Fradulant Transactions Investigation

Adam HAJA MOHIDEEN

TP079601

CT109-3-M-EINV **Individual Assignment** **3rd June 2024**

Agenda

01

Introduction

02

OSINT and Indicators of Compromise (IoCs)

03

Specific Types of Digital Evidence

Introduction

Overview: Increase in fraudulent transactions due to growing reliance on digital financial systems and online exchange.

Challenges: Rise in fraudulent transactions, financial losses, and damage to reputation.

Task 1 - Identification and collection of IoCs and PDE for fraudulent transactions.

Definitons

Open Source Intelligence (OSINT) and Indicators of Compromise (IoCs)

OSINT

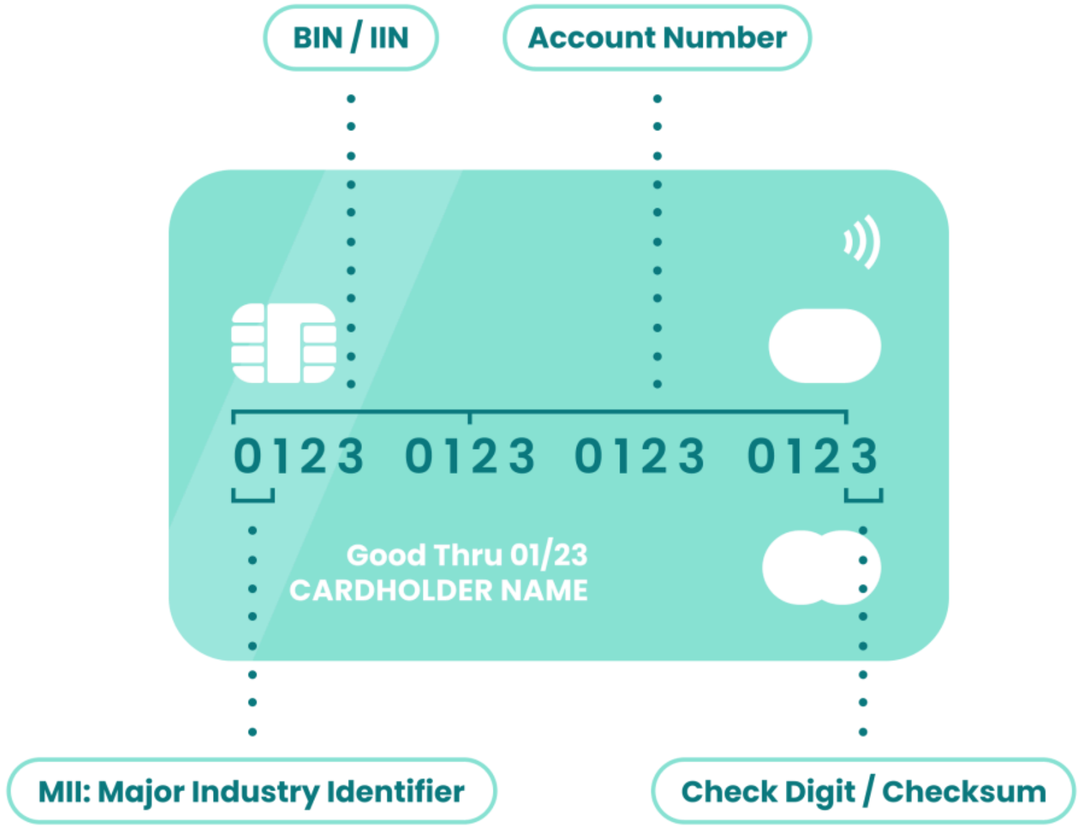
Techniques to gather publicly available information.

IoCs

Elements or remnants left by malicious activities, helping to understand attacks.

IoCs - Card Credentials

Credit card numbers, expiration dates, CVV codes.



