



ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for Electronic Crime Investigation (IJECI)



VOL: 6
ISSUE: 4 Year 2022

Email ID: ijeci@lgu.edu.pk

Digital Forensics Research and Service Center
Lahore Garrison University, Lahore, Pakistan.

International Journal for Electronic Crime Investigation
Volume 6(4) Year (2022)

SCOPE OF THE JOURNAL

The International Journal for Crime Investigation IJECI is an innovative forum for researchers, scientists and engineers in all the domains of computer science, white Collar Crimes, Digital Forensics, Nano Forensics, Toxicology and related technology, Criminology, Criminal Justice and Criminal Behaviour Analysis. Moreover, the scope of the journal includes algorithm, high performance, Criminal Data Communication and Networks, pattern recognition, image processing, artificial intelligence, VHDL along with emerging domains like quantum computing, IoT, Hacking. The journal aims to provide an academic medium for emerging research trends in the general domain of crime investigation.

SUBMISSION OF ARTICLES

We invite articles with high quality research for publication in all areas of engineering, science and technology. All the manuscripts submitted for publication are first peer reviewed to make sure they are original, relevant and readable. Manuscripts should be submitted via email only.

To submit manuscripts by email with attach file is strongly encouraged, provided that the text, tables, and figures are included in a single Microsoft Word/Pdf file.

Contact: For all inquiries, regarding call for papers, submission of research articles and correspondence, kindly contact at this address:

IJECI, Sector C, DHA Phase-VI Lahore, Pakistan

Phone: +92- 042-37181823

Email: IJECI@lgu.edu.pk

International Journal for Electronic Crime Investigation
Volume 6(4) Year (2022)

CONTENTS

Research Article

Prof. Dr. Aftab Ahamd Malik, Dr. Mujtaba Asad and Dr. Waqar Azeem
Frauds in Banking and Entrepreneurs by Electronic Devices and
Combating Using Software and Employment of Demilitrized Zone
in the Networks 01-08

Research Article

Bisma Sher Ali
Application of nanotechnology in criminology and forensic Sciences 09-14

Research Article

Taseer Suleman and Nadia Liaquat
Cyber Security Incident Response and Reverse Engineering 15-28

Research Article

Muhammad Shairoze Malik, Arooj Fatima and Saad Waqas
Analysis of Packet to Detect Malware Files 29-36

Research Article

Asif Ibrahim and Syed Khurram Hassan
Role of Analytical Techniques in Crime Investigation 37-46

International Journal for Electronic Crime Investigation

Volume 6(4) Year (2022)

Patron in Chief: Maj General (R) Shahzad Sikander, HI(M)
Vice Chancellor, Lahore Garrison University

Advisory Board:

Mr. Kaukab Jamal Zuberi, HOD Department of Criminology and Forensic Sciences,
Lahore Garrison University, Lahore.
Dr. Abeo Timothy Apasiba, Temale Technical University, Central African Republic.
Dr. Atta-ur-Rahman. Imam Abdulrahman Bin Faisal University (IAU), Saudia Arabia.
Dr. Natash Ali Mian. Beaconhouse National University, Lahore.
Prof. Dr. Shahid Tufail, PCSIR, Lahore.
Prof. Dr. M. Pervaiz Khurshid, Govt College Science, Lahore.
Dr. Nadeem Abbas, Linnaeus University, Sweden

Editorial Board:

Dr. Badria Sulaiman Alfurhood, Abdulrahman University, Saudia Arabia.
Dr. Muhammad Adnan Khan, Gachon University, Seongnam, Republic of Korea.
Dr. Faheem Khan, Gachon University, Seongnam, Republic of Korea.
Prof. Dr. Peter John, GC University, Lahore
Prof. Dr. Saqib Shehzad, Higher Education Department, Lahore
Dr. Shabbir Hussain, KFUEIT, Rahim Yar Khan.
Dr. Kausar Perveen, Higher Education Department, Lahore
Dr. Tahir Alyas, ORIC Director, Lahore Garrison University
Dr. Zahida Perveen, Lahore Garrison University.
Dr. Ahmed Naeem, Lahore Garrison University
Dr. Sumaira Mazhar, Lahore Garrison University.
Dr. Roheela Yasmeen, Lahore Garrison University.

Editor in Chief: Dr. Syeda Mona Hassan, Lahore Garrison University.

Editor: Dr. Syed Ejaz Hussain, Lahore Garrison University.

Managing Editor: Ms. Fatima, Lahore Garrison University.

Assistant Editors: Ms. Shaheera Safdar, Lahore Garrison University.
Mr. Qais Abaid, Lahore Garrison University.

Reviewers Committee:

Dr. Qaisar Abbas, Islamic University of Madinah, Madinah, Saudia Arabia.
Dr. Shehzad Ahmad. King Fahd University of Petroleum & Minerals, Saudia Arabia.
Dr. Haroon Ur Rasheed, University of Lahore.
Dr. Munawar Iqbal, University of Education, Lahore.
Engr. Dr. Shahan Yamin Siddiqui. Minhaj University Lahore.
Dr. Saima Naz, University of Education, Lahore.
Dr. Shagufta Saeed, UVAS, Lahore.
Dr. Shazia Saqib, University of Central Punjab, Lahore.
Dr. Mohsin Javed, UMT, Lahore.
Dr. Ayesha Atta, GC University, Lahore.
Dr. Nida Anwar, Virtual University of Pakistan, Pakistan.



Frauds in Banking and Entrepreneurs by Electronic Devices and Combating Using Software and Employment of Demilitrized Zone in the Networks

Prof. Dr. Aftab Ahamd Malik¹, Dr. Mujtaba Asad² and Dr. Waqar Azeem³

¹University of Kent, England.

