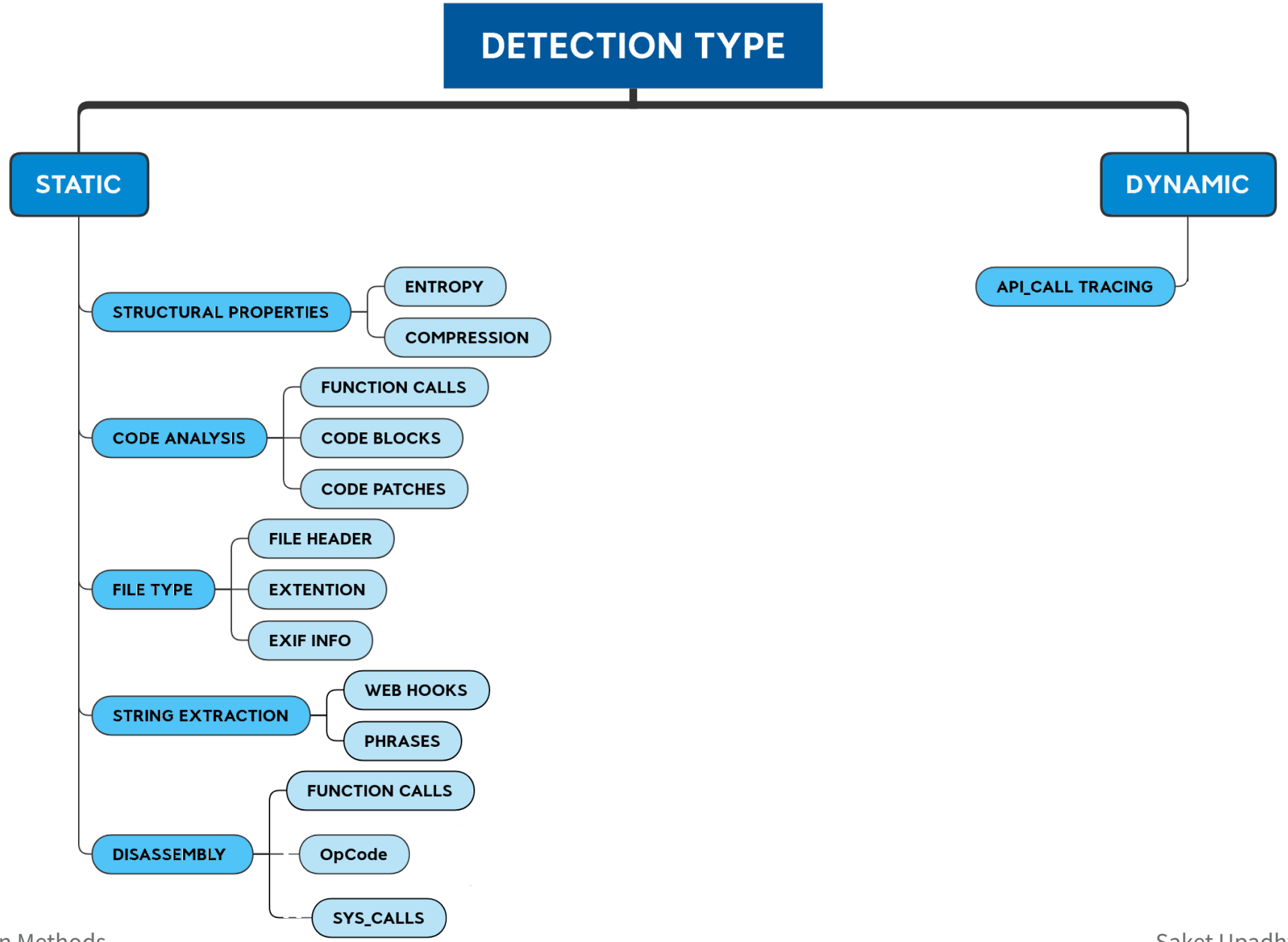
STATIC & DYNAMIC Analysis



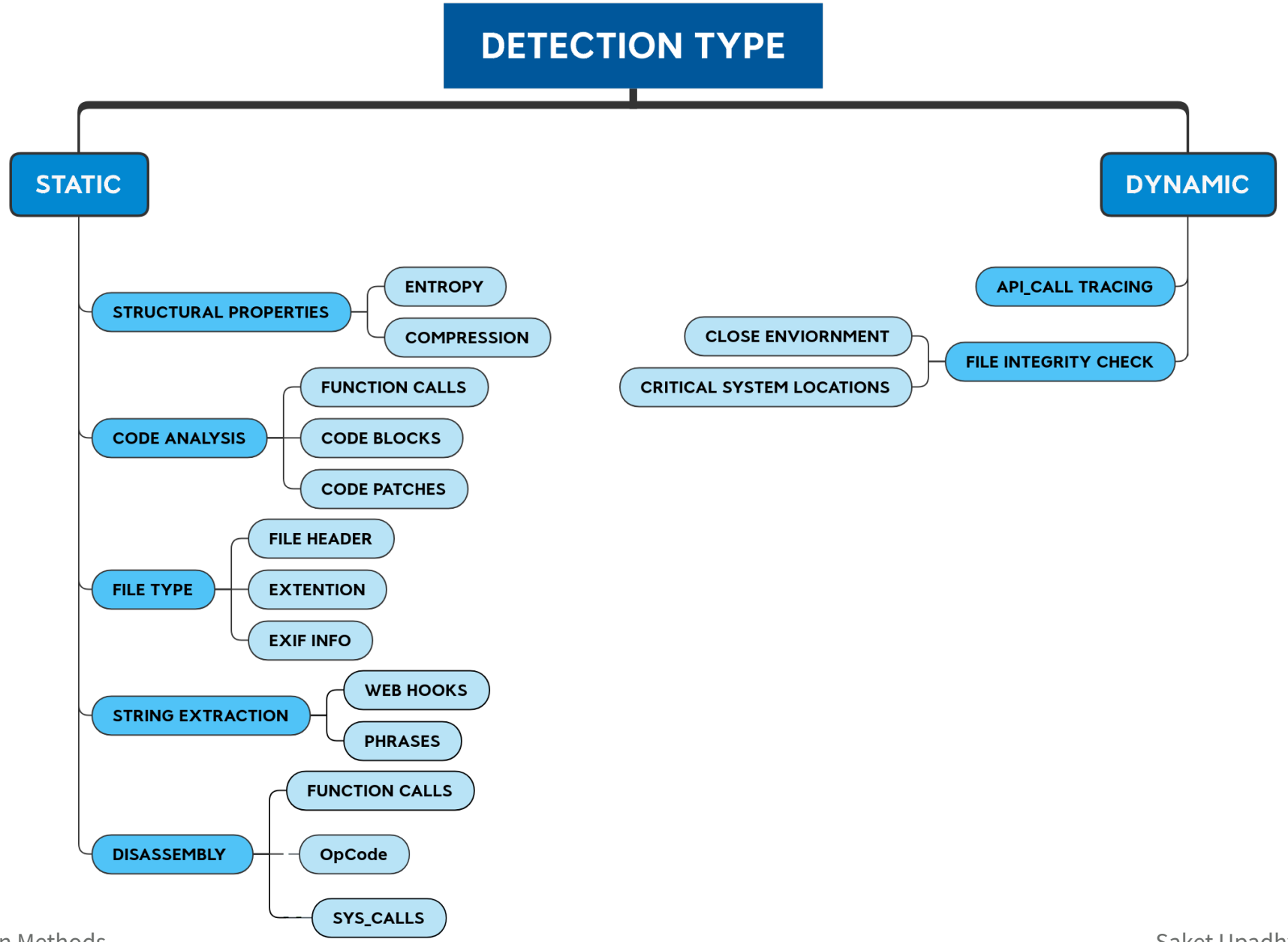
STATIC & DYNAMIC Analysis



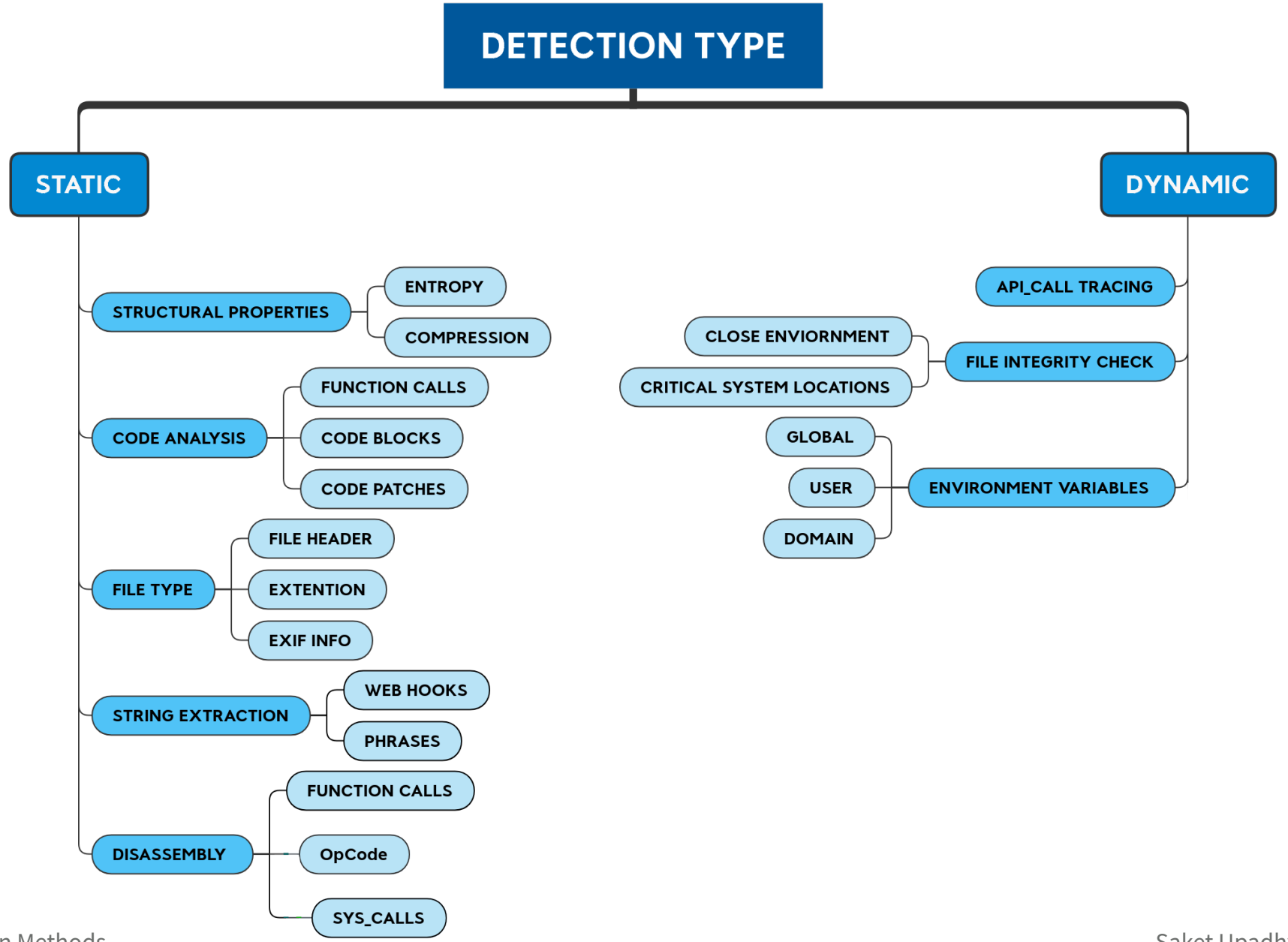
STATIC & DYNAMIC Analysis



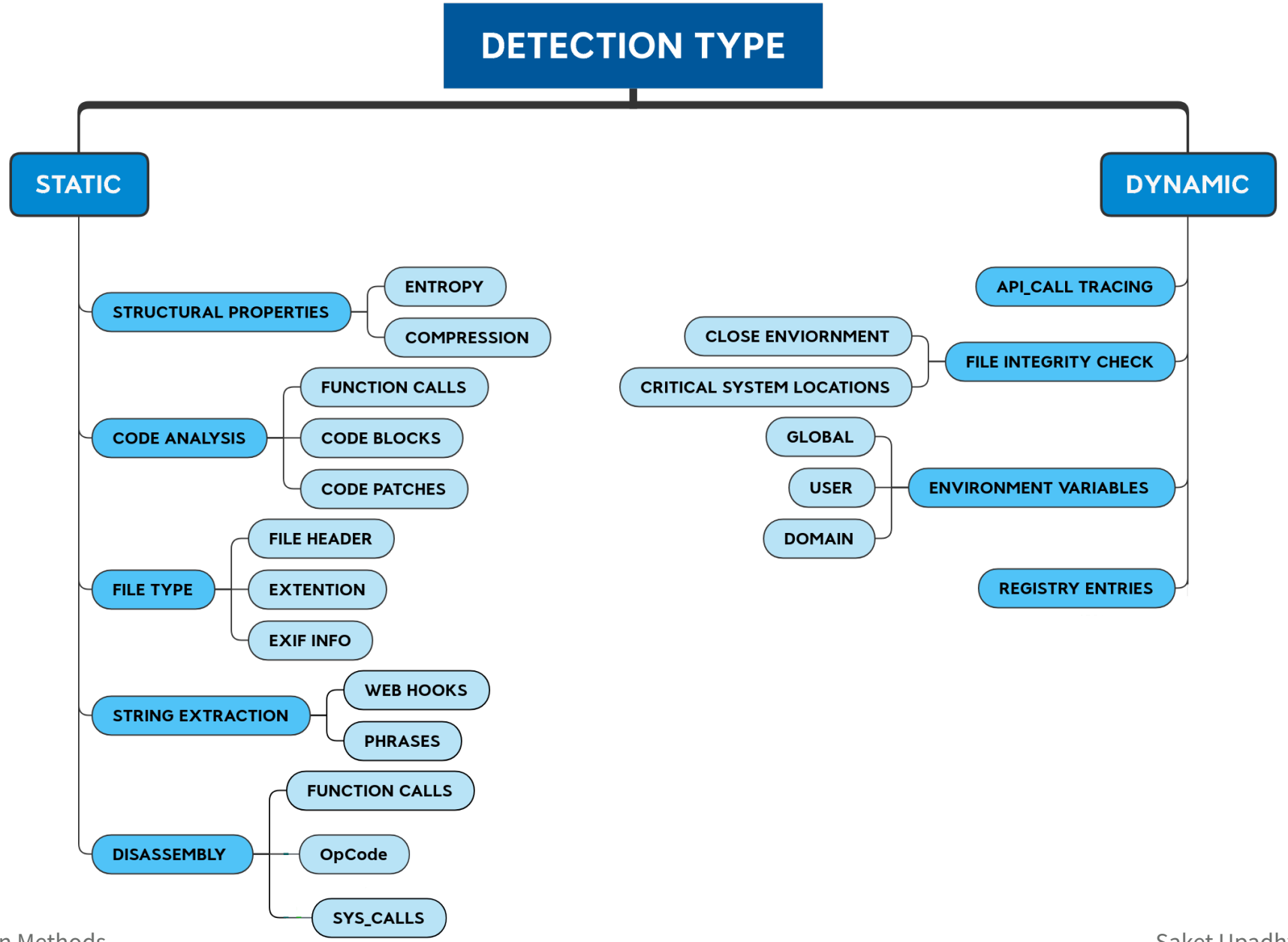
STATIC & DYNAMIC Analysis



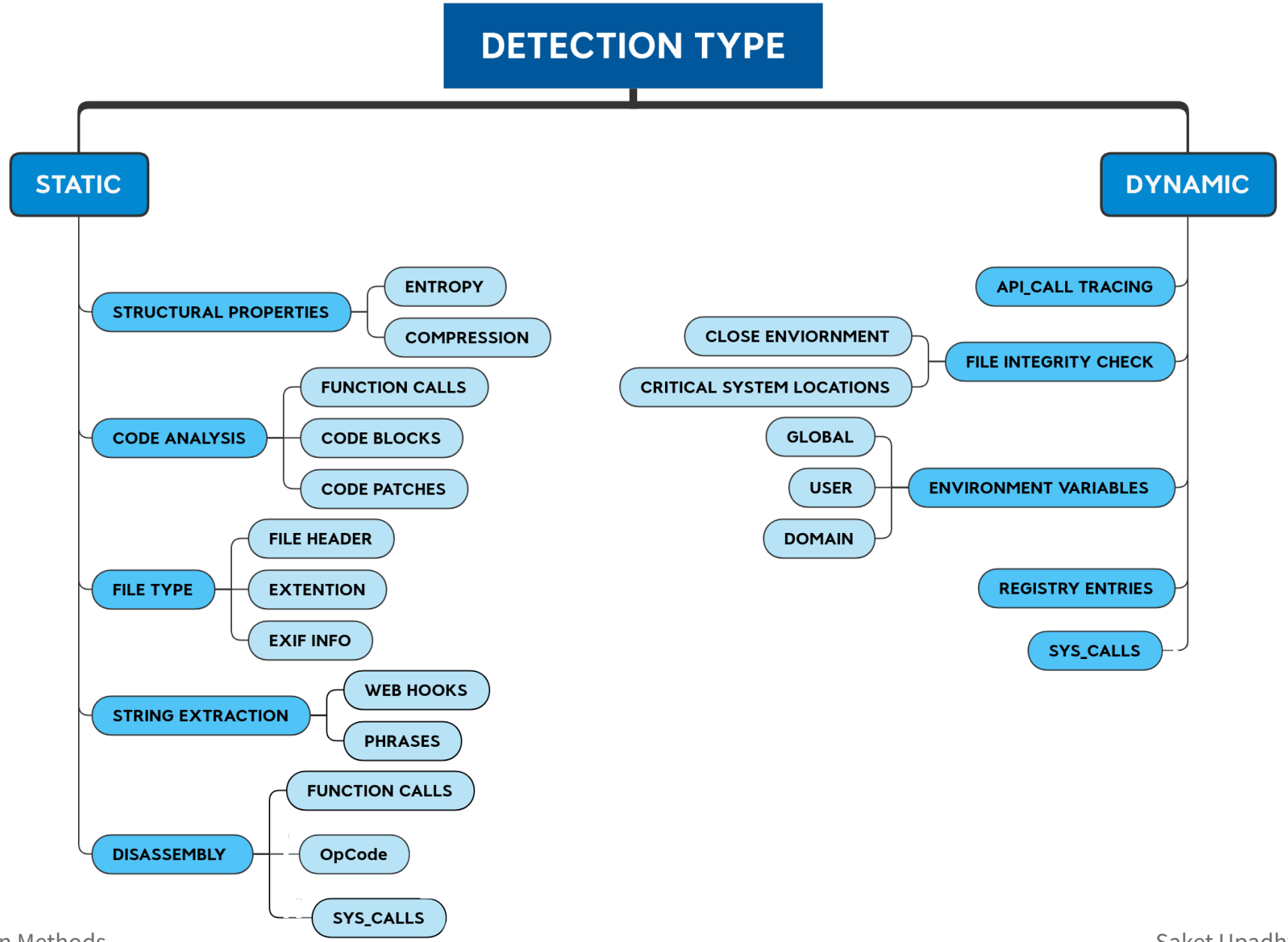
STATIC & DYNAMIC Analysis



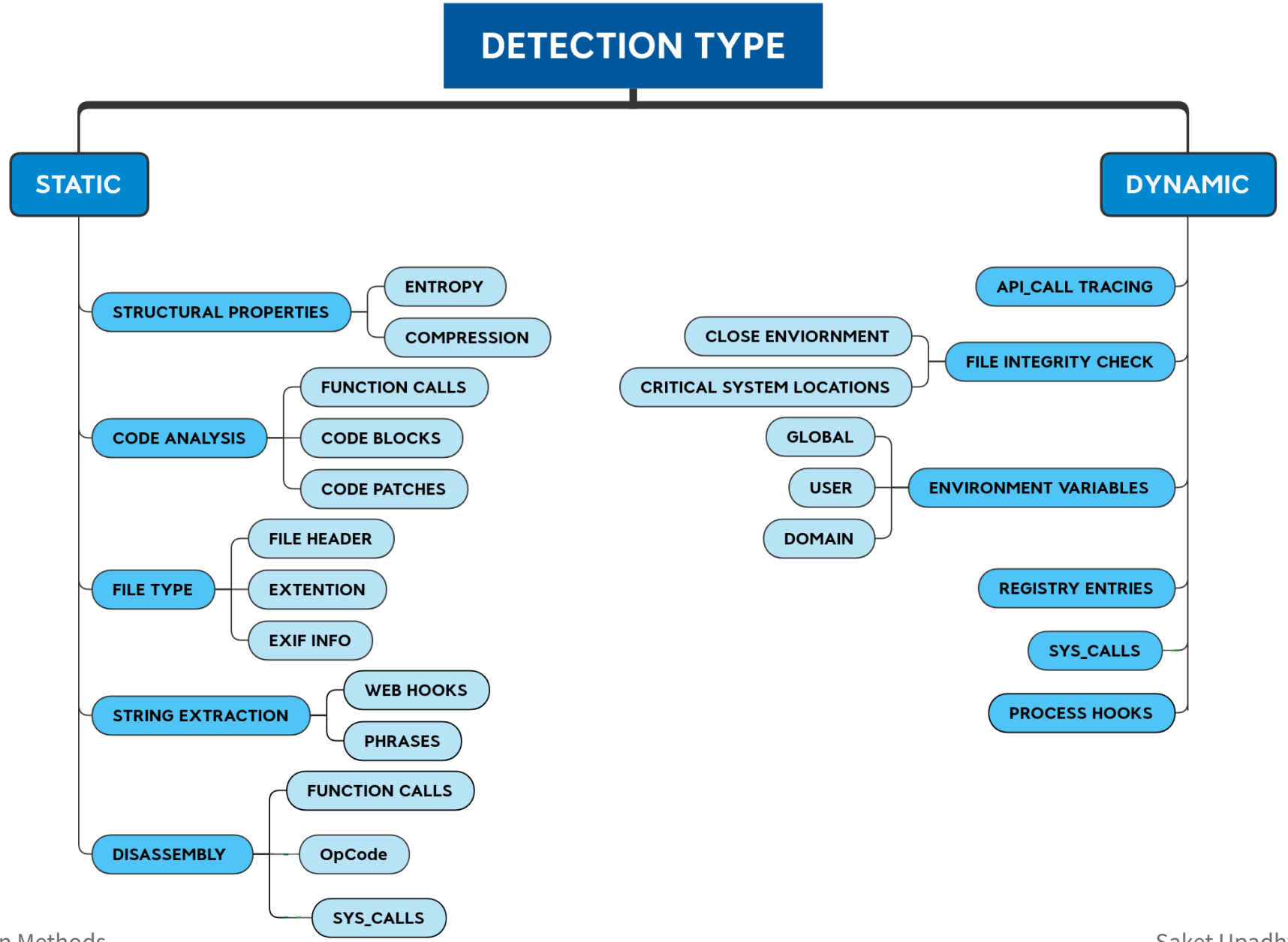
STATIC & DYNAMIC Analysis



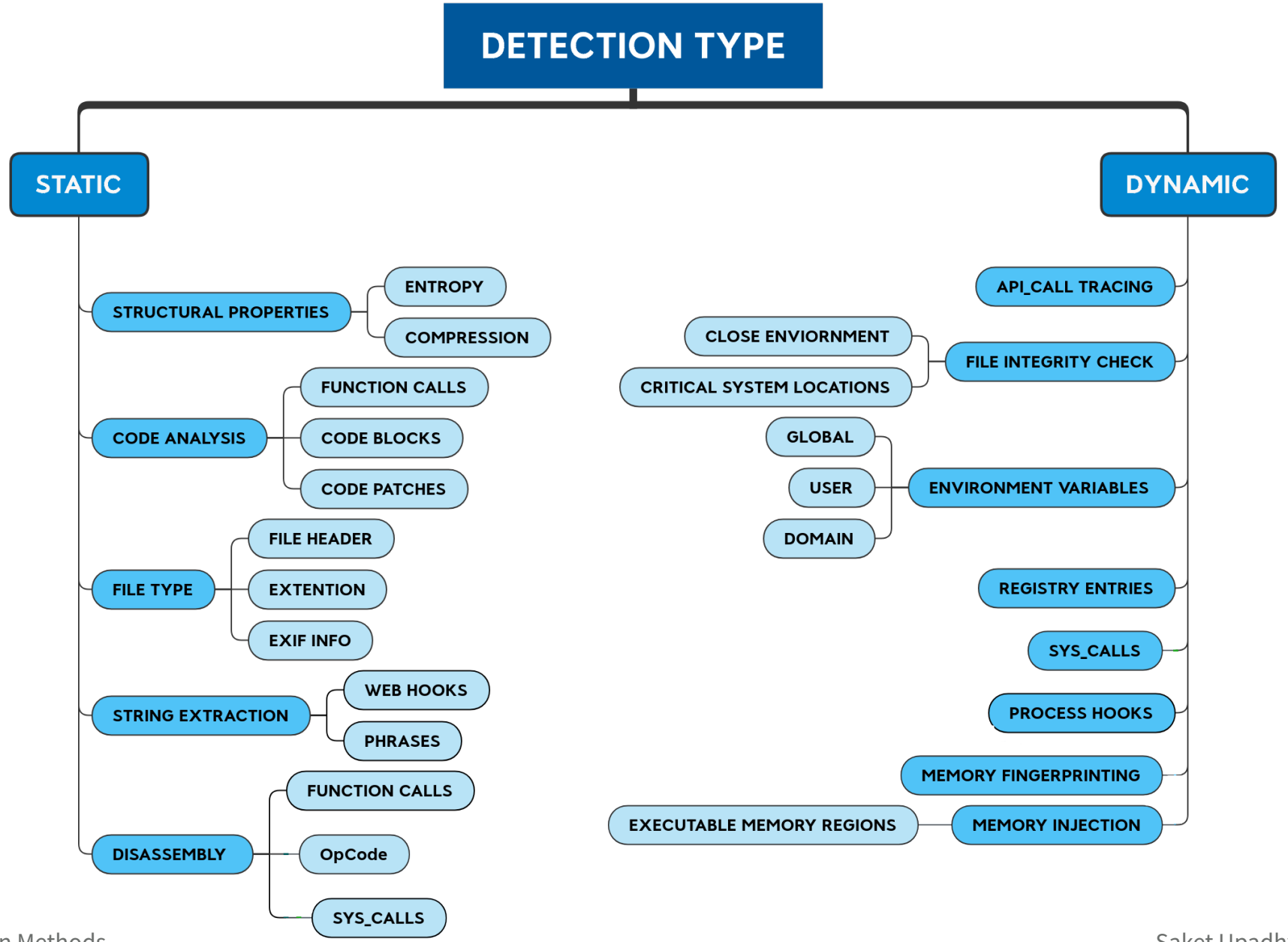
STATIC & DYNAMIC Analysis



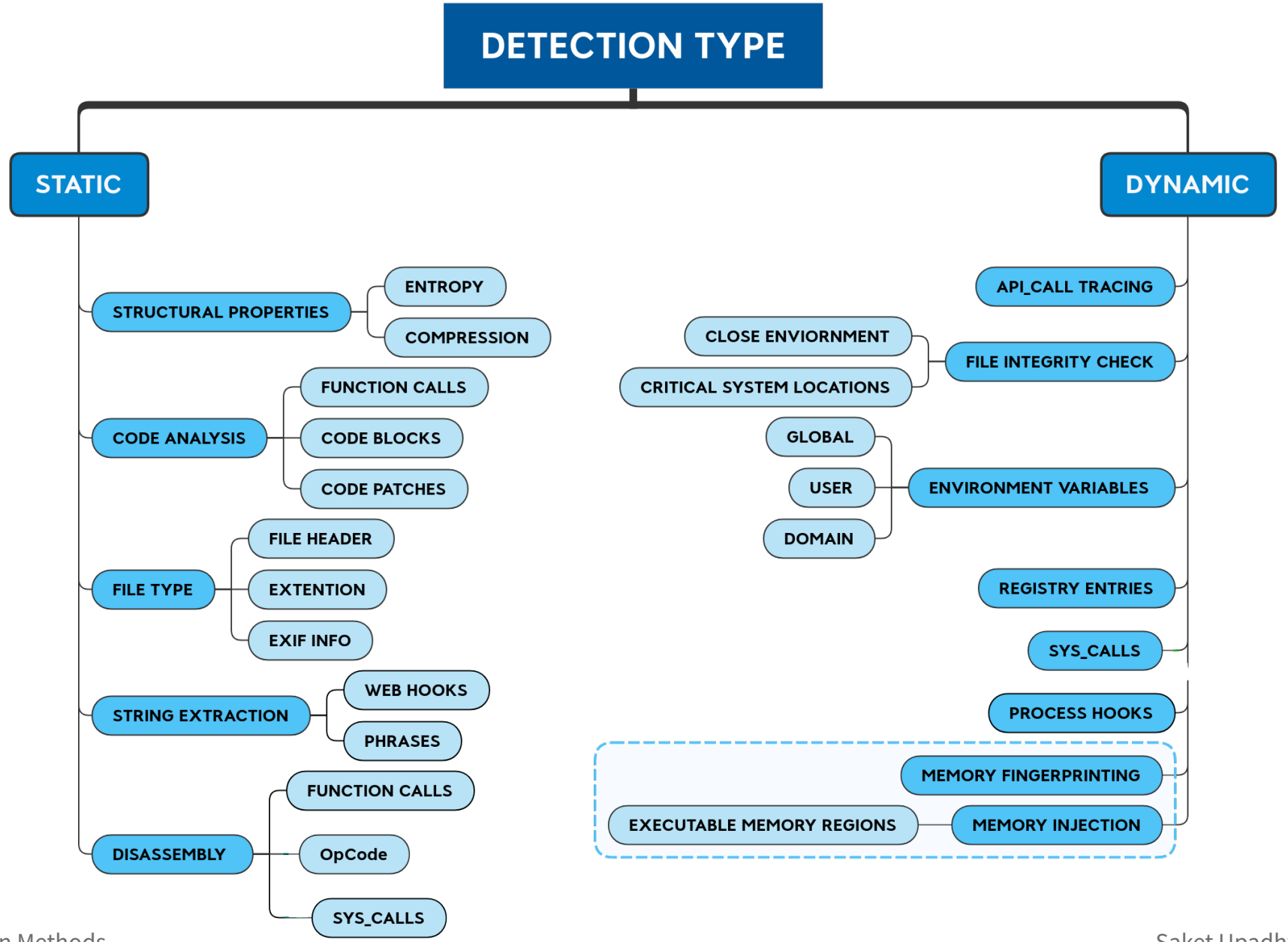
STATIC & DYNAMIC Analysis



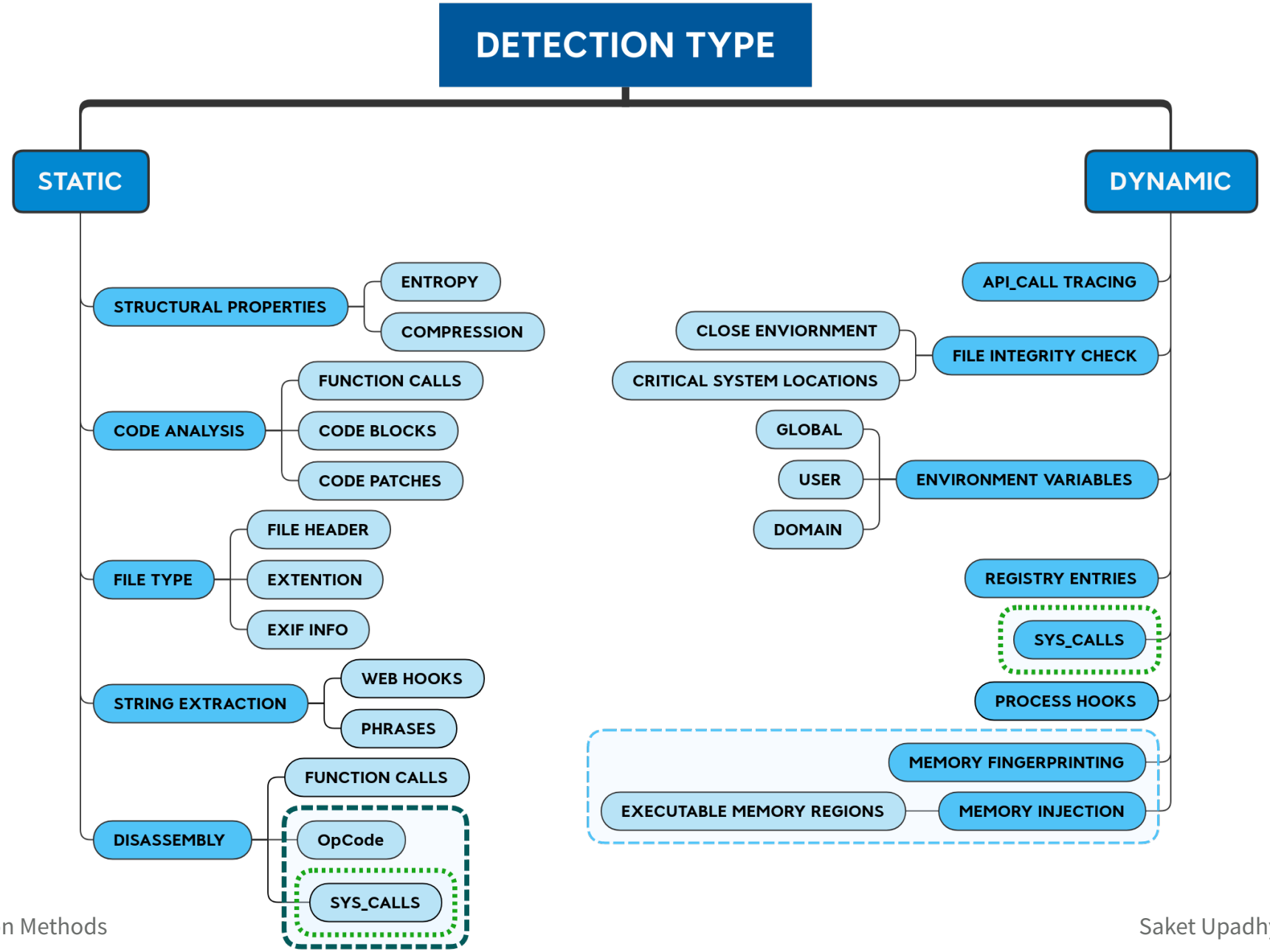