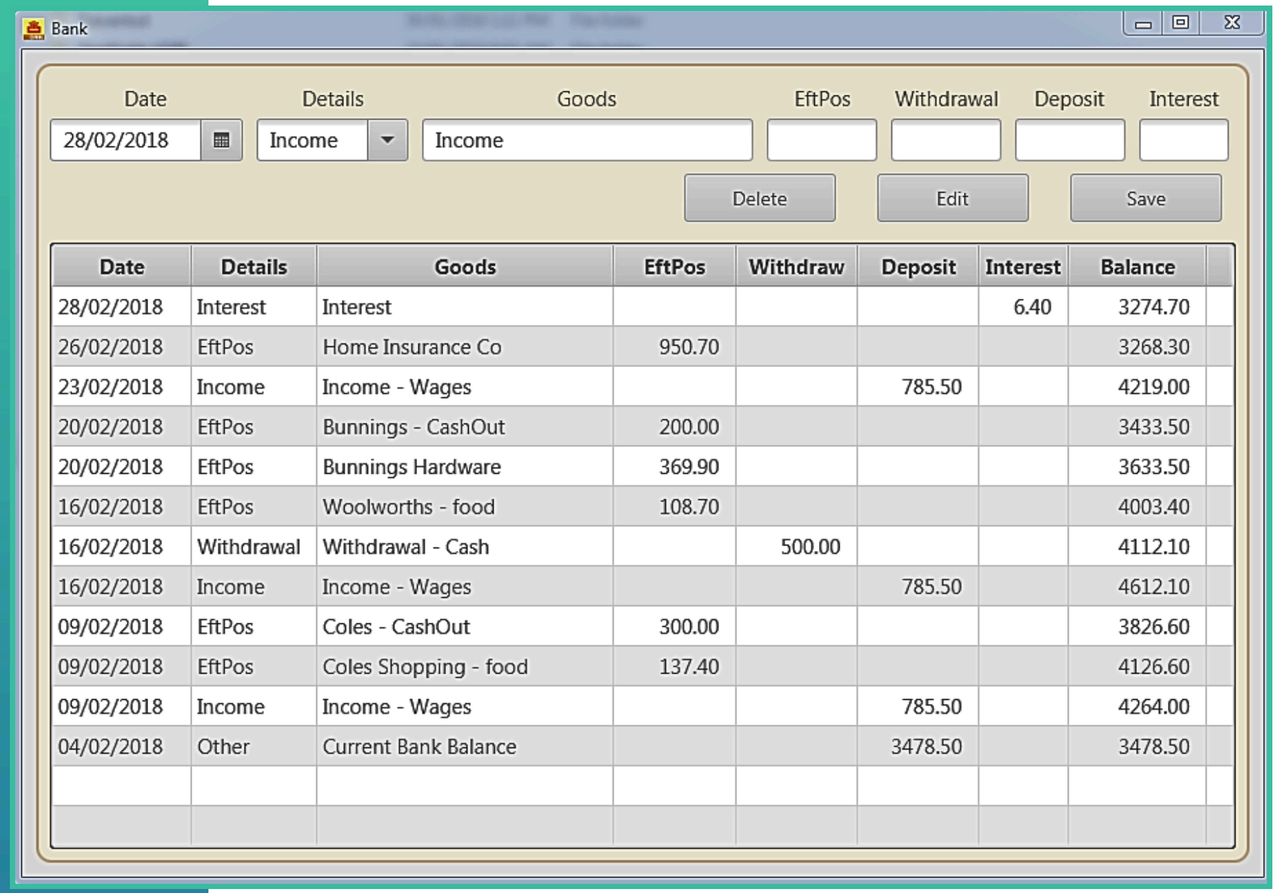
Indicators:

- Multiple incorrect attempts
- Sudden canceled purchases.

Sources: Bank account activity/history.

IoCs - Transactional Irregularities

Patterns of unusual transaction times.



