22618 ETI (Emerging Trends in Computer & Information Technology) Notes

6th Sem MCQ Test Series (All Subjects) : click here
6th Sem MCQ PDFs (All Subjects) : click here

Unit -1
Artificial intelligence

Course Outcome

Describe Artificial Intelligence, Machine learning and deep learning

Concept of AI

- **Concept of Artificial intelligence (AI)**
- Artificial intelligence (AI) is the simulation of human intelligence processes by machines, especially computer systems.

Particular applications of AI include

Expert systems :- An expert system is a computer program that uses artificial intelligence (AI) technologies to simulate the judgment and behavior of a human or an organization that has expert knowledge and experience in a particular field.

Speech recognition:- Voice recognition systems enable consumers to interact with technology simply by speaking to it.

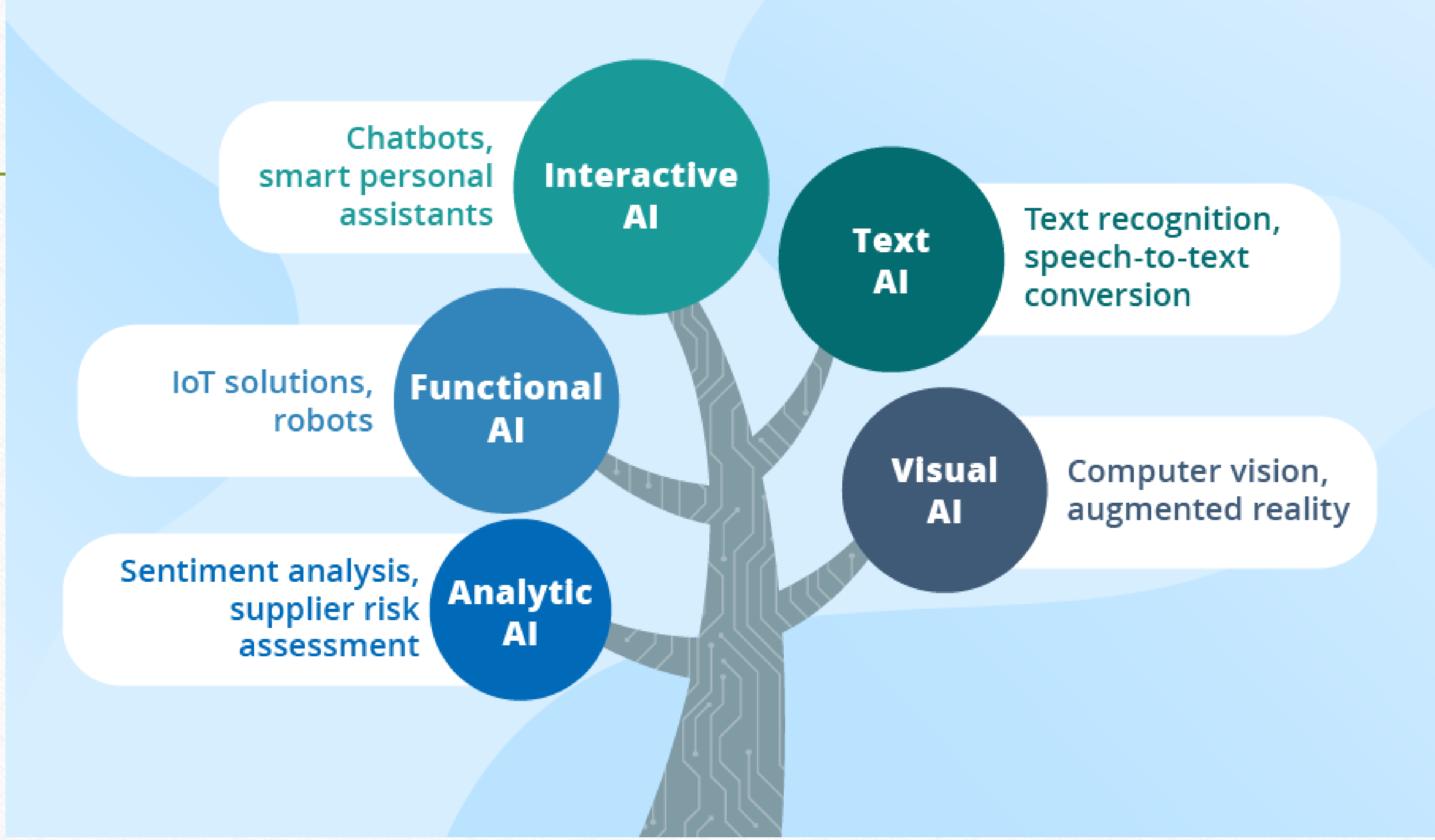
Machine vision:- Machine vision is the ability of a computer to see; it employs one or more video cameras, analog-to-digital conversion (ADC) and digital signal processing (DSP). The resulting data goes to a computer or robot controller.

Components of AI

- There are six key components that are essential to AI.

1. **AI Applications**: Packaged applications that solve a business problem (i.e., virtual agents, financial planning)
2. **Data Prep and Cleansing**: Make your data ready for AI
3. **Model, Build, Train and Run**: The studio of a data science artist to build, train and run models (machine learning)
4. **Consumer Features**: Speech, images and vision, primarily used in consumer use cases
5. **Natural Language Processing:** The nervous system of enterprise AI
6. **Lifecycle Management**: Managing the lifecycle of AI models and understanding how they perform