STATIC & DYNAMIC Analysis



STATIC & DYNAMIC Analysis



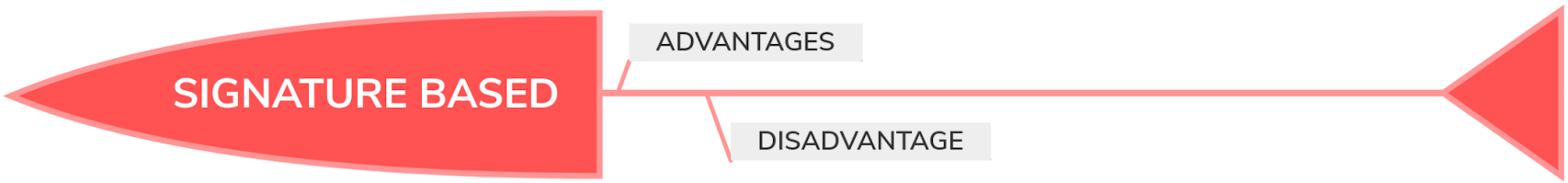
STATIC & DYNAMIC Analysis



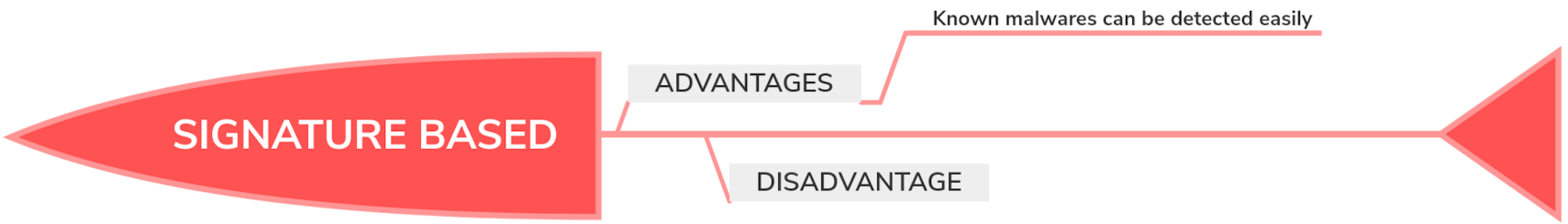
Advantages & Disadvantages

Advantages & Disadvantages

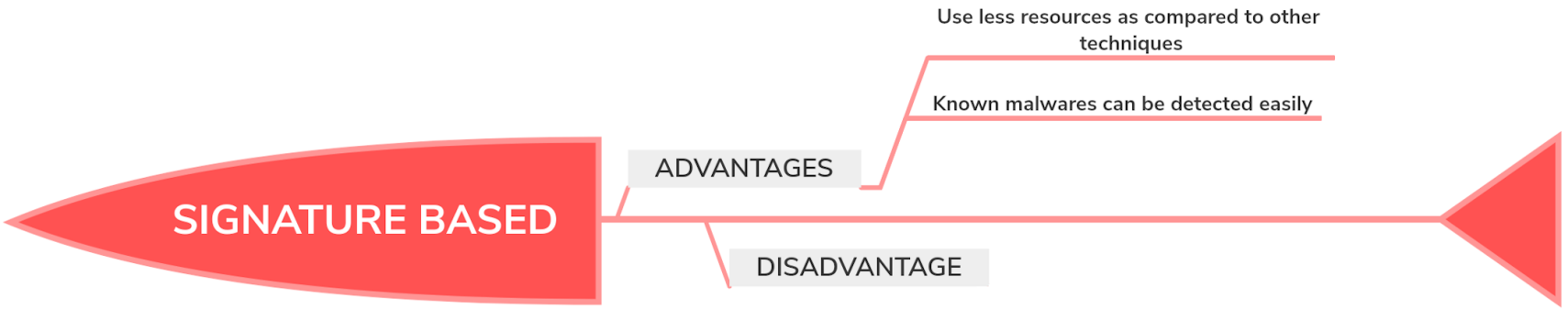
Advantages & Disadvantages



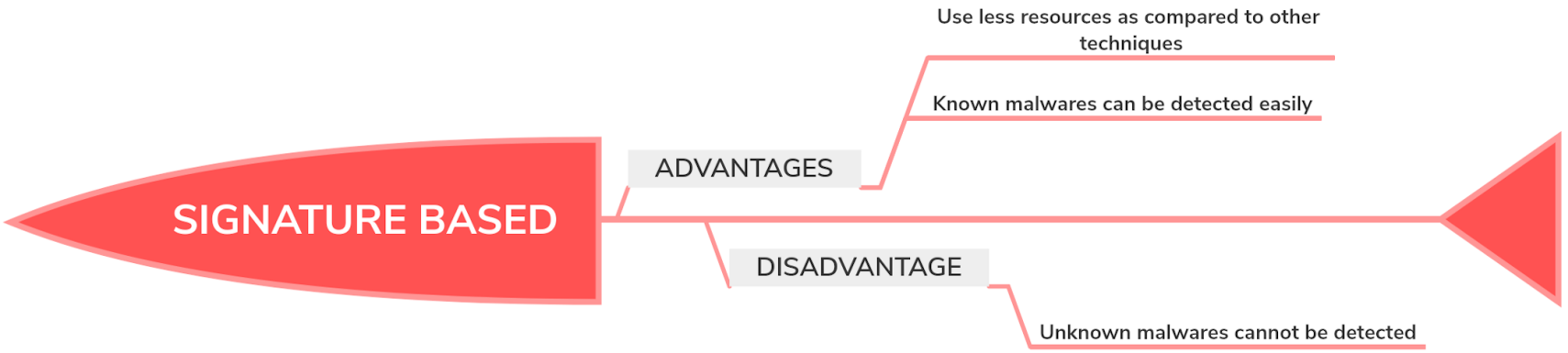
Advantages & Disadvantages



Advantages & Disadvantages



Advantages & Disadvantages

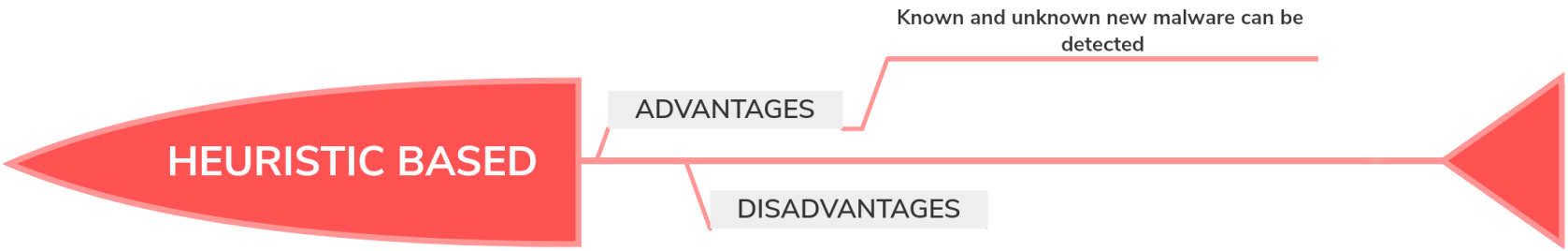


Advantages & Disadvantages

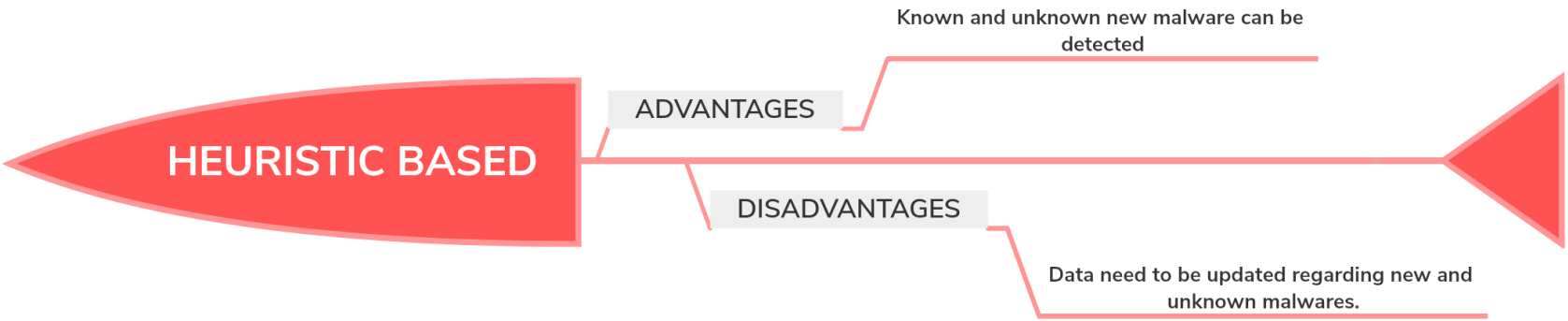
Advantages & Disadvantages

Advantages & Disadvantages

