Texila International Journal of Academic Research
ISSN: 2520-3088
DOI: 10.21522/TIJAR.2014.12.02.Art019

# Enhancing Cybercrime Investigations in Ghana: A Mobile Broadband Framework for Unmasking Perpetrators through Digital Footprints and User Profile Synthesis

Daniel Adjei Odai
*Department of Computer Science, Texila American University, Georgetown, Guyana*

***Abstract***

*Uncovering the origin of cybercrimes in Ghana continue to be a challenge for law enforcement agencies. Existing solutions had primarily focused on unmasking crime source within the Public Data Network (PDN) using methods such as geolocation of public Internet Protocol (IP) address or the Domain Name Server (DNS) lookup methods. Unfortunately, these approaches fall short at uncovering cybercrime sources from the mobile broadband (MBB) domain. This paper proposed a framework aimed at answering the question of processes around the MBB's packet data protocol (PDP) context procedure and its corresponding private IP attribution to User Equipment (UE) that might mask the UE's identity in a PDN. The study's outcome includes digital footprints collection like IP addresses and Transmission Control Protocol ports during PDP context and UE data sessions to cloud server in the PDN. Exploratory data analysis reveals the uniqueness of every session, i.e., making traceability feasible from a PDN to distinct sources in the MBB domain. This paper proposes a comprehensive framework by recommending the collection of datasets from the MBB domain infrastructure at three logical interfaces with network probes. Additionally, the study suggests enhancing the dataset with call detail records and leveraging Edgar Frank Codd's relational data model to synthesise the fragmented datasets to a unique entity thereby ensuring the unmasking of a cybercrime committed in a PDN effectively traceable to the MBB domain entity. This innovative approach adds to the knowledge of cybercrime investigations in Ghana's cybersecurity endeavours.*

***Keywords****: Cybercrime, IP Address, Mobile Broadband, PDP Context.*

## Introduction

About 5.5 billion individuals, as of the year 2024, representing 68% of the global population are online [1]. Each of these individuals are online with IP addressed device and accessing services mapped to transmission control protocol (TCP) or user datagram protocol (UDP) ports.

Access to the Internet or data services in Ghana is largely via two main technologies i.e.

1. The traditional fixed data services with underlying technologies such as the Asymmetric Digital Subscriber Line over copper or largely fibre, commercially referred to as the Fixed Broadband (FBB) or Fibre to the Home (FTTH).
2. The mobile data services with underlying technologies such as the 3rd Generation Partnership Project's (3GPP) mobile telecommunications standards i.e., the Second Generation (2G), Third Generation (3G) and Fourth Generation (4G) technologies, commercially referred to as the Mobile Broadband (MBB). Generations beyond 4G are yet to commercially take root in Ghana though 5G is launched in November 2024.

As of June 2023, MBB achieved a 31.11% year-on-year growth of total internet traffic with

***Received: 17.02.2025*** ***Accepted: 24.02.2025*** ***Published on:30.04.2025***
****Corresponding Author: adjeido@gmail.com***

a 22.34 million subscriptions and 69.6% penetration rate [2]; this makes it the dominant medium for access to the internet in Ghana and also a fertile ground for cybercrime activities.

In Ghana, uncovering the origin of cybercrimes perpetrated within the MBB domain continue to be a challenge for law enforcement agencies. In [3], several challenges faced by the Ghana Police at effectively dealing with cybercrime were highlighted. These challenges included a lack of cooperation from Internet Service Providers (ISPs) in adducing electronic evidence regarding the specific crime's source. Furthermore, the Cyber Security Authority (CSA) has emphasised the difficulty state agencies face in obtaining electronic evidence that meets the requisite standards for criminal prosecutions [4]. In addition, the significance of computer and cyber forensics at combating crime and enhancing security in Ghana was examined leading to a call for coordinated effort at equipping the security agencies with the necessary tools and training [5].

Concrete solutions to cyber-attack attribution are confronted with multifaceted challenges and calls for the need of improved resources, methodologies, and public discourse to enhance the overall quality of attribution efforts [6]. Technically, various attempts and methods that have been made regarding IP address attribution to cybercrimes have largely focused on the Public Data Network (PDN) by using methods like geolocation of public IP address, whois and the rest. Unfortunately, these approaches have fallen short at uncovering cybercrime sources from the mobile broadband (MBB) domain. This paper proposed a framework at addresses this gap by answering the question of processes around the MBB's PDP context procedure and its corresponding private IP attribution to UE that might mask the UE's identity in a PDN when a cybercrime is committed.

### Cyber Crime Impact

The growth of the Internet and its accompanying cybercrime menace has plagued every society and Ghana is not an exception. In 2023, there was about 880,418 cybercrime complaints from the US public to the Internet Crime Complaint Centre (IC3); a private entity in partnership with the Federal Bureau of Investigation (FBI) to fighting cybercrime in various fronts including anonymity. These complaints represent a 10% increase relative to 2022. The FBI posited that; this value could represent about a quarter of the actual incidents based on their past experience.; the loss incurred to victims exceeds $12.5 billion [7].