Types of AI



Interactive AI

Chatbots, smart personal assistants

Text AI

Text recognition, speech-to-text conversion

Functional AI

IoT solutions, robots

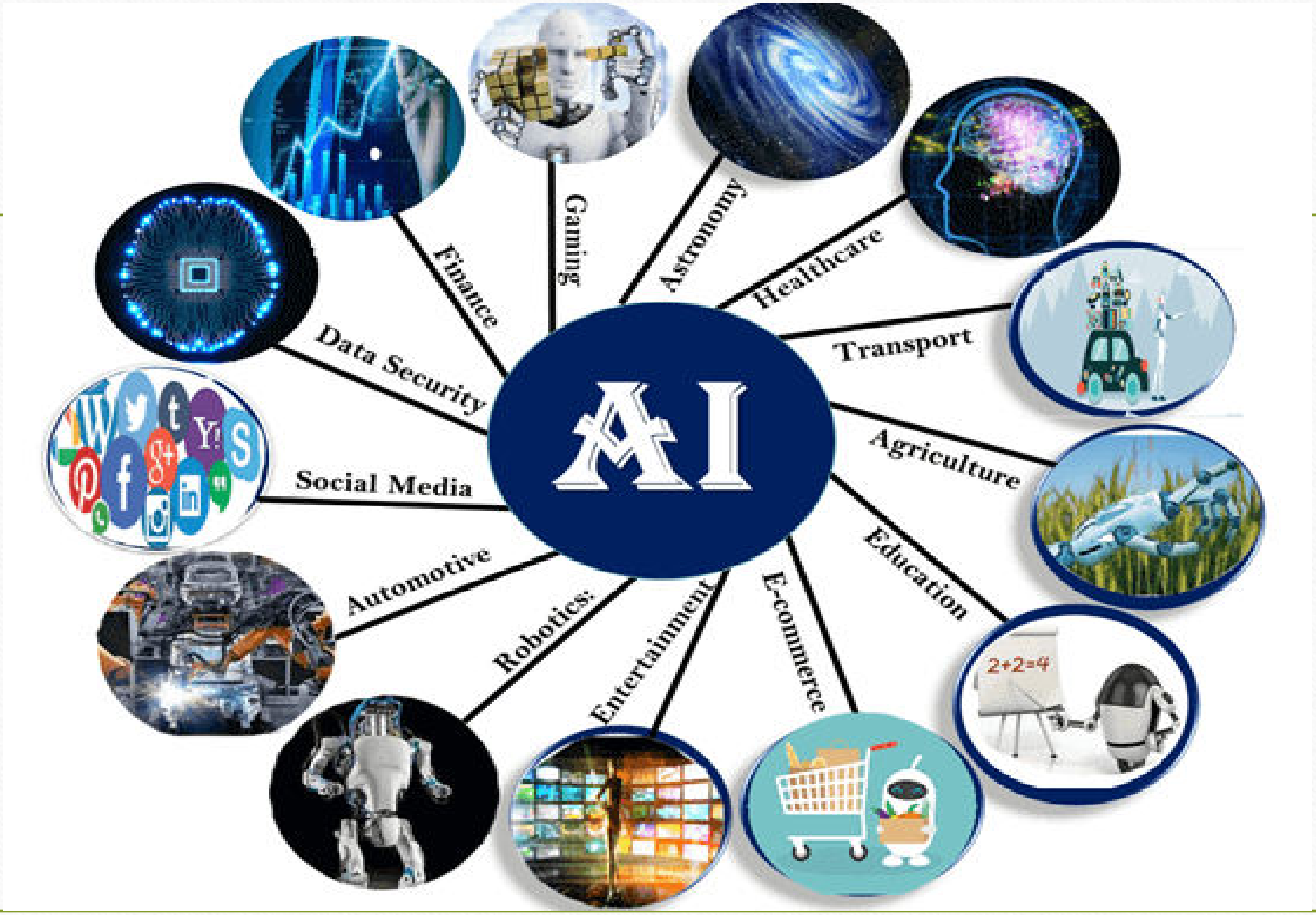
Visual AI

Computer vision, augmented reality

Analytic AI

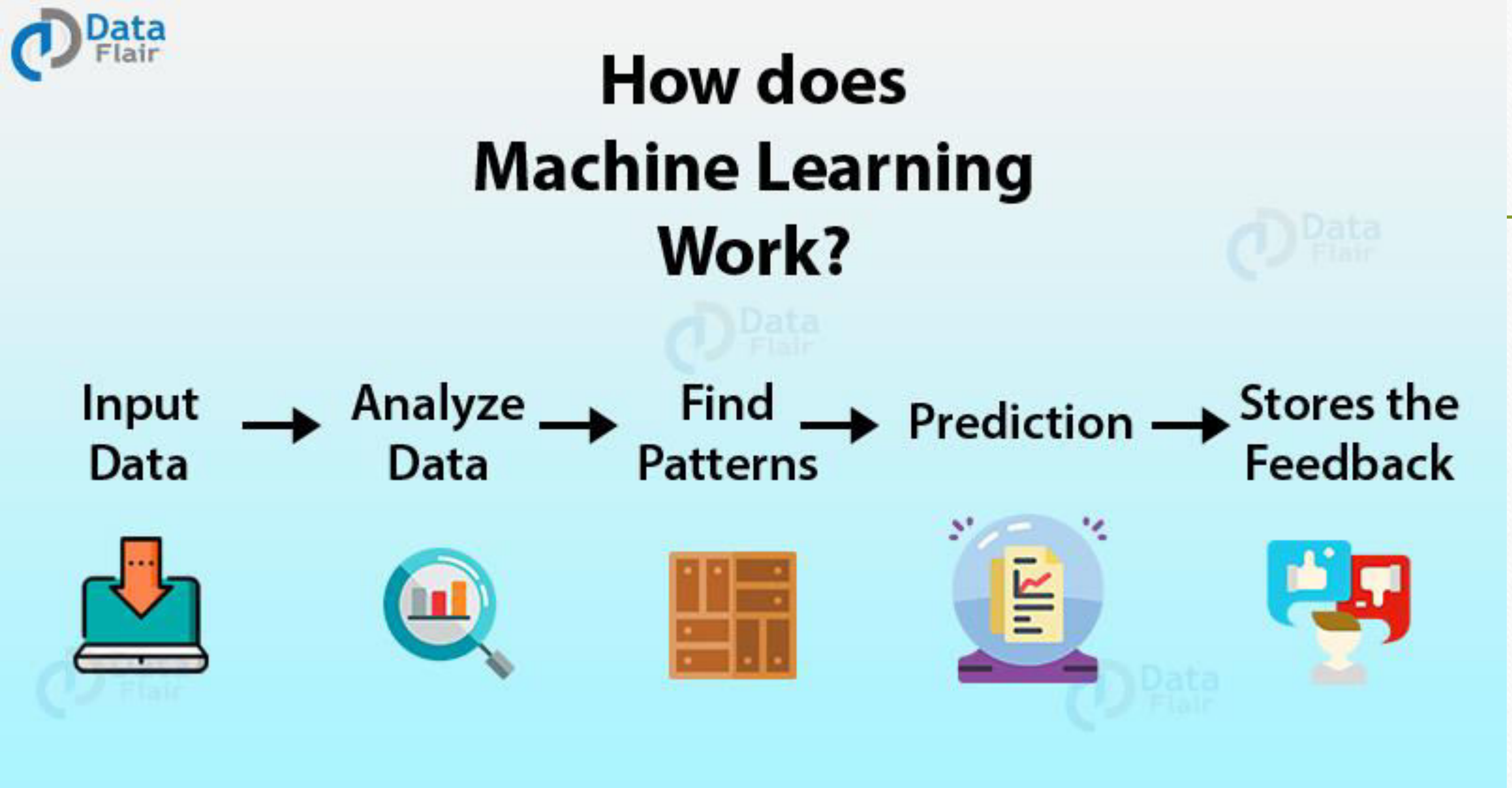
Sentiment analysis, supplier risk assessment

Application of AI



What is Machine Learning?

- Machine Learning
  - Study of algorithms that
  - improve their performance
  - at some task
  - with experience
- Optimize a performance criterion using example data or past experience.
- Role of Statistics: Inference from a sample
- Role of Computer science: Efficient algorithms to
  - Solve the optimization problem
  - Representing and evaluating the model for inference



How does Machine Learning Work?

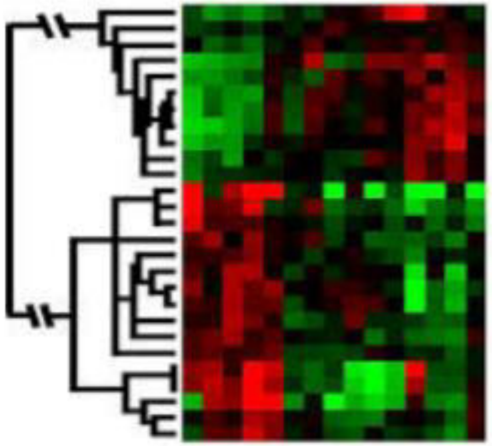
Input Data → Analyze Data → Find Patterns → Prediction → Stores the Feedback

Growth of Machine Learning

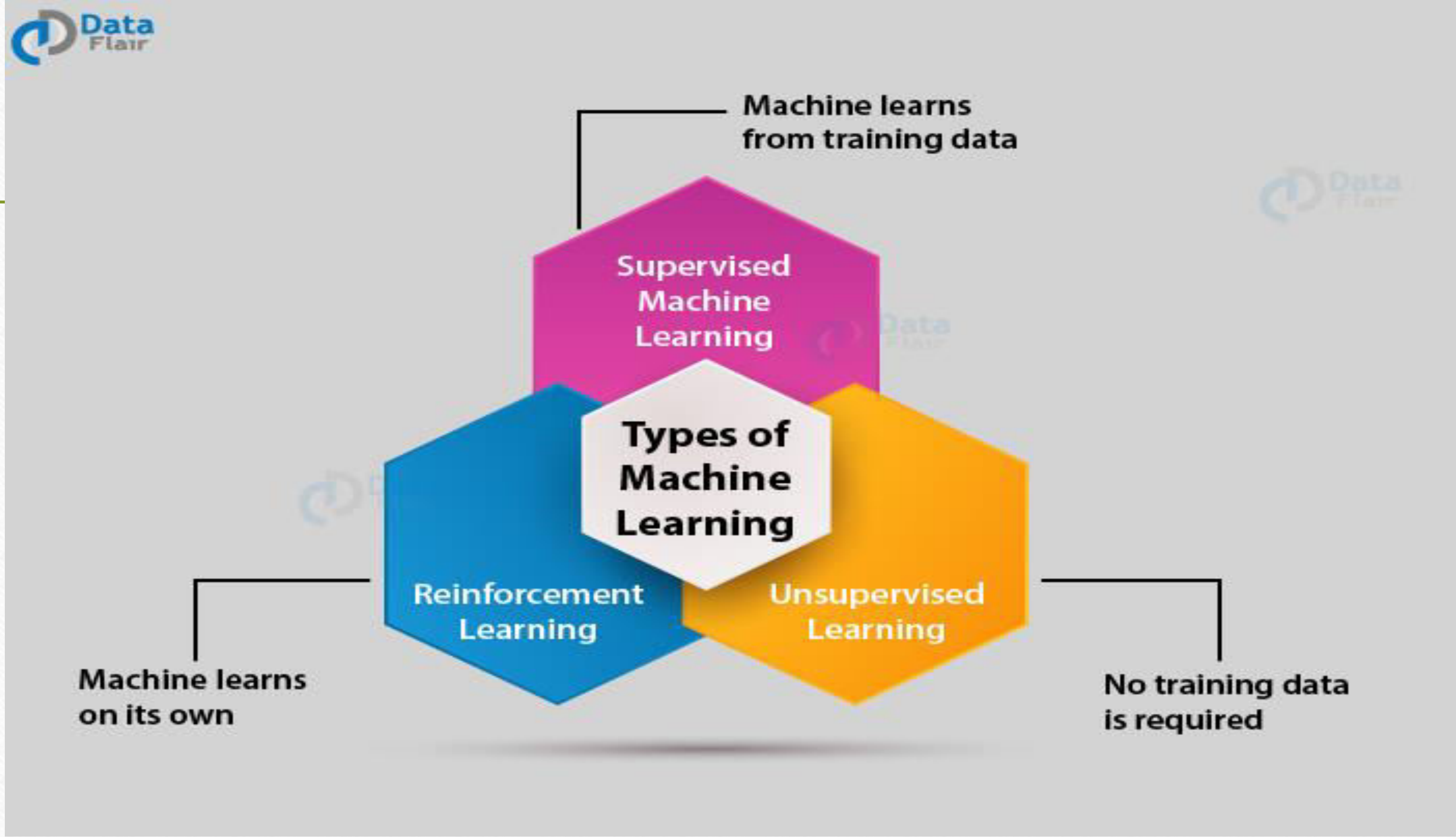
- Machine learning is preferred approach to
  - Speech recognition, Natural language processing
  - Computer vision
  - Medical outcomes analysis
  - Robot control
  - Computational biology
- This trend is accelerating
  - Improved machine learning algorithms
  - Improved data capture, networking, faster computers
  - Software too complex to write by hand
  - New sensors / IO devices

