DIGITAL FORENSICS & CYBERSECURITY DATABASE

Data Book : Part-1 : Narrative

In this modern digitalized era, cyber threats are rapidly changing concerns, so it's crucial for organizations, law enforcement, and cybersecurity firms to keep track of and analyze these threats effectively. The Digital Forensics & Cybersecurity Databook is a centralized system that helps manage cyber incidents, track digital evidence, and comply with security regulations. By organizing data systematically, the database helps in investigative capabilities and allows organizations to respond proactively to cybersecurity threats. Imagine a cybersecurity firm investigating a series of ransomware attacks on financial institutions. With a well-organized database, analysts can record each incident, identify related threats, and track evidence gathered during forensic analysis.

The INCIDENT table logs attack details, linking them to known cyber threats in the THREAT table. Analysts are tracked in ANALYST table, and the forensic tools they use, like network traffic analyzers, are logged in TOOL table. Digital evidence, such as log files and malware samples, is stored securely in EVIDENCE table, maintaining the integrity of the investigation. Beyond investigations, this database plays a crucial role in regulatory compliance. Companies following frameworks like GDPR, HIPAA, or ISO 27001 must ensure their cybersecurity protocols meet legal requirements. The REGULATION table helps map security incidents to compliance standards. Each security breach is evaluated against relevant regulations, and compliance status is updated in REGULATORY_COMPLIANCE table, making it easy for auditors to review past events.

Training and preparedness are essential in cybersecurity. Investigators and analysts regularly update their skills to stay ahead of new threats. The TRAINING table logs specialized training attended by professionals. Analysts who complete certifications in areas like malware analysis have their credentials recorded in ATTENDANCE, allowing organizations to track their workforce's expertise. Collaboration is another key aspect of effective cybersecurity. Agencies often work together to counteract sophisticated cybercriminal networks. The PARTNERSHIP table records collaborations, whether for intelligence sharing or joint

investigations. By maintaining structured records of these partnerships, agencies can improve coordination and enhance their response to cyber threats.

The database's efficiency is reinforced by its Real time updating capabilities. When an incident is reported, its status is immediately updated, ensuring that investigators have access to the most current information. Digital evidence is logged with timestamps, ensuring its admissibility in legal proceedings. Analysts can seamlessly retrieve data, reducing the risk of fragmented investigations and miscommunication.

The bridge tables facilitate critical many-to-many relationships and enhance operational efficiency. ANALYST_TOOL tracks which tools analysts use, including the last usage date, while EVIDENCE_TOOL maps tools to evidence analysis with timestamps for forensic integrity. INCIDENT_PARTNERSHIP links incidents to partnerships, categorizing collaboration levels (Low/Medium/High), and INCIDENT_ASSIGNMENT assigns analysts to incidents, specifying roles and assignment dates for accountability. ANALYST_TRAINING_ATTENDANCE logs training participation, completion status, and dates to monitor skill development and compliance. Lastly, FORENSIC_SPECIALIST extends analysts' profiles with certifications, specialty areas, and lab access levels, ensuring expertise is effectively utilized in complex investigations. Together, these tables streamline resource tracking, collaboration, and regulatory compliance in cybersecurity workflows.

Data integrity is vital in this system. Each table follows strict database normalization rules, preventing anomalies and maintaining accurate records. The system enforces relationships such as one-to-many (1:M) between threats and incidents, many-to-many (M:N) between analysts and tools, and one-to-one (1:1) between analysts and their assigned roles. To avoid inconsistencies, placeholders like "Former Analyst" or "Unknown Threat" are used instead of null values, ensuring that historical data remains intact even when personnel changes or new cyber threats arise. As cyber threats continue to evolve, the need for a robust and scalable forensic database becomes more critical. This database is designed for current threat tracking and future enhancements, such as AI-driven predictive analysis and automated compliance auditing. With its comprehensive structure, the

Digital Forensics & Cybersecurity Databook empowers organizations to combat cyber threats efficiently while maintaining a strong legal and regulatory foundation.

Data Dictionary:

Table Name	Attribute Name	Contents	Data Type	Format	Range	Required	PK/FK	Reference
TOOL_TYPE	TOOL_TYPE_ID	Unique identifier for toold types	SMALLINT	999	1-999	Y	PK	
	TOOL_TYPE_NAME	Name of the tool category	VARCHAR (100)	xxxx		Y		
	TOOL_TYPE_DESCRIPTION	Description of the tool category	VARCHAR (255)	xxxx		Y		
	TOOL_TYPE_CREATED_DATE	Date when this type was added	DATE	YYYY-MM-DD		Y		
THREAT	THREAT_ID	Unique identifier for a cyber threat	SMALLINT	9999	1-99999…	Y	PK	
	THREAT_NAME	Name of the cyber threat type	VARCHAR (255)	xxxxx		Y		
	THREAT_TYPE	Category of the threat	VARCHAR (100)	xxxx		Y		
	THREAT_SEVERITY_LEVEL	Describes the severity of the threat	ENUM	H/M/L		Y		
	THREAT_REPORTED_DATE	Date when the threat was first reported	DATE	YYYY-MM-DD		Y		

