Investigating VoIP Calls: Law Enforcement Perspective

SH. ARJUN CHETRY[1]
DR. UZZAL SHARMA[1,2]

[1] Assam Don Bosco University, Guwahati, Assam
[2] Birangana Sati Sadhani Rajyik Viswavidyalaya,
Golaghat, Assam
[1]chetry.arjun@gmail.com
[2]druzzalsharma@gmail.com

Abstract. Technology is advancing at an unprecedented pace, playing a pivotal role in benefiting society across various domains. However, it also presents formidable challenges for law enforcement agencies. Among the most significant current hurdles, lies in the anonymity criminals can maintain on the internet, particularly through VoIP calls. Policing is an ever-evolving field, demanding investigators to be adaptable in mastering novel investigative techniques. Whether dealing with conventional or tech-related crimes, call detail records have become indispensable components of any investigation. With the surge in smartphone usage and mobile data connections, IP address-based investigations have become imperative, especially when dealing with VoIP calls. Consequently, the ability to trace IP addresses has become a pressing necessity for investigators handling numerous cases involving VoIP calls. This research paper delves into the investigation of VoIP calls, employing IPDR and PCAP files to identify IP addresses.

Keywords: VoIP calls, WhatsApp calls, IPDR analysis, CDR analysis, anonymous communication, mobile technology, anonymity, anonymous calls.

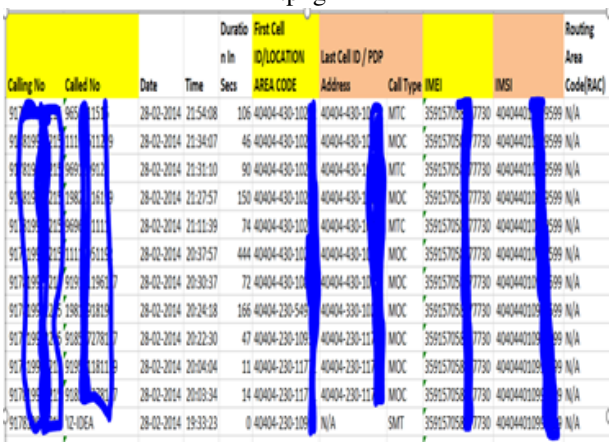
(Received December 12th, 2023 / Accepted June 28th, 2024)

1 Introduction

Mobile technology has become an integral part of modern society, and regardless of whether the crime is traditional or technical in nature, Call Detail Records (CDRs) and Internet Protocol Detail Records (IPDRs) have become essential components of investigations conducted by law enforcement agencies[22][13][18]. The widespread use of VoIP calls through applications such as WhatsApp, Duo, Facebook Messenger, etc., over mobile data connections has made IPDRs the starting point for policing investigations [6][29]. Various crimes are being committed using VoIP calls, with perpetrators exploiting the anonymity provided by the internet and utilizing different applications and online servers [8][19][27]. Technological criminals have the advantage of using platforms like social engineering toolkits, Linux distributions for anonymity, proxy servers, VPN servers, and applications like WhatsApp, Signal, Telegram, Skype, among others, unintentionally facilitating criminal activities. Detecting and intercepting VoIP calls poses a significant challenge due to the implementation of robust encryption[14][11]. Consequently, investigators face numerous challenges when dealing with crimes involving data connections. However, it is worth noting that despite the exploitation of secure technology by criminals, many cases have been successfully solved through IP address tracing and analysis. It is important to mention that despite exploitation of secure technology by criminals, many cases solved with the help of IP Address tracing or analysis[31][32][9]. Few example of crimes or challenge may be as under:

a) Registration of fake numbers on application like WhatsApp, telegram, etc. using publicly available