¹Department of Criminology and forensic Sciences, Lahore Garrison University, Lahore

²Shanghai Jiao Tong University, China

³South Eastern Regional College, Downpatrick, Ireland UK

Corresponding author: dr_aftab_malik@yahoo.com

Received:02 september,2022; Accepted:05 November,2022; Published: 20 December,2022.

Abstract

The malpractices and frauds are exponentially rising in developed and developing countries in the entrepreneurs, banking as well as medium sized companies. The criminals are utilizing most modern information technology structures and such electronic media to accomplish their offence regarding fraud to cause wrongful loss and harm in the areas of white collar crimes, banking, business and to individuals. The purpose of this research paper is make these companies realize the essence of using most recent, most reliable and most authentic software and need to make their networks more secure from outside attacks. The use of advanced features of tracking and hacking confidential information using information technology resources enables the criminals to achieve their objectives. Basically, their modes operandii depend upon dishonesty and deception to complete the offence. In the banking and white collar frauds most of the time the employees of the concerned organizations are involved, who help and collaborate external criminals by passing confidential information. The fraud is constituted by parody, distortion, misrepresentation and twisting the fact/truth or concealment of a real information detrimental to someone else. The legislation seems very naïve to punish the criminal who have committed frauds. There are several reasons for the criminals to escape, for example their identity is most of the times remains hidden. Lack of evidence, feeble investigation and naïve role of prosecution in the court of law enables the criminals to go towards exoneration and release. The paper also presents analysis of various types of frauds existing in the society and how to combat with them effectively. The main objective of the fraudsters is to deprive people or entrepreneurs of their money, property, valuable documents and private information. The authors of this paper express their deep concern on taking strict measures to safeguard the rights of bank customers by introducing most recent software versions and the government must introduce stern and stringent legislation in this direction.

Keywords: Demilitarized zone (DMZ), Fraud, Hacking, Financial Crimes, Cyber Crime

1. Introduction

According to [1] the corruption purchasing and selling of securities from the period 1870 to 1940 and [2] from 1940 to 1980 is discussed in depth; while [3] highlights the history of frauds in American Business and designing of self-regulations related to the period 1895 to 1932. According to [4] and [5] frauds in the American history have been discussed and [6] emphasizes on understanding the legal procedures, plan, policy and practice. The behavior in case of committing frauds involves the ingredients such as apparent, superficial financial need and reasoning for validation and its rationalization. Legally speaking, the fraud is constituted in the court as a state of affairs where by misrepresentation occurs to act upon the fraudulent behavior. It is an act with criminal obligation for fraud to gain money or “services” with dishonest intention. Deception, illegal gain, opportunity and motive are essential constituents of frauds.



Figure 1: The Fraud Triangle hypothesizes
[Reference: Fraud Examiners Manual]

There is another large Money crime Fraud reported in [8] regarding loans and savings

crisis. The assertions of the authors are based on 100 interviews and several documents on the subject matter of this big-money criminals. This case may be termed as worst fraud of the twentieth century happened in 1980. Inclusive of the interest, the fraud amount is estimated to be US \$ 175 billion. This fraud involves a chain of white collar crimes, not found in United States of America. The famous financial specialists have discussed this fraud and the authors of [8] are of the opinion that this fraud is as “systematic political collusion” due to the presence of political involvement. In this case notorious offender was as central criminal named Charles Keating. The performance of law enforcement agencies had not been adequate. According to vision of [9], there is tremendous scope of research in the area of frauds particularly in accounting, society, organizations and public private sector autonomous and semi-autonomous bodies.

2. Vision of British Law on Frauds

The legislation promulgated in UK reported in [7] is called the Fraud Act 2006. Its sections (1),(3),(4),(5) and (12) are important for discussions on the topic of this paper. Section 1, deals with breaching the law by misrepresentation implicitly or explicitly; while Section (3) discusses the frauds and to cause harm to others by failing to reveal information and the Section (4) relates to fraud by misuse, exploitation and abusing the position of the offender by omission or commission of offence. In Section (5) it is termed by fraud as permanent or temporary “gain” and “loss” in terms of money, things or imperceptible or incorporeal property, which is distinguished. According to Section (12), the frauds commit-

ted by the officers of an entrepreneur is regarded as Obligation, Accountability and Liability of the entrepreneur or company or corporate body concerned. Section (13) provides all the necessary legal aspects regarding the question of “Evidence”, which an enquiry officer must keep in mind because the entire case of prosecution depends upon the collection of strong evidence during enquiry. The offender must not be excused on issues of not answering any question regarding the property, accounts of property and relevant documents. If there exists any conspiracy in fraud, it must also be highlighted and reported in the enquiry.

3. The Frauds committed using Internet

The fraudsters involved in the frauds utilize modern software tools and programs, coupled with internet connection to access the information, particularly the Email of the victim and other identity features. The frauds committed on internet therefore are called Email-based or online cybercrime. The fraudsters are interested to hack identity to further commit other cybercrimes and defraud victims of their money. In this way millions of dollars of frauds are carried out by dint of internet scams using online facilities. The number of frauds on internet is exponentially increasing with design of new techniques.

Cybercriminals possess advanced information technologies, which are coupled with internet to carry out offences. Mostly they initiate their offence from having personal information and identity of their victims. They commence a series of attacks using different schemes and algorithms and messaging services to capture

user's data. There are several groups and types of internet attacks such as Business email compromise (BEC), spoofing and Phishing, Ransomware, Lottery Fee Fraud, Credit Card Scams, Online Dating Scams. In 2020, 95% of all attacks on company networks were spear phishing-related, and 22% of all data breaches included a phishing attack, according to research from Security Boulevard. Additionally, about 2 million new phishing websites are launched, 97% of users cannot identify a sophisticated phishing email, and 78% of users are aware that clicking links in emails can be dangerous. Email-based phishing scams are always evolving, ranging from simple attacks to sophisticated threats that specifically target certain individuals.