Table Name	Attribute Name	Contents	Data Type	Format	Range	Required	PK/FK	Reference
INCIDENT	INCIDENT_ID	Unique identifier for a cyber incident	SMALLINT	9999	1-99…	Y	PK	
	THREAT_ID	Associated cyber threat	SMALLINT	9999	1-99…	Y	FK	THREAT
	INCIDENT_DATE	Date of the incident occurrence	DATE	YYYY-MM-DD		Y		
	INCIDENT_IMPACT_LEVEL	Level of damage caused (Low, Medium, High)	ENUM	H/M/L		Y		
	INCIDENT_RESOLUTION_STATUS	Status of the incident (Open, Resolved)	VARCHAR (30)	xxxxx		Y		
EVIDENCE	EVIDENCE_ID	Unique identifier for digital evidence	SMALLINT	999	1-99…	Y	PK	
	INCIDENT_ID	Associated cyber incident	SMALLINT	99	1-99…	Y	FK	INCIDENT
	EVIDENCE_TYPE	Type of evidence	VARCHAR (50)	xxxx		Y		

Table Name	Attribute Name	Contents	Data Type	Format	Range	Required	PK/FK	Reference
	EVIDENCE_STORAGE_LOCATION	Secure storage location of the evidence	VARCHAR (200)	xxxx		Y		
	EVIDENCE_INTEGRITY_HASH	Cryptographic hash for verification	CHAR (64)	xxxxx		Y		
ANALYST	ANALYST_ID	Unique identifier for a cyber analyst	SMALLINT	9999	1-99…	Y	PK	
	ANALYST_NAME	Analyst's full name	VARCHAR (100)	xxxxx		Y		
	ANALYST_ROLE	Job title of the analyst	VARCHAR (50)			Y		
	ANALYST_CONTACT_INFO	Contact email of the analyst	VARCHAR (100)	xxxxx		Y		
	ANALYST_EXPERIENCE	Work experience of the analyst	SMALLINT	9	1-99…	Y		
TOOL	TOOL_ID	Unique identifier for forensic tools	SMALLINT	9999	1-999…	Y	PK	

Table Name	Attribute Name	Contents	Data Type	Format	Range	Required	PK/FK	Reference
	TOOL_TYPE	Unique identifier of tool type	SMALLINT	9999	1-999…	Y	FK	TOOL_TYPE
	TOOL_NAME	Name of the forensic tool	VARCHAR (100)	xxxxx		Y		
	TOOL_VENDOR	Manufacturer of the tool	VARCHAR (100)	xxxx		Y		
	TOOL_LICENSE_EXP_DATE	Expiry date of the tool's license	DATE	YYYY-MM-DD		Y		
TRAINING	TRAINING_ID	Unique identifier for a training program	SMALLINT	999	1-999….	Y	PK	
	TRAINING_NAME	Name of the training program	VARCHAR(100)	xxxxx		Y		
	TRAINING_TYPE	Type of training (Malware Analysis, Forensics)	VARCHAR(50)	xxxxx		Y		
	TRAINING_DURATION	Duration of the training program	SMALLINT	999	1-99….	Y		

Table Name	Attribute Name	Contents	Data Type	Format	Range	Required	PK/FK	Reference
	TRAINING_PROVIDER	Organization conducting the training	VARCHAR(100)	xxxxx		Y		
PARTNERSHIP	PARTNERSHIP_ID	Unique identifier for a partnership	MEDIUMINT	99999	1-99…	Y	PK	
	PARTNERSHIP_AGENCY_NAME	Name of the collaborating agency	VARCHAR(100)	xxxxx		Y		
	PARTNERSHIP_TYPE	Type of partnership (Intel Sharing, Joint Investigation)	VARCHAR(50)	xxxxx		Y		
	PARTNERSHIP_START_DATE	Date when the partnership started	DATE	YYYY-MM-DD		Y		
	PARTNERSHIP_END_DATE	End date of the partnership	DATE	YYYY-MM-DD		Y		
REGULATORY_COMPLIANCE	REGULATORY_COMPLIANCE _ID	Unique identifier for compliance check	SMALLINT	999	1-99….	Y	PK	
	REGULATION_ID	Associated compliance framework	SMALLINT	9999	1-99…	Y	FK	REGULATION