1.png



Calling No	Called No	Date	Time	Duration In Secs	First Cell ID/LOCATION AREA CODE	Last Cell ID / POP Address	Call Type	IMEI	IMSI	Routing Area Code(RAC)
[redacted]		28-02-2014	21:54:08	106	40404-430-10[redacted]	40404-430-10[redacted]	MTC	[redacted]	[redacted]	N/A
[redacted]		28-02-2014	21:34:07	46	40404-430-10[redacted]	40404-430-1[redacted]	MOC	[redacted]	[redacted]	N/A
[redacted]		28-02-2014	21:31:10	90	40404-430-10[redacted]	40404-430-1[redacted]	MTC	[redacted]	[redacted]	N/A
[redacted]		28-02-2014	21:27:57	150	40404-430-10[redacted]	40404-430-1[redacted]	MOC	[redacted]	[redacted]	N/A
[redacted]		28-02-2014	21:11:39	74	40404-430-10[redacted]	40404-430-1[redacted]	MTC	[redacted]	[redacted]	N/A
[redacted]		28-02-2014	20:37:57	444	40404-430-10[redacted]	40404-430-1[redacted]	MOC	[redacted]	[redacted]	N/A
[redacted]		28-02-2014	20:30:37	72	40404-430-10[redacted]	40404-430-1[redacted]	MOC	[redacted]	[redacted]	N/A
[redacted]		28-02-2014	20:24:18	166	40404-230-54[redacted]	40404-330-1[redacted]	MOC	[redacted]	[redacted]	N/A
[redacted]		28-02-2014	20:22:30	47	40404-230-109[redacted]	40404-230-11[redacted]	MOC	[redacted]	[redacted]	N/A
[redacted]		28-02-2014	20:04:04	11	40404-230-117[redacted]	40404-230-11[redacted]	MOC	[redacted]	[redacted]	N/A
[redacted]		28-02-2014	20:03:34	14	40404-230-117[redacted]	40404-230-11[redacted]	MOC	[redacted]	[redacted]	N/A
[redacted]	VI2-IDEA	28-02-2014	19:33:23	0	40404-230-109[redacted]	N/A	SMT	[redacted]	[redacted]	N/A

Figure 1: Call Details Record

2.png

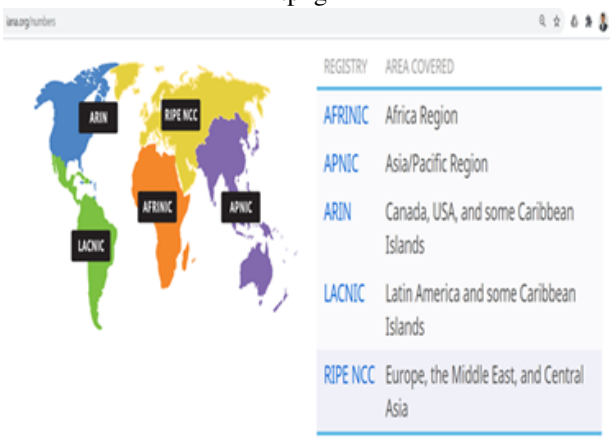


Figure 2: IP Address Registry ? source: iana.org

3.png

Figure 3: Information of IP Address

websites for receiving online OTP instead of OTP on sim card and then performing criminal activity using that account on the application [17][3].

b) Registration of fake documents for getting sim card and then using data connection of this sim card for committing crimes like identity theft for performing phishing attack, social engineering attack, etc.[34][5][30].

c) Creation of fake profile on social network platform maintaining anonymity by using the fake number and online OTP. Such fake number/fake profiles are being use for spreading viral messages, photos, videos, etc., for defamation, threatening, blackmailing, etc.[26][10][23].

2 INVESTIGATION OF SUCH CRIME:

Whenever any crime is committed, investigator have to start the investigation from the receiving end. Therefore, it imposes a challenge to trace the source from target end. From the point of view of mobile network, if somebody is threatening any person over calls, then finding the details about that person is not challengeable as CAF, CDR, etc. is available with mobile service provider[28][16]in Figure 1.

Call details record reveals that the calling party is connected to called party on date time, location, device, etc. By analysing such information, we may find the details of user involved in calls with criminal?s number. Also, by analysis of CDR, we may find out information about towers that this criminal is using to know the exact location or patterns of movements. If the criminal is not using the calls or SMS facility of mobile technology, then entry of records is not available in CDR so the challenges are more to investigator [36][2]. It is noticed that the criminals are slowly and gradually avoiding calls and SMS and in fact using these facilities to manipulate the investigator during investigation by showing that their location was different from crime scene. Therefore, involvement of IP Address is creasing day by day in investigation as the criminal is using IP based connections in committing crimes[35][21].