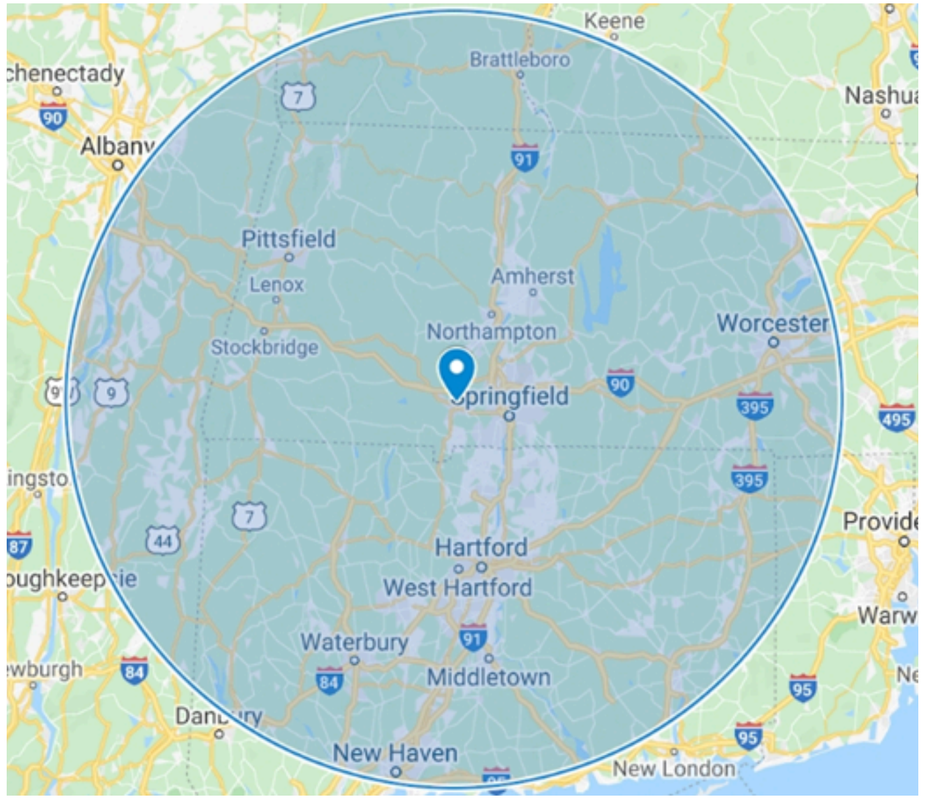
Date	Details	Goods	EftPos	Withdraw	Deposit	Interest	Balance
28/02/2018	Interest	Interest				6.40	3274.70
26/02/2018	EftPos	Home Insurance Co	950.70				3268.30
23/02/2018	Income	Income - Wages			785.50		4219.00
20/02/2018	EftPos	Bunnings - CashOut	200.00				3433.50
20/02/2018	EftPos	Bunnings Hardware	369.90				3633.50
16/02/2018	EftPos	Woolworths - food	108.70				4003.40
16/02/2018	Withdrawal	Withdrawal - Cash		500.00			4112.10
16/02/2018	Income	Income - Wages			785.50		4612.10
09/02/2018	EftPos	Coles - CashOut	300.00				3826.60
09/02/2018	EftPos	Coles Shopping - food	137.40				4126.60
09/02/2018	Income	Income - Wages			785.50		4264.00
04/02/2018	Other	Current Bank Balance			3478.50		3478.50

Indicator: Small transactions followed by large ones

Sources: Bank account activity/history.

IoCs - Delivery Addresses

Common fake addresses used by fraudsters.