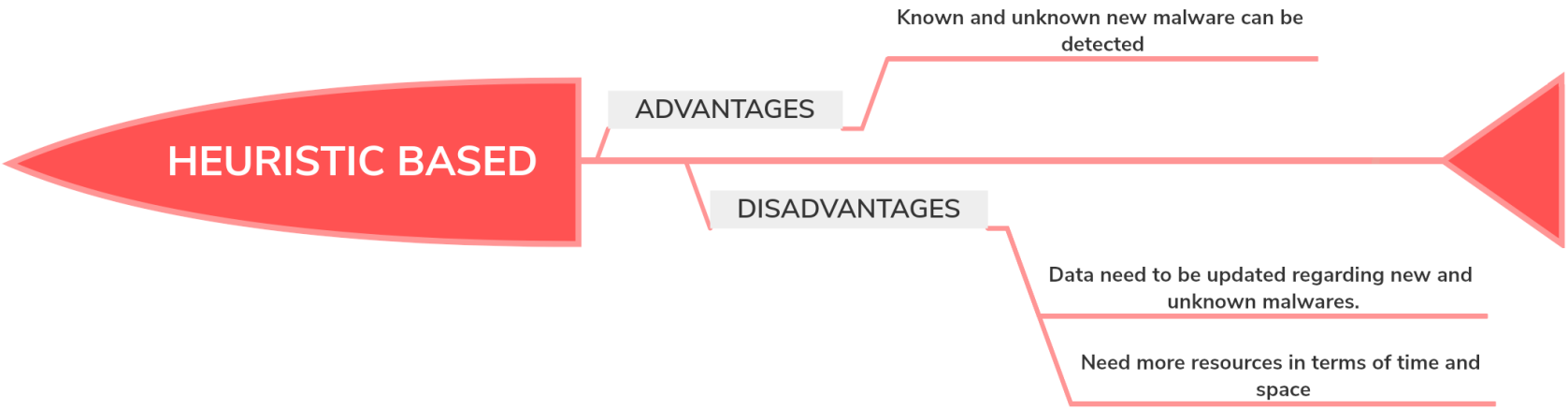
Advantages & Disadvantages



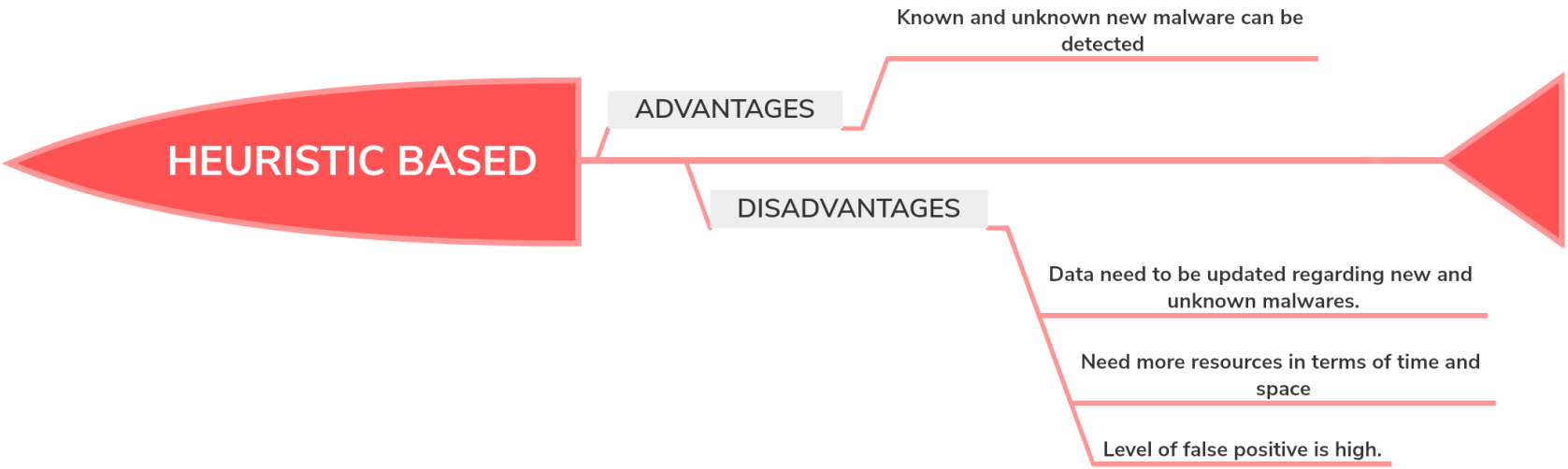
Advantages & Disadvantages



Advantages & Disadvantages



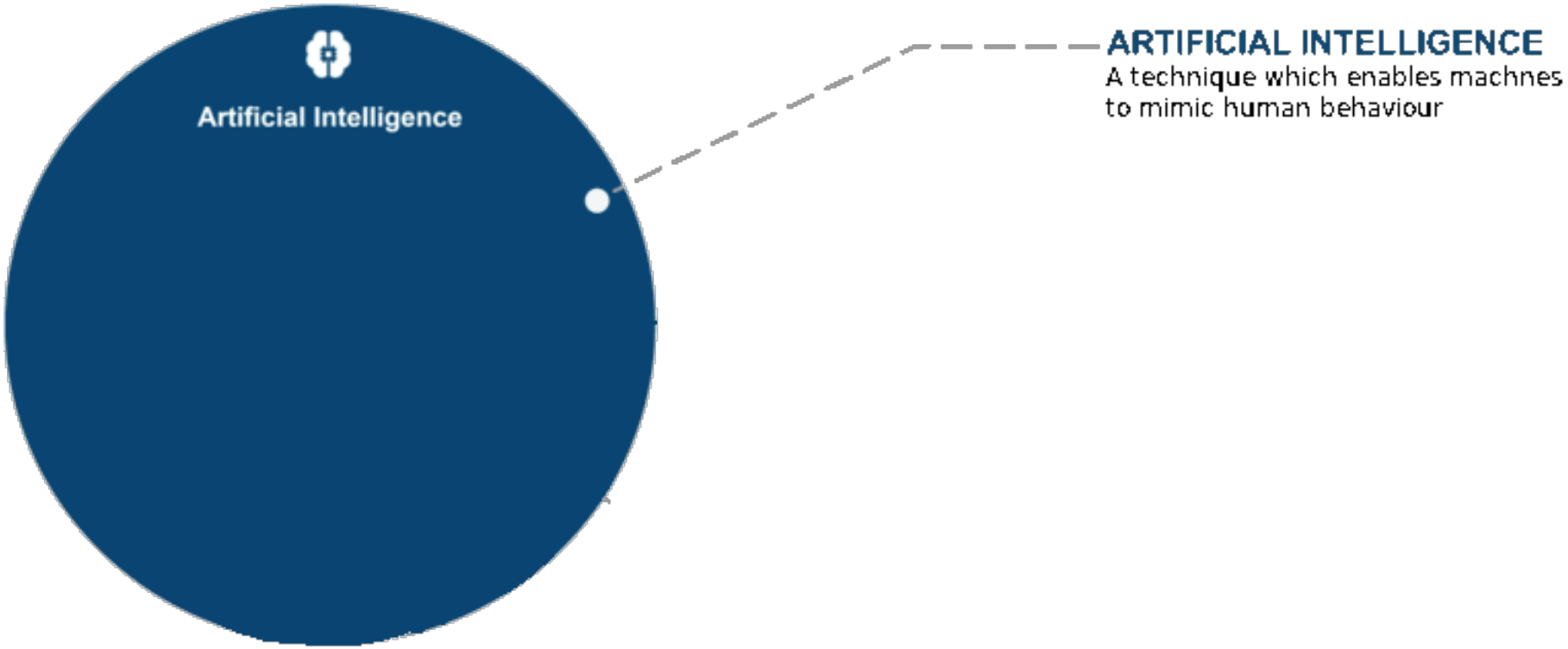
Advantages & Disadvantages



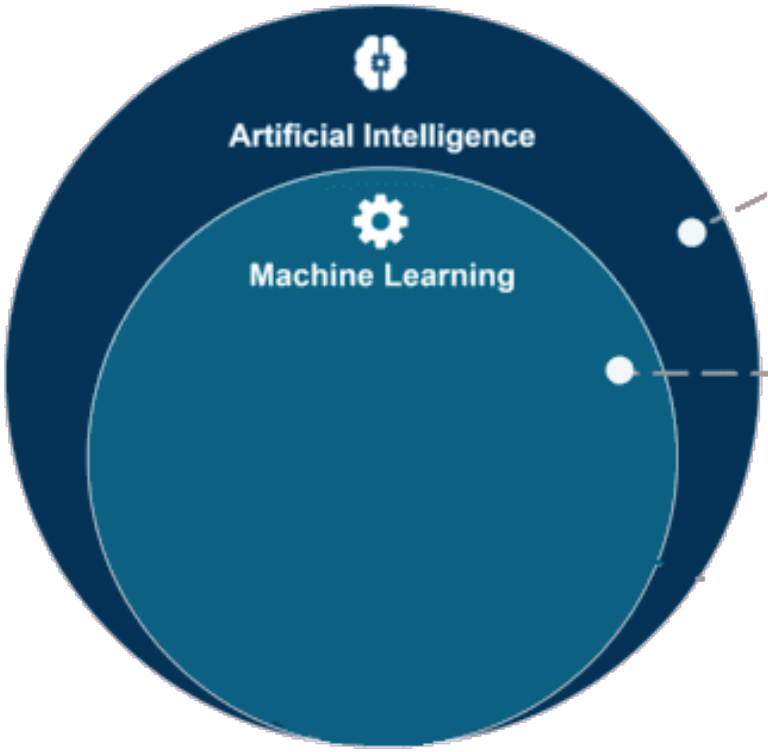
Basic Idea of Machine Learning in detection

Saket Upadhyay

Artificial Intelligence



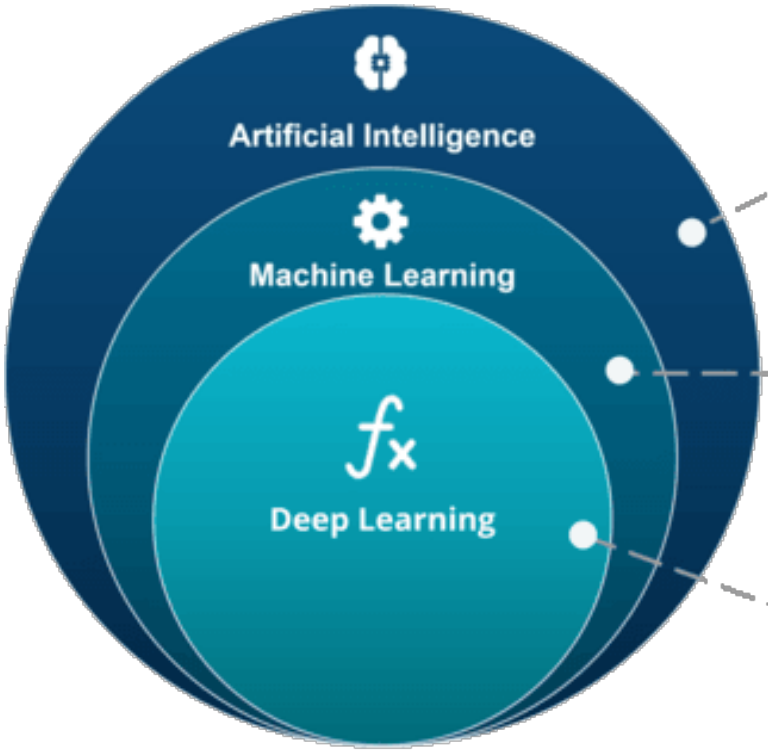
Artificial Intelligence



ARTIFICIAL INTELLIGENCE
A technique which enables machnes to mimic human behaviour

MACHINE LEARNING
A subset of AI technique which use statistical methods to enable machines to improve with experience