Cybercrime in Ghana is growing with the expansion of its digital space. Notably, online romance scams and financial fraud are common forms of cybercrime with unemployment and poverty as the main drivers [8]. The head of Ghana's Cyber Security Authority (CSA) made known the following facts as reported in The Ghanaian Times (a reputable national news media outlet): The CSA received 41,285 complaints regarding cybercrime related issues between October 2019 and July 2023; the CSA claimed more cases are not reported. The Ghanaian Times further reported that, for the first half of 2023, Ghana has lost GHS49.5 million [9].

We are living in a moment of tremendous revolutionised digital landscape i.e., the Internet. This exciting contemporary digital landscape, unfortunately, is quite bedevilled with objectionable cyber threats and there seem to be no end in sight. This calls for counter technical measures to further promote digital advancement and give space for productivity to digital citizens.

## Materials and Methods

### Research Design

This paper sought to add to knowledge, the challenges associated with back tracing the source of cybercrimes, primarily, the focus

being on the communication parameters acquired in the MBB (Mobile Broadband) domain during Packet Data Protocol (PDP) context and how those parameters are presented in a Public Data Network (PDN) during data sessions. It also sought to understand the processes through which User Equipment (UE) acquires IP addresses and how these IP addresses, might in turn, be used in a way that masked the identity of the UE within a PDN. This study is quantitative and made use of experimental case study design.

PDP context activations and data session initiations were performed randomly within the available highest generations (4G and 3G) at limited geographical areas, i.e. Accra, the capital city of Ghana. Data about the following parameters were captured during PDP context activation and session initiations from the UE to the PDN:

1. The IP address assigned to the UE during PDP context.
2. The source and destination TCP ports of the UE's client application used to access the PDN was captured.
3. The destination IP intended to be accessed by the UE client application was captured.
4. The IP address of the UE as seen in the PDN was captured.
5. The source TCP port of the UE as seen in the PDN was captured.

**Research Instruments**

With reference to the setup for exploration and data collection via PDP context and session initiations in Figure 1 below, the following tools were used at the radio access network (RAN) domain:

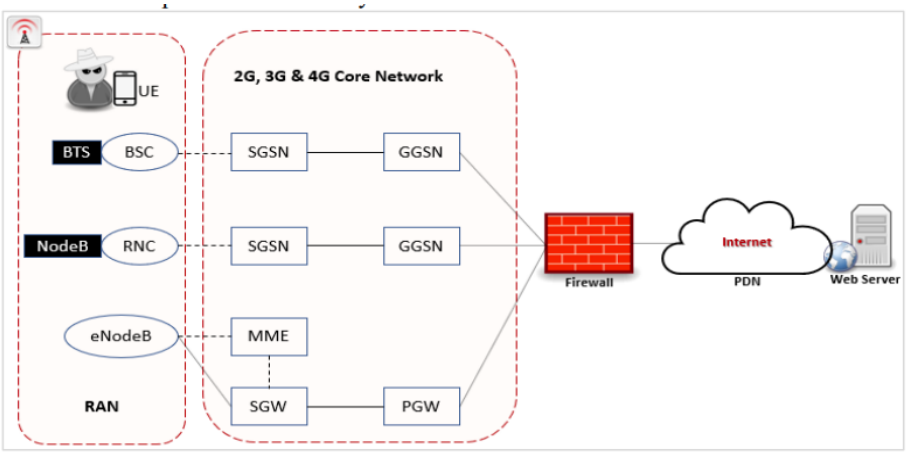


**Figure 1.** The Setup

With reference to the setup diagram in the following tools were used:

1. Two Samsung phones i.e., the UEs with Android OS
2. Three Nano SIM cards acquired from ISPs 1, 2 and 3 and registered with the NCA
3. Network Analyzer (an app installed on the UEs): “an all-in-one iPhone and Android app for network analysis, scanning and problem detection [10]”. In real time, this app was used to capture PDP IP address assigned to the UE.
4. Packet Capture (an app installed on the UEs): "a network traffic sniffer app with SSL decryption capabilities". It employs a-man-in-the-middle technique without requiring the UE OS to be rooted [11]. The preferred data file generated with the app was the pcap file extension type.
5. Web Browsers: FireFox Focus, Microsoft EDGE and Google Chrome. These apps were used as clients for initiation of data sessions to the PDN.
6. Wireshark (program installed on a Windows PC): “an open source network

packet/protocol analyser" [12]. This program was used to analyse the pcap trace data from the UE.

This paper had no control or direct access to network elements within the RAN and core i.e., BTS(Base transceiver station), BSC(Base Station controller), RNC(Radio Network Controller), eNodeB(Evolved Node B), SGSN(GPRS support node), GGSN(Gateway GPRS support node), MME(Mobility Management Entity), SGW(Serving Gateway) and PGW(Packet Gateway). The setup depicts the 3GPP proposed standard architecture.