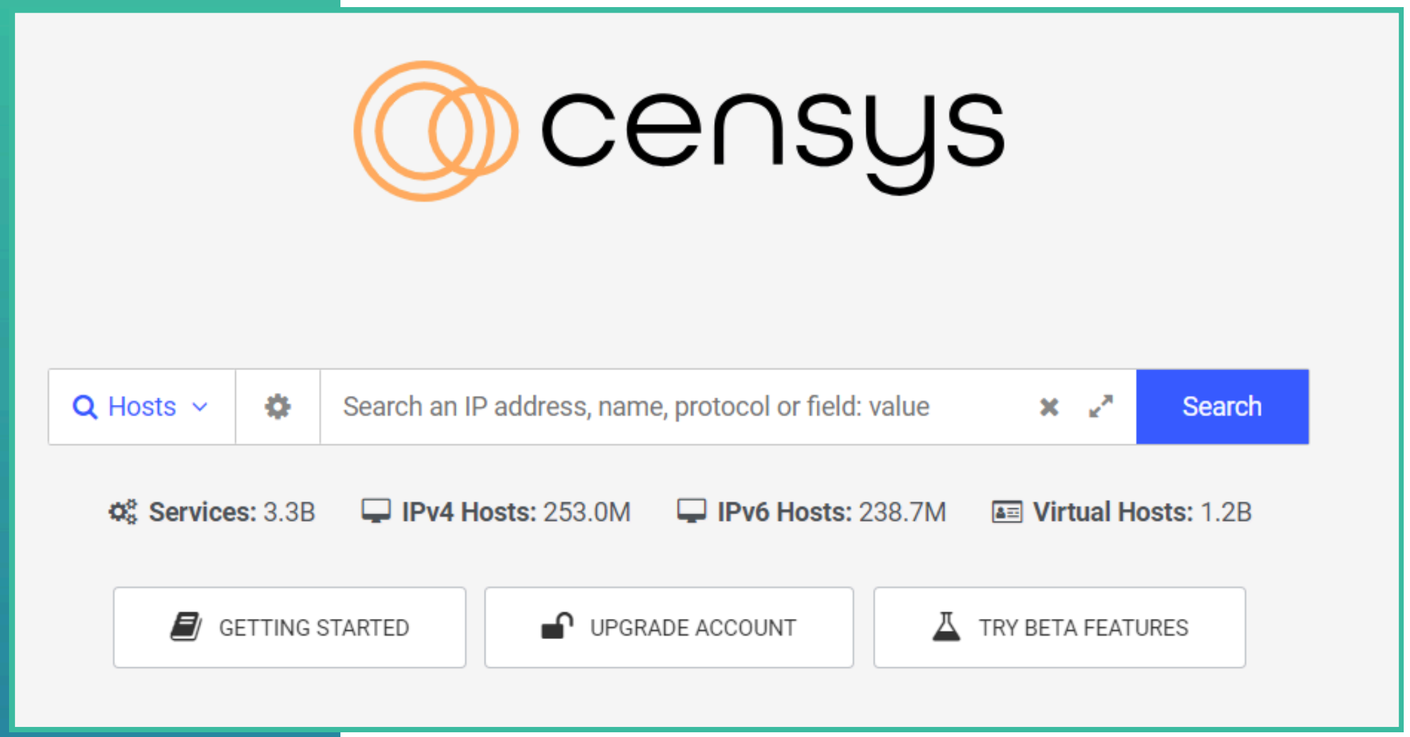


Indicator: Multiple orders to the same address with different payment methods.

Sources: Order and delivery records.

IoCs - IP Addresses

Unfamiliar locations, known malicious sources.

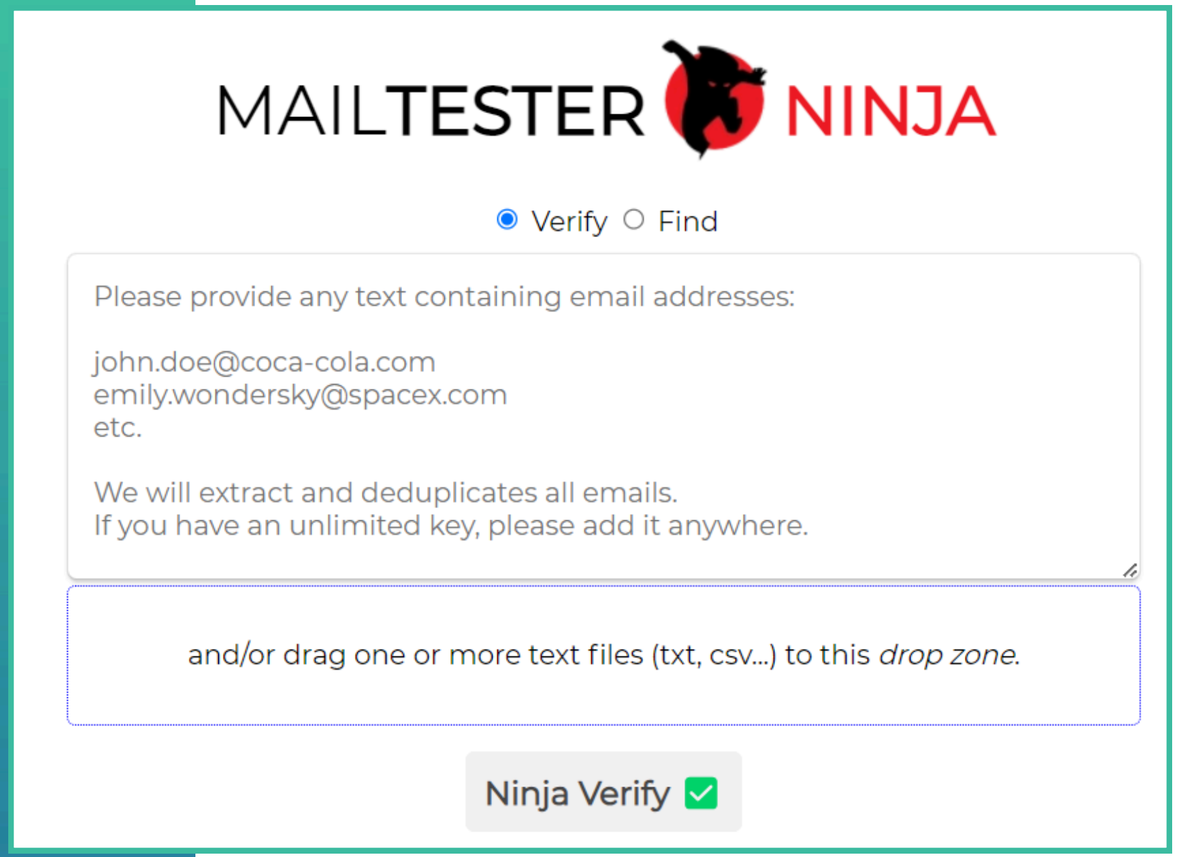


Indicator: Transactions from blacklisted or unusual IP addresses.