3.1 Cyber Crimes

In Pakistan people keep them busy on internet in the areas of social networking, audio and video exchange, and do online shopping and online banking transactions. During Covid epidemic the academic institution held online classes and examinations. The Cyber Crimes are carried out using computer or other digital devices and networks. The spread of different viruses, sending messages of insult and to harm the users, the criminal trespass their accounts and networks, especially they take away heavy amounts of money from the banks using illegally acquired information. Apart from other offences, one of the occupations of such criminal is also drug trafficking. The can hack the data from any network within 3 to 4 seconds with recent softwares. The digital piracy and electronic terrorism are also serious areas of cybercrime to combat.

4. Internet Frauds and Protective Measures

The user's may adopt adequate measures to protect their useful and private information to avoid the outside attacks. Users also must use powerful anti-spam. Computer fraud is closely

related to online fraud, is described as using a computer or computer system to facilitate the execution of a scheme or illegal conduct and aiming a computer with the intention to modify, harm, or disable it. While not working with internet, one muss switch off Wi-Fi Network as well as Wi-Fi routers.

Table 1: Protective measures

SR #	Measures to avoid internet frauds
1.	<u>While not working with internet switch of Wifi</u>
2.	<u>Be watchful and cautious to avoid being caught in a phishing</u>
3.	<u>Must have knowledge of common internet Frauds and modus operandi of hackers</u>
4.	<u>Never send money to anyone who is acquainted to you on internet</u>
5.	<u>Keep your personal and identity information strictly confidential to others, especially unknowns</u>
6.	<u>Avoid clicking on attachments or hyperlinks in the messages received from Emails</u>
7.	<u>In case of any attacks from hackers report to the concerned authority of Email.</u>
8.	<u>Keep on Checking frequently vor bank accounts to avoid fro Credit card frauds.</u>
9.	<u>If Credit Card Fraud occurs, immediately report to to Bank legal authorities</u>

5. Financial Frauds in Pakistan

Nowadays, almost all banks are providing their customers the facility of online banking to open accounts, payments of utility bills, online payment taxes, credit and debit cards, processing of the loan applications and having bank statement online. These facilities sometimes involve technical and operational errors and mistakes. Most of fraudsters aim at depriving the victims of their money. The financial frauds involve, Phishing. Card skimming, prize Bonds, false Lottery Schemes, frauds though online payment networks, though, Imitating, Copying and Impersonating organizations and banks. The initiation of fraud begins from obtaining personal information and Identity theft of the victim. The malpractices in credit and debit card are exceeding at very high limit in Pakistan. Another type of frequent fraud occurs in the field of loans and

property mortgage, falsehood in employment, online collection of advance fees.

In banking applications, most of the complaints logged by customers are due to corrupt practice s of bank employees and officers, delaying tactics to handle the customer's grievances, criticisms and complaints. Sometimes the banks do not strictly act upon the policy and instructions of the State Bank. The banks must adopt most recent development in banking to deal with banking-business using new information technologies and protective measures to combat the frauds at large scale. The Bank customers may lodge their complaints regarding unresolved complaints and issues with banks to "Mohtasib Pakistan". The usual modus operandi in Frauds related to banking is accomplished by mafias of fraudsters is that firstly they call the consumers misrepresenting as bank personnel

and representatives to cheat, betray and deceive the customer to get the financial information. Then this information is used to harm the consumer in the fraudulent offence, consequential in financial loss. In 2022, the federal Government of Pakistan decided to compensate a relief of Rs 1.9 Million to account holders facing frauds, particularly to victims ordering Bank Alfalah Ltd (BAL) to refund the defrauded money. For the consumers, the State Banks of Pakistan issues fraud warnings from time to time therefore, the consumer must look into the guidelines. “In a recent warning to the general public, the State Bank has told that name “State Bank”, its official and authorized logo is used by the fraudsters for deceitful purposes and determinations. Then the victim is communicated of cash to be paid by way of inheritance by the State Bank’s Overseas

Branch.” Therefore, the victims are asked to give personal information such as identity, mobile numbers to have access to their funds in banks, particularly in case of overseas.

The study presented in [12] discusses the involvement of bank employees and they pledge and commit various types of frauds to harm the victims. The researchers have proposed several measures in this regard. The most important is that individual banks must also take positive initiatives to minimize and control the harm caused to the bank and hence the innocent victims. The reader may consult the research contents and results from [12].

In this section very briefly the usefulness of Demilitarization Zone (DMZ) is mentioned which is used to secure the Network (LAN) from the hackers and trackers. It must be

Table 2: Statistics

Region	Complaints received during the year	Complaints Carried forward from last year	Total
Punjab	20885	2625	23510
Sindh	7614	1062	8676
Khyber Pakhtunkhwa	3028	421	3449
Balochistan	552	44	596
Gilgit Baltistan	63	3	66
Azad Kashmir	246	0	246
Overseas	808	13	821
Total	33196	4168	37364

employed in all the public and private organizations using Network (LAN). According to [14], applying DMZ ensures in refining the network security of web testing.

A DMZ configuration in a Local Area Network

allows additional defense mechanism against external attacks to (LAN). A DMZ is a physical or logical subnet that separates a LAN from untrusted networks, such as the public internet. Any service offered to open internet users should install the DMZ. The systems that run

services on a DMZ server are susceptible to attack by hackers and online criminals. For those servers to be able to withstand ongoing attacks, security must be enhanced. The purpose of the DMZ network is to safeguard the host's data and work.

DMZ networks are implemented to safeguard critical resources and systems. The DMZ is often shielded from access to everything on the external network by a second firewall. Most of the time, internal assaults like spoofing via email or other methods or sniffing communication with a packet analyzer are unaffected by the greater security given by external attacks.