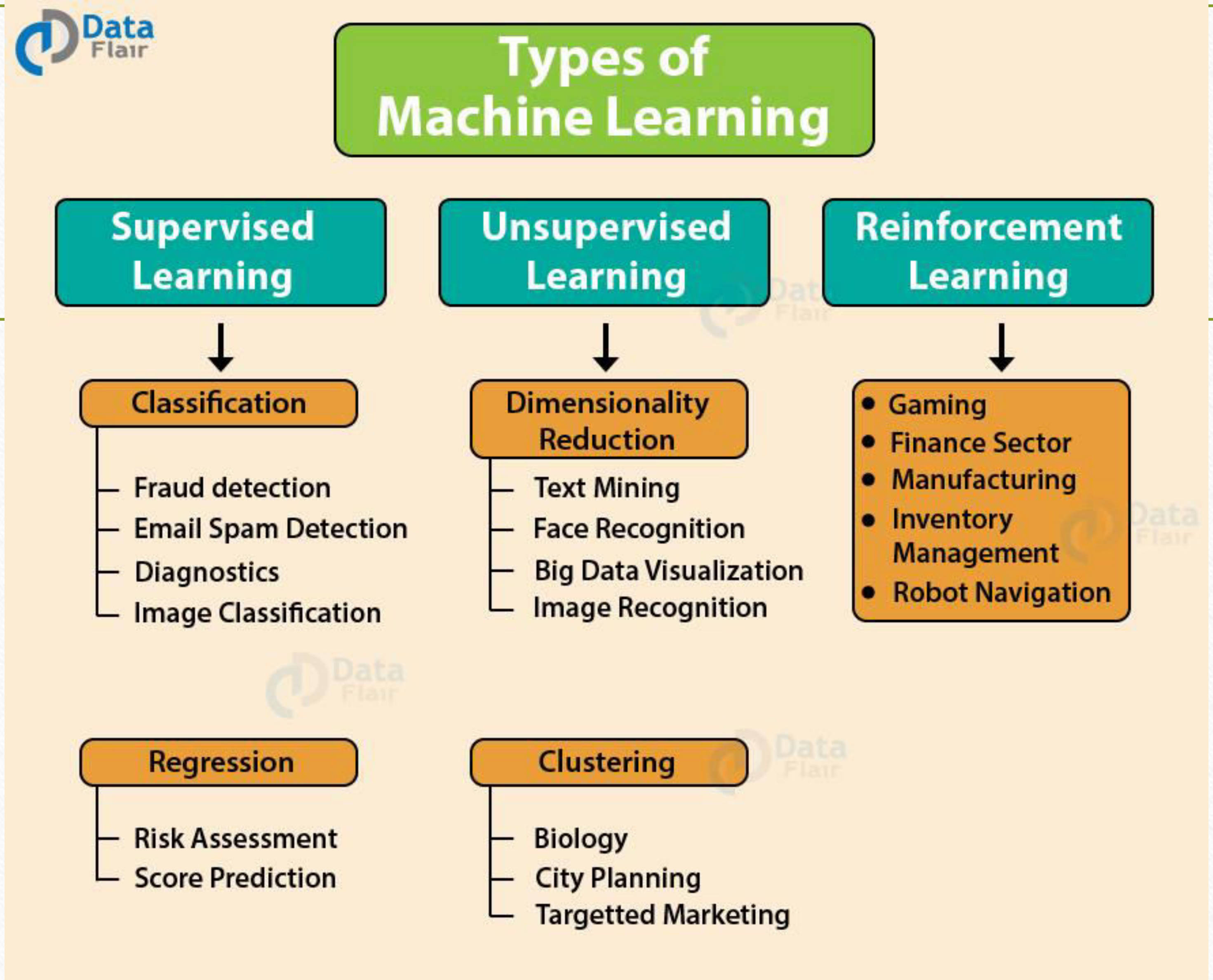
When Do We Use Machine Learning?

- ML is used when:
- Human expertise does not exist (navigating on Mars)
- Humans can’t explain their expertise (speech recognition)
- Models must be customized (personalized medicine)
- Models are based on huge amounts of data (genomics)



Types of Machine Learning


Data Flair
Machine learns from training data
Supervised Machine Learning
Types of Machine Learning
Reinforcement Learning
Unsupervised Learning
Machine learns on its own
No training data is required



Types of Machine Learning

Supervised Learning

Classification

- Fraud detection
- Email Spam Detection
- Diagnostics
- Image Classification

Regression

- Risk Assessment
- Score Prediction

Unsupervised Learning

Dimensionality Reduction

- Text Mining
- Face Recognition
- Big Data Visualization
- Image Recognition

Clustering

- Biology
- City Planning
- Targetted Marketing

Reinforcement Learning

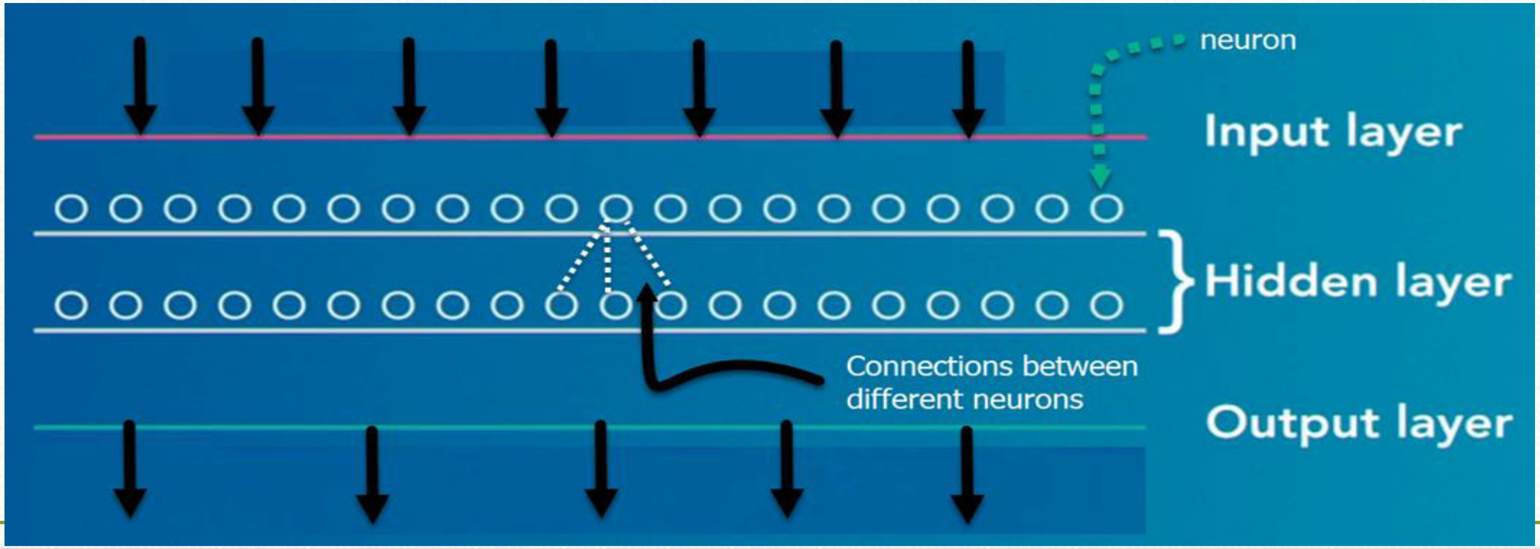
- Gaming
- Finance Sector
- Manufacturing
- Inventory Management
- Robot Navigation