The computer software and tools used in the PDN to capture data about the UE upon session initiation were as follows:

1. A registered domain name was procured and hosted in the cloud by a web host. This approach was adopted to avoid port forwarding when hosted privately.
2. A PHP server-side scripting language was used to capture the relevant parameters, such as global IPs and TCP ports numbers, when the UE visits the web site in the PDN as shown in Figure 2 below.
3. A relational database was created in the cloud with SQL language and Oracle MySQL RDBMS to archive the relevant UE parameters when UE visits the PDN [13] as shown in Figure 3.
4. cPanel web site management tool was used to administer the cloud hosting [14].

```php
<?php
// Get the UE data
$src_ip = $_SERVER['REMOTE_ADDR'];
$src_port = $_SERVER['REMOTE_PORT'];
$dst_ip = $_SERVER['SERVER_ADDR'];
$dst_port = $_SERVER['SERVER_PORT'];

// Database connection information
$host = 'localhost';
$username = '';
$password = '';
$database = '';

// Create a database connection
$mysqli = new mysqli($host, $username, $password, $database);

// Insert the captured data into the database
$query = "INSERT INTO tbl_traffic (src_ip, src_port, dst_ip, dst_port) VALUES (?, ?, ?, ?)";
$pq = $mysqli->prepare($query);

$pq->bind_param("sisi", $src_ip, $src_port, $dst_ip, $dst_port);

if ($pq->execute() === false) {
    die("Execute failed: " . $pq->error);
}

$pq->close();
$mysqli->close();
?>
```

**Figure 2.** PHP Code for Data Collection

```sql
CREATE TABLE tbl_traffic (
    id INT AUTO_INCREMENT PRIMARY KEY,
    src_ip VARCHAR(50),
    src_port INT,
    dst_ip VARCHAR(50),
    dst_port INT,
    date_time TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);
```

**Figure 3.** Database Table

**Ethical Considerations**

Three major mobile data ISPs platforms were used to camp their respective SIMs in conjunction with an acquired web domain hosted by a web service provider (WSP). This paper refrained from using known specific names of the ISPs but rather chose to categorise them as ISP-1, ISP-2 and ISP-3 not according to any rank, name or preference prescribed by the NCA. It is a public knowledge that, these ISPs are ranked by the NCA by their number of subscriptions, penetration rate, market share and the rest (NCA, 2023). No research permission was sought from any of the three major ISPs since the data collection procedure was conducted at public points of their infrastructure. The SIMs used are legally registered to the author of this paper.

**Data Collection Procedure**

PDP context activation and data session initiation, which are experimental, were randomly performed at various locations in Accra and the results recorded.

The collection of previously unimaginable data had been made quite manageable by the recent advancements in smart devices technology. The combination of cloud-based research architecture and smart devices like the UE have brought about research methodologies akin to the traditional methodologies of data collection. Some research activities are best accomplished not by the traditional data collection techniques like survey [15].

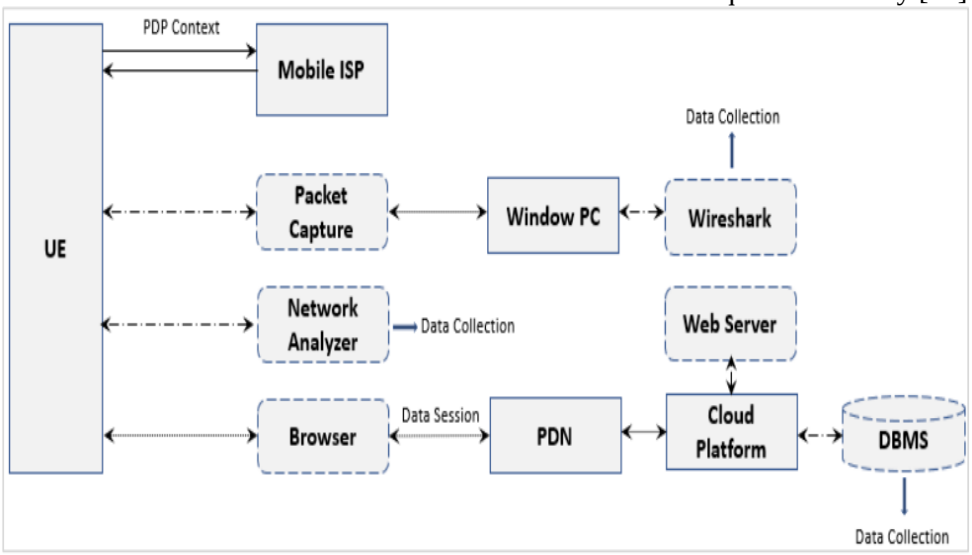


**Figure 4.** Data Collection Procedures Flow

Reference to Figure 4 above, the UE was made to initiates PDP context to obtain an IP address from the ISP by turning mobile data off and on; UE restart is another approach of initiating PDP context. The Network Analyser software was used to capture the assigned PDP IP address from the ISP's gateway node and subsequently recorded the data in an electronic spreadsheet. A browser installed in the UE was used to initiate a data session to the procured website in the PDN. The Packet Capture software was used to sniff the data packet units to and from the UE; the pcap trace file generated by the Packet Capture software was exported to a Windows PC and analysed its protocol stack with Wireshark software, as shown in window labelled "1" in Figure 5 below, to obtain and record the source IP, source TCP port, destination IP and destination TCP port; these values were recorded in the same electronic spreadsheet. Window labelled "2" in Figure 5 presented the TCP/IP layered protocol of the data unit captured. IPs and ports details were also verified from the window labelled "2" as well.

