


# DIGITAL FORENSICS

Presentation

# AGENDA

## 01 DIGITAL FORENSICS

I. Definition
II. Branches
III. Methodology

## 02 MEMORY FORENSICS

I. What is memory?
II. Why does it matter?
III. How is it investigated?

## 03 DEMONSTRATION

- Malware Incident

01

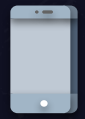
# DIGITAL FORENSICS


# DEFINITION

Digital Forensics refers to the investigation of digital devices and data in order to gather evidence of an incident.

# Branches

COMPUTER



MOBILE

NETWORK

DATABASE

Sub-Branches

MEMORY

DISK

# Methodology

# Tools

## Imaging

## Cracking

## Recovery

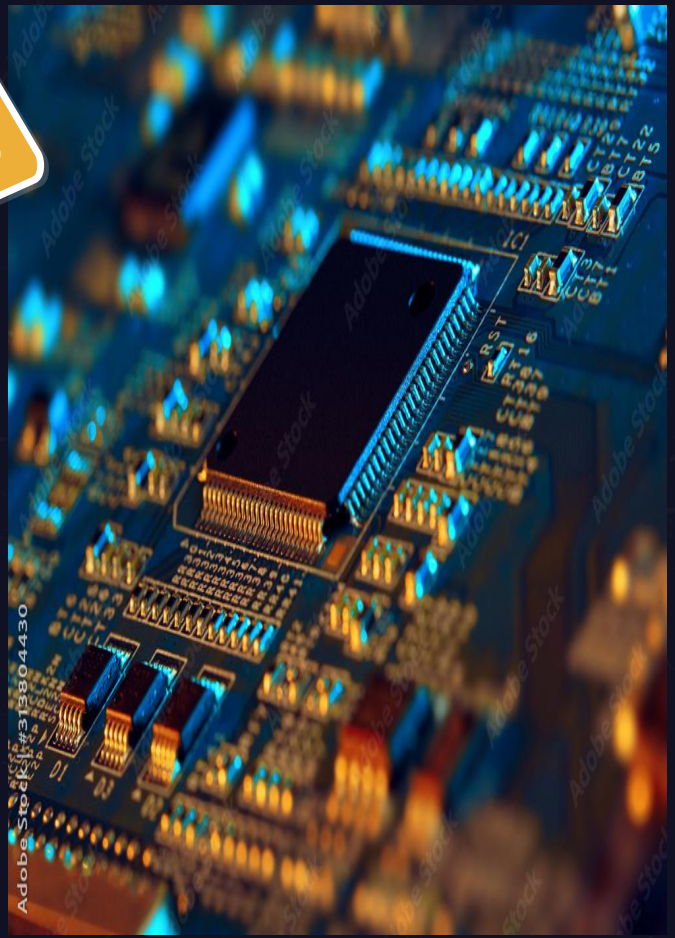
## Other

02

# MEMORY FORENSICS

# BACK TO THE BASICS:
# MEMORY

A component that stores data and instructions that are currently being used or are expected to be used in the future.

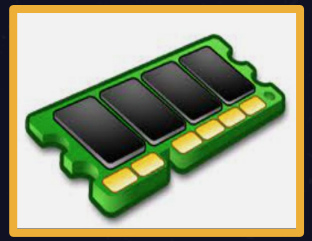


# WAIT, BUT WHY?

Runtime state of the system provides critical information about the incident.

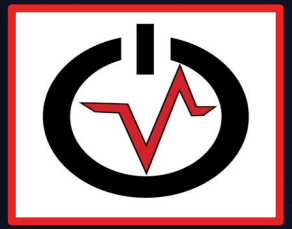
# Methodology

# Tools



DumpIt


Rekall



Volatility

03

# Demonstration

Malware Incident

# Next Steps

## Further Malware Analysis


## Optional Malware Removal

## Continue learning!

Research, CTFs, etc.

# THANK YOU!

DO YOU HAVE ANY QUESTIONS?