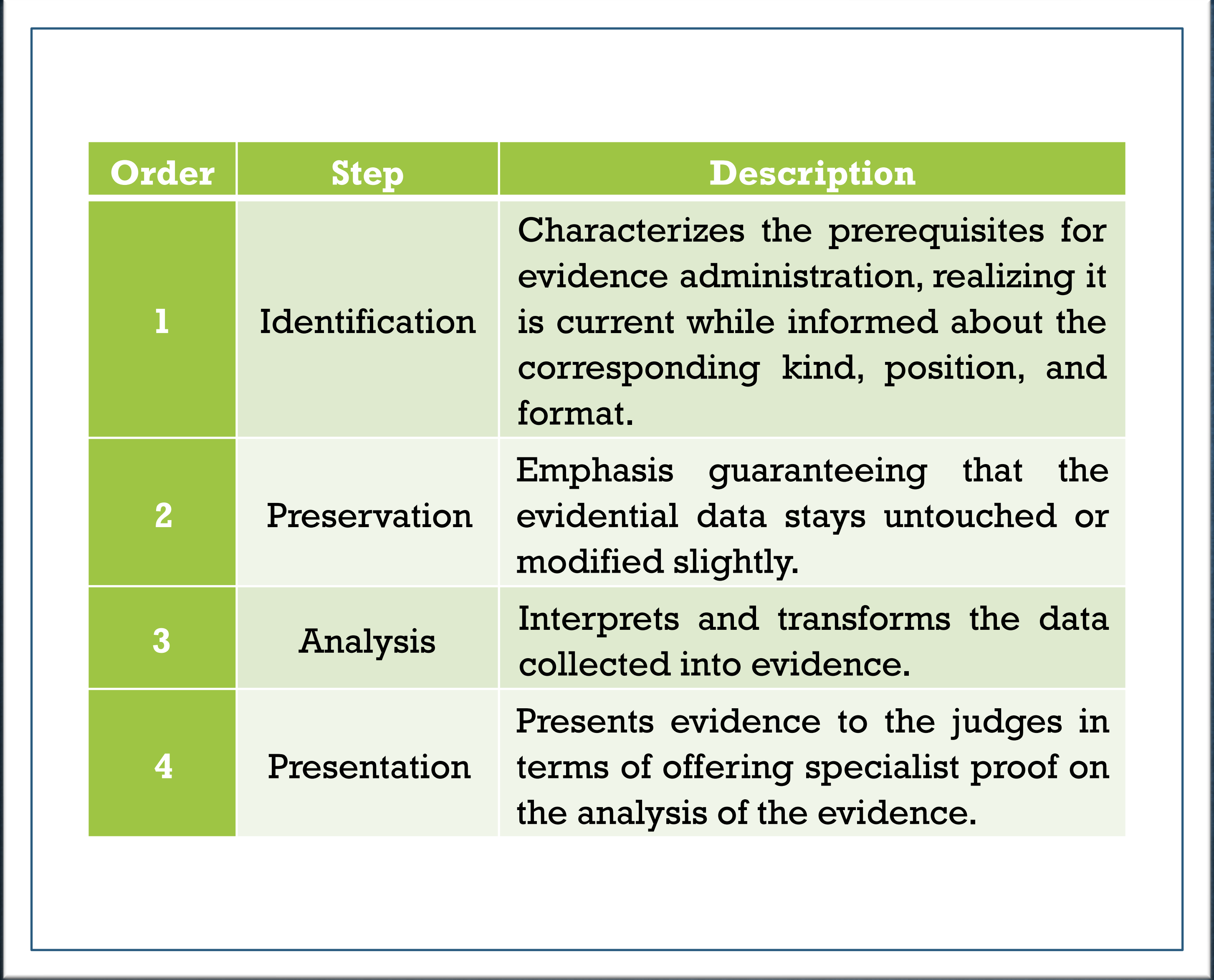
CHAPTER 4

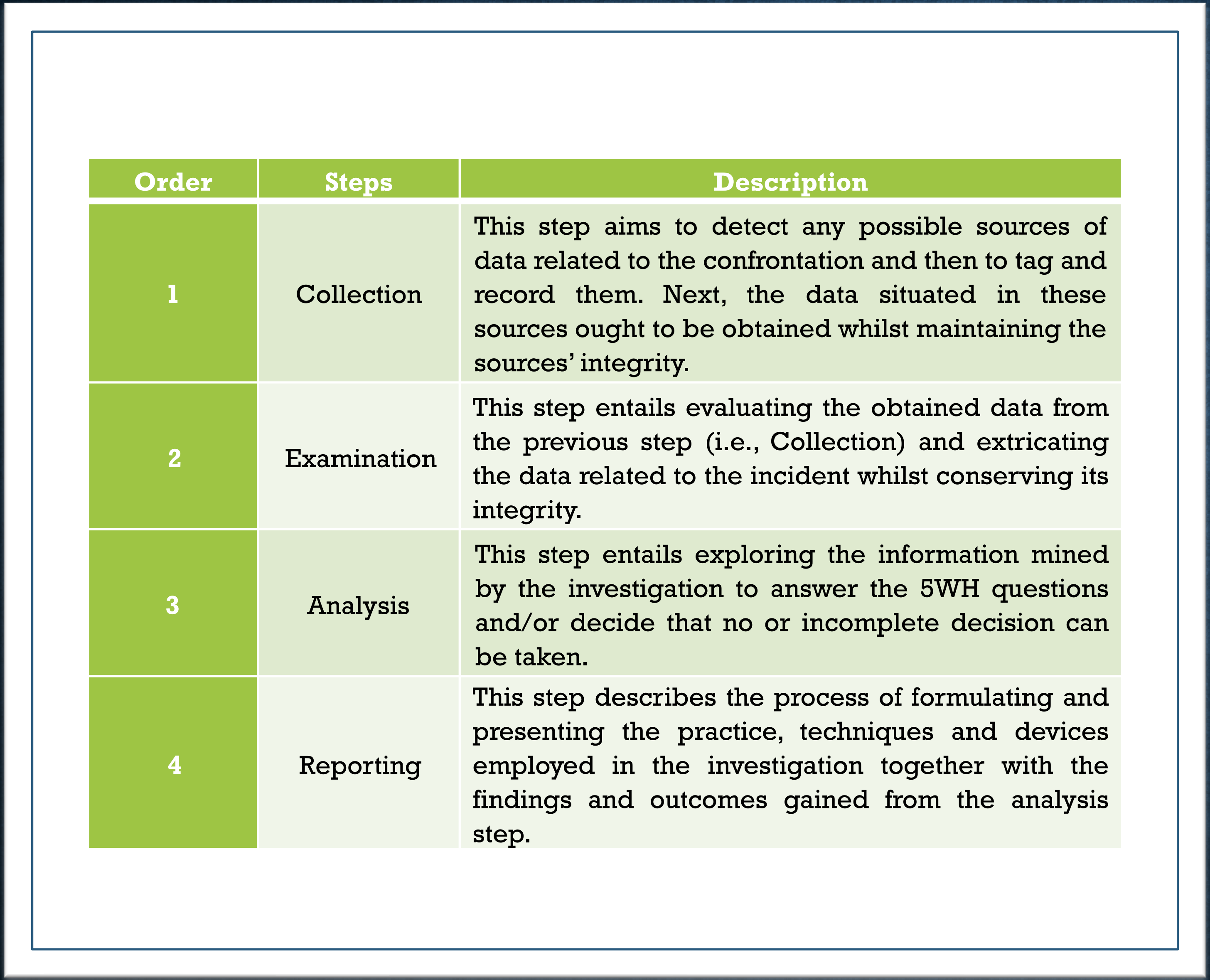
Digital Forensics in Internet of Things

WHAT IS DIGITAL FORENSIC?