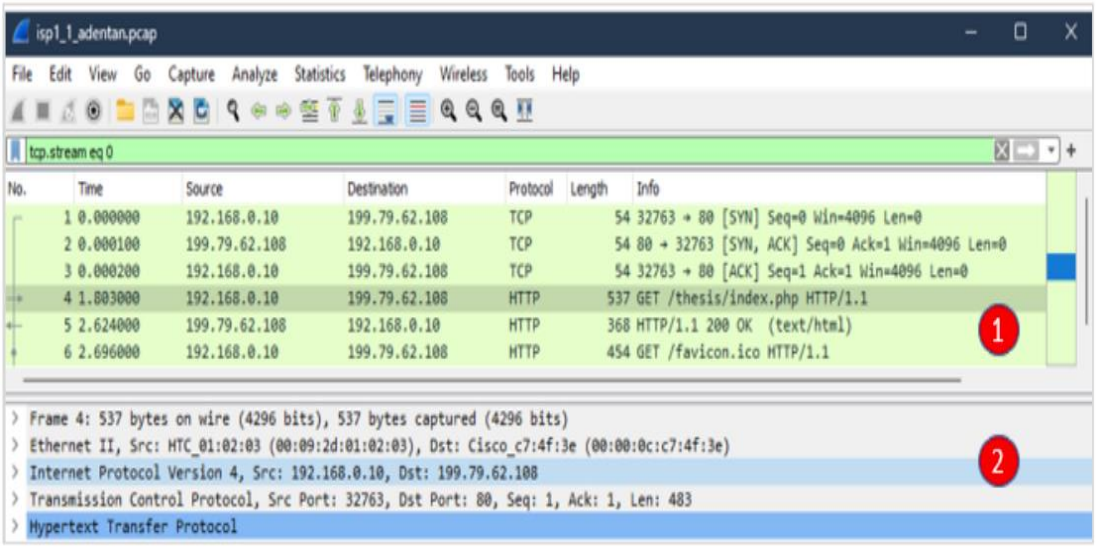


**Figure 5.** Packet Capture - Analysis

Simultaneously and automatically to the packet capture process, the cloud domain captured the UE parameters on the cloud web host platform in the PDN and the values were recorded in the MySQL database. These values were also manually exported to the electronic spreadsheet.

**Data Analysis**

Data from the three data collection points, as shown in Figure 4 above, were aggregated and cleaned using simple data aggregation method with Microsoft's Power Query. It is typical of aggregated data measures to reveal an insight that individual datasets could not [16].

Exploratory Data Analysis (EDA) approach, with Pandas (a Python language data analysis package), was adopted to analyse the datasets. As explained in [17], EDA is about looking at data from various angles for insight of a particular interest or of importance within its context but EDA primarily aims not at validating the existence of an effect and it does not rely on a statistical model that incorporates a mathematical representation of the effect.

**Sample Data Frame**

```
import pandas as pd
df = pd.read_csv('pdp_csv.csv')

<class 'pandas.core.frame.DataFrame'>
RangeIndex: 120 entries, 0 to 119
Data columns (total 11 columns):
 #   Column          Non-Null Count  Dtype
---  ------          --------------  -----
 0   ISP             120 non-null    object
 1   PDP             120 non-null    int64
 2   App             120 non-null    object
 3   Location        120 non-null    object
 4   AppSrc_IP       120 non-null    object
 5   Dst_IP          120 non-null    object
 6   AppSrc_Port     120 non-null    int64
 7   Dst_Port        120 non-null    int64
 8   PDPIP_Address   120 non-null    object
 9   Global_IP       120 non-null    object
 10  Global_Port     120 non-null    int64
```

**Figure 6.** Data Frame Sample

To answer research questions, absolute frequency statistical method was used to determine TCP port and IP address retention during PDU sessions; same method was used to

verify PDP IP address retention. The captured data in an electronic spreadsheet data was converted to csv i.e. pdp_csv.csv. The csv data (pdp_csv.csv) was read into a pandas data frame (df ) as shown in Figure 6 above.

**TCP Ports & IP Address Retention Verification**

The following actions were undertaken with Pandas to determine the IP and TCP ports retention to answer the paper's objectives:

1. Checked for duplicated record in whole data frame
   df.duplicated().sum()
   Output: 0
2. Created a record set (df_globalIP) for column Global_IP
   df_globalIP = df["Global_IP"]
3. Checked for duplicated entry in df_globalIP
   df_globalIP.duplicated().sum()
   Output: 0
4. Created a record set (df_GlobalPort) for column Global_Port
   df_GlobalPort = df["Global_Port"]
5. Checked for duplicated entry in column Global_Port
   df_GlobalPort.duplicated().sum()
   Output: 0

## Results

This study aimed at finding the difficulty in tracing IP address used to commit cybercrime within the public digital communication space to its MBB source. PDP context activations were performed with SIMs belonging to three mobile data ISPs from various geographical locations from where the SIMs were camped. The following sample dataset, as shown in Table 1 above, is the sample data of the total 120 PDP activations that were collected and exploratory data analysis performed on it.