As per IANA[20][25], IP Addresses are managed by registry as shown in Figure 2

From IANA, IP Address are distributed to Regional registry and as per their concern registry ISP are purchasing the IP Address and further allocating the IP Address to the end users or organizations. Details of public IP Address may be available on surface web [1] [12] as shown in Figure 3

In general, ISP details is available from the whois information for any particular IP Address. So, trac-

4.png

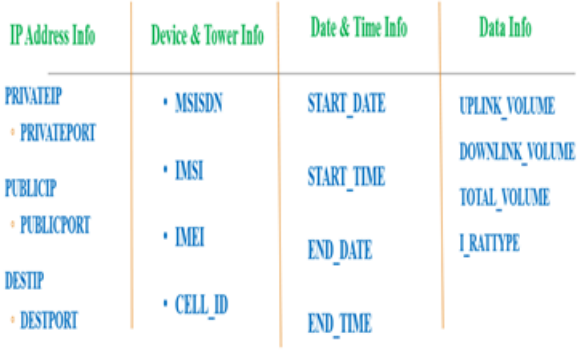


Figure 4: Heading of IPDR

ing the IP address for any types of crimes are fully dependent on ISP and their IP allocation details for any particular date and time. So, the analysis of IP details record(IPDR), stored fields as shown in Figure 4 , which is received from ISP is very important for investigation.

With the types of records available on IPDR, it is realized that tracing of IP Address is not easy due to reasons, not limited to: -

1 IP based communication is happening with three IP addresses, namely, source IP address, connection IP address and destination IP address.

2 Details of source IP, ISP and destination is reflected in the IPDR records maintained by the ISP but merely having these three details are not enough to identify who is connected in the other side of the conversation, either text messages or voice over calls. So, as compare to CDR, where two end user mobile numbers are clearly record in the CDR, end user connected over internet or data connections are not clear, which directly impose a challenge to the investigator for proceeding the investigation. From the IPDR records, it is clear that the connection from user IP to server IP is maintained but from that server to recipient IP is not maintained in the IPDR records. So, analysis of IPDR is not revealing the two connected person over chat or over VOIP calls.

3 Location of IP Address is not directly connected to the end users as GPS coordinates of end user devices are not recorded in the IPDR records maintained by the ISPs in this IPDR. Merely giving the IP Address is not satisfying the criteria of investigation as the same IP Address is allocated to multiple users over the internet from different locations.

3 EXPERIMENTAL SETUP

For experiment purpose, we have taken the scenarios where internet is used for making threatening calls over any of these platform, like WhatsApp, Telegram, Signal, etc. by maintaining anonymity over internet.

3.1 Investigation requirement during such cases is as under: -

a. Getting the Information of remote/accused IP Address from Server involved for this conversation. It is pertinent to mention that the server may not be responding as per the requirements based on different reasons, not limited to, beyond national jurisdiction, non-cooperation with LEAs, non-friendly country, etc.

b. Alternate method used in this paper is to Setup the WhatsApp call with the accused and then capture the packets of VoIP call and then perform the Analysis for locating the remote/accused IP Address.

3.2 Finding the details of IP Address:

a. Based on the open source information using whois, we may find the details of ISP/organization/Individual responsible for the concern IP Address.

b. Perform the IPDR analysis on that IP Address for identification of device details like IMEI, IMSI, MSDN, etc. for the concern conversation date/time or for the particular Cell-Id or location.

4 SIMULATION SCENARIO

Accused is asking the money or ransomware by blackmailing, based on the scenarios of the cases. So, technically, there is one accused person, say Mr. A, bearing number as +91-9485xxx139 and the victim, say Mr. B, bearing number +91-94840xxx13.

The initial step in the investigation involves requesting information from the Mobile Service Provider to verify the validity of the provided number. If the number found to be invalid or associated with false documents, alternative methods are pursued. One such method is reaching out to the respective server, like WhatsApp, to obtain the IP Address linked to the active account if it is currently in use. However, it is important to note that this IP Address may not always be the most up-to-date, potentially limiting its utility.