Artificial Intelligence



ARTIFICIAL INTELLIGENCE
A technique which enables machnes to mimic human behaviour

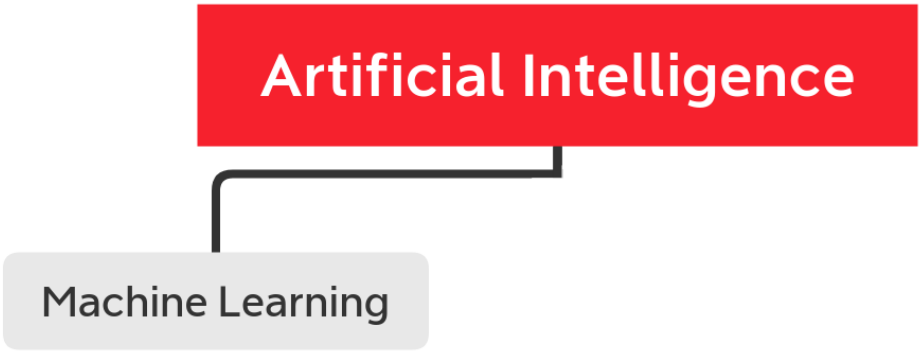
MACHINE LEARNING
A subset of AI technique which use statistical methods to enable machines to improve with experience

DEEP LEARNING
A subset of ML which make the computation of multi-layer neural network feasible

What we will talk about ?

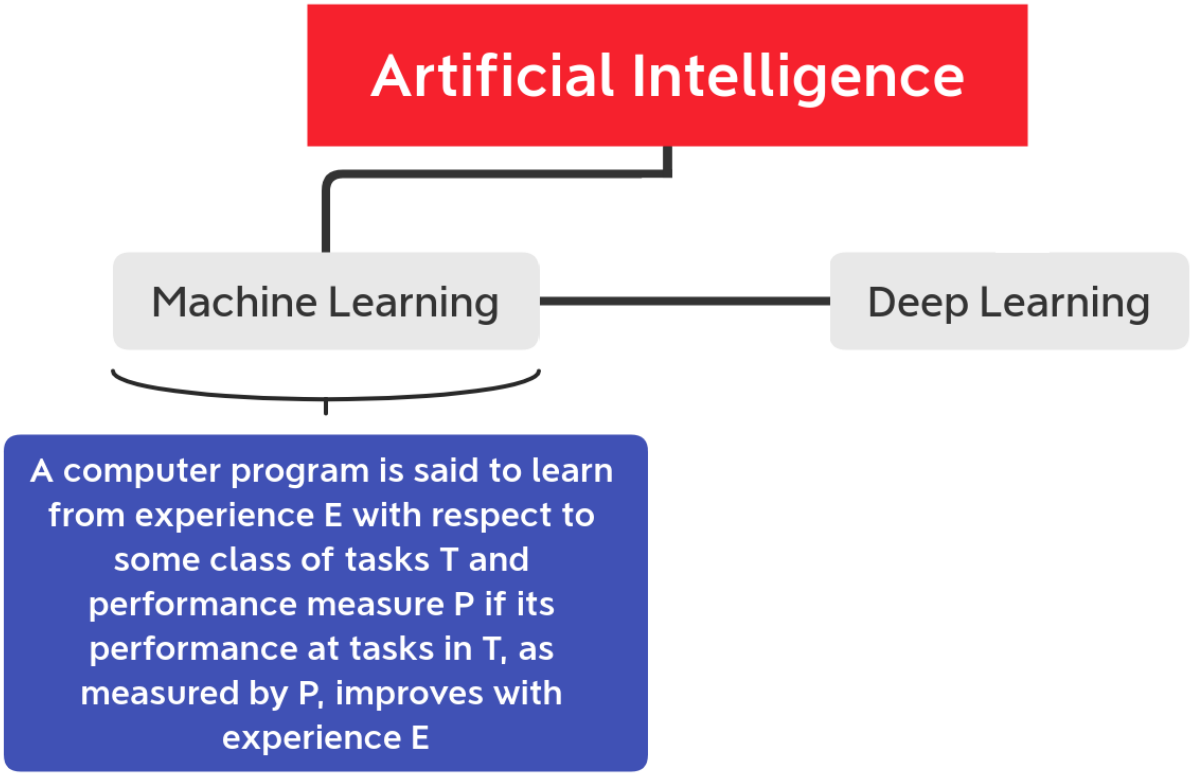
Artificial Intelligence

What we will talk about ?

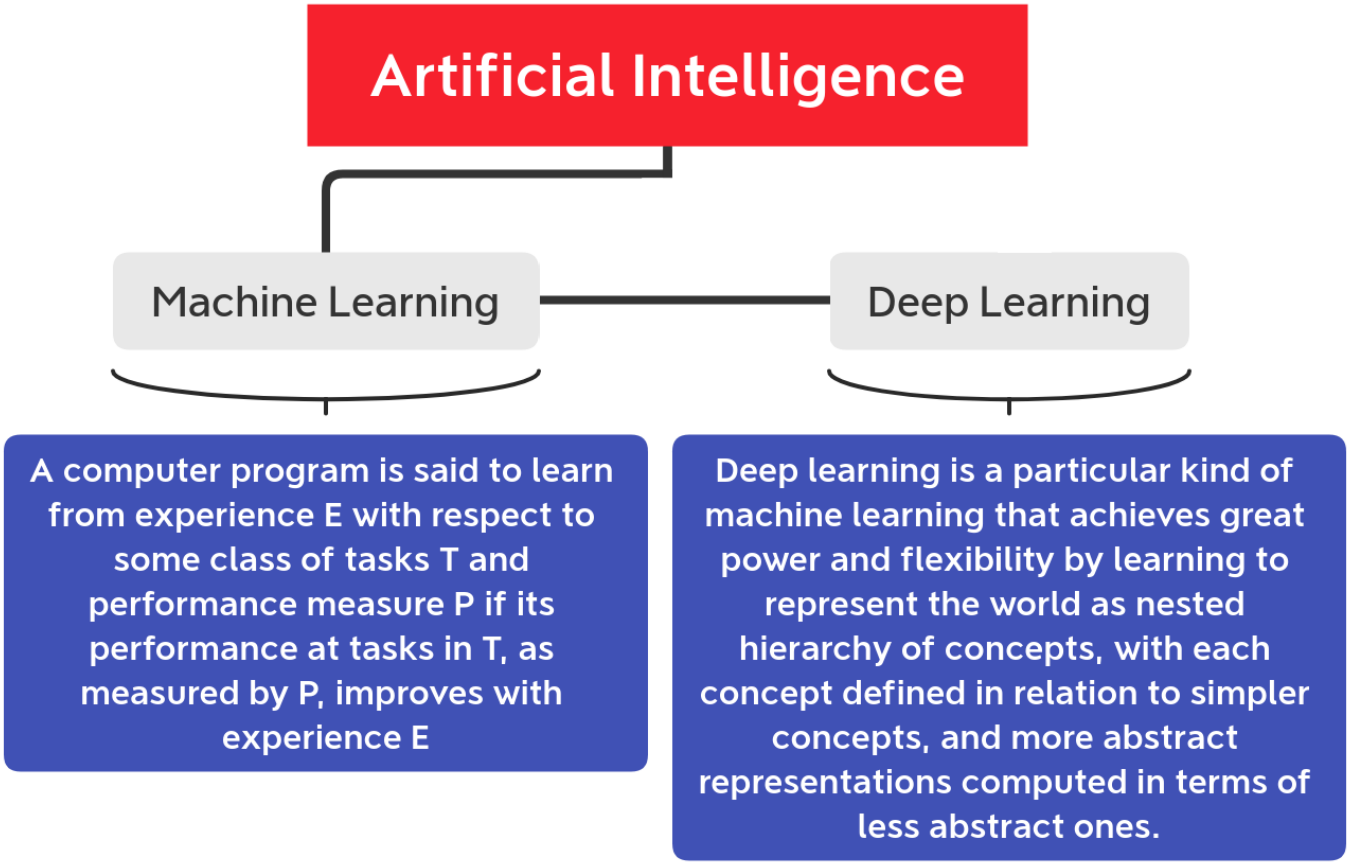


What we will talk about ?