No duplicate record was observed in the data frame. This establishes the uniqueness of every session i.e.; it should be possible for every session to be traced from the PDN to its unique source. Every PDP activation resulted in new PDP IP; no subsequent PDP IP is maintained from the previous observed. This implies that, the PDP IPs are not statically assigned to the UE but rather dynamically assigned and no lease period is granted to the assigned PDP IP. This is worth noting because, the PDP IP once acquired is not changed until a phenomenon occasioned a new PDP context activation. This arrangement is quite ideal for the cybercriminal to assume a new identity by initiating a new PDP context to hide his/her identity after committing a cybercrime. A larger dataset might enhance the probability of a repeated PDP IP but not a subsequent one from the previous. This does not negate the established fact that, the PDP IP assignment arrangement provides a fertile ground for the cybercriminal to hide his/her identity. The PDP IPs were all noticed to be a private Class-A prefixes. These private prefixes were translated to global public IPs in the PDN as well as the source TCP port of every session also translated into another port numbers in the PDN. The characteristics of the results analysis resonates perfectly with the standard Port Address Translation (PAT) concept of private IP address and UDP/TCP port numbers into public IP addresses and TCP/UDP port numbers. The problem with PAT could be inferred that, it affords a maximum of 65,536 MBB UEs to connect to the Internet with the same public IP address due to its 16 bits representation. How could cyber security measures and tools such as IP address attribution be used to counter cybercrime in this situation? Who, with a UE in MBB domain, would be held responsible for a cybercrime when committed with a PAT public IP address? This paper discovered PAT from its data analysis and proposed a framework that could be used to address the problem PAT presents aside its touted advantages. In fact, it could be deduced from the findings that, multiple PATs were in play for each ISP.

**Proposed Solution**

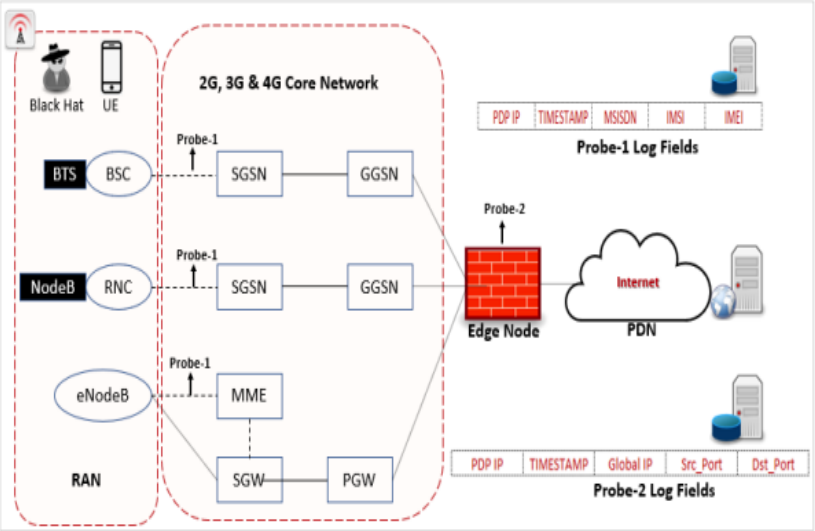


**Figure 7.** Proposed Solution – Logical Architecture

In [18], packet sniffing, which falls under a network probe, was highlighted as an effective technique for gathering evidence from network devices in forensics that involves the collection and analysis of data packets that traverse a network. The probes in Figure 7 above will sniff the packets and insert the relevant log fields of interest into a relational database. Probe-1 refers to the signalling interface between the core network and the RAN for each technology generation i.e., 2G, 3G and 4G where the probe is logically situated for packet capture. The captured data fields of interest by the probes are fed into a database (such as the relational database). The fields of interest are the PDP IP address (PDP IP), the date and time of capture (TIMESTAMP), the "Mobile Station International Subscriber Directory Number" (MSISDN) and "International Mobile Subscriber Identity" (IMSI) which are unique attributes of the SIM card owned by a user and the "International Mobile Equipment Identity" (IMEI); a unique attribute of the UE. As explained in [19], a research at identifying tourist by mining CDRs ("Call detail Records"), Telecommunication service providers mainly collect CDRs for billing purposes but CDRs could be mined to provide exact locations of a tourist. This paper is proposing the CDR to be mined to fight cybercrime in the MBB domain. This aspect also explains the difficulty in tracing crime committed in a PDN to the core network i.e., the MBB ISPs are basically focused on revenue, and rightly so, of which they have setup infrastructure for such purpose and not focused on setting up infrastructure to fighting cybercrime committed with the MBB domain.