5.png

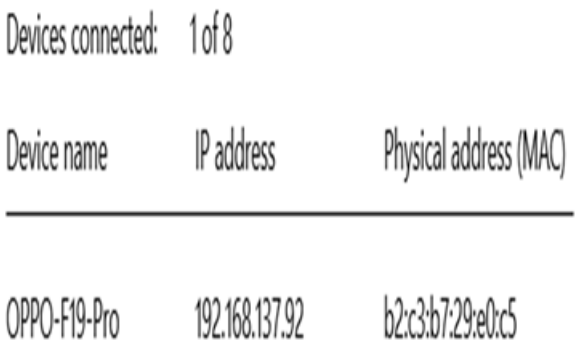


Figure 5: Mobile Details

6.png

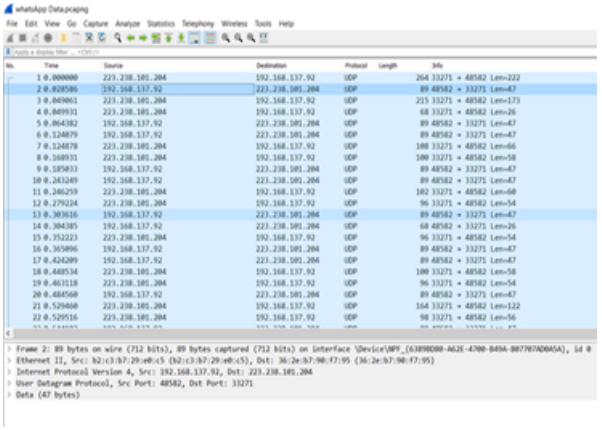
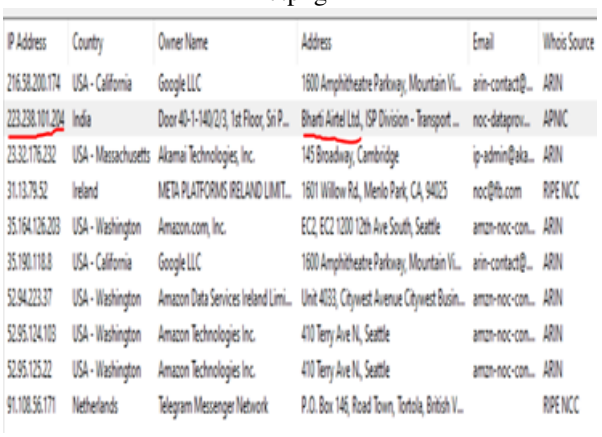


Figure 6: Packet Capture using Wireshark

7.png



IP Address	Country	Owner Name	Address	Email	Whois Source
216.58.200.174	USA - California	Google LLC	1600 Amphitheatre Parkway, Mountain Vi...	arin-contact@...	ARIN
223.238.101.204	India	Door 40-1-140/2/3, 1st Floor, Sri P...	Bharti Airtel Ltd., ISP Division - Transport ...	noc-dataprov...	APNIC
23.32.176.232	USA - Massachusetts	Akamai Technologies, Inc.	145 Broadway, Cambridge	ip-admin@aka...	ARIN
31.13.79.52	Ireland	META PLATFORMS IRELAND LIMIT...	1601 Willow Rd, Menlo Park, CA, 94025	noc@fb.com	RIPE NCC
35.164.126.203	USA - Washington	Amazon.com, Inc.	EC2, EC2 1200 12th Ave South, Seattle	amzn-noc-con...	ARIN
35.190.118.8	USA - California	Google LLC	1600 Amphitheatre Parkway, Mountain Vi...	arin-contact@...	ARIN
52.94.223.37	USA - Washington	Amazon Data Services Ireland Limi...	Unit 4033, Citywest Avenue Citywest Busin...	amzn-noc-con...	ARIN
52.95.124.103	USA - Washington	Amazon Technologies Inc.	410 Terry Ave N, Seattle	amzn-noc-con...	ARIN
52.95.125.22	USA - Washington	Amazon Technologies Inc.	410 Terry Ave N, Seattle	amzn-noc-con...	ARIN
91.108.56.171	Netherlands	Telegram Messenger Network	P.O. Box 146, Road Town, Tortola, British V...		RIPE NCC

Figure 7: Information about IP Address

To address this issue and obtain the most recent active IP Address, the researchers implemented a technique involving the capture of network packets during the conversation using Wireshark[33][24]. By employing this approach, the active IP Address of the remote user could be determined, offering a valuable lead in the investigation. In the context of this paper, the IP Address of the victim, Mr. B, also noted for reference during the course of the conversation analysis as shown in figure 5. It is evident that these methodologies are crucial in uncovering crucial information related to cybercrimes and tracking down individuals involved in illegal activities. The research efforts outlined in this paper contribute to advancing investigative techniques, thus enabling law enforcement to stay ahead in the battle against cyber threats and protect potential victims effectively.