Organizations no longer require internal web servers, thanks to cloud computing. Network

security for both individual users and large companies depends on DMZs. By prohibiting external access to internal servers and data, which can be seriously compromised, they securely protect the computer network. Before incoming network packets reach the servers, a firewall or other security tools can monitor them; thanks to the DMZ firewall configuration.

7. Design and Structure of the DMZ

A DMZ can be used to build a network in a variety of ways. A single firewall (also known as a three-legged architecture) or twin firewalls are the two main strategies for accomplishing this. Both of these technologies can be devel-

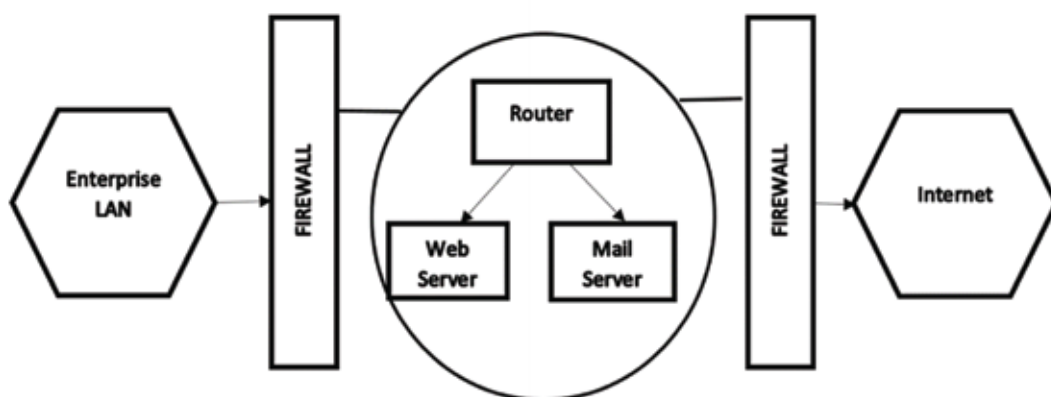


Figure 2: Architecture of Demilitarize zone in a Computer network (LAN)

oped further to create intricate DMZ designs that meets network needs.

8. Advantages of DMZ

A DMZ can be used to build a network in a variety of ways. A single firewall (also known

as a three-legged architecture) or twin firewalls are the two main strategies for achieving this. Both of these technologies can be developed further to create complex DMZ designs that meet network needs. The DMZ guards against efforts to spoof an IP address in order to gain access to systems. Such attempts can be detect-

ed and stopped by a DMZ while another service verifies

9. Recommendations

- a. Protective measure for Cyber Crime,
- b. Face Book must be secured,
- c. Take essential security measures such as Login alert and security code,
- d. Permit to your restricted friends to view your videos and pictures,
- e. Login notification must be adhered to and used,
- f. Also limit your contacts,
- g. Disable your debit/credit card as soon as possible if you lose them,
- h. Adopt a secure way to communicate your Cash Transfers,
- i. The banks must adopt most recent developments in banking to deal with banking-business using new information technologies and protective measures to combat the frauds,
- j. For online Shopping, the customer must choose the mode of payment by cash on receipt of the parcel.
- k. For the consumers, the State Banks of Pakistan issues fraud warning from time to time therefore, the consumer must look into the guidelines. Therefore, follow up the guidelines in accordance with reference [11]. Further, ignore any

incoming message from State Bank as a result of fraudulent misrepresentation of fraudsters

- l. The Bank customers may lodge their complaints regarding unresolved complaints and issues with banks, to the “Mohtasib Pakistan”.
- m. In case of security and problem related to cybercrime, Cyber Crime Prevention, Federal investigation agency, National response center for cybercrime: <https://nr3c.gov.pk/cybercrime.html>
- n. May also contact, National Police Foundation Building, Mauve Area Second Floor, Sector G-10/4, Islamabad, Pakistan. Phone: +92 51 9106 384; Email: helpdesk@nr3c.gov.pk.

10. Acknowledgement

The authors are deeply indebted to Mr. Kaukab Jamal Zuberi Head, Department of Criminology and Forensic Sciences Lahore Garrison University for guidance and Dr. Syeda Mona Hassan Chief Editor of the Journal for encouragements.

11. References

- [1]. C. Armstrong. “Blue skies and boiler rooms: Buying and selling securities in Canada”, 1870– 1940. Toronto: University of Toronto Press. 1997.
- [2]. C. Armstrong. “Moose pastures and mergers: the Ontario Securities Commis-

- sion and the regulation of share markets in Canada, 1940-1980". Toronto: University of Toronto Press. 2001.
- [3]. E. J. Balleisen. "Private cops on the fraud beat: The limits of American business self-regulation", 1895-1932. *Business History Review*, vol. 83, pp. 113–160. 2009.
- [4]. E. J. Balleisen. "Fraud An American history from Barnum to Madoff". Princeton: Princeton University Press. 2017.
- [5]. H. Berghoff. "Organized irresponsibility"? The Siemens corruption scandal of the 1990s and 2000s. *Business History*, vol. 60, pp. 423–445. 2018.
- [6]. R. Baldwin, M. Cave and M. Lodge. "Understanding regulation: Theory, strategy and practice", (2nd ed.). Oxford: Oxford University Press. 2012.
- [7]. Fraud Act 2006 - Legislation.gov.uk; <https://www.legislation.gov.uk>.
- [8]. K. Calavita, H. N. Pontell, and R. H. Tillman. "Big money crime: Fraud and politics in the savings and loan crisis". Berkeley, CA: University of California Press. 1997.
- [9]. D. J. Cooper, T. Dacin and D. Palmer. "Fraud in accounting, organizations and society: Extending the boundaries of research". *Accounting, Organizations and Society*, vol, 38, pp. 440–457. 2013.
- [10]. Cyber Crime Prevention, Federal investigation agency, National response center for cybercrime: <https://nr3c.gov.pk/cybercrime.html>
- [11]. Fraud Warning - State Bank of Pakistan, <https://www.sbp.org.pk/pdf/PublicWarning-01>
- [12]. M. Younus. "The rising trend of fraud and forgery in Pakistan's banking industry and precautions taken against", *Qualitative Research in Financial Markets*, Vol. 13 No. 2, pp. 215-225. 2021.
- [13]. H. Driel. "Financial fraud, scandals, and regulation: A conceptual framework and literature review", *Business History*. Vol. 61, no. 8, pp. 1259-1299, 2019.
- [14]. A. Iskandar, E. Virma, and A. S. Ahmar. "Implementing DMZ in improving network security of web testing in STMIK AKBA". *arXiv preprint arXiv:1901.04081*. 2019
- [15] What is a DMZ. <https://intellipaat.com/blog/what-is-dmz-network>.