GSMA is an organisation that primarily serves the interest of telecommunications service providers globally. In its security guide to protect the confidentiality of users, GSMA stated the following: It is imperative to safeguard sensitive data against unauthorised disclosure. The first step to ensuring confidentiality is to isolate the distribution infrastructure and exercise strict control over the distribution of sensitive information [20]. From the proposed architectural framework, the 2G/3G/4G core networks are isolated from the PDN and all fields associated with Probe-1 capture are expected not to be transmitted to the edge node where the PAT is believed to be implemented. PDP IP obviously would be an exception since results from the research findings indicated it is needed for the PAT. It is important to note that, PDP address which is acquired temporarily and used until a phenomenon occasions a next PDP context

procedure, the IP is not transmitted to the PDN. Should these obviously personal data, such as the MSISDN, IMSI and IMEI, be routed to the PDN, it might expose users to various privacy and security risks. For example, it could lead to unsolicited communication, spam and potentially more severe issues like identity theft or fraud. "Ghana's Data Protection Act, 2012" is a law that basically protects the privacy of individuals by regulating the processing of personal information [21]. By regulating the processing of personal information, the legislation established the "Data Protection Commission (DPC)" to safeguard individual privacy and personal data. The Commission outlines the procedure for obtaining, retaining, using, or disclosing personal data as well as other associated matters that touch on data protection. [22].

Probe-2 in Figure 7 above is logically situated at the edge node where the following fields is expected to be collected i.e., the PDP IP address (PDP IP), date and time of capture (TIMESTAMP), source TCP/UDP port number (Src_Port), socket to be accessed TCP/UDP port in the PDN (Dst_Port) and finally the global IP address (Global IP). The exercise proposed leveraging the “Entity Relationship data model” to establish a relationship between the two probes since the relational data model had earlier been proposed as the data repository for the capture by the probes.

The conceptual representation of data and its organisation which in turn defines the structure, relationships, and constraints of data without specifying how the data is stored or accessed is known as a data model. Chen, the original architect of the Entity-Relationship data model (E-R Model) for relational data modelling, in 1976 put forward the following: The entity-relationship model brings to the fore, a natural perspective of viewing the real world as a collection of distinct entities and the relationships amongst them. In contrast, the relational model is anchored in the relational theory that is focused on achieving high data independence but might overlook crucial semantic details about the real world in its approach. The E-R model works to attain data independence and is grounded in set theory and relation theory, employing a specialized diagrammatic technique for crafting databases. It delves into the implications associated with data integrity, information retrieval, and data manipulation. When delving into a data model, it's essential to come to terms with the specific levels of logical data views that the model seeks to address. An entity is a representation of a distinct "thing" with its own unique identity. For example, a particular person, company, or event could serve as an entity. On the other hand, a relationship signifies an association between entities. For instance, the connection of "father-son" defines a relationship between two entities labelled as "person" [23].