Sample Applications

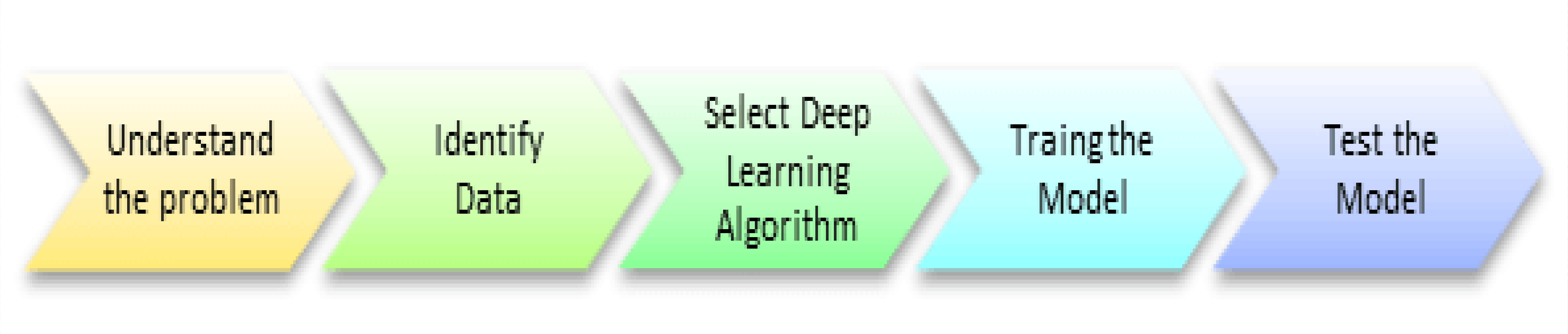
- Web search
- • Computational biology
- • Finance
- • E-commerce
- • Space exploration
- • Robotics
- • Information extraction
- • Social networks
- • Debugging software

What is Deep Learning?

- Deep learning is a computer software that **mimics the network of neurons in a brain**. It is a subset of machine learning and is called deep learning because it makes use of deep **neural networks.**
- **Deep learning algorithms are constructed with connected layers.**
- The first layer is called the Input Layer
- The last layer is called the Output Layer
- All layers in between are called Hidden Layers. The word deep means the network join neurons in more than two layers.



Deep learning Process



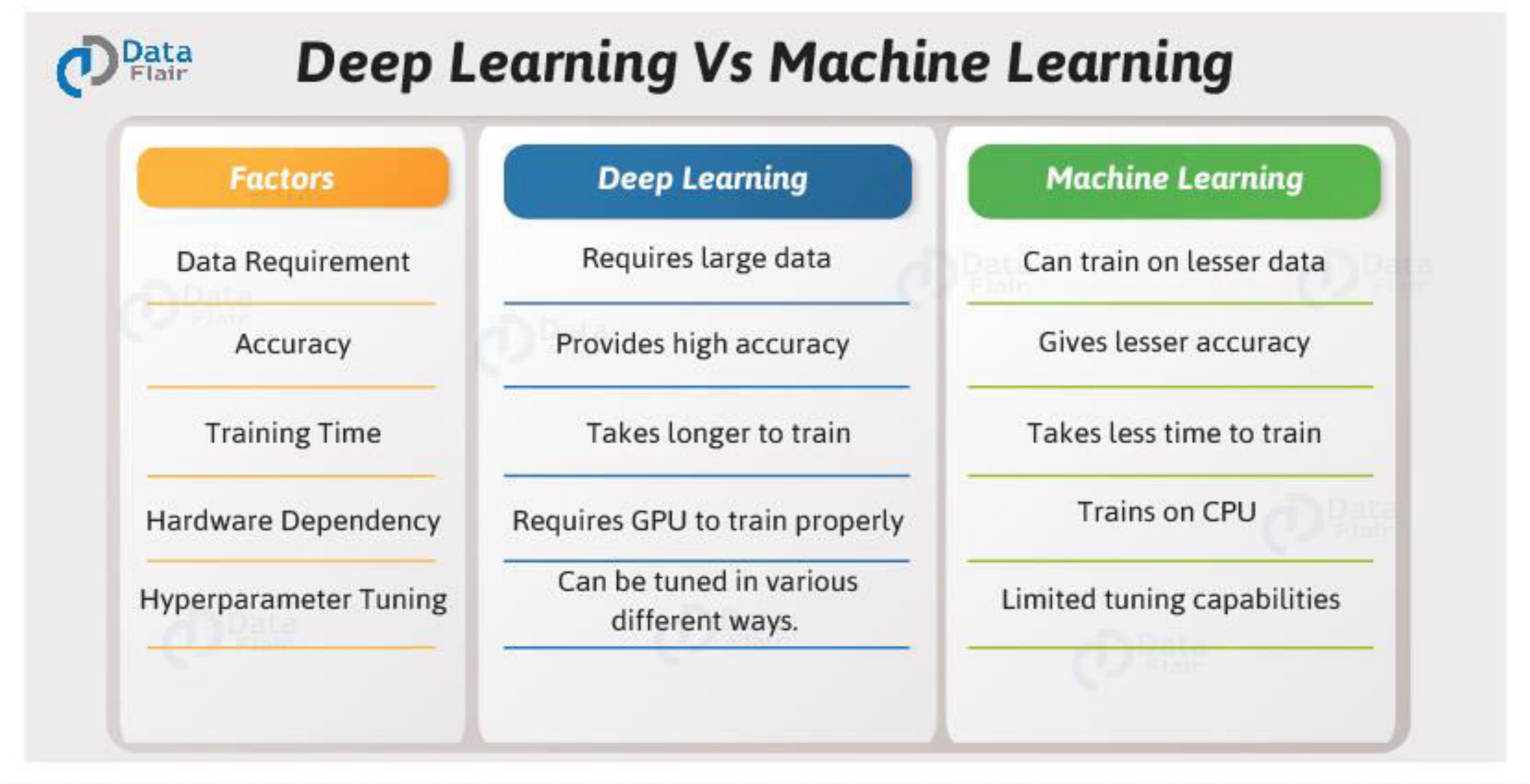
Understand the problem

Identify Data

Select Deep Learning Algorithm

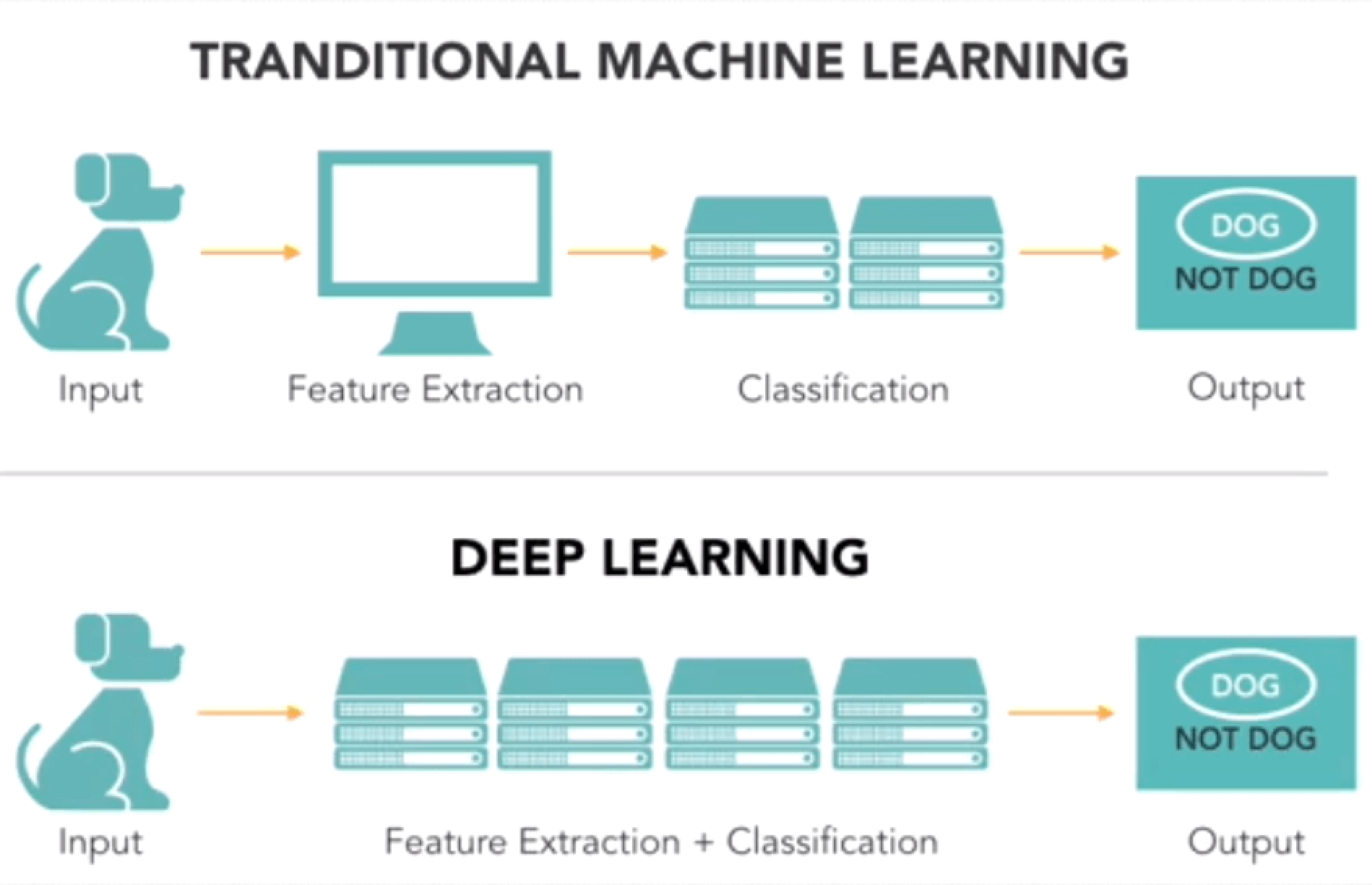
Traing the Model

Test the Model



Deep Learning Vs Machine Learning

Factors	Deep Learning	Machine Learning
Data Requirement	Requires large data	Can train on lesser data
Accuracy	Provides high accuracy	Gives lesser accuracy
Training Time	Takes longer to train	Takes less time to train
Hardware Dependency	Requires GPU to train properly	Trains on CPU
Hyperparameter Tuning	Can be tuned in various different ways.	Limited tuning capabilities



TRANDITIONAL MACHINE LEARNING

DEEP LEARNING

Unit 2: Internet Of Things (IOT)

Course Outcome

Interpret IoT concepts

What is Embedded Systems?