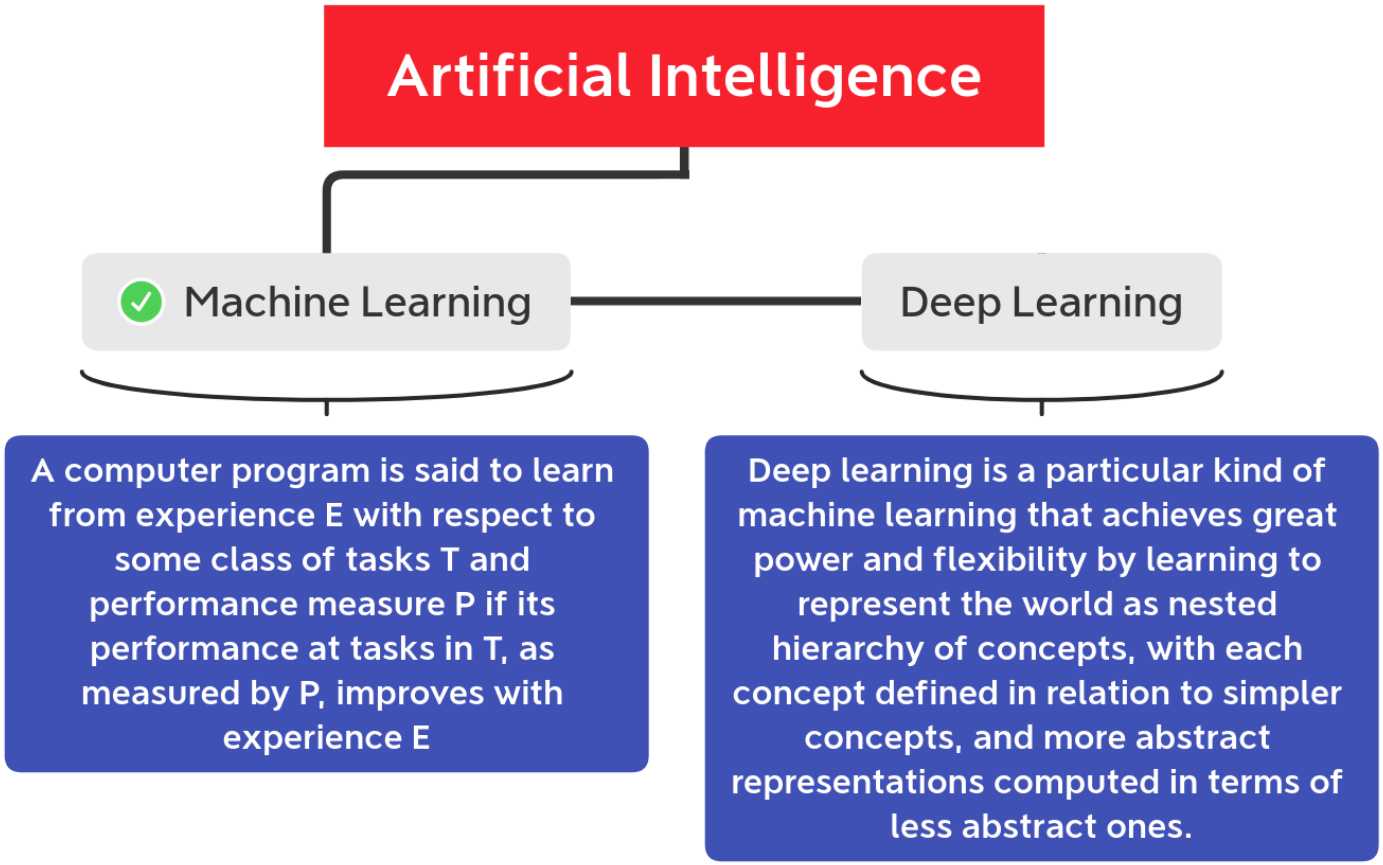
What we will talk about ?



What we will talk about ?



What we will talk about ?



Use of ML and DL

Scenario 1:
We have to build a survilance system which will scan the faceses of people and raise an alarm if not recogonised.

Use of ML and DL

Scenario 1:
We have to build a survilance system which will scan the faceses of people and raise an alarm if not recogonised.

Scenario 2:
Given a bank's transaction details and credit transfers history we have to detect fraud transactions.

Use of ML and DL

Scenario 1:
We have to build a survilance system which will scan the faceses of people and raise an alarm if not recogonised. **[DEEP LEARNING]**

Scenario 2:
Given a bank's transaction details and credit transfers history we have to detect fraud transactions. **[MACHINE LEARNING]**

Classification

In machine learning and statistics, classification is the problem of **identifying to which of a set of categories (sub-populations) a new observation belongs**, **on the basis of a training set** of data containing observations (or instances) whose category membership is **known**.

Classification

In machine learning and statistics, classification is the problem of **identifying to which of a set of categories (sub-populations) a new observation belongs**, **on the basis of a training set** of data containing observations (or instances) whose category membership is **known**.

source : wikipedia

Classification Algorithms in ML

Classification Algorithms in ML

- Linear Classifiers: Logistic Regression, Naive Bayes Classifier

Classification Algorithms in ML

- Linear Classifiers: Logistic Regression, Naive Bayes Classifier
- Nearest Neighbor

Classification Algorithms in ML

- Linear Classifiers: Logistic Regression, Naive Bayes Classifier
- Nearest Neighbor
- Support Vector Machines

Classification Algorithms in ML

- Linear Classifiers: Logistic Regression, Naive Bayes Classifier
- Nearest Neighbor
- Support Vector Machines
- Decision Trees

Classification Algorithms in ML

- Linear Classifiers: Logistic Regression, Naive Bayes Classifier
- Nearest Neighbor
- Support Vector Machines
- Decision Trees
- Boosted Trees

Classification Algorithms in ML

- Linear Classifiers: Logistic Regression, Naive Bayes Classifier
- Nearest Neighbor
- Support Vector Machines
- Decision Trees
- Boosted Trees
- Random Forest

Classification Algorithms in ML

- Linear Classifiers: Logistic Regression, Naive Bayes Classifier
- Nearest Neighbor
- Support Vector Machines
- Decision Trees
- Boosted Trees
- Random Forest
- Neural Networks

Visualisation of SVM

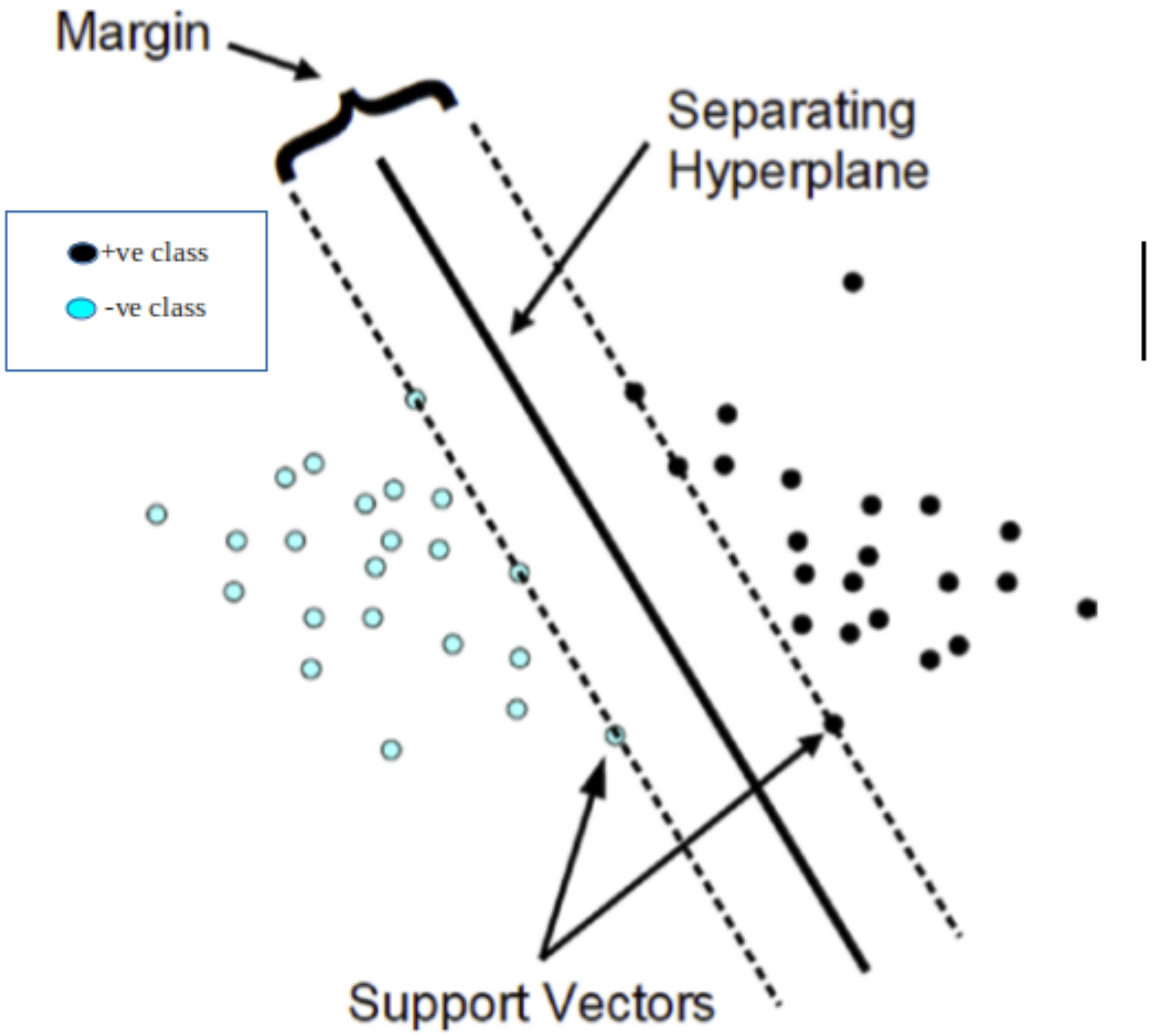


Fig 1:SVM Visualisation

Visualisation of KNN

Fig 2:KNN Visualisation

Steps to follow ...

1. Collect Samples of malware and benign applications

Steps to follow ...

1. Collect Samples of malware and benign applications
2. Feature engineering

Steps to follow ...

1. Collect Samples of malware and benign applications
2. Feature engineering
3. Training and testing

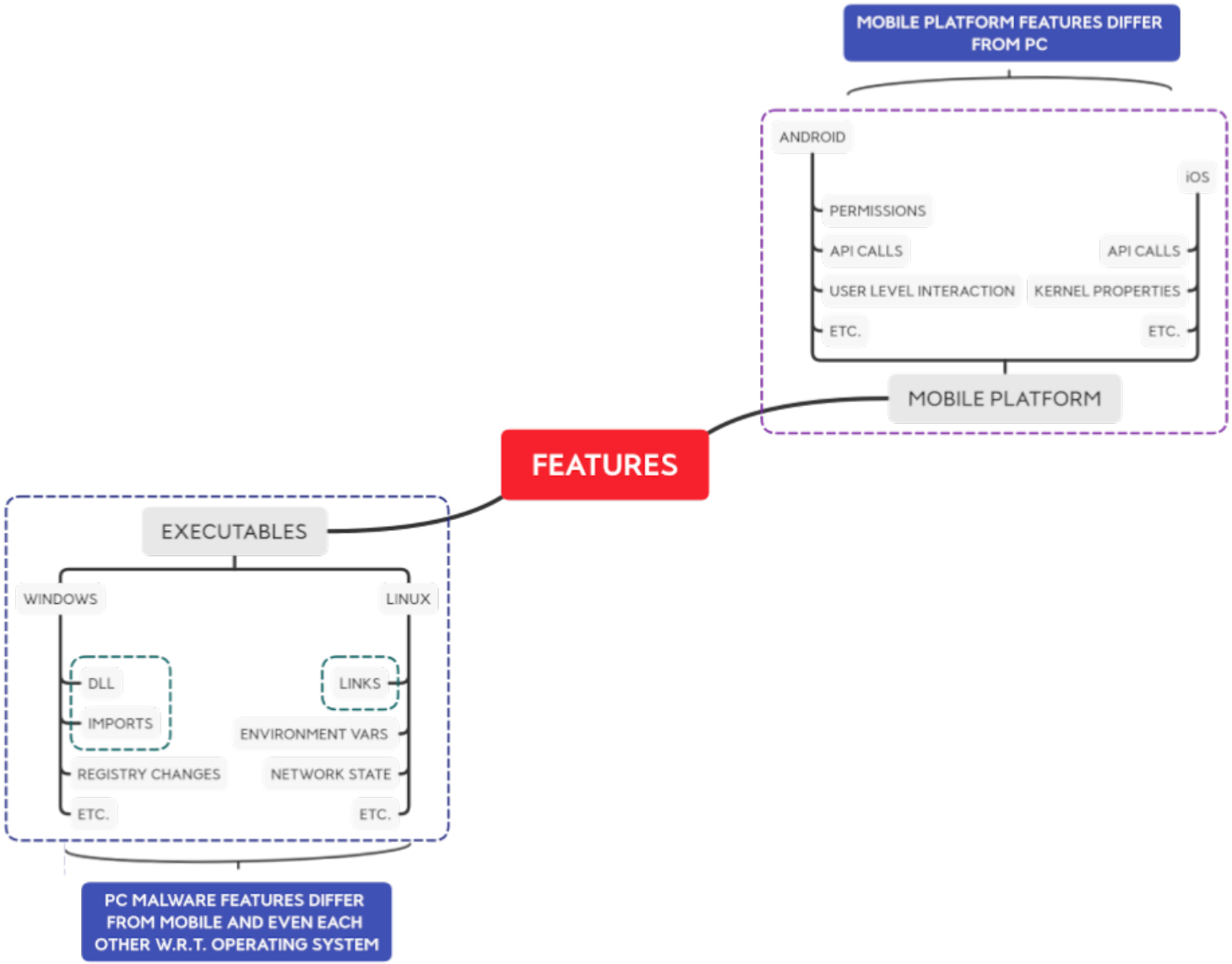
Steps to follow ...

1. Collect Samples of malware and benign applications
2. Feature engineering
3. Training and testing
4. Deployment

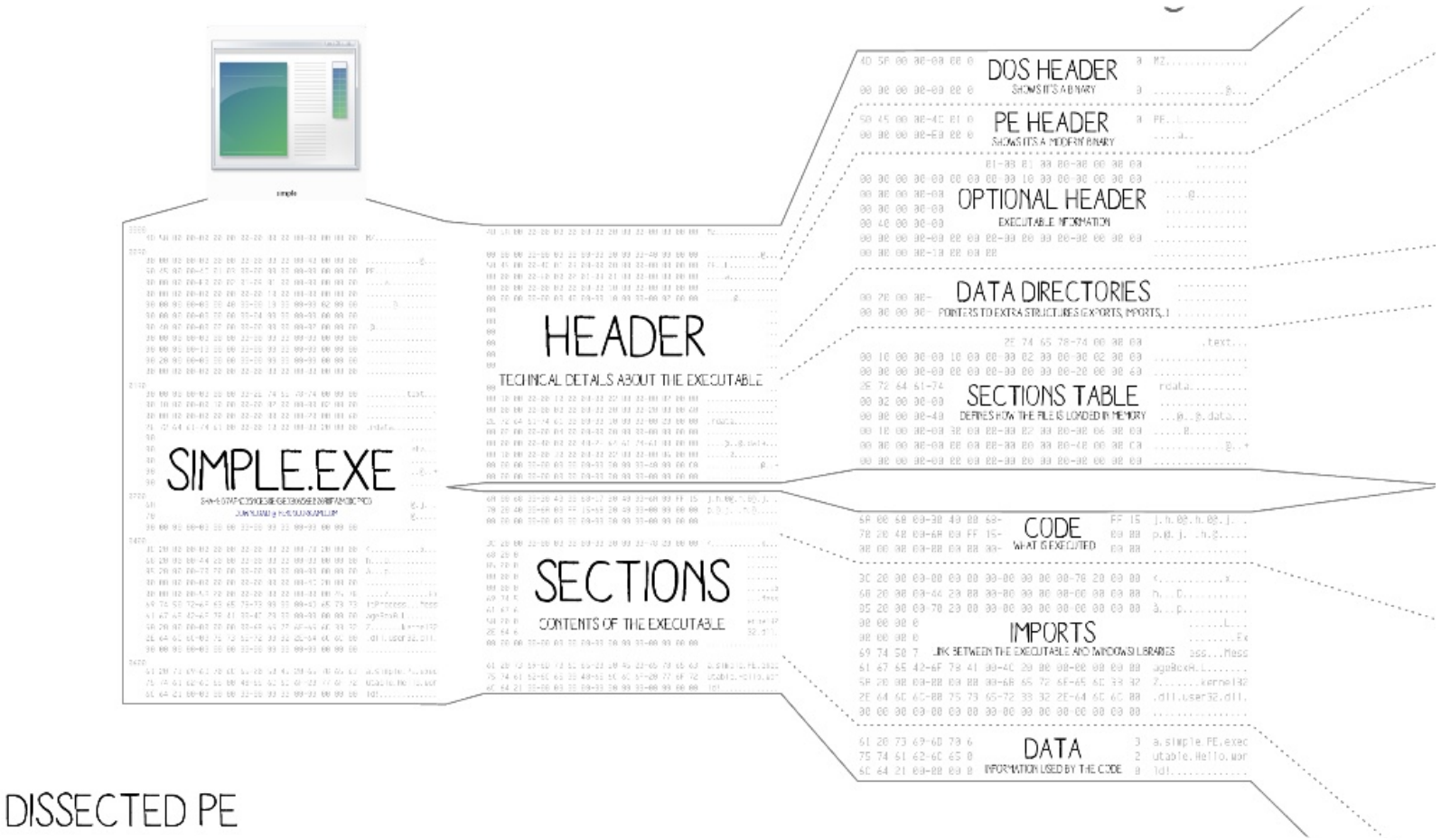
Feature Extraction of Malware Samples

Saket Upadhyay

What we should look for in malware?