To find out the real IP Address of this anonymous accused, remote WhatsApp user, packets was captured for the WhatsApp calls over internet using Wireshark software as shown in figure 6. There are many remote IP Addresses and UDP protocol is visible in picture. Analysis of WhatsApp voice calls may be different then the analysis of messages[7] as the protocol engaged for transmission as well as encryption may be different. In this paper, we intend to analyse the VoIP calls of WhatsApp.

5 RESULTS AND DISCUSSION

In VoIP call, TCP connection is used for establishing the connection between the users and then UDP Protocols is engaged for actual transfer of packets. So, during analysis, it is found that the UDP packets are exchanged between the IP Address, 192.168.137.92 (Mr B, Victim) on mac address, b2:c3:b7:29:e0:c5 and remote IP Addresses.

Some of the probable remote IP Address connected during VoIP calls are identified and accordingly IP Address resolution through online whois records is performed. Result of the same is is shown in Figure 7

Therefore, from this IP Address resolution, it is found that the most probable IP Address engaged during VoIP call is 223.238.101.204 as all other remote IP Address are engaged for some of the renown servers. It is further identified that this IP Address is connected through UDP protocol as shown in figure 8 , which further supports that this IP was engaged for VoIP Calls.

Further analysis was made by giving filter on both IP Address and port number engaged for UDP protocol and clearly visible that this two IP Address was exchanging the packets as shown in figure 9