Unit 3: Basics of Digital Forensics

Course Outcome

Compare models of Digital Forensics Investigation

Introduction to Digital Forensics

- Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law.
- It is a science of finding evidence from digital media like a computer, mobile phone, server, or network.
- https://www.youtube.com/watch?v=jrDwZy8I-pg

History of Digital forensics

- Hans Gross (1847 -1915): First use of scientific study to head criminal investigations
- FBI (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.

- In 1978 the first computer crime was recognized in the Florida Computer Crime Act.
- Francis Galton (1982 - 1911): Conducted first recorded study of fingerprints
- In 1992, the term Computer Forensics was used in academic literature.
- 1995 International Organization on Computer Evidence (IOCE) was formed.
- In 2000, the First FBI Regional Computer Forensic Laboratory established.
- In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called "Best practices for Computer Forensics".
- In 2010, Simson Garfinkel identified issues facing digital investigations.

Rules of digital forensics

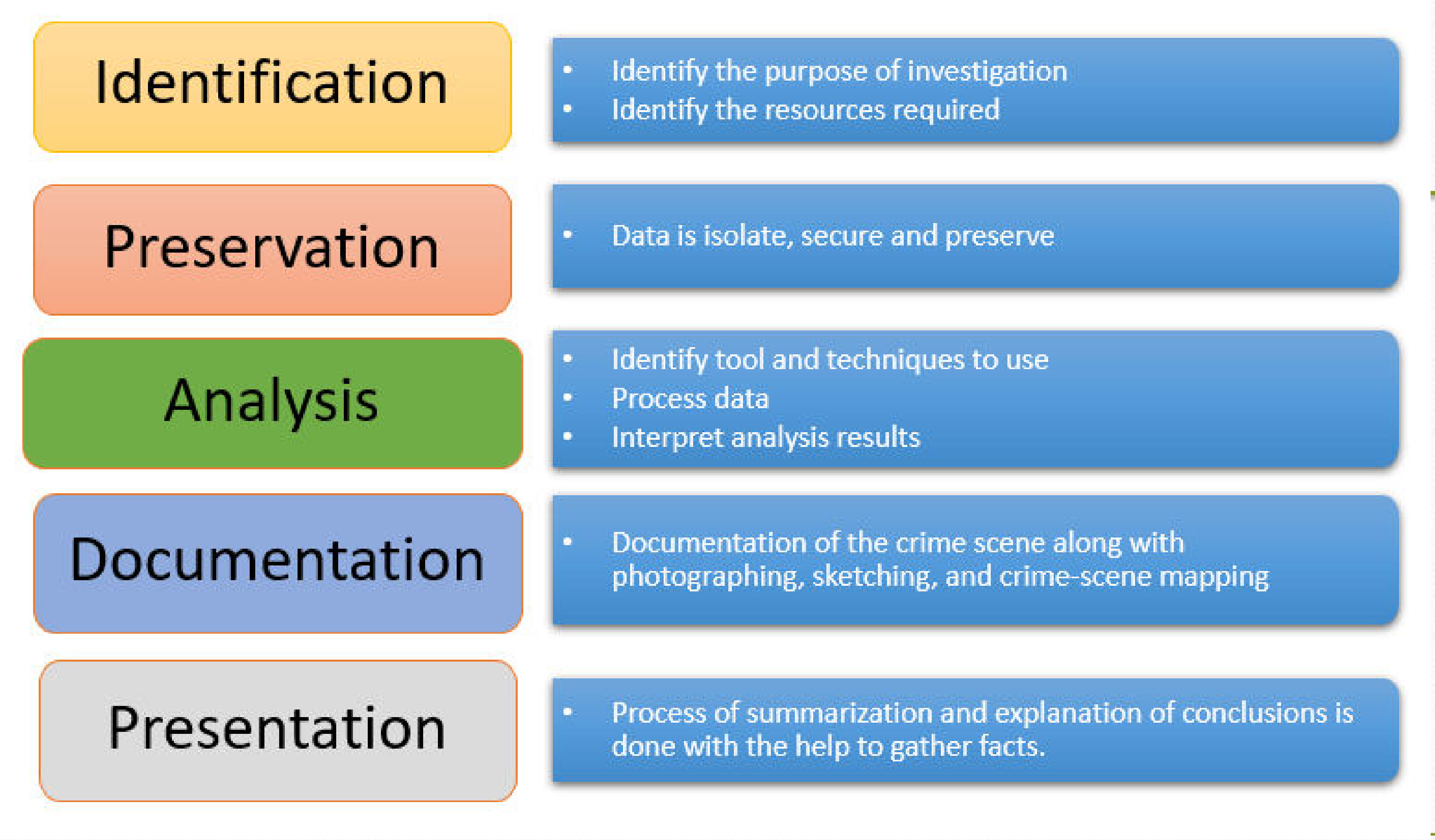
- **Rule 1.** An examination should never be performed on the original media.
  Rule 2. A copy is made onto forensically sterile media. New media should always be used if available.
- **Rule 3.** The copy of the evidence must be an exact, bit-by-bit copy. (Sometimes referred to as a bit-stream copy).
  Rule 4. The computer and the data on it must be protected during the acquisition of the media to ensure that the data is not modified. (Use a write blocking device when possible)
  Rule 5. The examination must be conducted in such a way as to prevent any modification of the evidence.
  Rule 6. The chain of the custody of all evidence must be clearly maintained to provide an audit log of whom might have accessed the evidence and at what time.

Goal of digital forensics

- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.

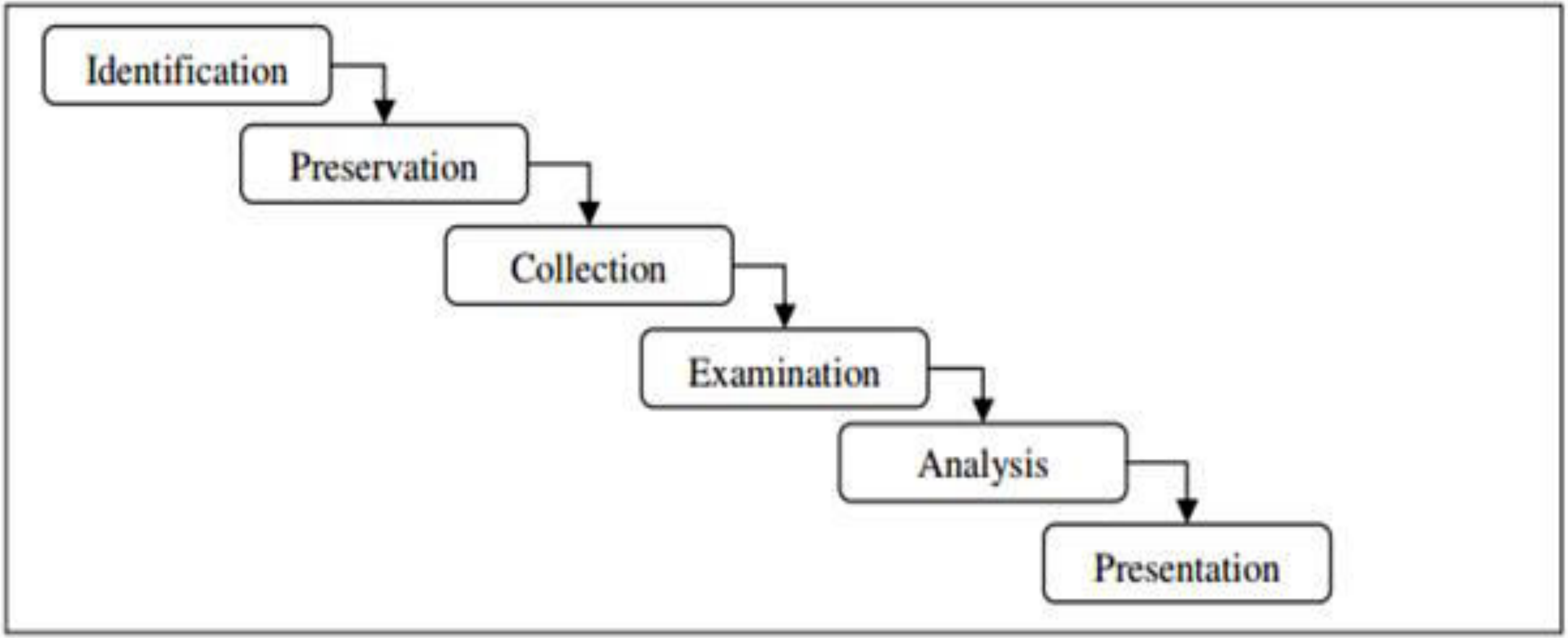
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.