Application of nanotechnology in criminology and forensic Sciences

Bisma Sher Ali

Department of Chemistry, University of Education, Lahore

Corresponding author: bisma96khan@gmail.com

Received: 10 September, 2022; Accepted: 11 November, 2022; Published: 20 December, 2022.

Abstract:

Nanotechnology being a new discipline of the research has many advances. Due to its properties nanostructures are involved in revealing many evidences and cases. Nanostructures play an important part in forensic study and criminology. It is evident that gold and silver nanostructures are greatly used in fingerprint detection. However different nanotechniques are employed to detect trace materials from the crime scene. Fragmentation of DNA, amplification and cooperation is taken place by using nanoparticles with the help of PCR technique. Nanostructures can act as sensors for a variety of chemical and biological components, including explosives, according to contemporary studies on nanomaterial research and development. Nano-gold (Au-NPs), nano-silver, and nano-titanium dioxide (TiO₂) particles along with capillary electrophoresis, SEM, TEM, and FTIR are used in forensic toxicology. Incubation of nanostructures in saliva and nerve agent detection is also observed. In the realm of forensic science, nanotechnology is projected to play a significant role in the future by bringing more specialised and sensitive methods of case detection and revelation, as well as flawless evidence. In this review article all the aspects where nanostructures are applied in forensic sciences are studied in detail.

Key words: Nanotechnology, Forensics, nanoparticles, toxicology, nanotechniques

1. Introduction

Nanotechnology is growing rapidly with the application of various fields like physical sciences, natural sciences and computational and biological sciences. Nanotechnology is the controlled development of structures at atomic, molecular and macromolecular level with in the length scale ranging from 1- 100 nanometer. These materials are known as

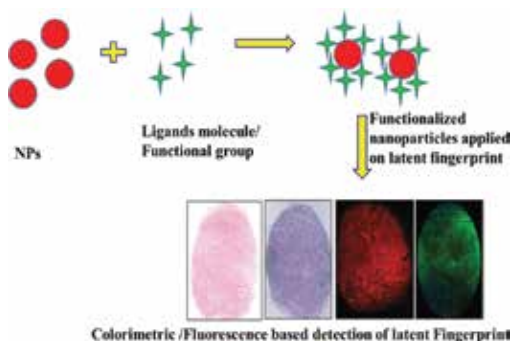
“nanostructures” which are unique in their properties and functionality. They are actually of small size, easily soluble, multifunctional and surface tailorable [1] Owing to their properties they are applied in various fields. An important and significant approach of the nanotechnology is their benefit in criminology and forensic sciences as their use disclosed significant evidences which proves significant in criminal investigation [2].

Many areas in forensic nanotechnology are covered which comprises of forensic toxicology, nanosensors, sequencing of DNA, scanning probe microscopy, nerve gas detection, saliva detection, latent fingerprint detection, fiber and hair analysis, analysis of drug detection and trace evidence analysis [3].

2. Application of nanotechnology in forensic sciences

2.1 Fingerprint detection

To ensure the safety of the person defense industries introduced the finger print detection. Fingerprints are of three kinds: visible, indented, or latent. Visible fingerprints can be seen explicitly. Indented fingerprints are those obtained from malleable materials. Latent fingerprints are invisible and more difficult to detect to detect latent fingerprints fluorescent nanoparticles or quantum dots can be used. Due to their small size, nanoparticles have the capability to recognize smaller with more accuracy. For instance, gold and silver nanostructures are utilize in latent finger detection. Titanium oxide or zinc oxide nanostructures are able to detect fingerprints on surfaces. When used as nanocrystals or nanocomposites, metal sulphide nanoparticles are very effective at locating fingerprints on aluminium foil and soft drink cans [4].



In forensic science, the study of fingerprints serves as the primary proof of individualization. The traditional methods for developing fingerprints don't have the sensitivity or dependability to work on a variety of surfaces or older prints. For the development of latent fingerprints, nanotechniques are used [5].

In addition to producing superior prints and being naturally UV fluorescent, 20 nm zinc oxide particles can function in wet environments, which is something that traditional micron-sized powders cannot. In order to enhance the creation of fingerprints, other researchers have been employing particles smaller than 10 nm that also glow under UV light. They have been creating nanopowders with special engineering that will allow them to work with SALDI-TOF2-MS. This implies that when a fingerprint is created with these powders, the chemicals—both those ejected and those left behind after coming into touch with other materials—that make up the fingerprint may be examined and identified [6].

2.2 Trace evidence material analysis:

Minute quantities that are present at crime scene known to be trace evidence. Nanostructures play a vital role in analyzing these materials. Trace evidence include hair, fibers, paint, glass, gunshot residue (GSR), and explosives [7].