Table Name	Attribute Name	Contents	Data Type	Format	Range	Required	PK/FK	Reference
	INCIDENT_ID	Associated cyber incident	SMALLINT	9999	1-999…	Y	FK	INCIDENT
	REGULATORY_COMPLIANCE _STATUS	Status (Compliant, Non-Compliant)	ENUM	C/NC		Y		
	REGULATORY_COMPLIANCE_AUDIT_DATE	Date of last compliance audit	DATE	YYYY-MM-DD		Y		
ATTACK_PATTERN	ATTACK_PATTERN _ID	Unique identifier for an attack pattern	SMALLINT	9999	1-99…	Y	PK	
	THREAT_ID	Associated cyber threat	SMALLINT	999	1-999….	Y	FK	THREAT
	ATTACK_PATTERN _VECTOR	Method used in the attack (Phishing, SQL Injection)	VARCHAR(100)	xxxxx		Y		
	ATTACK_PATTERN _DETECTION_METHOD	Technique used to detect the attack	VARCHAR(100)	xxxxx		Y		

Table Name	Attribute Name	Contents	Data Type	Format	Range	Required	PK/FK	Reference
	ATTACK_PATTERN_COUNTERMEASURE	Recommended mitigation strategy	VARCHAR(100)	xxxxx		Y		
ATTENDANCE	ATTENDANCE_ID	Unique identifier for training attendance	SMALLINT	999	1-99…	Y	PK	
	ANALYST_ID	Analyst attending the training	SMALLINT	999	1-99…	Y	FK	ANALYST
	TRAINING_ID	Attended training program	SMALLINT	999	1-99..	Y	FK	TRAINING
	ATTENDANCE_COMPLETION_STATUS	Status (Completed, In Progress)	VARCHAR(20)	xxxx		Y		
	ATTENDANCE_CERTIFICATION	Type of certification received (if any)	VARCHAR(50)	xxxx		Y		
	REGULATION_ID	Unique identifier for a regulation	SMALLINT	999	1-99…	Y	PK	

Table Name	Attribute Name	Contents	Data Type	Format	Range	Required	PK/FK	Reference
REGULATION	REGULATION_NAME	Name of the compliance framework	VARCHAR(100)	xxxx		Y		
	REGULATION_COMPLIANCE_STANDARD	Compliance category (GDPR, HIPAA)	VARCHAR(50)	xxxxx		Y		
	REGULATION_EFFECTIVE_DATE	Date when the regulation became effective	DATE	YYYY-MM-DD		Y		
	REGULATION_ISSUING_AGENCY	Organization that issued the regulation	VARCHAR(100)	YYYY-MM-DD		Y		
ANALYST_TOOL	TOOL_ID	Unique identifier for analyst tool	SMALLINT	999	1-99…	Y	PK/FK	TOOL
	ANALYST_ID	Analyst using the forensic tool	SMALLINT	999	1-99…	Y	PK/FK	ANALYST
	ANALYST_TOOL_LAST_USED_DATE	Tool last used date	DATE	YYYY-MM-DD		Y		
INCIDENT_PARTNERSHIP	INCIDENT_ID	Associated incident id	SMALLINT	999	1-99…	Y	PK/FK	INCIDENT

Table Name	Attribute Name	Contents	Data Type	Format	Range	Required	PK/FK	Reference
	PARTNERSHIP_ID	Associated partnership id	SMALLINT	999	1-99…	Y	PK/FK	PARTNERSHIP
	INCIDENT_PARTNERSHIP_COLLABORATION_LEVEL	Level of partnership involvement	ENUM	Low, Medium, High		Y		
ANALYST_TRAINING_ATTENDANCE	ANALYST_ID	Unique identifier for analyst	SMALLINT	999	1-99…	Y	PK/FK	ANALYST
	TRAINING_ID	Unique attendance for training	SMALLINT	999	1-99…	Y	PK/FK	TRAINING
	ANALYST_TRAINING_ATTENDANCE_DATE	Date of Training	DATE	YYYY-MM-DD		Y		
	ANALYST_TRAINING_ATTENDANCE_COMPLETION_STATUS	Status of the training	VARCHAR(20)	Xxxxx		Y		
EVIDENCE_TOOL	EVIDENCE_ID	Unique identifier of evidence	SMALLINT	999	1-99…	Y	PK/FK	EVIDENCE

Table Name	Attribute Name	Contents	Data Type	Format	Range	Required	PK/FK	Reference
	TOOL_ID	Unique identifier of tool	SMALLINT	999	1-99…	Y	PK/FK	TOOL
	EVIDENCE_TOOL_ANALYSIS_DATE	Date of analysis date	DATE	YYYY-MM-DD		Y		
INCIDENT_ASSIGNMENT	INCIDENT_ID		SMALLINT	999	1-99…	Y	PK/FK	INCIDENT
	ANALYST_ID		SMALLINT	999	1-99…	Y	PK/FK	ANALYST
	INCIDENT_ASSIGNMENT_DATE		DATE	YYYY-MM-DD		Y		
	INCIDENT_ASSIGNMENT_ROLE		VARCHAR(50)	Xxxx		Y		
FORENSIC_SPECIALIST	ANALYST_ID	Unique identifier (inherited from ANALYST)	SMALLINT	999	1-99…	Y	PK/FK	ANALYST
	FORENSIC_SPECIALIST_CERT	Forensic certification	VARCHAR(100)	Xxxx		Y		