Process of Digital forensics

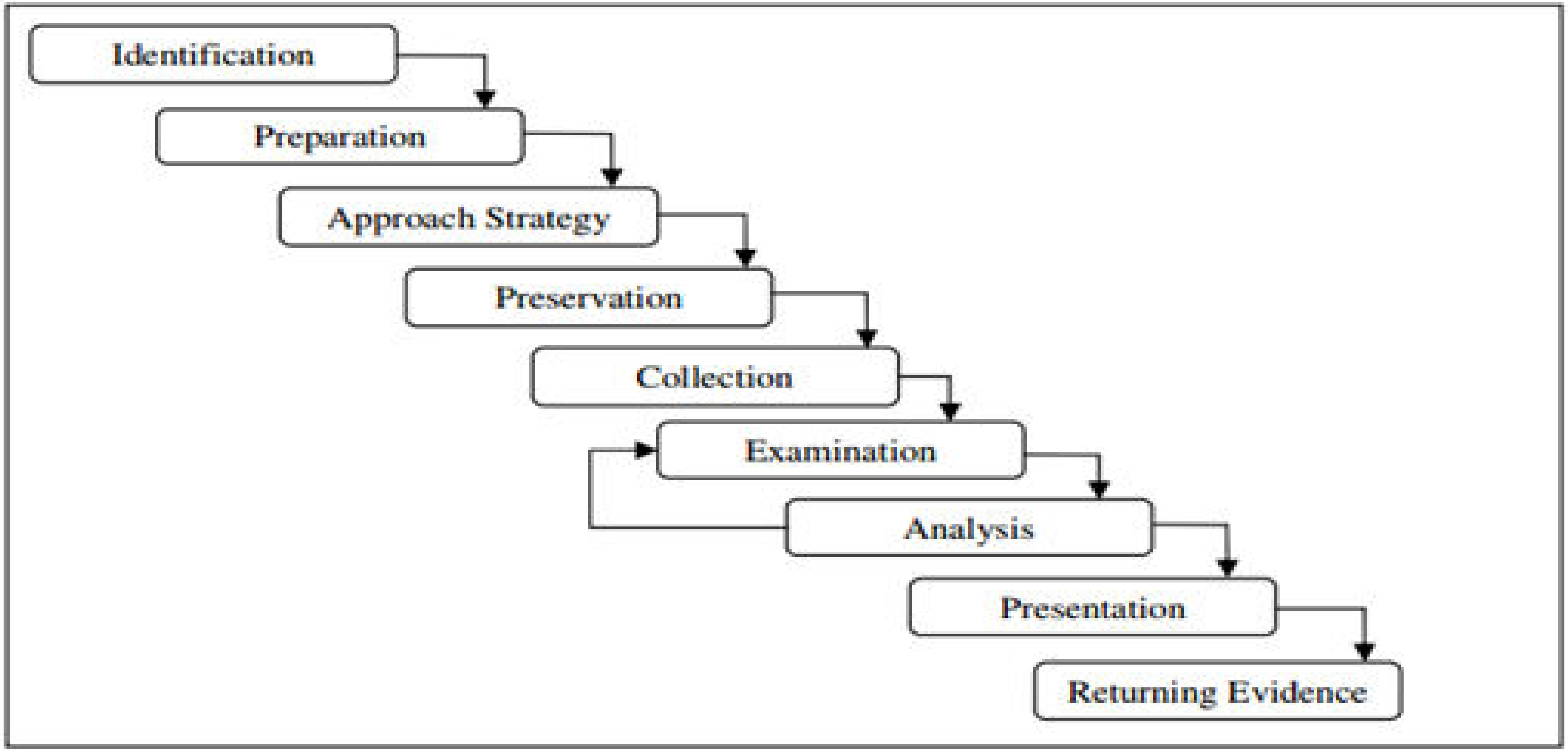


Identification	• Identify the purpose of investigation • Identify the resources required
Preservation	• Data is isolate, secure and preserve
Analysis	• Identify tool and techniques to use • Process data • Interpret analysis results
Documentation	• Documentation of the crime scene along with photographing, sketching, and crime-scene mapping
Presentation	• Process of summarization and explanation of conclusions is done with the help to gather facts.