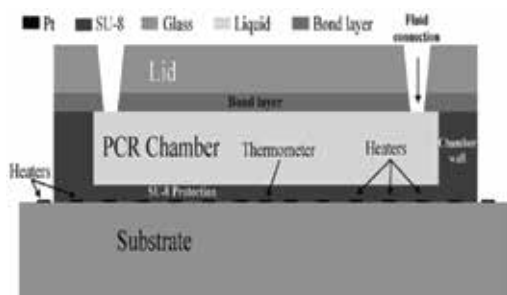
For trace evidence analysis atomic force microscopy is applied. Due to its capacity to discriminate between various environmental exposures or forced damages to fibres, AFM is a very effective instrument in the forensic investigation of fibre evidence.

2.3 DNA Analysis:

DNA extraction and amplification are made more effective by the use of nanoparticles (NPs). Gold nanoparticles significantly increase the polymerase chain reaction (PCR) [5].

In contrast to the traditional sieving mechanism and the transitory mechanism, new separation methodologies for DNA analysis employing nanostructures have been devised [9].

The polymerase chain reaction (PCR) is a popular technique for making duplicates of particular DNA fragments. A single DNA molecule is quickly multiplied into many billions of molecules using PCR. Consequently, PCR is a useful technology in forensic DNA analysis that can be used to identify an individual or a group of individuals. Gold nanoparticles have been found to significantly increase the polymerase chain reaction's (PCR) effectiveness. The reaction time is shortened and the heating/cooling thermal cycle rates are raised when 0.7 nm of 13 nm Au-NPs are added to the PCR reagent. As a result, significant increases in PCR efficiency are attributed to Au nanoparticles' excellent heat transfer properties [10].



Silver and gold nanoparticles, for example, scatter light in a size-dependent manner, and the absorbance and emission spectra of semiconductor quantum dots are size-tunable.

These characteristics make it easier for them to be used in multitarget assays, as does the capacity to affix almost any biologic recognition element to the particle surfaces. For instance, using size-dependent features as just one example, both quantum dots and metal nanoparticles can be coupled to either DNA sequences or proteins so that fluorescence or light scattering, respectively, can be used as an output signal [11].

2.4 Nanosensors

Modern studies on nanomaterial research and development have shown that nanostructures can serve as sensors for many chemical and biological components consisting of explosives. One of the fundamental promises of the nanosensor sector is the development of ultra-small devices with powerful sensing capabilities. The most promising nanosensor ideas for trace explosive detection include electronic noses, nanocurcumin-based probes, lasing plasmon nano cavities, nanowire/nanotube, and nanomechanical devices [12].

Nanoparticles can be utilised in detectors and collectors that have a target warfare weapon recognition site. The target, which might be chemical, physical, or biological, determines the parameters for choosing the nanoparticles. There are a number of nerve agents, such as sarin and sulphur mustard, that only last a short time in the environment and may also be volatile, but others, such as ricin, VX, and others, are toxic nerve agents that need to be addressed and can be done so with the help of nanoparticle detectors with nanostructured recognition sites [13]. A very sensitive (1 nM) and selective (over other nitro explosives) ultrasensitive nanocurcumin-based nanomaterials surface energy transfer (NSET) sensor is designed for the detection of tiny amounts of

Trinitrotoluene (TNT), and we discovered the highest fluorescence enhancement for sensing TNT to date (up to 800 times) [14].

Barcodes and trackers are employed to stop crime. Injecting the inmates with nano trackers makes it easier to find them if they manage to escape. Nano trackers make it possible to keep tabs on prisoners after their release [10].

2.5 Nanostructures in toxicology and drug analysis

The effective use of current nanotechnology in forensic toxicology includes the identification and quantification of various poisonous substances from a wide range of forensic evidence, including blood, hair, saliva, urine, vitreous humour, fingerprints, and skeletal remains. The development uses nano-gold (Au-NPs), nano-silver, and nano-titanium dioxide (TiO₂) particles along with capillary electrophoresis, SEM, TEM, and FTIR [15].

Using nano-techniques like HPLC, FT-IR, XPS, and Tof-MS, a wide variety of both legal medications (like paracetamol and loratadine) and illegal substances (like cocaine and ecstasy) are regularly detected and identified. Nano-grams of pharmaceuticals and drug formulations can now be found in a variety of media, including blood, urine, and hair, thanks to modern advancements in these procedures. Modern forensic investigators now have access to a multitude of data on drugs, paraphernalia, and excipients, including information on morphology, chemical composition, and surface stiffness, because of advances made in these procedures [16].

2.6 Saliva detection analysis

Forensic saliva identification is a useful

supplemental tool in criminal investigations. Techniques for detecting salivary bacteria have been found to be effective ways to determine the presence of saliva. The creation of SiC nanoparticles that have been stabilised by bovine serum albumin (SiC-BSA NPs) is described as a one-pot process. To enable the fluorometric detection and imaging of bacteria in saliva, SiC@BSA NPs were coupled to the antimicrobial peptide GH12. More specifically, the oral bacteria *S. salivarius* levels were detected using a nanoprobe having fluorescent excitation/emission maxima at 320/410 nm. The assay can be completed in 40 minutes, and the detection limit is 25 cfu/mL/1. Blood, urine, and semen were among the forensic body fluids in which the nanoprobe was employed to identify microorganisms [17].

A quick and affordable smartphone-based bacteria sensor that tests for two oral bacteria in actual samples of saliva is developed. In order to create a series of test strips for this bacterium sensor, blue-emitting silicon carbide quantum dots (SiC Qds) and red-emitting gold nanoclusters (AuNCs) were used. This technique has good sensitivity for the selective detection of two types of oral bacteria, *S. salivarius* and *S. sanguinis*. The test strips were exposed to bacterium solutions, which encouraged the evolution of dose-sensitive colours under a 365 nm UV lamp, which were captured by a smartphone camera and assessed using a colour detector APP [18].