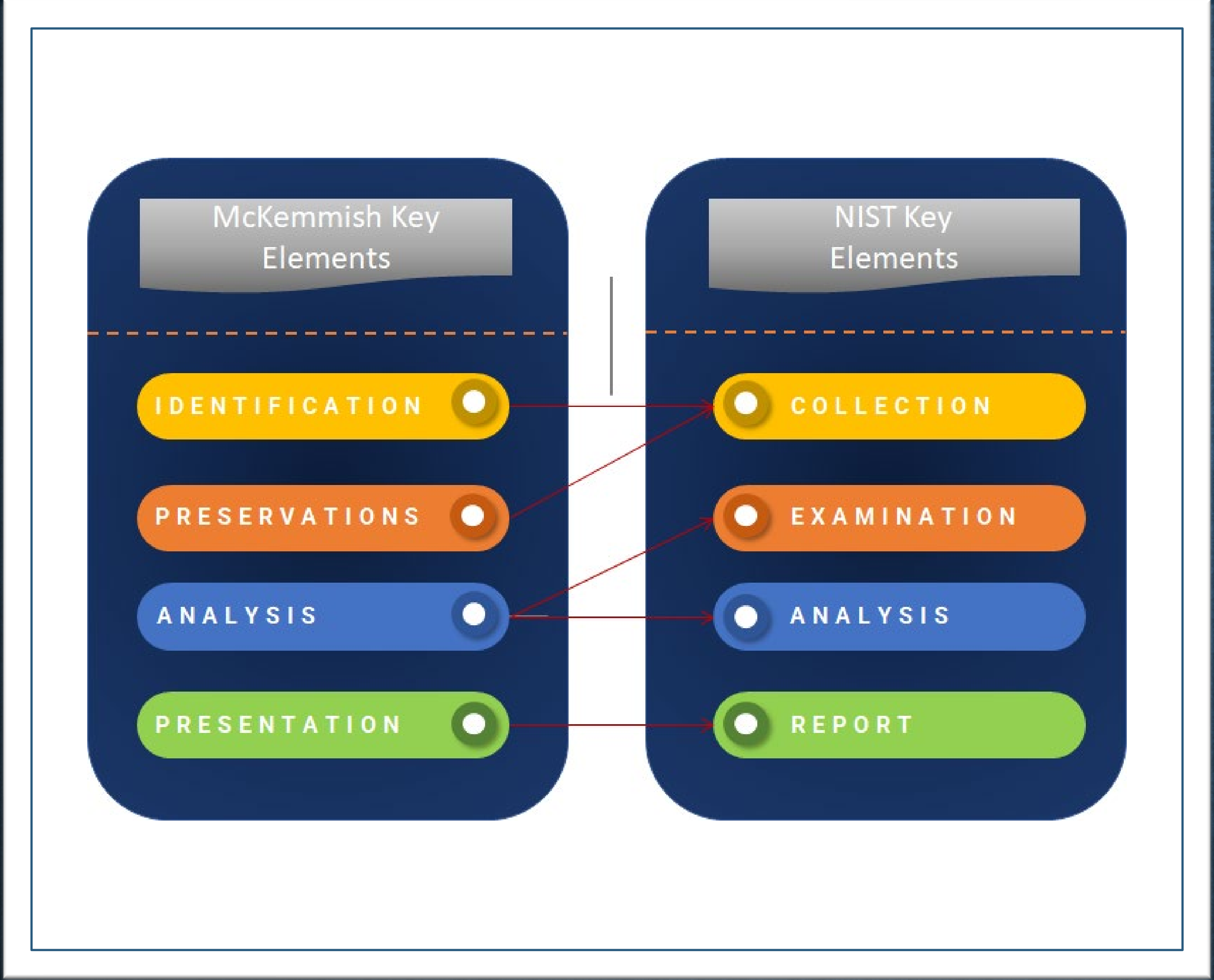
Order	Step	Description
1	Identification	Characterizes the prerequisites for evidence administration, realizing it is current while informed about the corresponding kind, position, and format.
2	Preservation	Emphasis guaranteeing that the evidential data stays untouched or modified slightly.
3	Analysis	Interprets and transforms the data collected into evidence.
4	Presentation	Presents evidence to the judges in terms of offering specialist proof on the analysis of the evidence.

WHAT IS DIGITAL FORENSIC?