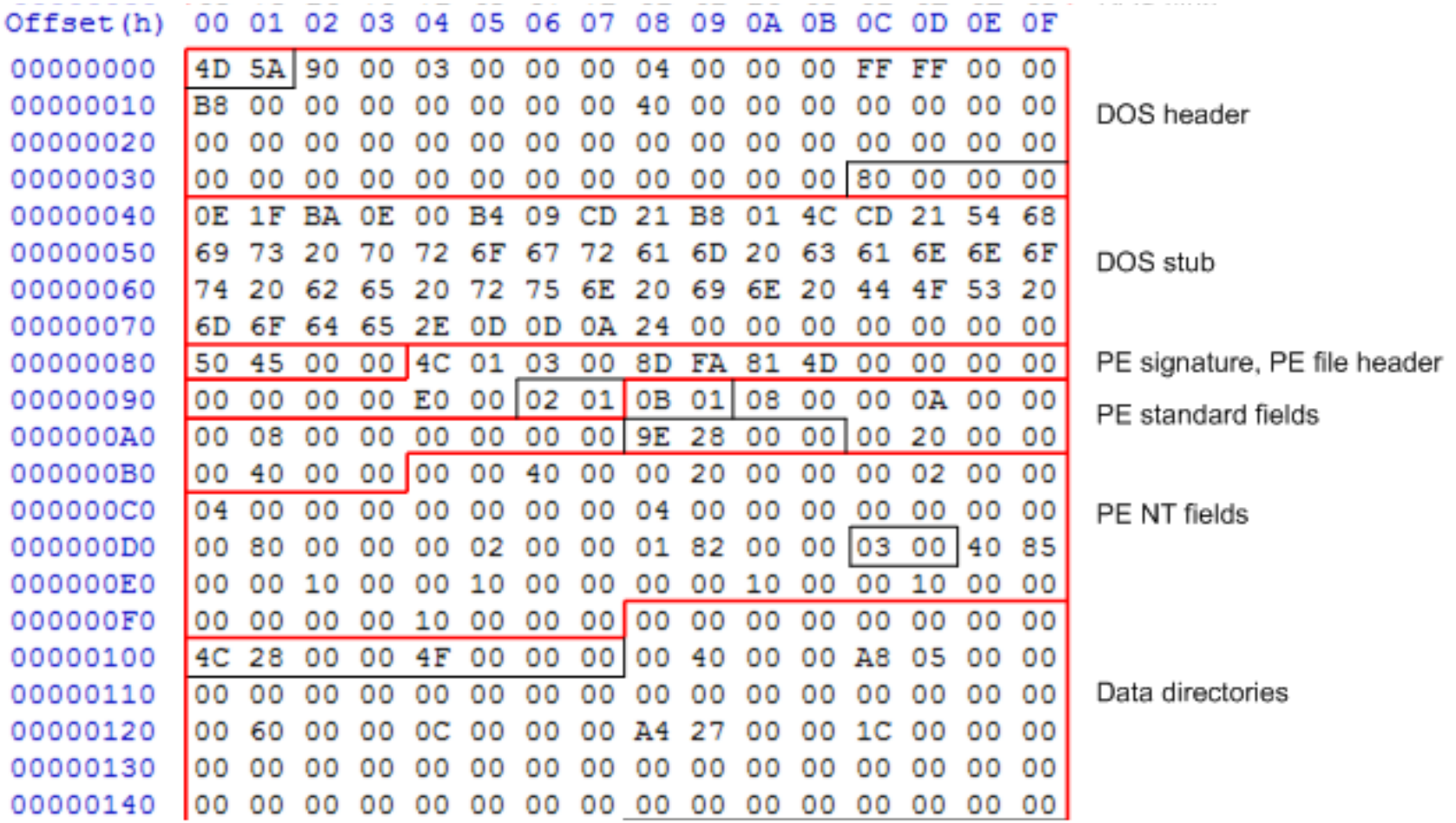
PE File Format



DISSECTED PE

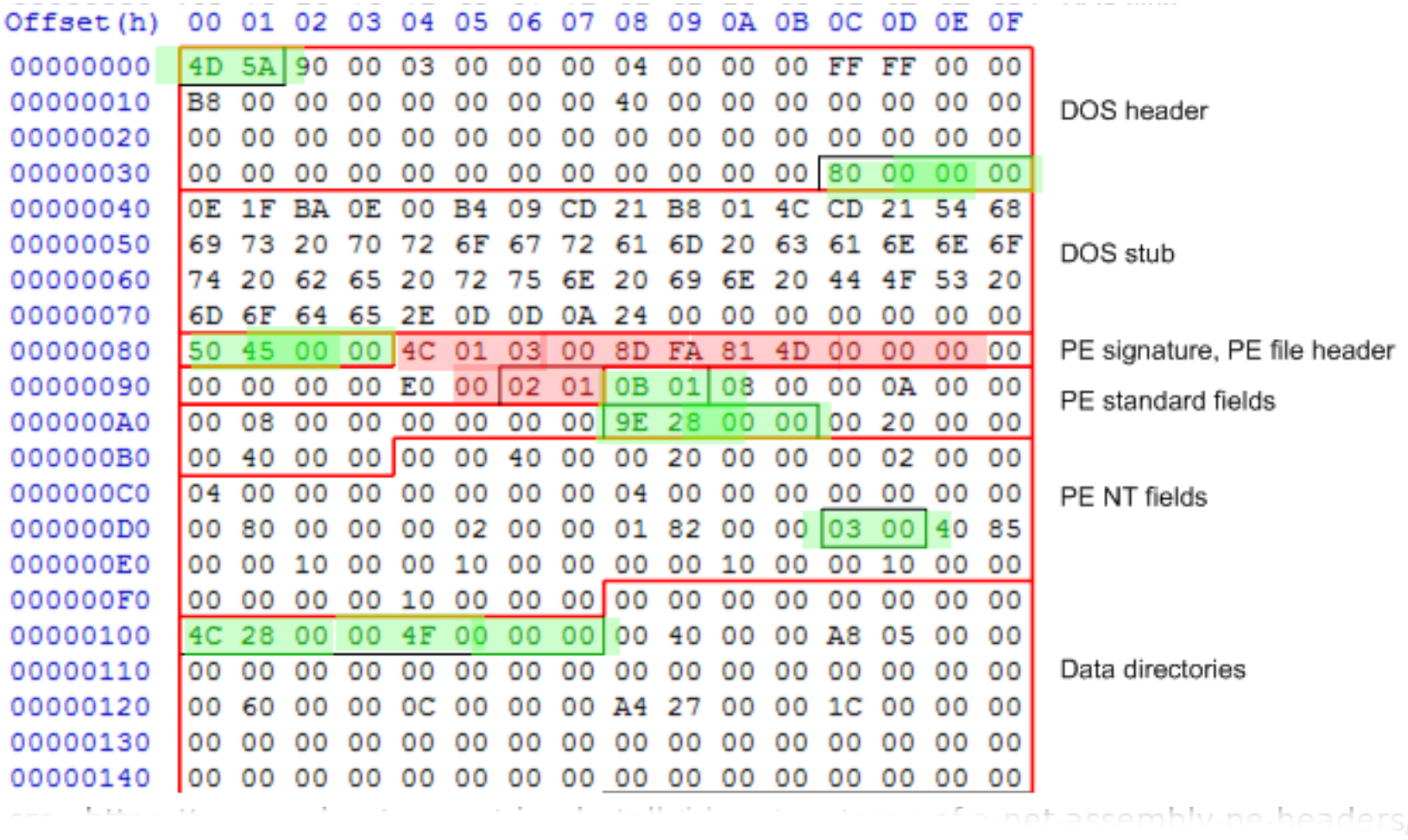
src : https://www.slideshare.net/ange4771/44con2013-workshop-exploring-the-portable-executable-format

PE File Format



src : https://www.red-gate.com/simple-talk/blogs/anatomy-of-a-net-assembly-pe-headers/

PE File Format



How we can store the features?

Now we know how and what to extract,

How we can store the features?

Now we know how and what to extract,

BUT

we need a well defined structure to store the features so that we can feed them in our ML training step

The Binary Array Approach [1/0]

STEPS

The Binary Array Approach [1/0]

STEPS

1. We create a global set of features

The Binary Array Approach [1/0]

STEPS

1. We create a global set of features
2. Take one sample at a time

The Binary Array Approach [1/0]

STEPS

1. We create a global set of features
2. Take one sample at a time
3. If it’s features exist in the global set, toggle value to ’1’ otherwise ’0’

The Binary Array Approach [1/0]

STEPS

1. We create a global set of features
2. Take one sample at a time
3. If it's features exist in the global set, toggle value to '1' otherwise '0'
4. Repeat 2-3 for all samples

Feature Extraction DEMO


Activities
Terminal
Sep 1 02:10
saketupadhyay@SPIDER: ~/PycharmProjects/Apk_Reverser
net.mudokorea.yeomyungmudo114kr.apk
net.neocorea.daeguyouth.apk

Training and Testing Models

Why divide the dataset into parts?

	Purpose	Yield	Used for Model training	Used for Parameter tuning
Train Data	To learn patterns from the data.	A model that makes near-expected predictions	Yes	Yes
Validation Data	To understand model behaviour and generalizibility on unseen data.	Insights on how to tune your model.	No	Yes
Test Data	To understand how the model would perform in real world scenario.	A completely unbiased estimate of model performance.	No	No

Table 1: Test Train Split

src : medium.com/datadriveninvestor/data-science-essentials-why-train-validation-test-data-b7f7d472dc1f

Test Train Split Architecture

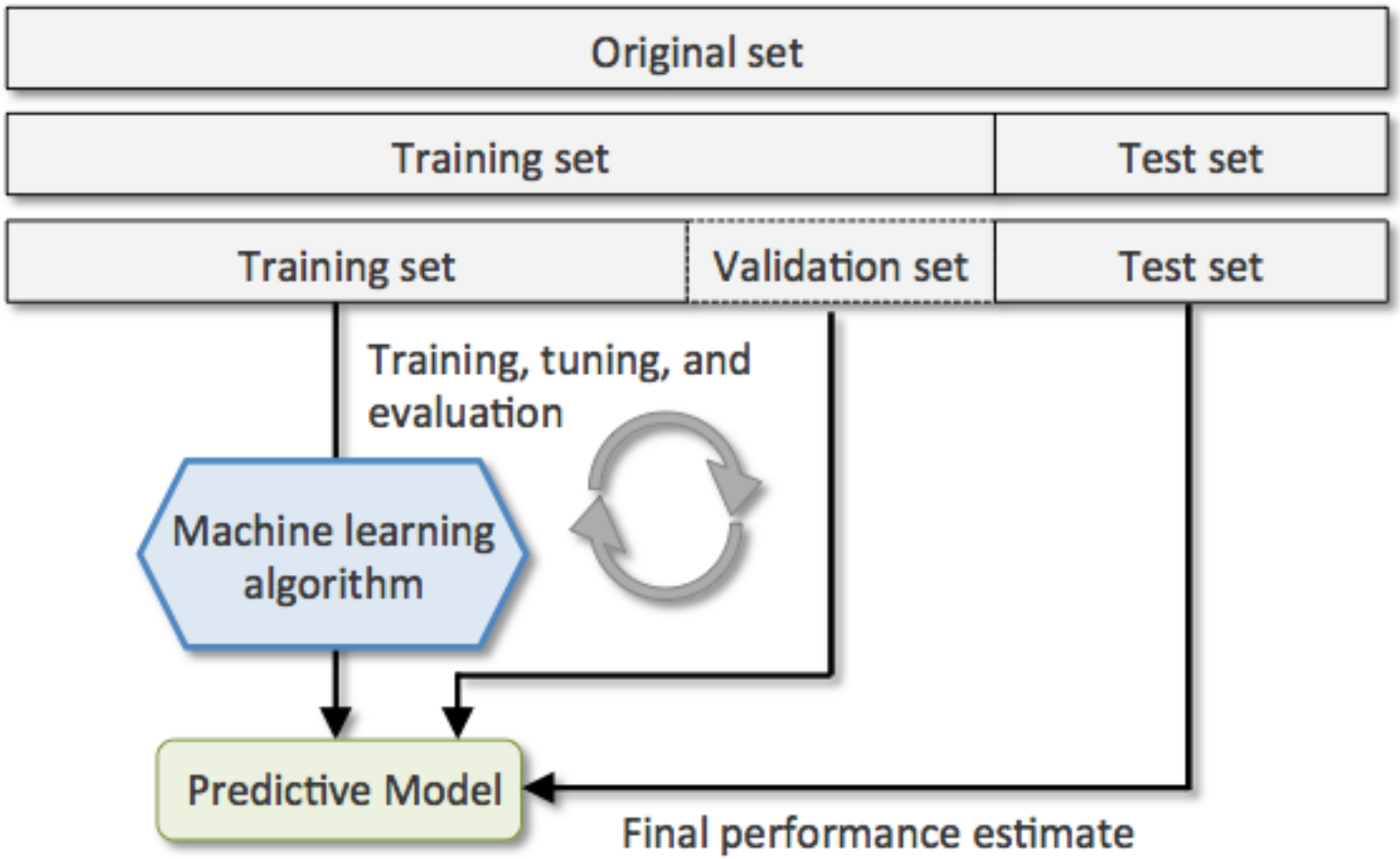


Fig 3: Test Train Arch. src :

medium.com/datadriveninvestor/data-science-essentials-why-train-validation-test-data-b7f7d472dc1f

Model Evaluation

Model Evaluation

1. Confusion Matrix

Model Evaluation

1. Confusion Matrix
2. F1 Score

Model Evaluation

1. Confusion Matrix
2. F1 Score
3. Gain and Lift Charts

Model Evaluation

1. Confusion Matrix
2. F1 Score
3. Gain and Lift Charts
4. Kolmogorov Smirnov Chart

Model Evaluation

1. Confusion Matrix
2. F1 Score
3. Gain and Lift Charts
4. Kolmogorov Smirnov Chart
5. AUC – ROC

Model Evaluation

1. Confusion Matrix
2. F1 Score
3. Gain and Lift Charts
4. Kolmogorov Smirnov Chart
5. AUC – ROC
6. Log Loss

Model Evaluation

1. Confusion Matrix
2. F1 Score
3. Gain and Lift Charts
4. Kolmogorov Smirnov Chart
5. AUC – ROC
6. Log Loss
7. Gini Coefficient

Model Evaluation

1. Confusion Matrix
2. F1 Score
3. Gain and Lift Charts
4. Kolmogorov Smirnov Chart
5. AUC – ROC
6. Log Loss
7. Gini Coefficient
8. Concordant – Discordant Ratio

Model Evaluation

1. Confusion Matrix
2. F1 Score
3. Gain and Lift Charts
4. Kolmogorov Smirnov Chart
5. AUC – ROC
6. Log Loss
7. Gini Coefficient
8. Concordant – Discordant Ratio
9. Root Mean Squared Error

Model Evaluation

1. Confusion Matrix
2. F1 Score
3. Gain and Lift Charts
4. Kolmogorov Smirnov Chart
5. AUC – ROC
6. Log Loss
7. Gini Coefficient
8. Concordant – Discordant Ratio
9. Root Mean Squared Error
10. etc.

src : https://www.analyticsvidhya.com/blog/2019/08/11-important-model-evaluation-error-metrics/

Confusion Matrix Example

n = 165	Predicted: No	Predicted: Yes
Actual: No	50	10
Actual: Yes	5	100

Fig 4: Confusion Matrix src : www.geeksforgeeks.org/confusion-matrix-machine-learning/

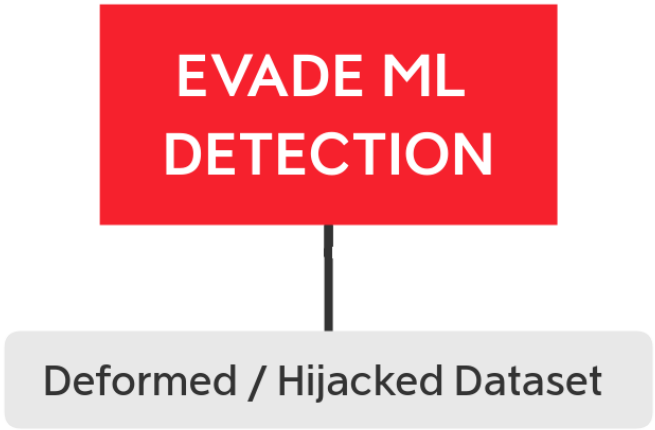
ML Model Test DEMO

Trying to Evade Single Feature Detection.