Table Name	Attribute Name	Contents	Data Type	Format	Range	Required	PK/FK	Reference
	FORENSIC_SPECIALIST_SPECIALTY_AREA	Area of forensic specialty	VARCHAR(100)	Xxxx		Y		
	FORENSIC_SPECIALIST_LAB_ACCESS_LEVEL	Security clearance level for lab access	VARCHAR(20)	Xxxxx		Y		

Entity-Relationship Model (ERM): Digital Forensics & Cybersecurity Database

ENTITY	RELATIONSHIP	CONNECTIVITY	ENTITY
THREAT	…triggers…	(0:M)	INCIDENT
INCIDENT	…generates…	(0:M)	EVIDENCE
EVIDENCE	…analyzed with…	(1:M)	EVIDENCE_TOOL
TOOL	...associated with...	(1:M)	EVIDENCE_TOOL
ANALYST	…assigned to…	(0:M)	INCIDENT_ASSIGMENT
INCIDENT	…assigned via …	(1:M)	INCIDENT_ASSIGNMENT
ANALYST	…uses…	(0:M)	ANALYST_TOOL
TOOL	… used by …	(1:M)	ANALYST_TOOL
ANALYST	…attends…	(1:M)	ANALYST_TRAINING_ATTENDANCE
TRAINING	.. attended via …	(1:M)	ANALYST_TRAINING_ATTENDANCE
TOOL	…associated with…	(1:1)	TOOL_TYPE
PARTNERSHIP	…collaborates on...	(1:M)	INCIDENT_PARTNERSHIP
INCIDENT	..collaborated via…	(1:M)	INCIDENT_PARTNERSHIP
THREAT	…exhibits…	(1:M)	ATTACK_PATTERN
REGULATION	…. requires….	(1:M)	REGULATORY_COMPLIANCE
INCIDENT	…evaluated for…	(1:M)	REGULATORY_COMPLIANCE
ANALYST	…specializes as….	(0:1) (subtype)	FORENSIC SPECIALIST
TOOL	…analyzes….	(1:M)	EVIDENCE_TOOL
TRAINING	…recorded in…	(1:M)	ANALYST_TRAINING_ATTENDANCE

Business Rules with Related Tables

THREAT/INCIDENT

1. A THREAT can trigger no incidents (e.g., dormant threats) or many incidents.
2. Every INCIDENT must be linked to exactly one THREAT (via THREAT_ID)

INCIDENT/EVIDENCE

1. An INCIDENT can generate no evidence (e.g., unresolved) or many pieces of evidence.
2. Every EVIDENCE record must be tied to exactly one INCIDENT (via INCIDENT_ID)

ANALYST/INCIDENT_ASSIGNMENT

1. An ANALYST can be assigned to no incidents (e.g., new hire) or many incidents (via INCIDENT_ASSIGNMENT).
2. Every INCIDENT_ASSIGNMENT must involve exactly one ANALYST and one INCIDENT.
3. INCIDENT_ASSIGNMENT_ROLE (e.g., Lead Investigator) must be recorded,
   and INCIDENT_ASSIGNMENT_DATE cannot be null.

TOOL/EVIDENCE_TOOL

1. A TOOL can analyze at least one piece of evidence or many pieces of evidence (via EVIDENCE_TOOL).
2. Every EVIDENCE_TOOL record must be linked to exactly one TOOL and one EVIDENCE.
3. EVIDENCE_TOOL_ANALYSIS_DATE must be recorded when a tool is used

TRAINING/ATTENDANCE

1. A TRAINING program can have no attendees (e.g., upcoming) or many attendees (via ATTENDANCE).
2. Every ATTENDANCE record must link to exactly one TRAINING and one ANALYST.
3. ATTENDANCE_COMPLETION_STATUS (Completed/In Progress) must be recorded.

ANALYST/ANALYST_TOOL

1. An ANALYST can use no tools (e.g., unassigned) or many tools (via ANALYST_TOOL)
2. Every ANALYST_TOOL record must be linked to exactly one ANALYST and one TOOL.
3. ANALYST_TOOL_LAST_USED_DATE is required if a tool is assigned

INCIDENT/REGULATORY_COMPLIANCE

1. An INCIDENT can have one or many checks (via REGULATORY_COMPLIANCE).
2. Every REGULATORY_COMPLIANCE record must be linked to exactly one INCIDENT.
3. REGULATORY_COMPLIANCE_STATUS (Compliant/Non-Compliant) and audit date are mandatory.