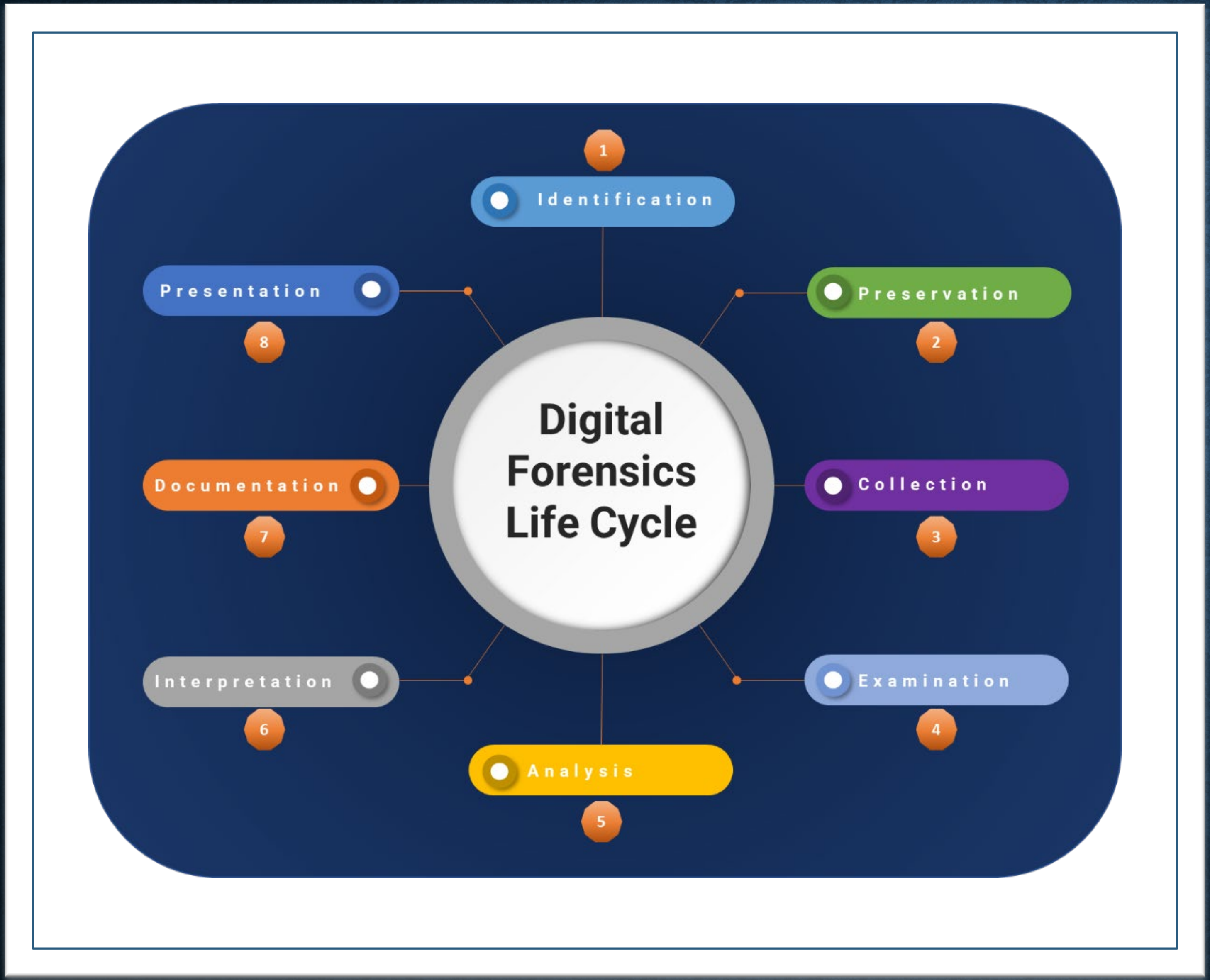


Order	Steps	Description
1	Collection	This step aims to detect any possible sources of data related to the confrontation and then to tag and record them. Next, the data situated in these sources ought to be obtained whilst maintaining the sources' integrity.
2	Examination	This step entails evaluating the obtained data from the previous step (i.e., Collection) and extricating the data related to the incident whilst conserving its integrity.
3	Analysis	This step entails exploring the information mined by the investigation to answer the 5WH questions and/or decide that no or incomplete decision can be taken.
4	Reporting	This step describes the process of formulating and presenting the practice, techniques and devices employed in the investigation together with the findings and outcomes gained from the analysis step.