Sources: Login records, transaction logs.

IoCs - Email Addresses

Used in fraudulent account registrations or transaction confirmations.

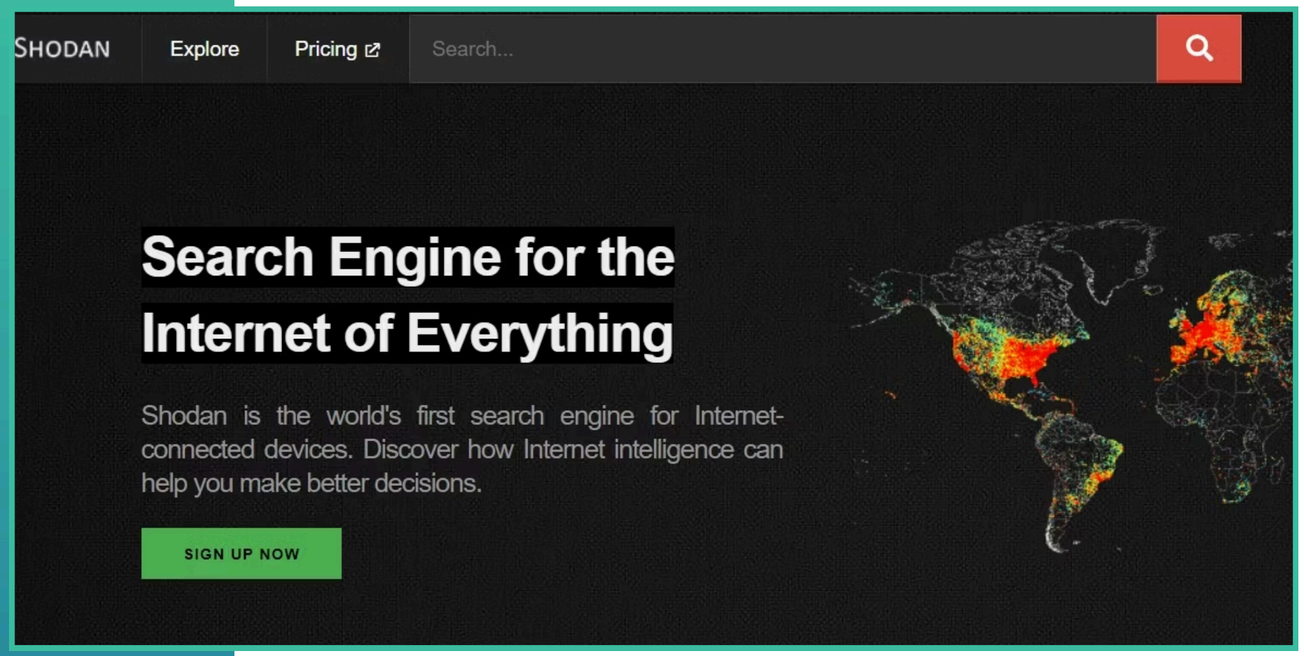


Indicator: Suspicious or fake email accounts.

Sources: Registration records, email verification tools (VerifyEmail, MailTester)

IoCs - Device Fingerprints

Information about the device used for transactions.