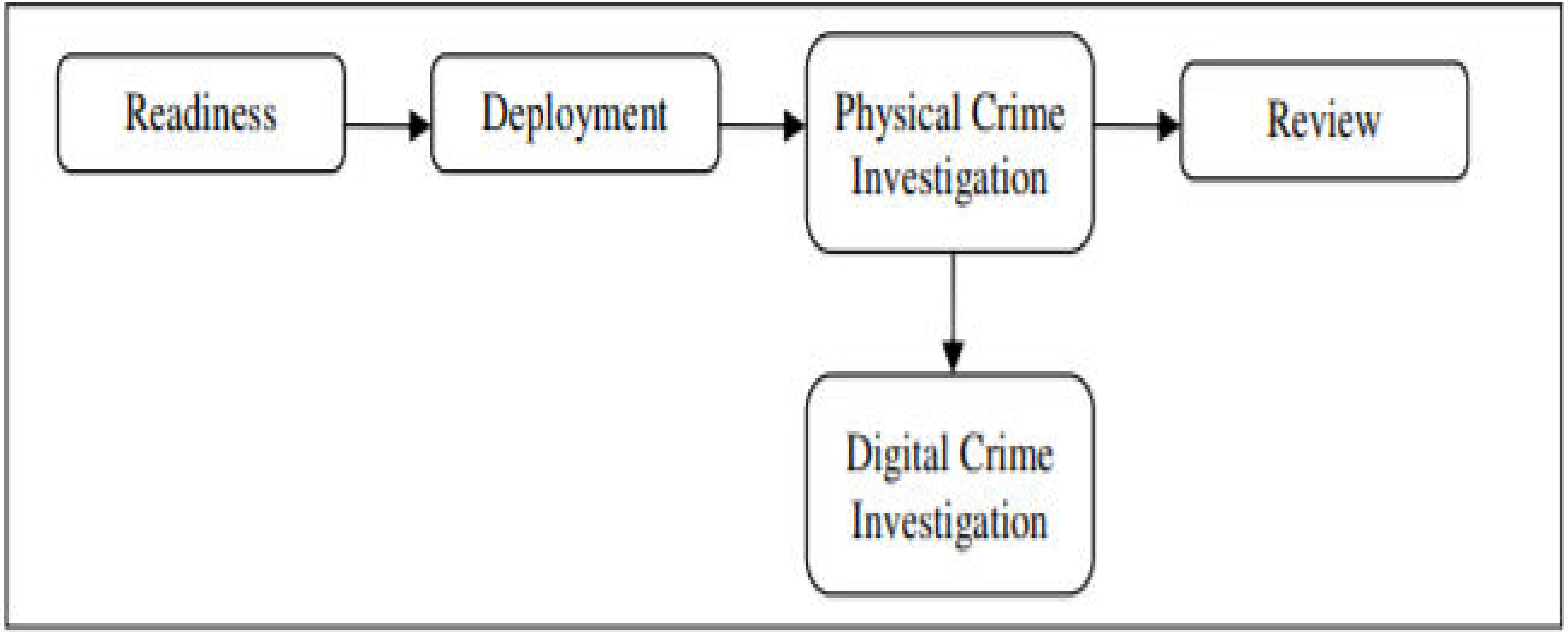
DFRWS Investigative Model



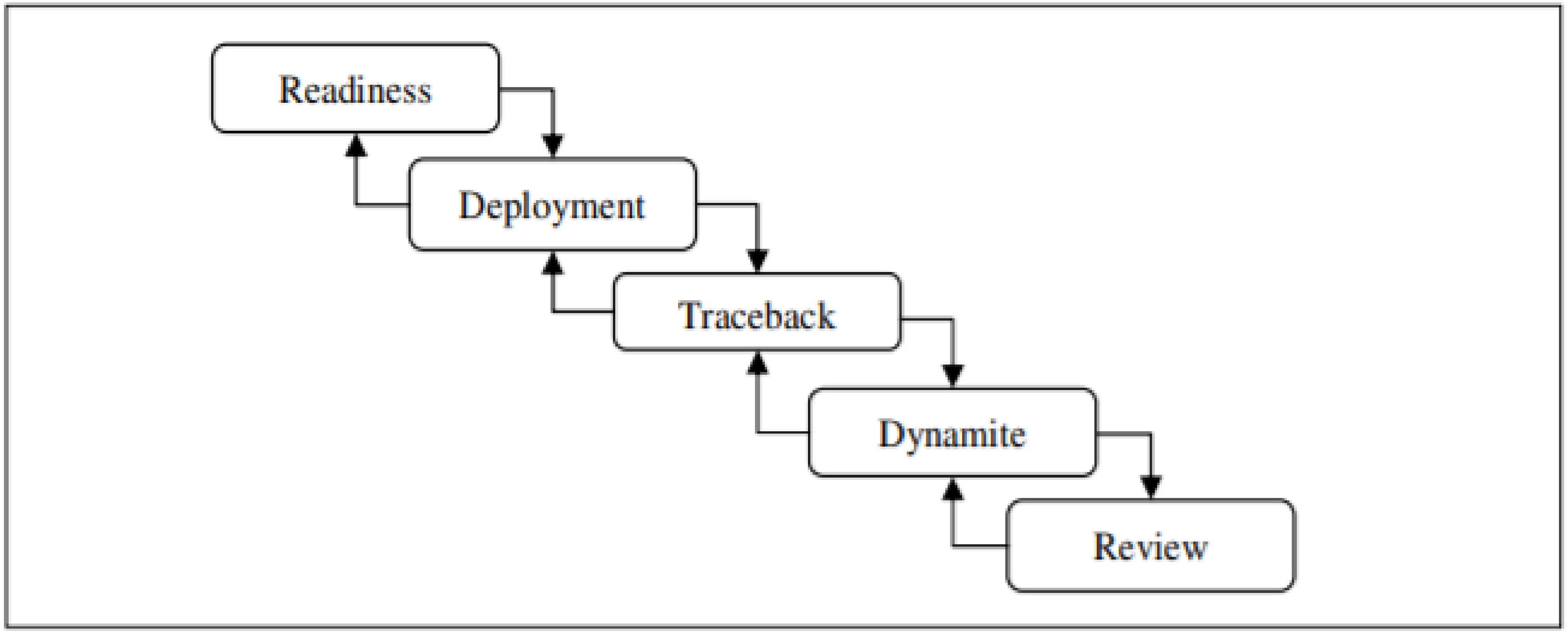
Abstract Digital Forensics Model (ADFM)



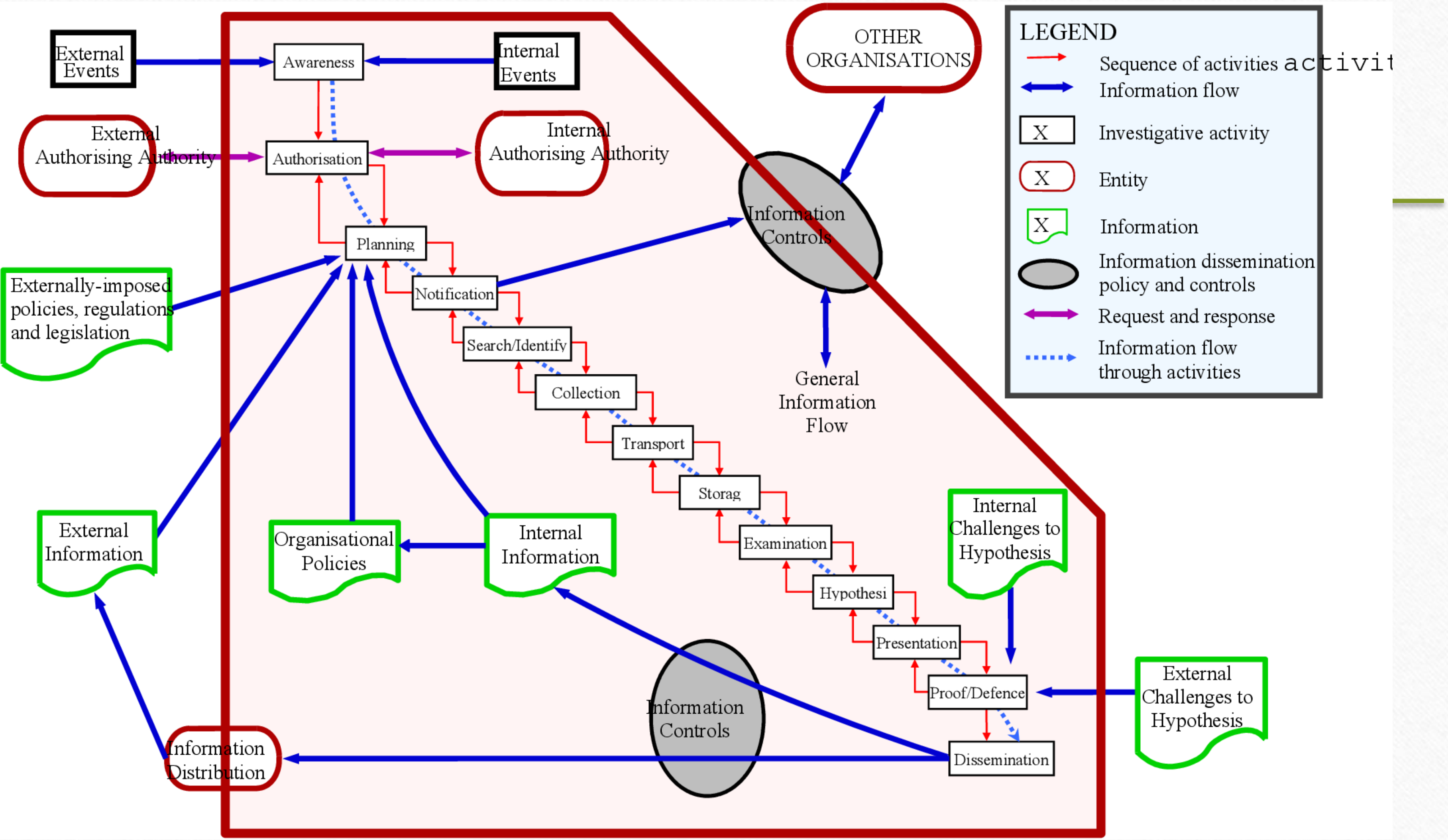
Integrated Digital Investigation Process (IDIP)



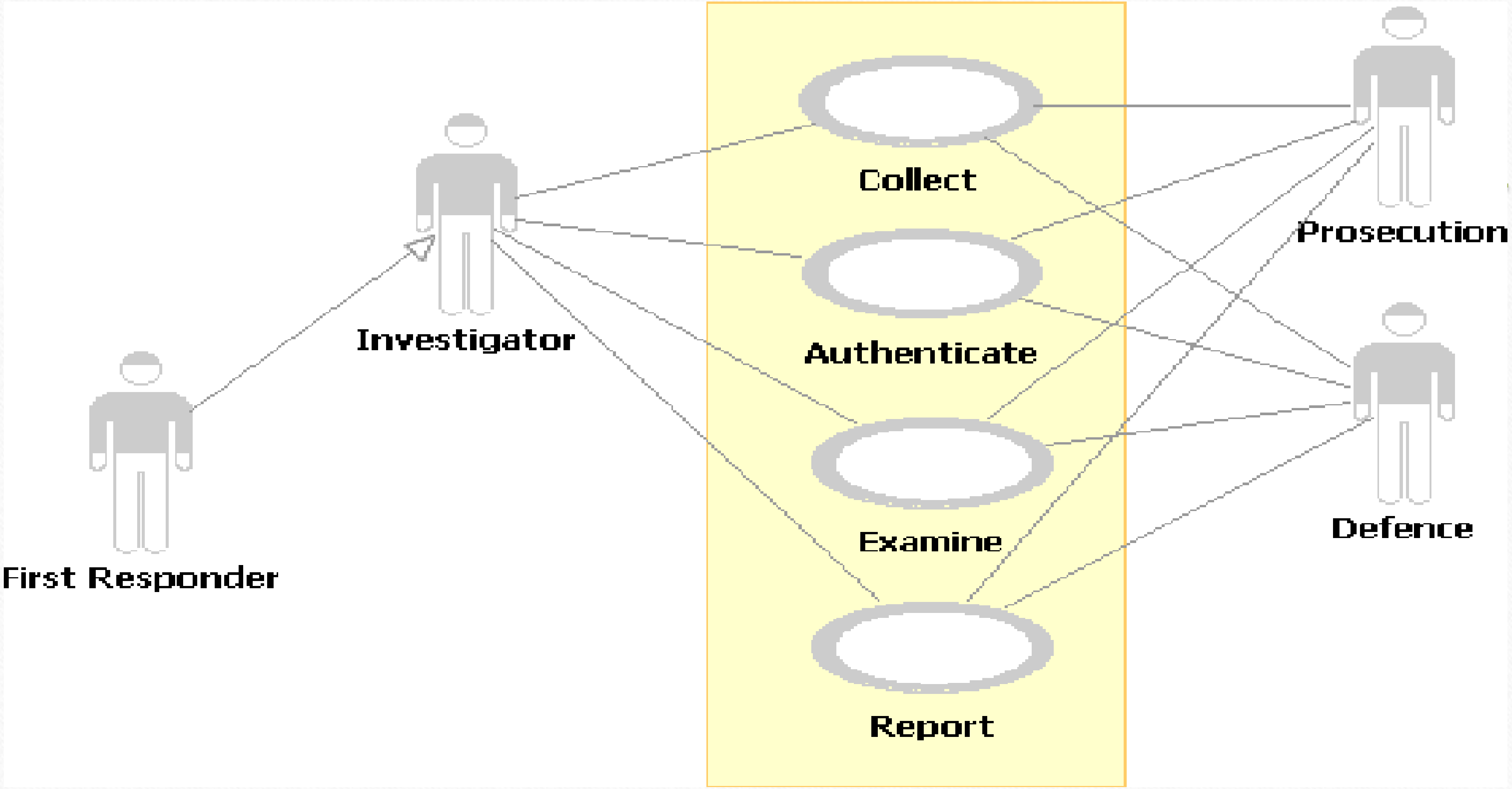
Enhanced Digital Investigation Process Model (EDIP)