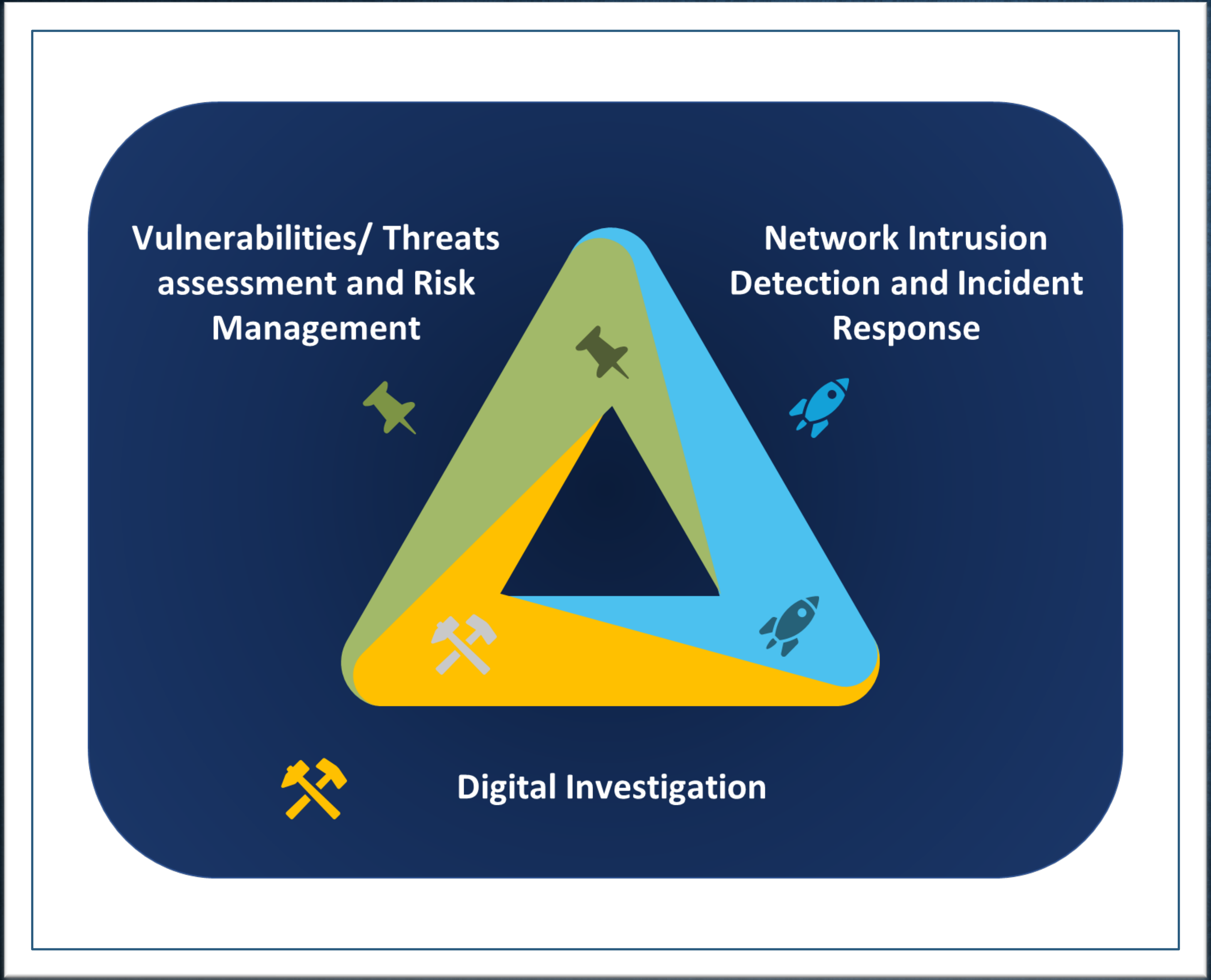
MCKEMMISH NIST KEY ELEMENTS



DIGITAL FORENSIC LIFE CYCLE