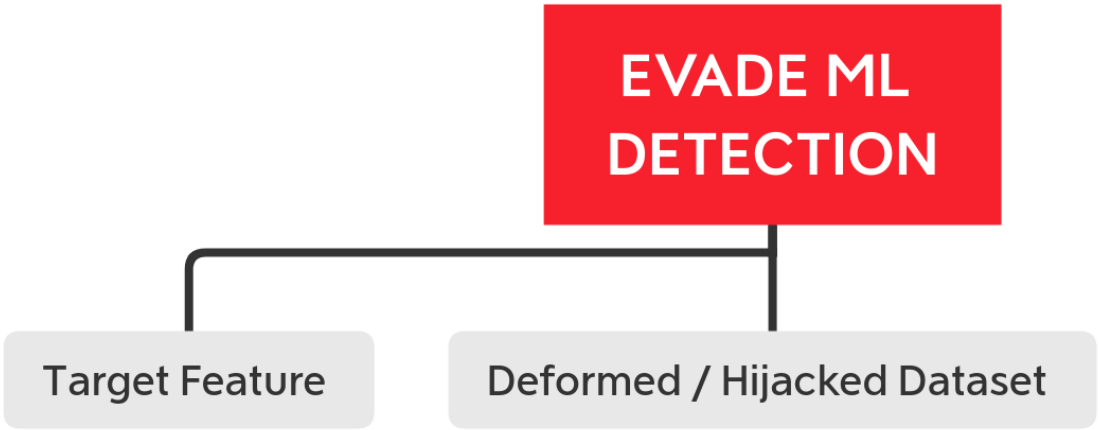
How can we evade?

EVADE ML DETECTION

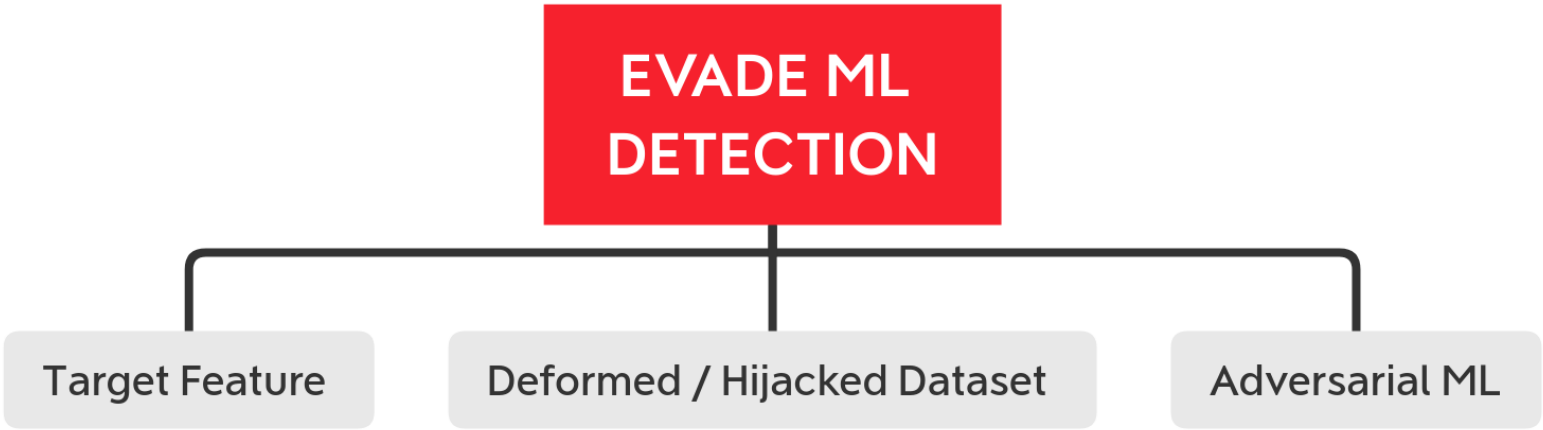
How can we evade?



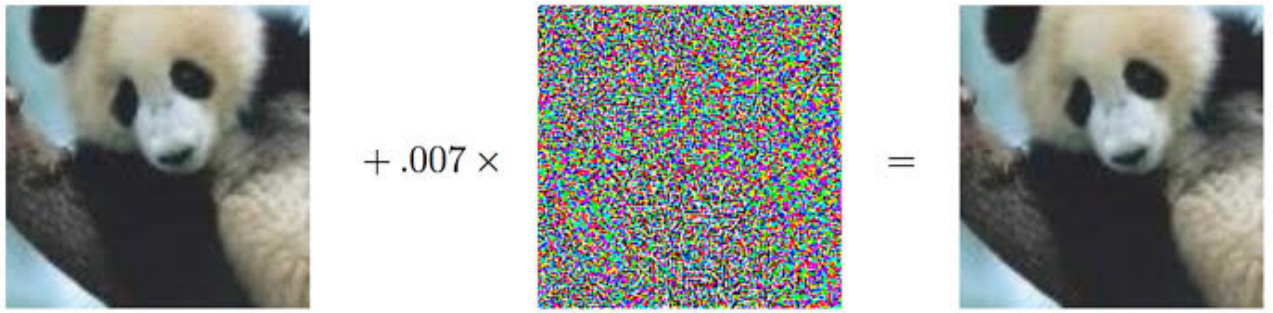
How can we evade?



How can we evade?



Generative Adversarial Networks



src

: google images

GAN in Image Recognition

=

src : google images

Evasion PoC


3. AI Evasion — Konsole
(DevMode) x64mayhem$python3 AdversarialTestDemo.py
ADVERSARIAL Malware Mutator - SAKET UPADHYAY
[[0 0 0 ... 0 0 0]]
The classification is = Malware
With accuracy of (Malware | Safe) = 94.0 | 6.0

```
(DevMode) x64mayhem$python3 AdversarialTestDemo.py
ADVERSARIAL Malware Mutator - SAKET UPADHYAY
[[0 0 0 ... 0 0 0]]
The classification is = Malware
With accuracy of (Malware | Safe) = 94.0 | 6.0
ROUND [1] : Activated Bit Count = 101   setting random limit = 50       pass = 407      || Activated Bit Count = 151
ROUND [2] : Activated Bit Count = 101   setting random limit = 50       pass = 19732    || Activated Bit Count = 151
ROUND [3] : Activated Bit Count = 101   setting random limit = 50       pass = 77       || Activated Bit Count = 150
ROUND [4] : Activated Bit Count = 101   setting random limit = 50       pass = 286      || Activated Bit Count = 151
ROUND [5] : Activated Bit Count = 101   setting random limit = 50       pass = 7636     || Activated Bit Count = 151

MUTATION COMPLETED
======================
best mutation = 150


The classification is = Safe
With accuracy of (Malware | Safe) = 26.1 | 73.9
```

P.A.C.E.

Platform for Android Malware Classification and Performance Evaluation

P.A.C.E.

Platform for Android Malware Classification and Performance Evaluation

PACE, a unified solution to offer **open and easy implementation access to several machine learning-based Android malware detection techniques** that make most of the research in this domain reproducible. The benefits of PACE are offered using three interfaces i.e. through REST API, Web Interface and ADB interface.

P.A.C.E.

Platform for Android Malware Classification and Performance Evaluation

PACE, a unified solution to offer **open and easy implementation access to several machine learning-based Android malware detection techniques** that make most of the research in this domain reproducible. The benefits of PACE are offered using three interfaces i.e. through REST API, Web Interface and ADB interface.

Presented in: *The 3rd International Workshop on Big Data Analytic for Cyber Crime Investigation and Prevention, IEEE International Conference on Big Data 2019*

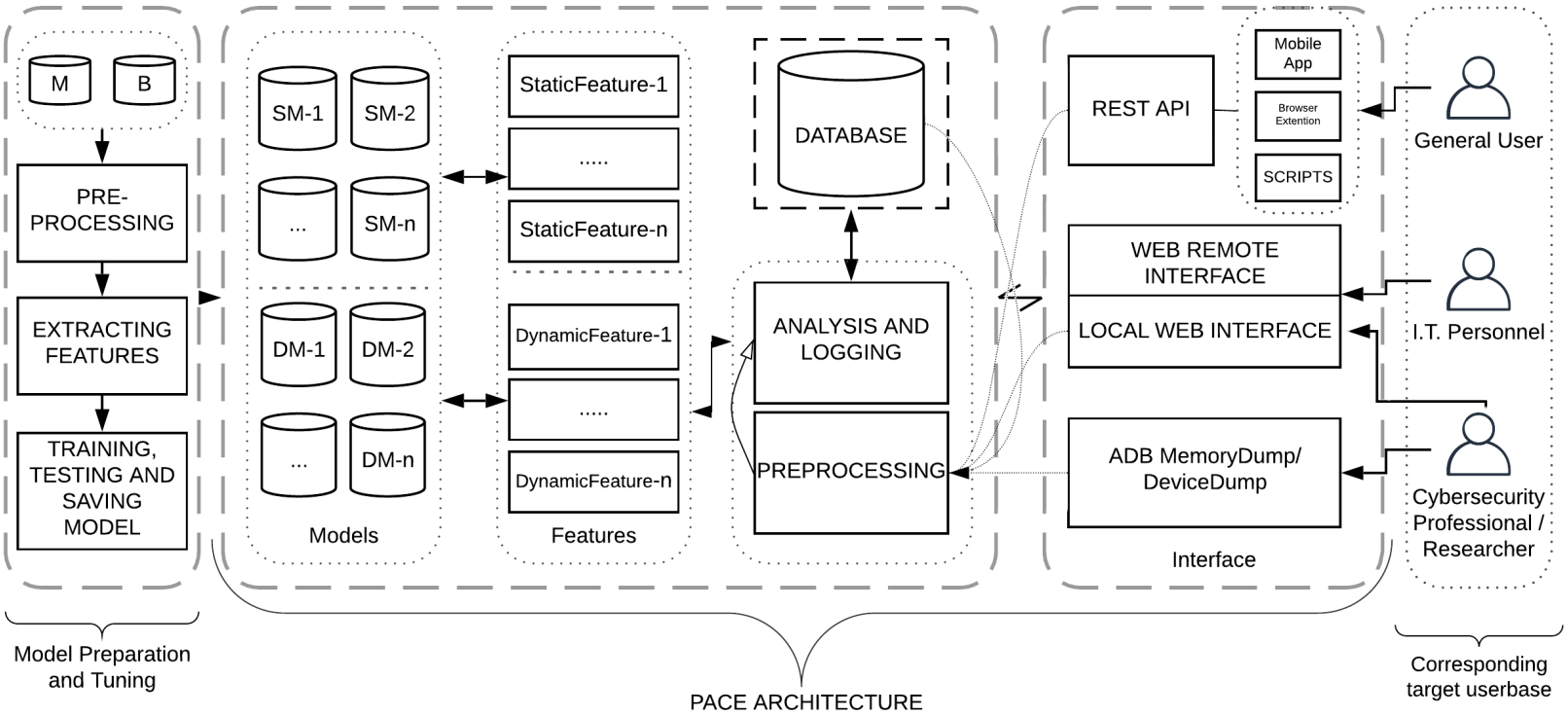


Fig 5: P.A.C.E. Architecture

UPLOAD FOR ANALYSIS

Browse... No file selected.

Upload and analyse

PACE ☰

Search for...

Dashboard

Charts

Tables

Dashboard / Overview

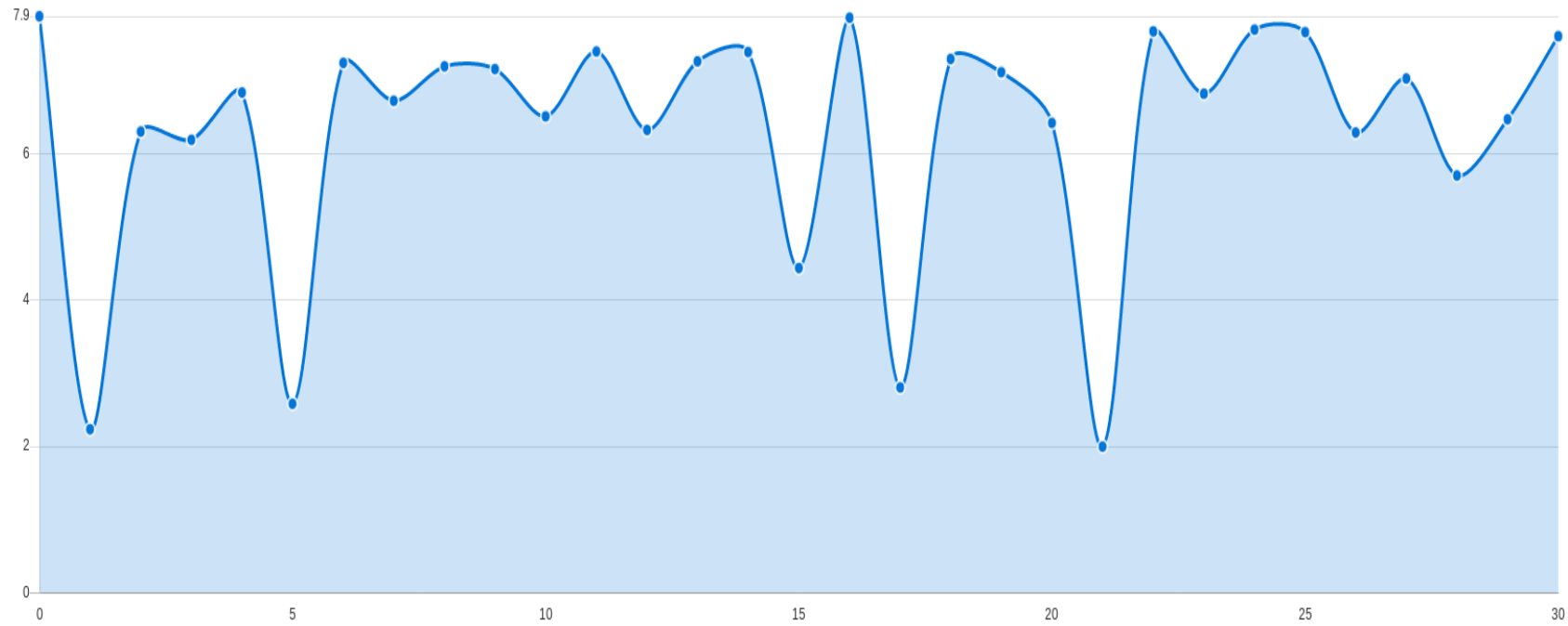
20
Permissions

Download Source Code
Download ›

0
SAFE HITS

8
MALWARE HITS

Entropy Chart SHA256: dd3b7f7b15f222e249bcf18538082d4b20c763914cd7f29209ef8629e826d661