THREAT/ATTACK_PATTERN

1. A THREAT can exhibit one attack pattern (e.g., theoretical) or many patterns (via ATTACK_PATTERN).
2. Every ATTACK_PATTERN must map to exactly one THREAT (via THREAT_ID).

PARTNERSHIP/INCIDENT_PARTNERSHIP

1. A PARTNERSHIP can collaborate on one or many incidents (via INCIDENT_PARTNERSHIP).

2. Every INCIDENT_PARTNERSHIP record must be linked to exactly one PARTNERSHIP and one INCIDENT.
3. PARTNERSHIP_COLLABORATION_LEVEL (Low/Medium/High) must be specified.

ANALYST/FORENSIC_SPECIALIST

1. An ANALYST can have no forensic specialization (e.g., general role) or one specialization (via FORENSIC_SPECIALIST).
2. Every FORENSIC_SPECIALIST must inherit from exactly one ANALYST (via ANALYST_ID)

TOOL/TOOL_TYPE

1. A TOOL must belong to exactly one TOOL_TYPE (e.g., Disk Imaging).
2. A TOOL_TYPE can categorize no tools (e.g., deprecated) or many tools.

Part-2: The Entity Relationship Diagram

Task-1: Relational Schemas

1) **THREAT Table:**

   THREAT (**THREAT_ID**, THREAT_NAME, THREAT_TYPE, THREAT_SEVERITY_LEVEL, THREAT_REPORTED_DATE)

2) **INCIDENT Table:**

   INCIDENT (**INCIDENT_ID, THREAT_ID**, INCIDENT_DATE, INCIDENT_IMPACT_LEVEL, INCIDENT_RESOLUTION_STATUS)

3) **EVIDENCE Table:**

   EVIDENCE (**EVIDENCE_ID, INCIDENT_ID**, EVIDENCE_TYPE, EVIDENCE_STORAGE_LOCATION, EVIDENCE_INTEGRITY_HASH)

4) **ANALYST Table:**

   ANALYST (**ANALYST_ID,** ANALYST_NAME, ROLE, ANALYST_CONTACT_INFO, ANALYST_EXPERIENCE)

5) **TOOL Table:**

   TOOL (**TOOL_ID**, TOOL_TYPE, TOOL_NAME, TOOL_VENDOR, TOOL_LICENSE_EXP_DATE)

6) **TRAINING Table:**

   TRAINING (**TRAINING_ID**, TRAINING_NAME, TRAINING_TYPE, TRAINING_DURATION, TRAINING_PROVIDER)

7) **PARTNERSHIP Table:**

   PARTNERSHIP (**PARTNERSHIP_ID,** PARTNERSHIP_AGENCY_NAME, PARTNERSHIP_TYPE, PARTNERSHIP_START_DATE, PARTNERSHIP_END_DATE)

8) **REGULATORY_COMPLIANCE Table:**

REGULATORY_COMPLIANCE (**COMPLIANCE_ID**, **REGULATION_ID**, **INCIDENT_ID**, REGULATORY_COMPLIANCE_STATUS, REGULATORY_COMPLIANCE_AUDIT_DATE)

9) **ATTACK_PATTERN Table:**

ATTACK_PATTERN (**ATTACK_PATTERN_ID, THREAT_ID**, ATTACK_PATTERN_VECTOR, ATTACK_PATTERN_DETECTION_METHOD, ATTACK_PATTERN_COUNTERMEASURE)

10) **ATTENDANCE Table:**

ATTENDANCE (**ATTENDANCE_ID**, **ANALYST_ID**, **TRAINING_ID,** ATTENDANCE_COMPLETION_STATUS, ATTENDANCE_CERTIFICATION)

11) **REGULATION Table:**

REGULATION (**REGULATION_ID**, REGULATION_NAME, REGULATION_COMPLIANCE_STANDARD, REGULATION_EFFECTIVE_DATE, REGULATION_ISSUING_AGENCY)

Bridge Tables:

12) **TOOL_TYPE Table:** TOOL_TYPE *(Bridge — M:N between TOOL and TYPE)*

TOOL_TYPE (**TOOL_TYPE_ID**, TOOL_TYPE_NAME, TOOL_TYPE_DESCRIPTION, TOOL_TYPE_CREATED_DATE)

13) **ANALYST_TOOL Table:**

ANALYST_TOOL (**TOOL_ID**, **ANALYST_ID**, ANALYST_TOOL_LAST_USED_DATE)

14) **INCIDENT_PARTNERSHIP Table:**

INCIDENT_PARTNERSHIP (**INCIDENT_ID**, **PARTNERSHIP_ID**, INCIDENT_PARTNERS HIP_COLLABORATION _LEVEL)

15) ANALYST_TRAINING_ATTENDANCE Table:

ANALYST_TRAINING_ATTENDANCE (**ANALYST_ID**, **TRAINING_ID**, ANALYST_TRAINING_ ATTENDANCE_DATE, ANALYST_TRAINING_ ATTENDANCE_COMPL ETION_STATUS)

16) EVIDENCE_TOOL Table:

EVIDENCE_TOOL (**EVIDENCE_ID, TOOL_ID,** EVIDENCE_TOOL_ANALYSIS_DATE)

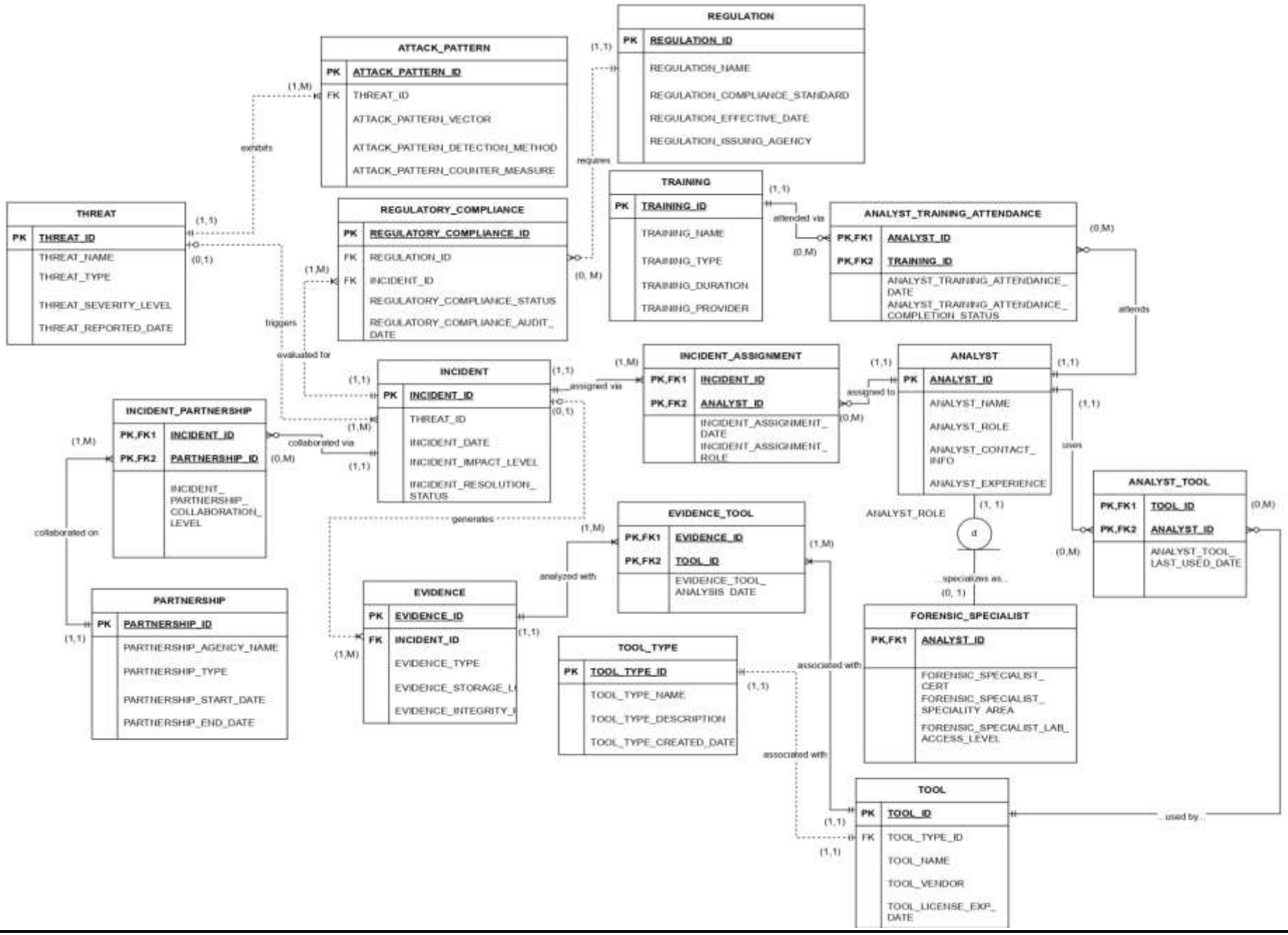
17) INCIDENT_ASSIGNMENT Table:

INCIDENT_AS SIGNMENT (**INCIDENT_ID, ANALYST_ID**, INCIDENT_ASSIGNMENT_DATE, INCIDENT_ASSIGNMENT_ROLE)

18) FORENSIC_SPECIALIST Table:

FORENSIC_SPECIALIST (**ANALYST_ID**, FORENSIC_SPECIALIST_CERT, FORENSIC_SPECIALIST_SPECIALTY_AREA, FORENSIC_SPECIALIST_LAB_ACCESS_LEVEL)