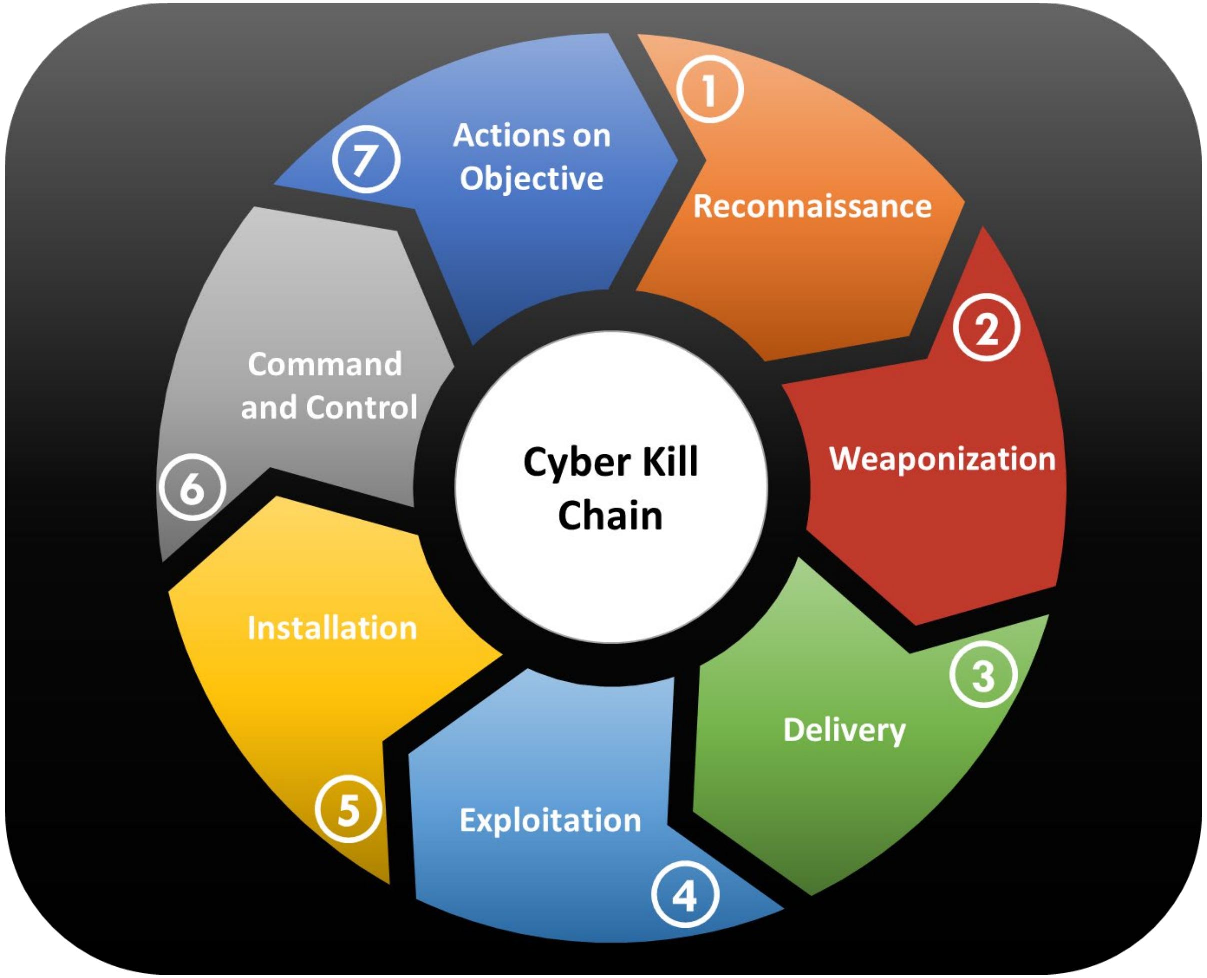
DIGITAL EVIDENCE



Vulnerabilities/ Threats assessment and Risk Management