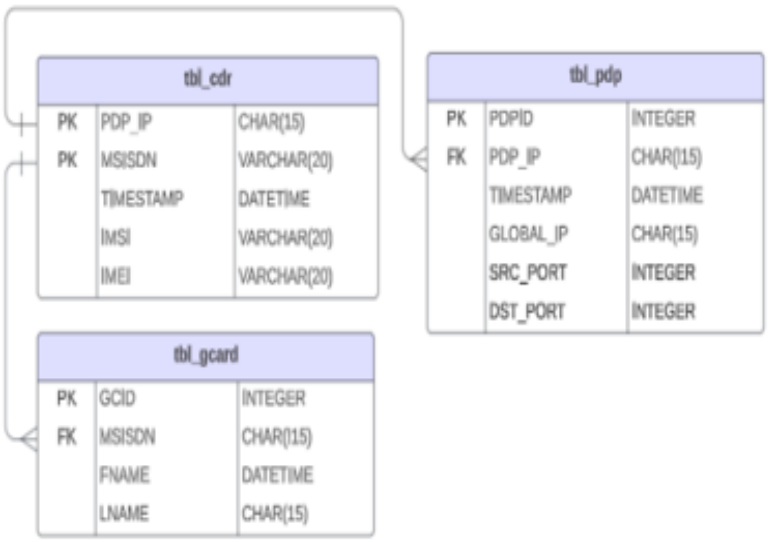


**Figure 8.** Data Model – Framework

**Table 1.** PDP Activations & Data Sessions - Sample Dataset.

| | UE | | | | | | | PDN | |
|---|---|---|---|---|---|---|---|---|---|
| | **App** | **Location** | **App Src-IP** | **Dst-IP** | **App Src-Port** | **Dst-Port** | **PDP IP Address** | **Global-IP** | **Global-Port** |
| **ISP-1** | Chrome | Adentan | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.121.96.193 | 102.176.94.129 | 41753 |
| | Chrome | Adentan | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.121.3.213 | 102.176.94.85 | 11025 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.137.32.206 | 102.176.94.142 | 36938 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.123.223.213 | 102.176.94.213 | 31555 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.136.217.92 | 102.176.94.220 | 61149 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.137.190.92 | 102.176.94.156 | 41071 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.137.234.187 | 102.176.75.187 | 59436 |
| | DuckDuckGo | Mamprobi | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.122.155.22 | 102.176.94.214 | 16418 |
| | DuckDuckGo | Mamprobi | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.137.117.209 | 102.176.75.145 | 10900 |
| | DuckDuckGo | Mamprobi | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.137.252.33 | 102.176.94.97 | 46322 |
| **ISP-2** | Firefox Focus | Korley Klotey | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.57.25.48 | 41.215.171.141 | 37834 |
| | Chrome | Korley Klotey | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.57.71.20 | 41.215.171.159 | 36813 |
| | Ms Edge | Korley Klotey | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.57.116.248 | 41.215.171.177 | 41291 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.56.215.42 | 41.215.173.65 | 10640 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.59.62.127 | 41.215.173.97 | 34520 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.57.148.98 | 41.215.171.59 | 41074 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.59.76.52 | 41.215.173.21 | 52770 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.58.67.99 | 41.215.171.235 | 16815 |
| | DuckDuckGo | Mamprobi | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.57.40.66 | 41.215.171.174 | 49390 |
| | DuckDuckGo | Mamprobi | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.56.147.76 | 41.215.173.20 | 21434 |
| **ISP-3** | Google Chrome | Ledzokuku-Krowor | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.41.220.119 | 154.160.10.0 | 59518 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Ms Edge | Ledzokuku-Krowor | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.19.242.126 | 154.160.7.250 | 10529 |
| | Firefox Focus | Ledzokuku-Krowor | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.18.171.28 | 154.160.11.188 | 43002 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.195.163.169 | 154.160.4.150 | 53139 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.104.150.223 | 154.160.1.98 | 36741 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.104.140.84 | 154.160.4.52 | 45442 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.7.239.184 | 154.160.6.97 | 20615 |
| | DuckDuckGo | Kasoa | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.21.197.107 | 154.160.7.11 | 53323 |
| | DuckDuckGo | Mamprobi | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.149.148.169 | 154.160.27.22 | 13490 |
| | DuckDuckGo | Mamprobi | 192.168.0.10 | 199.79.62.108 | 32763 | 80 | 10.182.188.74 | 154.160.27.118 | 22049 |

The high-level conceptual view of the proposed data model for packets to be captured by the probes is given in Figure 8 above. As already reviewed, mobile ISPs make use of CDRs basically for billing purposes. Key CDR fields relevant to the proposed solutions are captured in "tbl_cdr" table; table "tbl_cdr" primary key is the composite type. Also, per regulatory requirements, ISPs are to register SIMs with the Ghana card as the sole identification material of the user; user profile attributes are captured in the "tbl_gcard" table. Logical table "tbl_pdp" captures the parameters that were investigated in this exercise.

The framework is proposed to be used in the mobile broadband domain (MBB) that make use of digital footprints such as PDP context IP address as source IP, UEs application TCP or UDP source port, UEs application TCP or UDP destination port and destination IP address in the public data network. To complement these digital footprints to really get hold of the cybercrime when committed from the MBB, the framework also suggested the use of relevant aspects of call data records such as IMSI, MSISDN, IMEI and timestamp of acquiring the digital footprints parameters. To synthesise these dichotomous datasets to point to a unique entity, Dr.Codd's relational database model was leveraged. Table 2 below is the data dictionary for the data model in Figure 8.

**Table 2.** Data Dictionary for Data Model

| **tbl_cdr** | | |
|---|---|---|
| **Attribute** | **Explanation** | **Key** |
| PDP_IP | PDP context IP | Composite Key |
| MSISDN | Mobile Station International Subscriber Directory Number | Composite Key |
| TIMESTAMP | Date and time of CDR capture | |
| IMSI | International Mobile Subscriber Identity | |
| IMEI | International Mobile Equipment Identity | |
| **tbl_gcard** | | |
| GCID | Ghana card identification number | Primary key |
| MSISDN | Mobile Station International Subscriber Directory Number | Foreign key |
| FNAME | First name of user | |
| LNAME | Last Name of user | |
| **tbl_pdp** | | |
| PDPID | Surrogate unique identifiication of a PDP context | Primary key |
| PDP_IP | PDP context IP | Foreign key |
| TIMESTAMP | Date and time of PDP IP acquisition | |
| GLOBAL_IP | Dynamic NAT IP to PDN, i.e. Target IP | |
| SRC_PORT | Application source port | |
| DST_PORT | Target service port | |

## Conclusion

This paper set out to put forth an innovative framework primarily aimed at locating the sources of cybercrime, from the MBB domain, thereby addressing the need for improved identification and attribution of malicious online activities. The research revealed that, digital footprints collected within the MBB and PDN

domains when combined with call detail records and Ghana card user profile by leveraging Edgar Frank Codd's relational data model to synthesise the fragmented datasets to a unique entity, forms a comprehensive approach to locating cybercrime sources committed from the MBB domain. The proposed framework holds the potential for enhancing cybercrime forensics and attribution in Ghana by offering a detailed methodology for tracing malicious activity back to its source. While the framework offers valuable means for identifying cybercriminal sources from the MBB domain, its effective implementation relies heavily on cooperation between ISPs and state agencies mandated at fighting cybercrime. However, this paper is not oblivious to ongoing challenges posed by domain obfuscation, Virtual Private Networks and anonymous networks. The application or development of AI tools capable of analysing large data volumes is recommended.