Updated 23/10/2019 22:57:16

ML Engine Results

No.	Name	Classification [Confidence]	Feature Type	Base Operation	Author

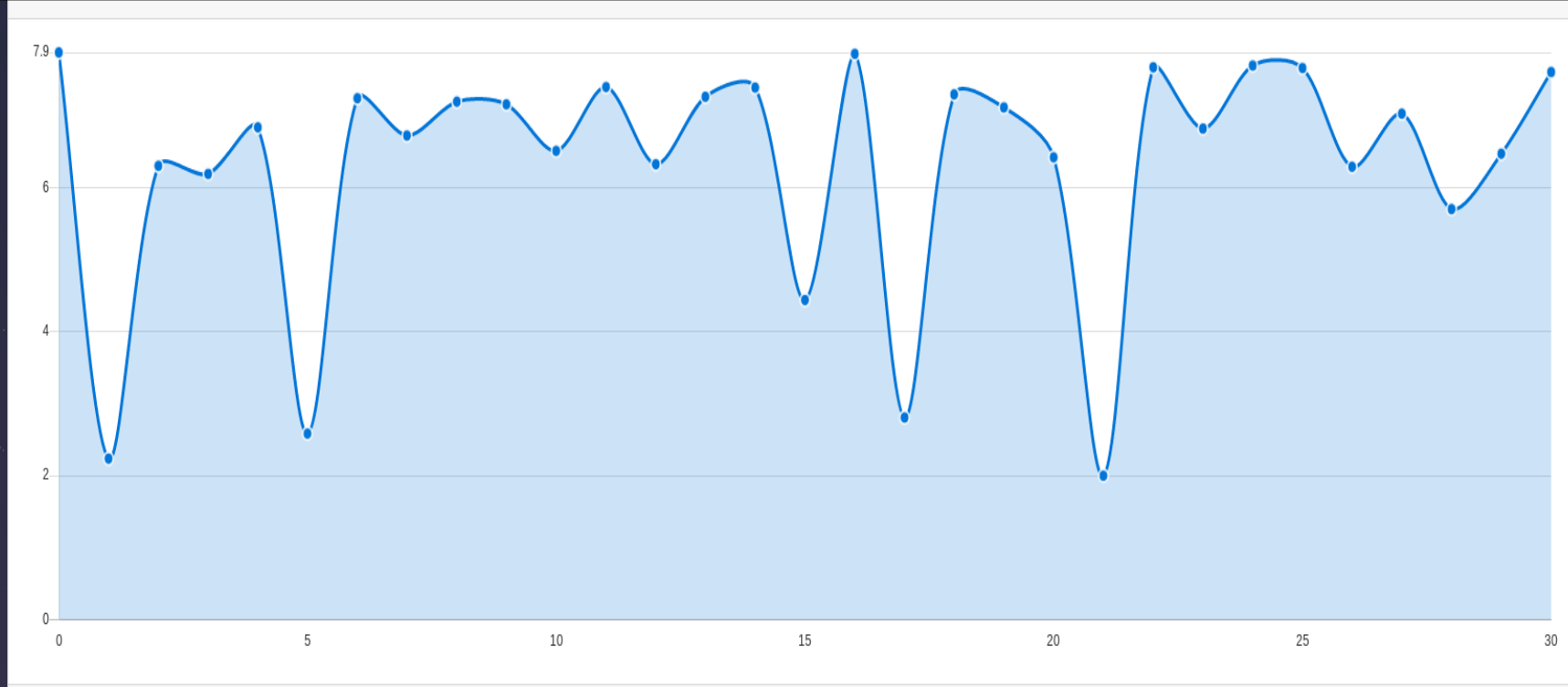
Updated 23/10/2019 22:57:16

ML Engine Results

No.	Name	Classification [Confidence]	Feature Type	Base Operation	Author
1	Random Forest (88%)	MALWARE [67.60000000000001]	Permissions	Random Forest	Bhawna Yadav
2	SVM (83%)	MALWARE [92.80000000000001]	Permissions	Support Vector Machine	Saket Upadhyay
3	KNN (78%)	MALWARE [80.0]	Permissions	K-Nearest Neighbours	Wang, Wei and Li, Yuanyuan and Wang, Xing and Liu, Jiqiang and Zhang, Xiangliang
4	BAGGING (90%)	MALWARE [98.8]	Permissions	DT	Naser Peiravian and Xingquan Zhu
5	PEPB (84%)	MALWARE [98.8]	Permissions	Support Vector Machine	Chun-Ying Huang, Yi-Ting Tsai, and Chung-Han Hsu
6	ADABOOST-GRADBOOST (84%)	MALWARE [98.8]	Permissions	Gradient Boosting	Yerima, Suleiman Y and Sezer, Sakir
7	APK Auditor: Permission-based Android malware detection (79%)	MALWARE [94.39999999999999]	Permissions	Logistic regression	- - - -
8	Permission-Based Android Malware Detection (89%)	NA [ ]	Permissions	K-means(Random forest)	Zarni Aung, Win Zaw
9	STATIC DETECTION OF ANDROID MALWARE BY USING PERMISSIONS AND API CALLS (88%)	MALWARE [69.19999999999999]	Permissions	Random Forest	Patrick P.K. Chan, Wen-Kai Song
No.	**Name**	**Classification [Confidence]**	**Feature Type**	**Base Operation**	**Author**

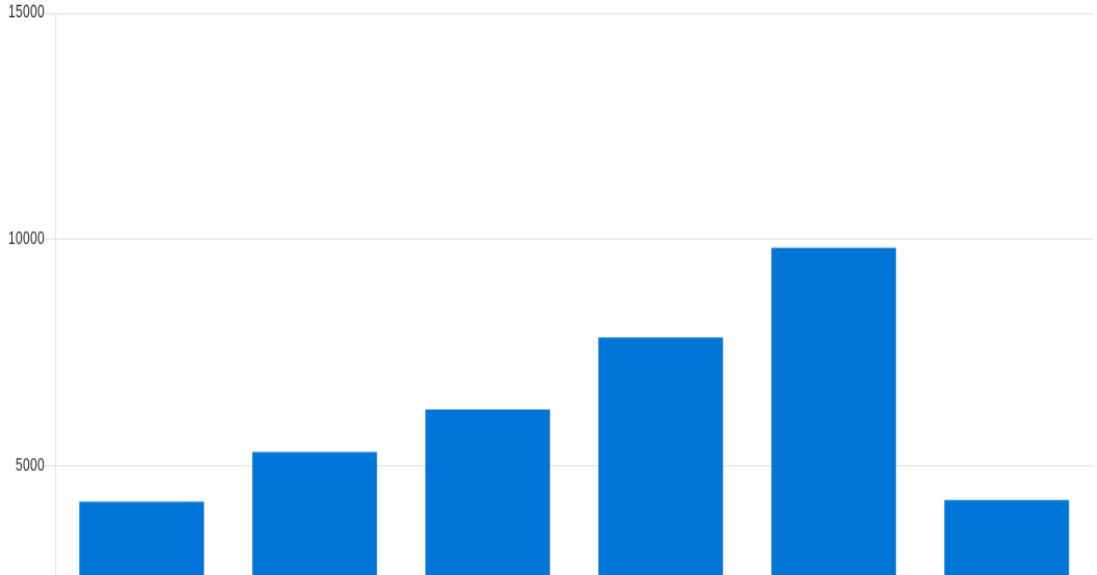
Updated yesterday at 11:59 PM

Tables

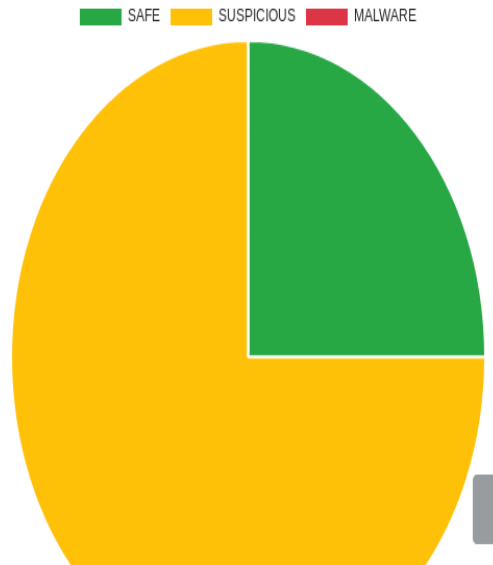


*Representational file entropy

Bar Chart



Confidence Distribution



Dashboard

Charts

Tables

Permissions

No.	Name	Stock	okay?	Normal?	Title
1	android.permission.VIBRATE	True	--	--	--
2	android.permission.WRITE_EXTERNAL_STORAGE	False	--	--	--
3	android.permission.WAKE_LOCK	True	--	--	--
4	android.permission.CAMERA	False	--	--	--
5	android.permission.READ_PHONE_STATE	False	--	--	--
6	android.permission.FOREGROUND_SERVICE	False	--	--	--
7	android.permission.REQUEST_DELETE_PACKAGES	False	--	--	--
8	android.permission.MOUNT_UNMOUNT_FILESYSTEMS	True	--	--	--
9	android.permission.ACCESS_NETWORK_STATE	True	--	--	--
10	android.permission.RECEIVE_BOOT_COMPLETED	True	--	--	--
11	android.permission.BIND_ACCESSIBILITY_SERVICE	True	--	--	--
12	com.android.launcher.permission.INSTALL_SHORTCUT	False	--	--	--
13	android.permission.GET_PACKAGE_SIZE	True	--	--	--
14	android.permission.REQUEST_INSTALL_PACKAGES	True	--	--	--
15	android.permission.FLASHLIGHT	True	--	--	--
16	android.permission.ACCESS_WIFI_STATE	True	--	--	--
17	com.google.android.c2dm.permission.RECEIVE	False	--	--	--

Exif Info

No.	Property	Value	--	--	--
1	File Name	APKPure_v3.12.1_apkpure.com.apk	--	--	--
2	File Size	12 MB	--	--	--
3	File Modification Date/Time	2019	--	--	--
4	File Access Date/Time	2019	--	--	--
5	File Inode Change Date/Time	2019	--	--	--
6	File Permissions	rw-r--r--	--	--	--
7	File Type	ZIP	--	--	--
8	File Type Extension	zip	--	--	--
9	MIME Type	application/zip	--	--	--
10	Zip Required Version	20	--	--	--
11	Zip Bit Flag	0x0808	--	--	--
12	Zip Compression	Deflated	--	--	--
13	Zip Modify Date	2019	--	--	--
14	Zip CRC	0x8f17ef4a	--	--	--
15	Zip Compressed Size	77719	--	--	--
16	Zip Uncompressed Size	225152	--	--	--
17	Zip File Name	META-INF/MANIFEST.MF	--	--	--
No.	**Property**	**Value**	**--**	**--**	**--**

Updated yesterday at 11:59 PM

PACE ≡

Search for...

Dashboard

Charts

Tables

Dashboard / Overview

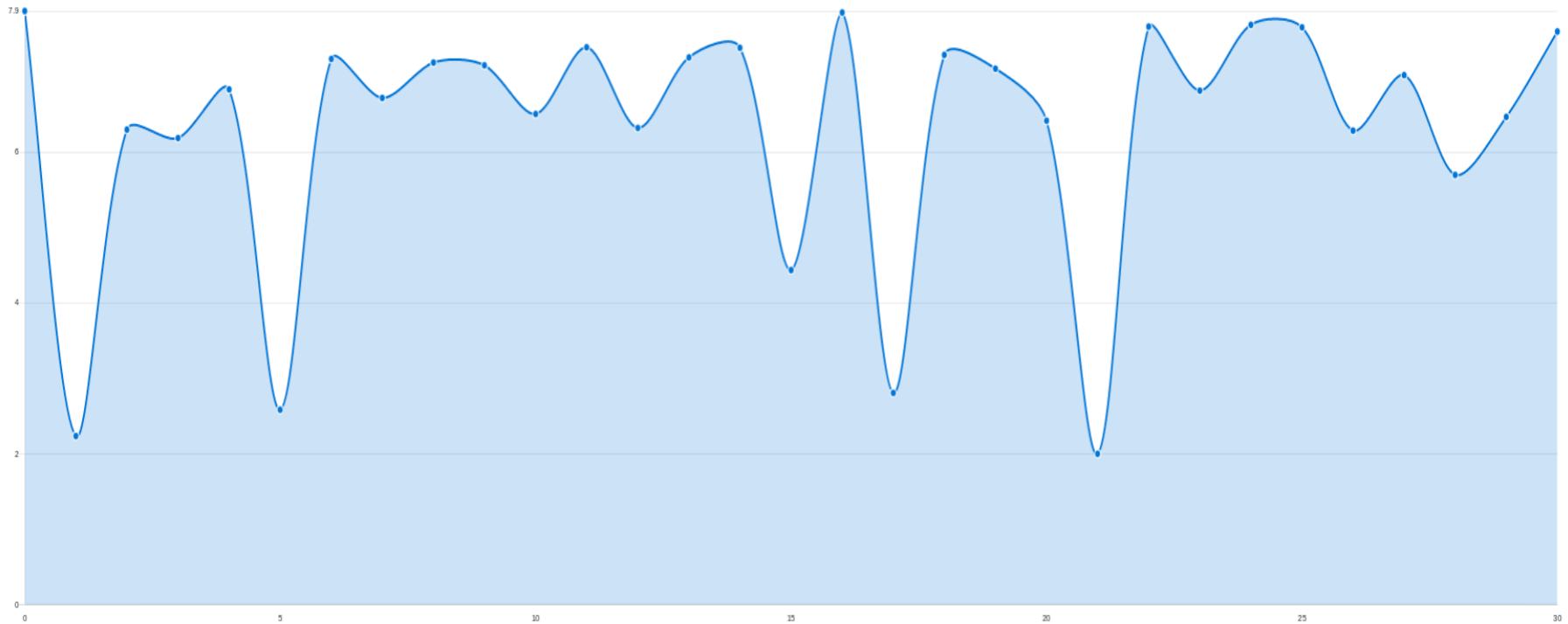
20
Permissions

Download Source Code
Download

0
SAFE HITS

8
MALWARE HITS

Entropy Chart SHA256: dd3b7f7b15f222e249bcf18538082d4b20c763914cd7f29209ef8629e826d661



Updated 23/10/2019 22:57:16

ML Engine Results

No.	Name	Classification [Confidence]	Feature Type	Base Operation	Author
1	Random Forest (88%)	MALWARE [67.60000000000001]	Permissions	Random Forest	Bhawna Yadav
2	SVM (83%)	MALWARE [92.80000000000001]	Permissions	Support Vector Machine	Saket Upadhyay
3	KNN (78%)	MALWARE [80.0]	Permissions	K-Nearest Neighbours	Wang, Wei and Li, Yuanyuan and Wang, Xing and Liu, Jiqiang and Zhang, Xiangliang
4	BAGGING (90%)	MALWARE [98.8]	Permissions	DT	Naser Peiravian and Xingquan Zhu
5	PEPB (84%)	MALWARE [98.8]	Permissions	Support Vector Machine	Chun-Ying Huang, Yi-Ting Tsai, and Chung-Han Hsu
6	ADABOOST-GRADBOOST (84%)	MALWARE [98.8]	Permissions	Gradient Boosting	Yerima, Suleiman Y and Sezer, Sakir

Conclusion

Closing Thoughts

Closing Thoughts

- Malware Detection and Elimination plays an critical role in defending critical digital infratucture.

Closing Thoughts

- Malware Detection and Elimination plays an critical role in defending critical digital infratucture.
- With advantage of AI & ML,Cyber- and Info -sec field is adapting significantly.

Closing Thoughts

- Malware Detection and Elimination plays an critical role in defending critical digital infratucture.
- With advantage of AI & ML,Cyber- and Info -sec field is adapting significantly.
- The defenders as well as adversaries have access to new tech. and research.

Closing Thoughts

- Malware Detection and Elimination plays an critical role in defending critical digital infratucture.
- With advantage of AI & ML,Cyber- and Info -sec field is adapting significantly.
- The defenders as well as adversaries have access to new tech. and research.
- There’s lot more to explore.

Due Credits and Mentions

Due Credits and Mentions

Co-Authors in the above discussed research.(PACE)

Dr. Ajit Kumar
Dr. Shishir K. Shandilya
Dr. Andrii Shalaginov
Dr. Vinti Agarwal
Bhawna Yadav

Thankyou

Q & A

x64mayhem

linkedin.com/in/saketupadhyay

x64mayhem@gmail.com

github.com/Saket-Upadhyay

Resources at : **github.com/Saket-Upadhyay/PennStateTalk2020**

Q & A

x64mayhem

linkedin.com/in/saketupadhyay

x64mayhem@gmail.com

github.com/Saket-Upadhyay

Resources at : **github.com/Saket-Upadhyay/PennStateTalk2020**