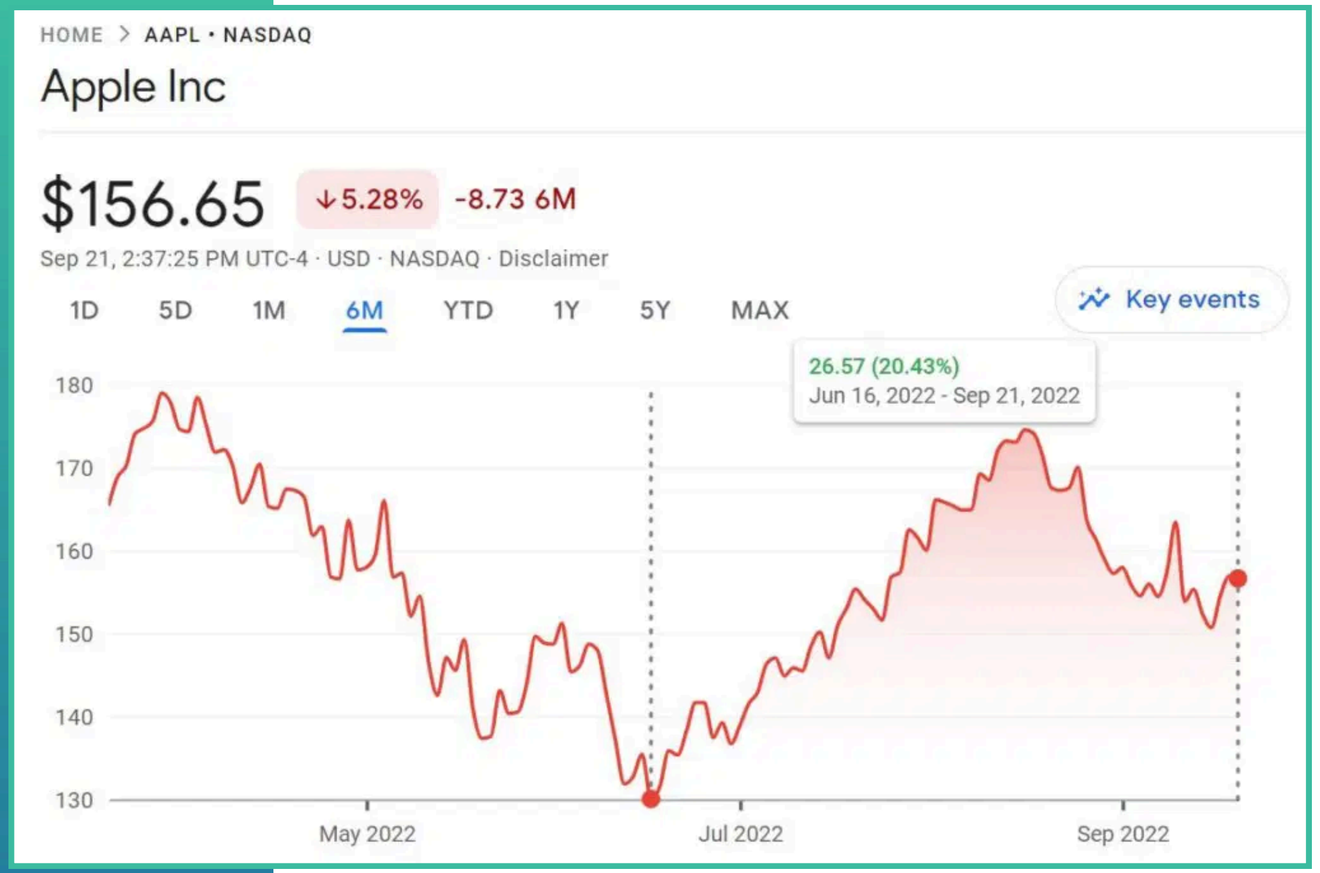


Indicator: Same device used for multiple accounts.

Sources: Device logs, OSINT tools (Shodan)

IoCs - Bank's Financial Health

Financial anomalies indicating potential fraud.



Indicator: Significant deviations or unexpected changes in financial statements.

Sources: Financial reports, business records (Google Finance, OpenCorporates)