2.7 Nerve agent detection

Forensic and clinical examination of the very lethal nerve toxin VX requires a screening approach. An effective method for VX detection with the human eye was devised utilising a straightforward colorimetric technique using

gold nanoparticles (AuNPs). When VX was added to the AuNPs under mildly acidic circumstances, the AuNPs turned from bright red to deep blue [19]. The creation of straightforward techniques for the quick and effective detection of these dangerous compounds is essential because organophosphorus nerve agents (OPNAs), such as Sarin (GB), Tabun (GA), Soman (GD), and VX, would be extremely harmful in military and terrorist strikes. AgNPs that have been functionalized and immobilised with acetylcholinesterase (AChE) and 5,5'-dithiobis-(2-nitrobenzoic acid) are used to create the detection substrate (DTNB). Acetylthiocholine (ATCh) is hydrolyzed by AChE in the absence of OPs to create thiocholine (TCh), which continues to interact swiftly with DTNB to create the extremely sensitive Raman probe molecule TNB [20].

3. Conclusion

Nanostructures play significant role in the field of science and technology. Hence, with their enhanced properties its demand is increasing. In forensic sciences they are used in almost every matter from security measures to crime scene investigation. This article covers almost every aspect in which nanoparticles are utilized. In future, they are also implanted in robotics and polymer sciences.

4. References

- [1]. S. E. McNeil. "Nanotechnology for the biologist". *Journal of leukocyte biology*, vol. 78, no. 3, pp. 585-594. 2005.
- [2]. V. Chauhan, V. Singh, and A. Tiwari, A. "Applications of nanotechnology in forensic investigation". *Int. J. Life. Sci. Scienti. Res.* vol. 3, no.3, pp. 1047-1051. 2017.
- [3]. B. Srividya. "Nanotechnology in forensics and its application in forensic investigation". *Res. Rev. J. Pharm. Nanotechnol*, vol.4, no. 2, pp. 1-7. 2016.
- [4]. C. Ngo, V. Voorde. "Nanotechnology for Defense and Security Nanotechnology in a Nutshell", Springer .pp. 413-432. 2014.
- [5]. H. M. Paikrao, D. S. Tajane, A. S. Patil and A. D. Dipale. "Applications of Nanotechnology in Forensic Science". *Engineered Nanomaterials for Innovative Therapies and Biomedicine*. pp. 257-276. 2022.
- [6]. V. R. Hallikeri, M. Bai and A. V. Kumar." Nanotechnology-The future armour of forensics: A short review". *Journal of the Scientific Society*, vol. 39, no.1, pp. 10-17. 2012.
- [7]. E. Mistek, M. A. Fikiet, S. R. Khandasammy and I. K. Lednev. Toward locard's exchange principle: recent developments in forensic trace evidence analysis. *Analytical chemistry*, vol 91, no. 1. pp. 637-654. 2018.
- [8]. Y. F. Chen. "Forensic applications of nanotechnology". *Journal of the Chinese Chemical Society*, vol. 58, no. 6, pp. 828-835. 2011.
- [9]. Y. W. Lin, M. F. Huang, and H. T. Chang. "Nanomaterials and chip-based nanostructures for capillary electrophoretic separations of DNA". *Electrophoresis*. vol. 26, no. 2, pp. 320-330. 2005.

- [10]. A. Pandya and R. K. Shukla. "New perspective of nanotechnology: role in preventive forensic". Egyptian Journal of Forensic Sciences. vol. 8, no. 1, pp. 1-11. 2018.
- [11]. C. A. Mirkin, C. S. Thaxton, and N. L. Rosi. "Nanostructures in biodefense and molecular diagnostics" . Taylor & Francis. vol. 4, pp. 749-751. 2004.
- [12]. A. Lodha, A. Pandya and R. Shukla. "Nanotechnology: an applied and robust approach for forensic investigation". Forensic Res Criminol Int J.vol. 2, no.1 pp 31-4. 2016.
- [13]. D. Chakraborty, G. Rajan, and R. Isaac. "A splendid blend of nanotechnology and forensic Science". Journal of Nanotechnology in Engineering and Medicine.vol. 6, no. 1,pp. 108-121. 2015.
- [14]. A. Pandya, H. Goswami, A. Lodha, and S. K. Menon. "A novel nanoaggregation detection technique of TNT using selective and ultrasensitive nanocurcumin as a probe". Analyst.vol. 137, no. 8, pp. 1771-1774. 2012.
- [15]. S. Kesarwani, K. Parihar, M. S. Sankhla and R. Kumar. "Nano-forensic: new perspective and extensive applications in solving crimes". Latent in applied nanobioscience. vol. 10, no. 1, pp. 1792-1798. 2020.
- [16]. V. Prasad, S. Lukose and L. Prasad. "Emerging forensic applications of nanotechnology". Int J Eng Allied Sci,vol. 2, pp. 1-8. 2016.
- [17]. X. Li, Y. Ding, J. Ling, W. Yao, L. Zha, and J. Cai. "Bacteria-targeting BSA-stabilized SiC nanoparticles as a fluorescent nanoprobe for forensic identification of saliva". Microchimica Acta, 186(12), 1-10. 2019.
- [18]. X. Li, J. Li, J. Ling, C. Wang, Y. Ding, Y. Chang, and Cai, J. "A smartphone-based bacteria sensor for rapid and portable identification of forensic saliva sample". Sensors and Actuators B: Chemical, vol.4, no. 2. pp. 320-341. 2020.
- [19]. F. Takahashi, Y. Kazui, H. Miyaguchi, T. Ohmori, R. Tanaka and J. Jin. "Simple colorimetric screening of the nerve agent VX using gold nanoparticles and a hand-powered extraction device". Sensors and Actuators B: Chemical, pp. 327-335. 2021.
- [20]. J. Wu, Y. Zhu, Y. Liu, J. Chen, L. Guo and J. Xie. "A novel approach for on-site screening of organophosphorus nerve agents based on DTNB modified AgNPs using surface-enhanced Raman spectrometry". Analytical methods, vol. 14, no. 43, pp. 4292-4299. 2022.