The evolution of cyber threats continues unabatedly and calls for corresponding strategies and technological approaches at combating the menace. This paper provides a foundational approach to locating the sources of cybercrime from the MBB domain by offering valuable framework aimed at offering cybersecurity professionals and law enforcement agencies, with the collaboration of ISPs, to effectively fighting cybercrime in Ghana.

## Conflict of Interest

I, Daniel Adjei Odai, hereby declare that, there are no conflicts of interest regarding this research work.

All cost involved were solely financed by the author of this paper.

## Acknowledgement

My profound gratitude goes to my wife for her encouragement and motivation.

## References

[1]. ITU, Facts and Figures, 2024, International Telecommunications Union, https://www.itu.int/en/mediacentre/Pages/PR-2024-11-27-facts-and-figures.aspx

[2]. NCA, 2023, "Quarterly Statistical Bulletin on Communications in Ghana", National Communications Authority, 8(4), https://nca.org.gh/wp-content/uploads/2024/05/Q2-2023-Quarterly-Statistical-Bulletin-Final-Version.pdf

[3]. Ennin, D., Mensah, R. O., 2019, Cybercrime in Ghana and the Reaction of the Law, JL Pol'y & Globalization, vol. 84, no. 36

[4]. Gyesi, Z. K., 2020, Increased cybercrimes due to lack of successful investigations and prosecutions, Graphic, https://www.graphic.com.gh/news/general-news/increased-cybercrimes-due-to-lack-of-successful-investigations-and-prosecutions-dr-antwi-boasiako.html

[5]. Alhassan, M. M., Adjei-Quaye, A., 2017, Computer & Cyber Forensics: A Case Study of Ghana. American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS), 28(1), 167-176.

[6]. Rid, T., Buchanan, B., 2015, Attributing cyber attacks. Journal of strategic studies, 38(1-2), 4-37.

[7]. IC3, 2023, Federal Bureau of Investigation: Internet Crime Report, Internet Crime Complaint Centre

[8]. Obeng, C., Kumah, P. K., Asiedu, H. B., Senior, F. A. O., 2023, “Understanding Cybercrime in Developing Economies: Insights from Agona Swedru, Ghana”, Communications, 10(1), 1-10.

[9]. Ghanaian Times, 2023, “Ghana loses GHC49.5m to Cyber Fraud in six months”, https://www.ghanaiantimes.com.gh/ghana-loses-ghc49-5m-to-cyberfraud-in-six-mths

[10]. Jiri Techet, 2024, Network Analyzer, https://techet.net/netanalyzer

[11]. Softonic, 2024, Softonic, https://packet-capture.en.softonic.com/android

[12]. Wireshark, 2024, Wireshark Foundation, https://www.wireshark.org
[13]. Oracle, 2024, MySQL, https://www.mysql.com
[14]. cPanel, 2024, cPanel, https://cpanel.net
[15]. Ságvári, B., Gulyás, A., & Koltai, J., 2021, Attitudes towards participation in a passive data collection experiment. Sensors, 21(18), 6085
[16]. Starrin, B., Hagquist, C., Larsson, G., & Svensson, P. G., 1993, "Community types, socio-economic structure and IHD mortality—a contextual analysis based on Swedish aggregate data", Social Science & Medicine, 36(12), 1569-1578
[17]. Morgenthaler, S., 2009, Exploratory data analysis, Wiley Interdisciplinary Reviews: Computational Statistics, vol. 1, pp. 33-44
[18]. Kamble, D., Rathod, S., Bhelande, M., Shah, A., & Sapkal, P., 2024, "Correlating forensic data for enhanced network crime investigations: Techniques for packet sniffing, network forensics, and attack detection. J. Auton. Intell", 7, 1272.
[19]. Sikder, R., Uddin, M. J., & Halder, S., 2016, An efficient approach of identifying tourist by call detail record analysis, In 2016 International Workshop on Computational Intelligence (IWCI), IEEE, pp. 136-141
[20]. GSMA, 2014, GPRS Security Guide for Users, GSM Association, Vol. 3.1, https://www.gsma.com/newsroom/wp-content/uploads/SG.16-v3.1.pdf
[21]. DPA, 2012, "Ghana - Data Protection Act 2012"
[22]. Data Protection Commission of Ghana, 2024, "Home", https://dataprotection.org.gh
[23]. Chen, P. P. S., 1976, The entity-relationship model—toward a unified view of data, ACM transactions on database systems (TODS), 1(1), 9-36.