An Extended Model of Cybercrime Investigations



Uml modeling of digital forensic process models



Ethical issues in digital forensics

- **Ethical issues in Digital Forensics**
- Honesty
- Fairness
- Good reputation
- Consistency
- Goodwill
- Proficiency
- A sense of community

- https://www.youtube.com/watch?v=ojwruJep8Cs

Unit 4: Digital Evidences

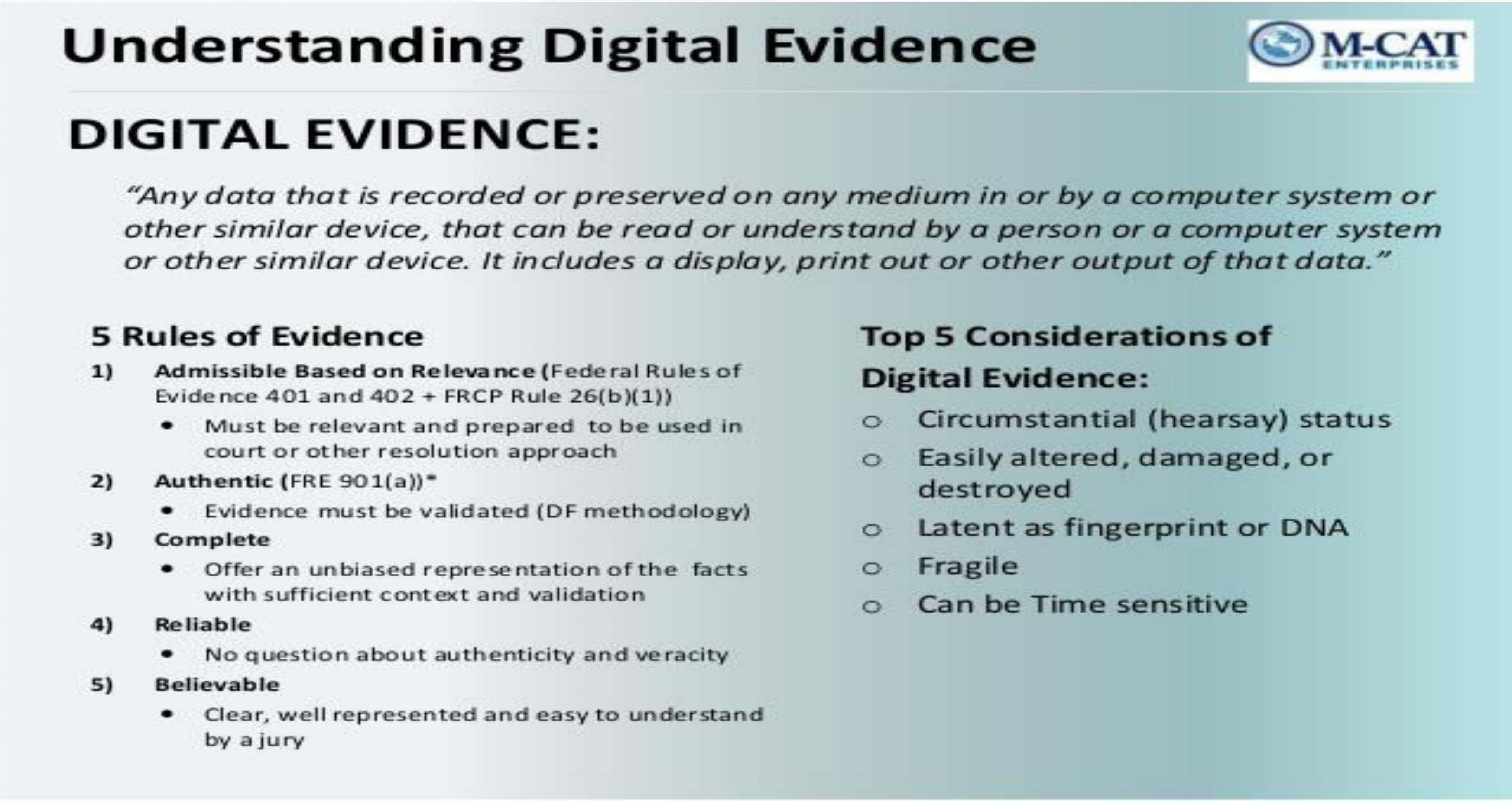
Course Outcome

Describe evidence handling procedures

Digital Evidences

- **Digital evidence**
- Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required.
- https://www.youtube.com/watch?v=03-0xADyv98
- Digital Signature
- https://www.youtube.com/watch?v=gQXnjZekPic

Rules of Digital evidences



Understanding Digital Evidence

M-CAT ENTERPRISES

DIGITAL EVIDENCE:

"Any data that is recorded or preserved on any medium in or by a computer system or other similar device, that can be read or understand by a person or a computer system or other similar device. It includes a display, print out or other output of that data."

5 Rules of Evidence

1) **Admissible Based on Relevance** (Federal Rules of Evidence 401 and 402 + FRCP Rule 26(b)(1))
   - Must be relevant and prepared to be used in court or other resolution approach
2) **Authentic** (FRE 901(a))*
   - Evidence must be validated (DF methodology)
3) **Complete**
   - Offer an unbiased representation of the facts with sufficient context and validation
4) **Reliable**
   - No question about authenticity and veracity
5) **Believable**
   - Clear, well represented and easy to understand by a jury

Top 5 Considerations of Digital Evidence:

- ○ Circumstantial (hearsay) status
- ○ Easily altered, damaged, or destroyed
- ○ Latent as fingerprint or DNA
- ○ Fragile
- ○ Can be Time sensitive

locard's exchange principle

- https://www.youtube.com/watch?v=NF8TEK63JTY
- Example
- https://www.youtube.com/watch?v=6xn9wPowHsI

Types of Evidences

- Illustrative evidences

https://www.youtube.com/watch?v=VrtXg8lyH4I

- Electronics evidences
- Documented evidences
- Explainable evidences
- Substantial evidences
- Testimonial evidences

Challenges in evidences handling

- Failure to adequately document the response to a computer security incident.

□ Properly retrieved evidence requires a paper trail.

□ Properly collecting evidence is a big challenge

□ Must be authenticated at a judicial proceedings and

1. Chain of custody for the evidence must be maintained.

Authentication of Evidence

- The many state laws, define computer data as “writings and recordings”.

□ Before they may be introduced into evidence, documents and recorded material must be authenticated.

□ Authentication, defined basically means that whomever collected the evidence should testify during direct examination that the information is what the proponent claims.

□ You meet the demands of authentication by ensuring that whomever collected the evidence is a matter of record.

Chain of Custody

- Maintaining chain of custody requires that collected evidence be stored in a tamper proof manner.
- Not to be accessed by unauthorized individuals.
- You need to maintain positive control (evidence within your possession or within your sight at all times) of all best evidence.
- Until it can be hand carried or shipped to evidence custodians for proper storage.
- Your organization's best evidence should always be stored within a safe or storage room that is inaccessible to anyone other than the appointed evidence custodian(s).
- Area referred to as an evidence safe

Evidence Validation

- volatile evidence (telephone numbers, voice mail, e-mail messages)

Unit 5: Basics of Hacking

Course Outcome

Describe Ethical Hacking Process

Ethical Hacking

https://www.youtube.com/watch?v=l77AgiphUQo