Specific Types of Digital Evidence

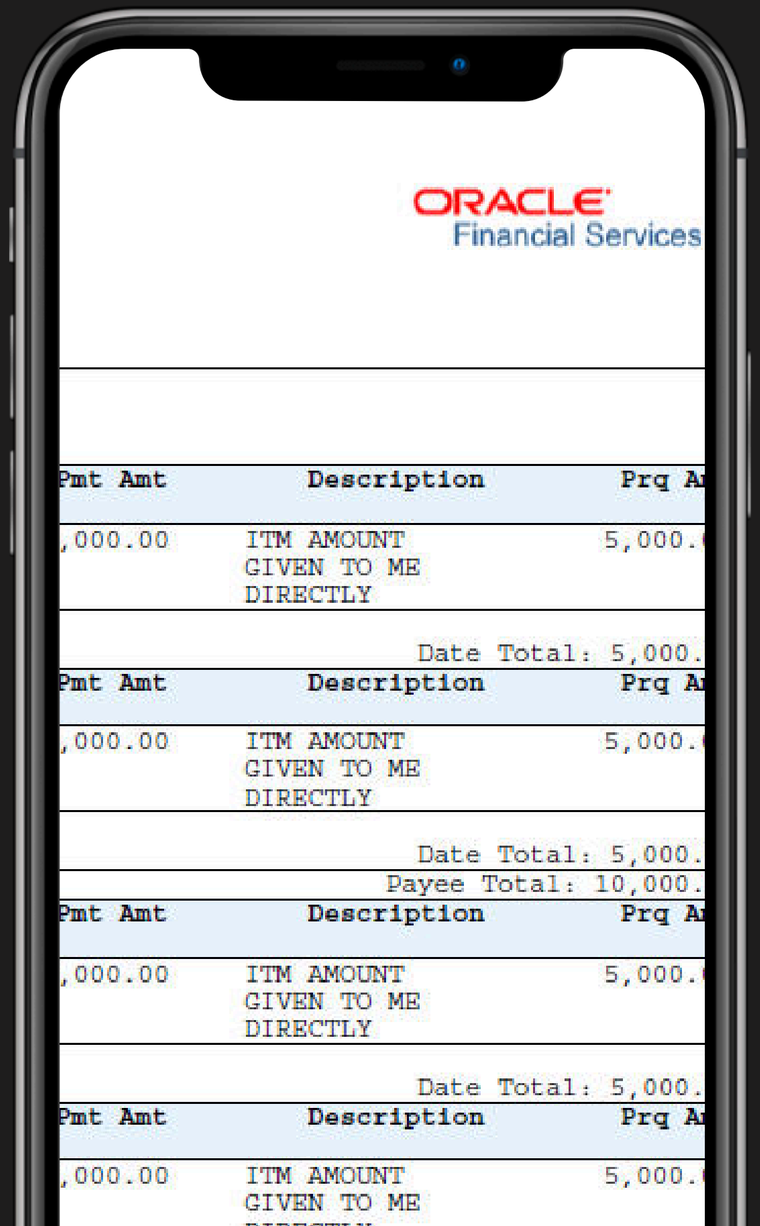
Information stored in digital form that can be used in investigations.

- **Account Access Logs**: Who accessed, when, from where, actions taken.

  -> Financial system logs

- **Transaction Records**: Details of every transaction.

  -> Bank databases



Specific Types of Digital Evidence

- **Communication Archives:** Emails and texts showing coordination.

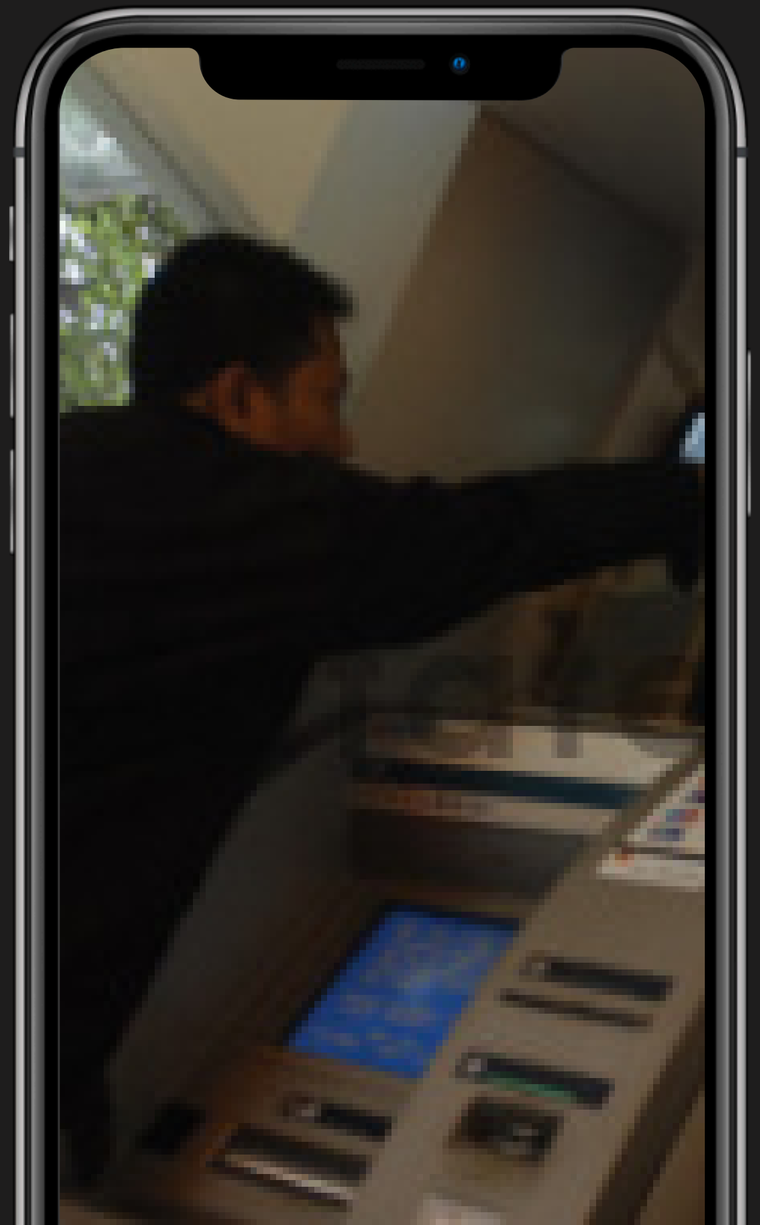
  -> Email servers, text message records