8.png

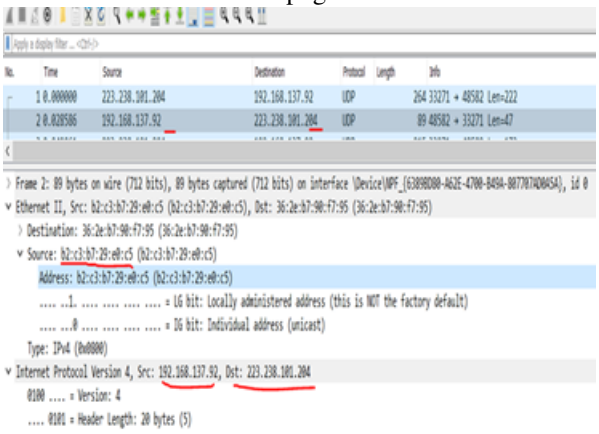


Figure 8: Mac Address and IP Address of mobile number in packet

9.png

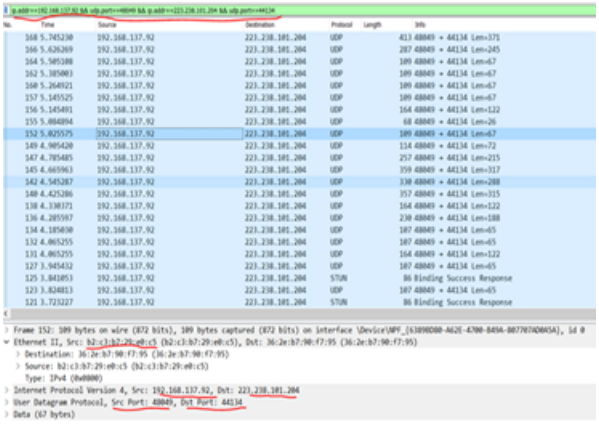


Figure 9: UDP packet between two IPs

10.png

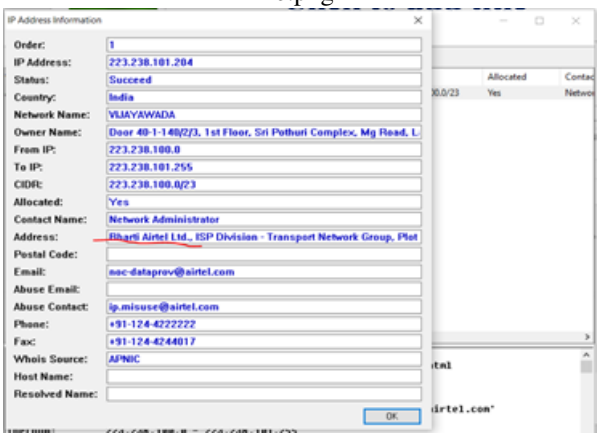


Figure 10: Remote ISP Bharti Airtel

Hence, it may be concluding that this remote IP may be the IP Address of the remote ISP, which is used for the WhatsApp call. Complete details of this public IP Address, 223.238.101.204, was checked and found that the IP Address belongs to Bharti Airtel Group, so the remote ISP is bharti airtel as shown in Figure 10

Absolutely, the technique of capturing packets during VoIP communication allows for the identification of remote IP Addresses. However, it is crucial to adhere to privacy policies and legal procedures when extracting further details about the concerned user. By conducting a thorough analysis of the IP Address and its IPDR records, investigators can effectively probe cases involving VoIP calls related to crimes such as threatening, harassment, ransomware, and others, especially those targeting vulnerable groups like women and children. IPDR analysis proves to be an invaluable tool in understanding user behaviour in cyberspace. It helps investigators identify the general patterns of internet connection usage associated with a particular IP Address. This method can be effectively employed when investigating cases involving servers like WhatsApp, Facebook, Google, Telegram, and other platforms. Embracing this technique allows law enforcement to tackle cybercrime more effectively and protect individuals from online threats. However, it is essential to ensure that all investigative efforts adhere to legal and ethical standards to maintain the integrity of the evidence and respect the privacy rights of individuals involved

During analysis of IPDR records, connection between the private IP, public IP Address and Destination con-

11.png

Row Labels	Count of PUBLICIP
223.238.101.204	1400
Google LLC	949
META PLATFORMS IRELAND LIMITED	441
SoftLayer Technologies Inc.	9
SoftLayer Technologies, Inc.	1

Figure 11: IP and selected server Analysis

12.png

Row Labels	Amazon Technologies Inc.	Google LLC	META PLATFORMS IRELAND LIMITED	SoftLayer Technologies Inc.	SoftLayer Technologies, Inc.	Grand Total
223.238.101.204	141	949	441	9	1	1541
10.93.134.252		2		4		6
10.98.57.224				2		2
10.98.195.90		1	2	1		4
10.14.200.105		3		1		4
100.100.64.113		4		1		5

Figure 12: IP and selected server with private IP and frequency

13.png

	1341800074047707	135330046143024	Grand Total
Row Labels	Google LLC	Google LLC	
223.238.101.204	21	1	22
10.164.129.126		1	1
10.92.131.175	21		21

Figure 13: IP and single target server

14.png

Count of PUBLICIP	Column Labels			
Row Labels	1341800074047707	355886052519280	356449061052720	356449061533020
223.238.101.204	21	2	4	1
Amazon Technologies Inc.				
Google LLC	21	2	1	1
META PLATFORMS IRELAND LIMITED			3	
SoftLayer Technologies Inc.				

Figure 14: IP and selected server with device IMEI

15.png

Count of PUBLICIP	Column Labels				
Row Labels	5222	5287	8005	8006	8009
223.238.101.204	84	3	1	1	4
Amazon Technologies Inc.	2				
Apple Inc.					
Google LLC					
PageBites, Inc.					
SoftLayer Technologies Inc.	5				
SoftLayer Technologies, Inc.	1				

Figure 15: IP Address with domain name and selected Port Number

nection may be identified along with frequency of connections among the IP Address which is shown in figure 11and figure 12

Similarly, the analysis may reveal the connection among the device (IMEI/MAC), Private and Public IP Address for a particular destination, say Google, as shown in figure 13and figure 14

Sometime online server may provide IP Address along with port number, then we may analyze the IPDR using Port no as displayed in figure 15 and figure 16

Indeed, the potential combinations for analysis are vast and can be tailored to suit the specific requirements of each case. By utilizing these techniques, investigators can effectively analyse VoIP calls involving anonymous users engaged in criminal activities. Once the accused parties are identified, the associated devices can be pinpointed and seized for further examination. Extracted evidence from these devices can then be sub-