Task-2: ER- Diagram


REGULATION
PK REGULATION_ID
REGULATION_NAME
REGULATION_COMPLIANCE_STANDARD
REGULATION_EFFECTIVE_DATE
REGULATION_ISSUING_AGENCY
ATTACK_PATTERN
PK ATTACK_PATTERN_ID
FK THREAT_ID
ATTACK_PATTERN_VECTOR
ATTACK_PATTERN_DETECTION_METHOD
ATTACK_PATTERN_COUNTER_MEASURE
THREAT
PK THREAT_ID
THREAT_NAME
THREAT_TYPE
THREAT_SEVERITY_LEVEL
THREAT_REPORTED_DATE
REGULATORY_COMPLIANCE
PK REGULATORY_COMPLIANCE_ID
FK REGULATION_ID
FK INCIDENT_ID
REGULATORY_COMPLIANCE_STATUS
REGULATORY_COMPLIANCE_AUDIT_DATE
TRAINING
PK TRAINING_ID
TRAINING_NAME
TRAINING_TYPE
TRAINING_DURATION
TRAINING_PROVIDER
ANALYST_TRAINING_ATTENDANCE
PK,FK1 ANALYST_ID
PK,FK2 TRAINING_ID
ANALYST_TRAINING_ATTENDANCE_DATE
ANALYST_TRAINING_ATTENDANCE_COMPLETION_STATUS
INCIDENT
PK INCIDENT_ID
THREAT_ID
INCIDENT_DATE
INCIDENT_IMPACT_LEVEL
INCIDENT_RESOLUTION_STATUS
INCIDENT_ASSIGNMENT
PK,FK1 INCIDENT_ID
PK,FK2 ANALYST_ID
INCIDENT_ASSIGNMENT_DATE
INCIDENT_ASSIGNMENT_ROLE
ANALYST
PK ANALYST_ID
ANALYST_NAME
ANALYST_ROLE
ANALYST_CONTACT_INFO
ANALYST_EXPERIENCE
INCIDENT_PARTNERSHIP
PK,FK1 INCIDENT_ID
PK,FK2 PARTNERSHIP_ID
INCIDENT_PARTNERSHIP_COLLABORATION_LEVEL
ANALYST_TOOL
PK,FK1 TOOL_ID
PK,FK2 ANALYST_ID
ANALYST_TOOL_LAST_USED_DATE
EVIDENCE_TOOL
PK,FK1 EVIDENCE_ID
PK,FK2 TOOL_ID
EVIDENCE_TOOL_ANALYSIS_DATE
PARTNERSHIP
PK PARTNERSHIP_ID
PARTNERSHIP_AGENCY_NAME
PARTNERSHIP_TYPE
PARTNERSHIP_START_DATE
PARTNERSHIP_END_DATE
EVIDENCE
PK EVIDENCE_ID
FK INCIDENT_ID
EVIDENCE_TYPE
EVIDENCE_STORAGE_L
EVIDENCE_INTEGRITY_I
TOOL_TYPE
PK TOOL_TYPE_ID
TOOL_TYPE_NAME
TOOL_TYPE_DESCRIPTION
TOOL_TYPE_CREATED_DATE
FORENSIC_SPECIALIST
PK,FK1 ANALYST_ID
FORENSIC_SPECIALIST_CERT
FORENSIC_SPECIALIST_SPECIALITY_AREA
FORENSIC_SPECIALIST_LAB_ACCESS_LEVEL
TOOL
PK TOOL_ID
FK TOOL_TYPE_ID
TOOL_NAME
TOOL_VENDOR
TOOL_LICENSE_EXP_DATE
exhibits
requires
triggers
evaluated for
attended via
assigned via
assigned to
attends
uses
collaborated via
collaborated on
generates
analyzed with
ANALYST_ROLE
d
specializes as...
associated with
used by...

Task-3: A documented walkthrough of a Normalized Tables

0NF: Unnormalized Cybersecurity Record

All attributes live in one wide table with repeating and multi-valued fields.

Table: (0NF) : Unnormalized Cybersecurity Record

INCIDENT_ID	INCIDENT_DATE	THREAT_ID	THREAT_NAME	TOOL1_ID	TOOL1_NAME	TOOL2_ID	TOOL2_NAME	TRAINING1_ID	TRAINING1_NAME	TRAINING2_ID	TRAINING2_NAME
1001	2025-05-01	T01	Ransomware	200	Wireshark	201	Volatility	TR01	Malware101	TR02	ForensicsA
1002	2025-05-02	T02	Phishing	200	Wireshark	202	Autopsy	TR01	Malware101	TR03	IncidentResp

Functional dependencies in 0NF:

- INCIDENT_ID → INCIDENT_DATE, THREAT_ID, THREAT_NAME, TOOL1_ID, TOOL1_NAME, …
- THREAT_ID → THREAT_NAME
- TOOL_ID → TOOL_NAME
- TRAINING_ID → TRAINING_NAME

This design violates 1NF due to multi-valued TOOL and TRAINING columns.