- **Security Camera Footage:** Visual evidence from ATMs.

  -> CCTV systems

- **Network Traffic Data:** Monitoring data flow for suspicious activities.

  -> Network monitoring tools

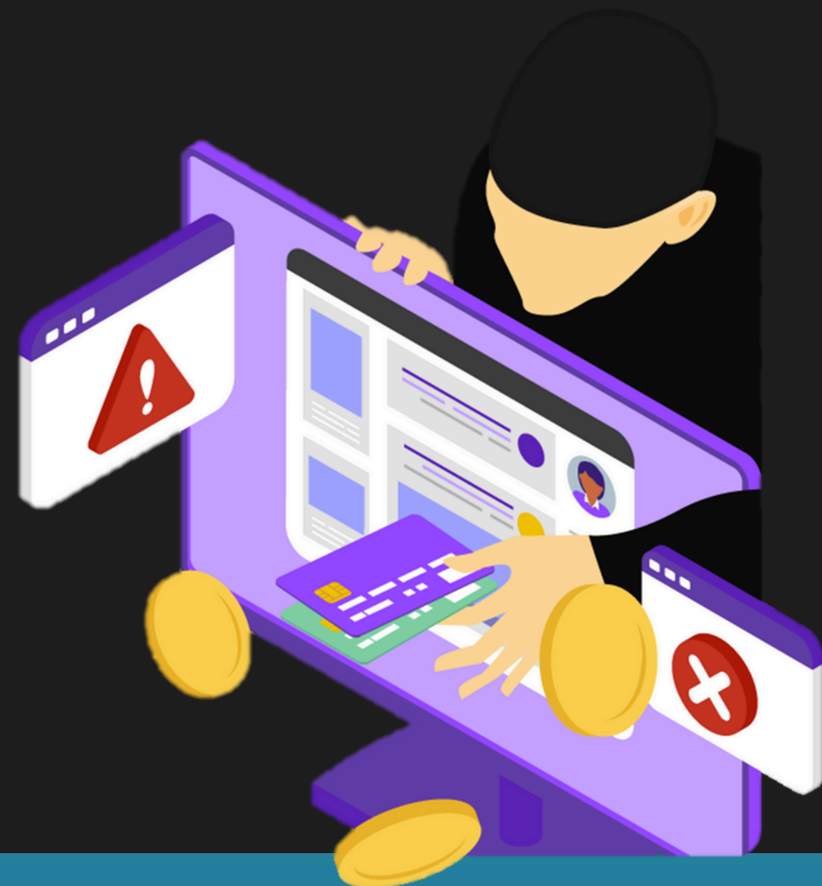


Conclusion

Summary: Identifying and collecting IoCs and PDE is crucial for investigating fraudulent transactions.

Impact: Provides a strong base for detecting and understanding fraudulent activities.

Task 2: Design a new framework with the help of AI and Machine Learning tools



References

- **RFC 9424**: *Indicators of Compromise (IoCs) and Their Role in Attack Defence*
- **OSINT tools**: *Blocklist.de, FireHOL IP Lists, AbuseIPDB, VerifyEmail, MailTester, Shodan*
- **Financial sources**: *Google Finance, OpenCorporates*