16.png

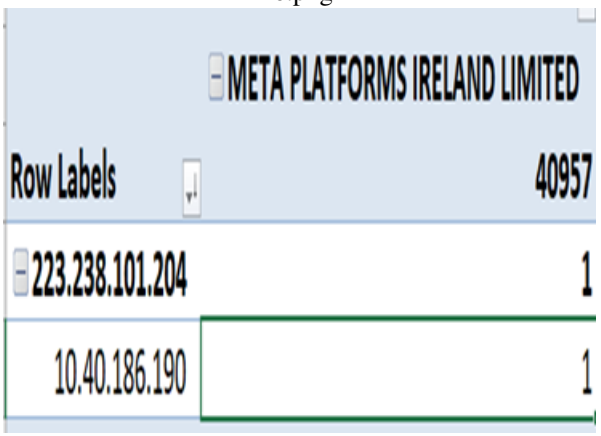


Figure 16: IP Address with private ip address and particular Port Number

jected to rigorous analysis, ensuring its admissibility in the court of law [4][15]. This comprehensive approach equips law enforcement with the necessary tools to build strong cases against perpetrators and contribute to upholding justice in the face of evolving technological challenges.

6 CONCLUSIONS AND FUTURE WORKS:

Dealing with technological crimes necessitates leveraging all available technical resources. With technology and cyberspace becoming a favoured platform for criminals, encompassing both traditional offenses like human trafficking, blackmailing, harassment, defamation, and technical crimes such as financial frauds and identity theft, investigators must have ample options to facilitate their investigations effectively. This research paper highlights a crucial finding that the captured IP packets can potentially reveal the IP Address of remote users, aiding investigators in their pursuit of justice by gathering relevant IPDR information. Looking ahead, similar methodologies could be applied to analyses other VoIP call platforms, exploring the possibilities of identifying remote user IP Addresses in various scenarios. This advancement promises to be a valuable tool in the ongoing battle against cybercrime and technology-related offenses, empowering law enforcement to stay one-step ahead in the ever-evolving landscape of criminal activity.

7 Bibliograph References

References

[1] Whois lookup for ip address 223.238.101.204. `https://whois.domaintools.com/223.238.101.204`, 2023. Accessed: 30th June 2023.

[2] Abba, E., Aibinu, A., and Alhassan, J. Development of multiple mobile networks call detailed records and its forensic analysis. *Digital Communications and Networks*, 5(4):256–265, 2019.

[3] Alghamdi, M. I. A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide. *International Journal of Engineering Research and Technology*, 9:731–735, 2020.

[4] Ashawa, M. and Otache Innocent, O. Forensic data extraction and analysis of left artifacts on emulated android phones: A case study of instant messaging applications. *Circulation in Computer Science*, 2:8–16, 2017.

[5] Atkins, B. and Huang, W. A study of social engineering in online frauds. *Open Journal of Social Sciences*, 1(03):23, 2013.

[6] Bellovin, S. M. and et al. Security implications of applying the communications assistance to law enforcement act to voice over ip. 2006.

[7] Cents, R. and Le-Khac, N. A. Towards a new approach to identify whatsapp messages. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 1895–1902. IEEE, December 2020.

[8] Chen, S., Wang, X., and Jajodia, S. On the anonymity and traceability of peer-to-peer, voip calls. *IEEE Network*, 20(5):32–37, 2006.

[9] Chetry, A. and Sharma, U. Dark web activity on tor?investigation challenges and retrieval of memory artifacts. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2020, Volume 1*, pages 953–964. Springer Singapore, 2021.

[10] Citron, D. K. Addressing cyber harassment: An overview of hate crimes in cyberspace. *Case W. Res. JL Tech. and Internet*, 6:1, 2014.

[11] Cuadra-Sanchez, A. and Aracil, J. A novel blind traffic analysis technique for detection of whatsapp voip calls. *International Journal of Network Management*, 27(e1968), 2017.

[12] Da-Yu, K. A. O., Chang, E. C., and Fu-Ching, T. S. A. I. Extracting suspicious ip addresses from whatsapp network traffic in cybercrime investigations. In *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pages 1108–1115. IEEE, February 2019.