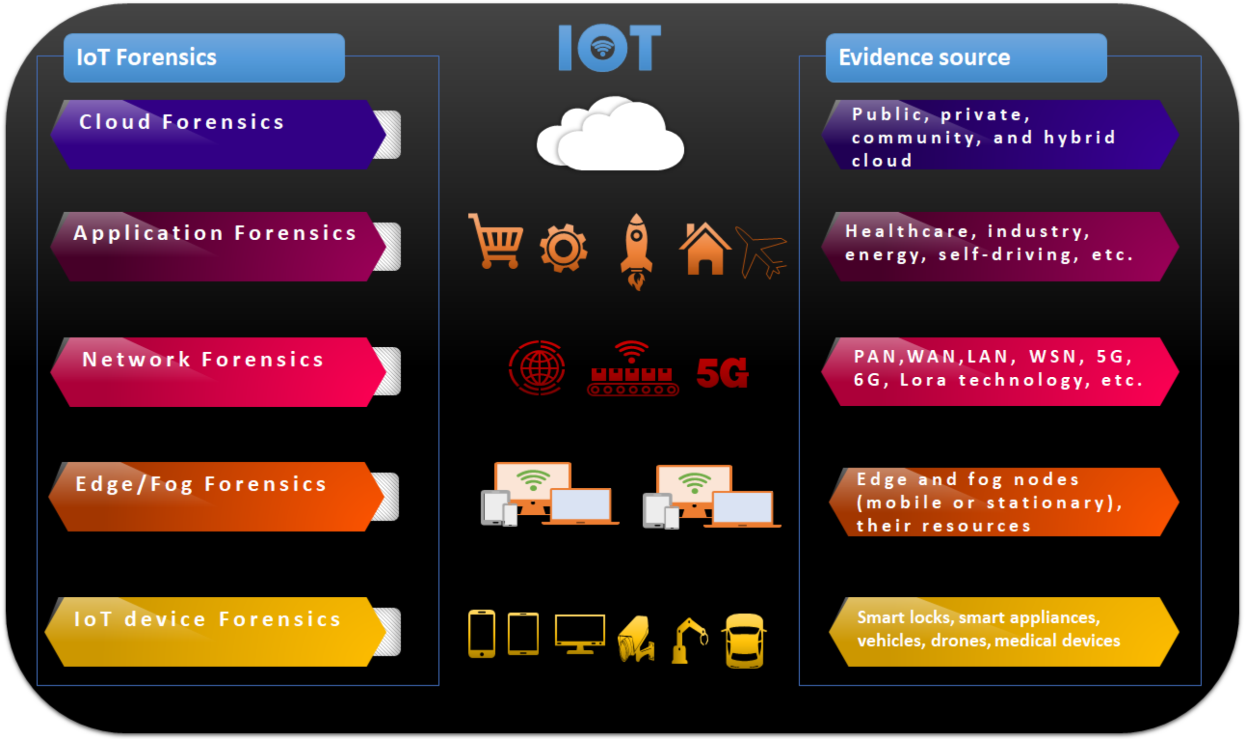
Network Intrusion Detection and Incident Response