1NF: Eliminate Repeating Groups & Ensure Atomicity

Splitting multi-valued attributes into separate rows and tables so each column holds a single value.

Tables after 1NF:

Table: INCIDENT

INCIDENT_ID	**INCIDENT_DATE**	**THREAT_ID**
1001	2025-05-01	T01
1002	2025-05-02	T02

Table: THREAT

THREAT_ID	**NAME**
T01	Ransomware
T02	Phishing

Table: TOOL

TOOL_ID	**NAME**
200	Wireshark
201	Volatility
202	Autopsy

Table: TRAINING

TRAINING_ID	NAME
TR01	Malware101
TR02	ForensicsA
TR03	IncidentResp

Table: INCIDENT_TOOL

INCIDENT_ID	TOOL_ID
1001	200
1001	201
1002	200
1002	202

Table: INCIDENT_TRAINING

INCIDENT_ID	TRAINING_ID
1001	TR01
1001	TR02
1002	TR01
1002	TR03

All columns are atomic, and no table has repeating groups.

2NF: Remove Partial Dependencies: Ensuring every non-key attribute fully depends on the table's primary key. Tables with single-column PKs already satisfy 2NF. For composite-key tables, all non-key fields depend on the entire key.

Composite-key tables and their dependencies:

Table: INCIDENT_TOOL

Composite PK	Non-Key Attribute
(INCIDENT_ID, TOOL_ID)	-

Since these bridge tables carry no extra attributes beyond FKs, they satisfy 2NF automatically.

3NF: Eliminate Transitive Dependencies

Removing attributes that depend on non-key attributes. Factor them into new tables so every non-key attribute depends only on the primary key.

New tables in 3NF:

Table: TOOL_TYPE

TOOL_TYPE_ID	NAME	DESCRIPTION
TT01	Network	Packet analysis
TT02	Memory	Volatile analysis

Table: TOOL (updated)

TOOL_ID	TOOL_TYPE_ID	TOOL_NAME
200	TT01	Wireshark
201	TT02	Volatility
202	TT02	Autopsy

Table: FORENSIC_SPECIALIST

ANALYST_ID	CERTIFICATION	SPECIALTY
A01	EnCE	Memory
A02	GCFA	Network

Table: ANALYST (updated)

ANALYST_ID	NAME	ROLE
A01	Alice	Lead
A02	Bob	Examiner

All non-key attributes now depend solely on their table's primary key, with no transitive links.

By following these steps-flattening (0NF), enforcing atomicity (1NF), removing partial dependencies (2NF), and eliminating transitive dependencies (3NF) the cybersecurity schema evolves into a normalized, redundancy-free design.

Part:3- Database and SQL Queries

1. **Single-Table Query**

   - **Question:** What are the current unresolved cyber incidents?

   - **Query:**

   ```
   SELECT INCIDENT.INCIDENT_ID, INCIDENT.INCIDENT_DATE, INCIDENT.INCIDENT_IMPACT_LEVEL
   FROM INCIDENT
   WHERE (((INCIDENT.[INCIDENT_RESOLUTION_STATUS])='OPEN'));
   ```

   - **Explanation:** Lists all cyber incidents that are still unresolved (status 'OPEN') from the table INCIDENTS.

2. **Two-Table Query**

   - Question: List all cyber incidents along with their associated threat names where the severity level of the threat is "HIGH"?

   - Query:

   ```
   SELECT I.INCIDENT_ID, I.INCIDENT_DATE, T.THREAT_NAME
   FROM INCIDENT AS I INNER JOIN THREAT AS T ON I.THREAT_ID = T.THREAT_ID;
   ```

   - **Explanation:** This query uses 2 tables -CYBER_INCIDENTS and CYBER_THREATS to answer the question by filtering threats with a severity level of HIGH.

3. **Query including a Sub-Query**

   - **Question:** Who are the analysts having work experience more than average?

   - Query:

   ```
   SELECT ANALYST.ANALYST_NAME, ANALYST.ANALYST_EXPERIENCE
   FROM ANALYST
   WHERE ANALYST.ANALYST_EXPERIENCE > (
   ```

```
    SELECT AVG(ANALYST.ANALYST_EXPERIENCE)
    FROM ANALYST
);
```

- Explanation: Finds all analysts with above-average work experience from the table ANALYST –

- Query Breakdown:

1. Subquery: (SELECT AVG(ANALYST_EXPERIENCE) FROM ANALYST) calculates the average experience of all analysts.

2. Main Query: The outer query selects ANALYST_NAME and ANALYST_EXPERIENCE from ANALYST where the experience is greater than the average experience.