[13] Dobbins, C. and Denton, P. Mywallmate: An investigation into the use of mobile technology in enhancing student engagement. *TechTrends*, 61(6):541–549, 2017.

[14] Freire, E., Ziviani, A., and Salles, R. Detecting voip calls hidden in web traffic. *IEEE Transactions on Network and Service Management*, 5:204–214, 2009.

[15] Harshwardhan, C., Sunny, D., Mehul, L., Rohit, N., and Patil, R. Management of digital evidence for cybercrime investigation–a review. In *International Conference on Soft Computing and Signal Processing*, pages 133–143, Singapore, June 2021. Springer Nature Singapore.

[16] Hidayati, A. N., Riadi, I., Ramadhani, E., and Al Amany, S. U. Development of conceptual framework for cyber fraud investigation. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, 7(2):125–135, 2021.

[17] Hunton, P. Cybercrime and security: A new model of law enforcement investigation. *Policing: A Journal of Policy and Practice*, 4(4):385–395, 2010.

[18] Hunton, P. The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law and Security Review*, 27(1):61–67, 2011.

[19] Ibrahim, M., Abdullah, M. T., and Dehghantanha, A. Voip evidence model: A new forensic method for investigating voip malicious attacks. In *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, pages 201–206. IEEE, June 2012.

[20] Internet Assigned Numbers Authority. IANA Numbering Services. `https://www.iana.org/numbers`, 2023. Accessed: 30th June 2023.

[21] Irwin, D. and Slay, J. *Extracting Evidence Related to VoIP Calls*, pages 221–228. 2011.

[22] Jeffries, S. and Apeh, E. Standard operating procedures for cybercrime investigations: a systematic literature review. *Emerging Cyber Threats and Cognitive Vulnerabilities*, pages 145–162, 2020.

[23] Laurensius, S., Situngkir, D., Putri, R., and Fauzi, R. Cyber bullying against children in indonesia. In *Proceedings of the first International Conference on Social Sciences, Humanities, Economics and Law*, March 2019.

[24] Musa, A. Forensic analysis of peer-to-peer network traffic with wireshark. *SLU Journal of Science and Technology*, 1(2):92–99, 2020.

[25] Prasad, R. and Rohokale, V. *Cyber Threats and Attack Overview*, pages 15–31. 2020.

[26] Putri, A. and Israhadi, E. Law enforcement of criminal defamation on social media. In *Proceedings of the 2nd International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2022*, August 2022.

[27] Sarhan, S. A. E., Youness, H. A., and Bahaa-Eldin, A. M. A framework for digital forensics of encrypted real-time network traffic, instant messaging, and voip application case study. *Ain Shams Engineering Journal*, 14(9):102069, 2023.

[28] Shalaginov, A., Johnsen, J. W., and Franke, K. Cyber crime investigations in the era of big data. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 3672–3676. IEEE, December 2017.

[29] Shubha, C., Sushma, S. A., and Asha, K. H. Traffic analysis of whatsapp calls. In *2019 1st International Conference on Advances in Information Technology (ICAIT)*, pages 256–260, 2019.

[30] Siddiqi, M. A., Pak, W., and Siddiqi, M. A. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, 12(12):6042, 2022.

[31] Swamy, K. K., Teakumalla, S., Vemula, D., Patil, S. R., and Deepika, P. Detection of ip masking using whois. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 14(03):115–124, 2023.

[32] Wickramasinghe, N., Nabeel, M., Thilakaratne, K., Keppitiyagama, C., and De Zoysa, K. Uncovering ip address hosting types behind malicious websites. *arXiv preprint*, 2021.

[33] Wireshark. Wireshark. https://www.wireshark.org, 2023. Accessed: 30th June 2023.

[34] Yasin, A., Fatima, R., Liu, L., Wang, J., Ali, R., and Wei, Z. Understanding and deciphering of social engineering attack scenarios. *Security and Privacy*, 4(4):e161, 2021.

[35] Yen, Y.-S., Lin, I.-L., and Wu, B.-L. A study on the forensic mechanisms of voip attacks: Analysis and digital evidence. *Digital Investigation*, 8:56–67, 2011.

[36] Zhu, Y. and Fu, H. Traffic analysis attacks on skype voip calls. *Computer Communications*, 34(10):1202–1212, 2011.