Digital Investigation



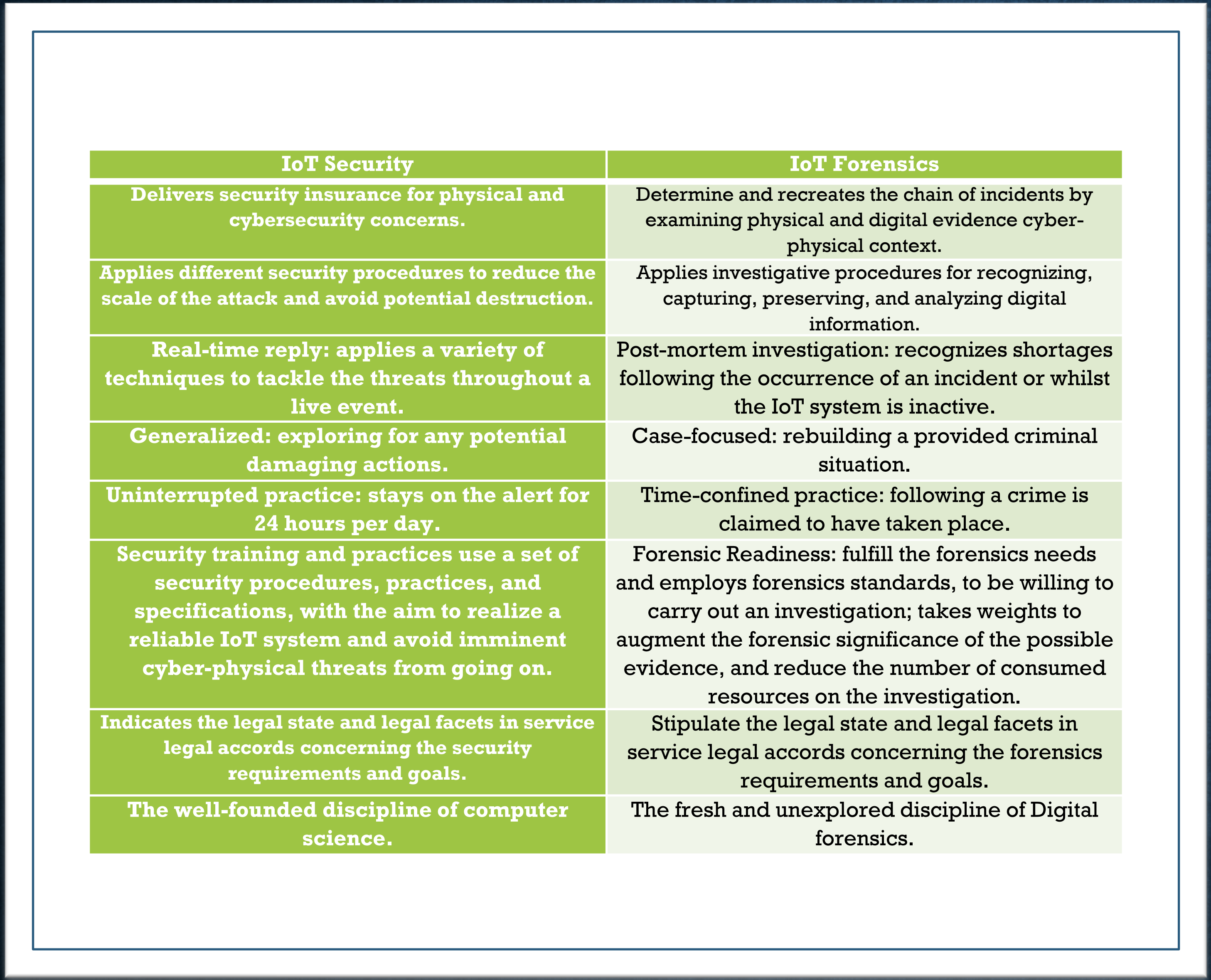
THE CYBER KILL CHAIN

IOT FORENSICS



IoT Forensics	Evidence source
Cloud Forensics	Public, private, community, and hybrid cloud
Application Forensics	Healthcare, industry, energy, self-driving, etc.
Network Forensics	PAN,WAN,LAN, WSN, 5G, 6G, Lora technology, etc.
Edge/Fog Forensics	Edge and fog nodes (mobile or stationary), their resources
IoT device Forensics	Smart locks, smart appliances, vehicles, drones, medical devices

SECURITY VS FORENSICS



IoT Security	IoT Forensics
Delivers security insurance for physical and cybersecurity concerns.	Determine and recreates the chain of incidents by examining physical and digital evidence cyber-physical context.
Applies different security procedures to reduce the scale of the attack and avoid potential destruction.	Applies investigative procedures for recognizing, capturing, preserving, and analyzing digital information.
Real-time reply: applies a variety of techniques to tackle the threats throughout a live event.	Post-mortem investigation: recognizes shortages following the occurrence of an incident or whilst the IoT system is inactive.
Generalized: exploring for any potential damaging actions.	Case-focused: rebuilding a provided criminal situation.
Uninterrupted practice: stays on the alert for 24 hours per day.	Time-confined practice: following a crime is claimed to have taken place.
Security training and practices use a set of security procedures, practices, and specifications, with the aim to realize a reliable IoT system and avoid imminent cyber-physical threats from going on.	Forensic Readiness: fulfill the forensics needs and employs forensics standards, to be willing to carry out an investigation; takes weights to augment the forensic significance of the possible evidence, and reduce the number of consumed resources on the investigation.
Indicates the legal state and legal facets in service legal accords concerning the security requirements and goals.	Stipulate the legal state and legal facets in service legal accords concerning the forensics requirements and goals.
The well-founded discipline of computer science.	The fresh and unexplored discipline of Digital forensics.