Cyber Security Incident Response and Reverse Engineering

Taseer Suleman and Nadia Liaquat

School of Electrical Engineering and Computer Sciences, NUST, Islamabad, Pakistan

Corresponding authors: nadialiaquat001@gmail.com, 12msccsmsuleman@seecs.edu.pk

Received: 11 September, 2022; Accepted: 14 November, 2022; Published: 20 December, 2022

Abstract

Although the incident response has always been a crucial component of information security, security administrators frequently ignore it. Whereas, Reverse engineering focuses on the difficult issue of analyzing legacy software code in the absence of appropriate documentation. This paper proposes an approach to understanding cyber security Incident Response and the services it provides followed by Reverse Engineering resources and the practical analysis of a malware named “Alice ATM Malware” in detail.

Key words: Cybersecurity Incident, Indicator of compromise, Digital defenses, Computer Security Incident Response Team, IDA de-compilers, Reverse Engineering.

1. Introduction

Highly skilled attackers provide a continuing threat to organizations. Attackers constantly discover new ways to breach organizations’ digital defenses to steal information or destroy their operations. The threat landscape is rapidly changing (Ahmad et al. 2019). There is a lot of ongoing research on how to reinforce these digital defenses, but relatively little is done to improve the process that takes over when things go wrong: incident response (IR) [1].

When digital defenses fail, cybersecurity incident response teams are at the forefront and must intervene to reinstitute services and call

problems are impeding the incident response team’s capacity to respond to cyber-attacks (Nyre-Yu et al. 2019) [2]. By removing these obstacles, organizations may be better able to respond to incidents in general. One method to achieve this is through training, particularly employing training scenarios, which can boost team cybersecurity performance by developing skills and spotting possible flaws. The most significant information technology advancements are right in front of us right now. Given that approximately one billion computers in our world are currently connected to the Internet and that mobile telephony services and e-commerce have converged, enormous amounts of information can go from one network to another with only

one request, command, or click (Global Reach, 2005). To this degree, numerous technologies, platforms, and infrastructures are flourishing to give services to the end user, who now serves as the target point because it is the user who asks for services, accesses networks, and resources, and needs security and privacy [3].

Expertise in fields like forensic investigation and malware reverse engineering is frequently needed for incident response. Reverse engineering is the process through which a variety of items, including software, types of machinery, and architectural structures, are disassembled to obtain design data and is also known as back engineering. The reverse engineering method typically involves disassembling the parts of larger, more important products. The reader will learn about reverse engineering's common principles, applications, stages, and future in this article. It demonstrates how Reverse Engineering is constantly developing and influencing the idea of cyber security [4].

Software development can also benefit from reverse engineering since it allows developers to examine their code and identify potential flaws that were overlooked during software development but that an adversary could find through reverse engineering. In Cybersecurity it is important because it enables the extraction of Indicators of Compromise (IoC) from samples [5]. Typically IoC is file's hashes, registry keys, import function and export functions, the programming language used, compilation date, IPs, emails, and even text strings that are present in the code, which are the traces left by attackers [6] [7].

2. Incident Response

The handling of diverse security incidents, cyber threats, and data breaches involves an organized technique called incident response. A cyber attack or live incident's cost is to be identified, contained, and reduced using incident response techniques [8]. Although it is not the end-all solution, a solid incident response (IR) plan can seal a potential weakness to avoid more attacks. The response is a part of incident handling, which in turn looks at the coordination, logistics, and planning required to deal with a problem. This kind of work is normally handled by the Computer Security Incident Response Team (CSIRT), with assistance from the Security Operation Center. While incident management is the primary function of CSIRT, it also has reporting, analysis, and reaction responsibilities. Before these phases, the incident must be located and promptly reported [9]. The function of a SOC Analyst becomes crucial at this point.

2.1 Incident Response Services

The most efficient incident response is carried out rapidly by trained responders. Organizations frequently lack the funding necessary to keep a fully functional incident response team on duty around the clock [10]. Working with an outside organization that provides qualified incident response services is one alternative.

Getting involved with these organizations offers the following advantages:

2.1.1 Availability

The cost and impact of an attack on the organization are reduced the faster the incident response team gets to work. Cybersecurity issues can happen at any time, and getting in touch with incident response team members

after hours might be challenging. To improve coverage and availability, professional incident response companies have numerous staff teams on hand.

2.1.2 Experience

Managing security issues improperly can increase costs and harm a company. For instance, a ransomware attack might cause a system to become unstable, making it unlikely that encrypted data will be restored after a system restart. Professional incident responders have the experience necessary to accurately and efficiently address such security issues.

2.1.3 Specialized expertise

Reverse engineering malware and forensic analysis are two skills that are frequently used in incident response. Even though the majority of businesses won't require these talents in-house, a specialized incident response team has access to the professionals they require to successfully manage cybersecurity problems.

2.1.4 Controlling all aspects of the incident response procedure

All of the organization's incident response requirements should be met by outsourced incident response providers. This includes putting incident response plans in place, controlling identified intrusions, and thwarting potential attacks.

3. Incident Response Plan Phases

It is a set of guidelines that must be followed during each stage of incident response. The components of a good incident response plan include a clear communication strategy, directives defining the duties and

responsibilities of each person and organization, and protocols that must be followed at all times [11].

3.1 Preparation

The steps a business should take in the case of a disruptive incident are outlined in an effective incident response strategy. The plan starts by describing how a company should reduce the danger of a data leak [12]. Organizational data protection policies should be in line with security objectives and technology defenses throughout the preparation stage. You must, at the very least, guarantee that staff members have received training on information security. They should ideally also have specialized training in incident response. To make sure your sensitive data is adequately protected, you should audit your systems as well.

3.2 Identification

The second component of incident response planning deals with the measures an organization takes to ascertain when one of its systems has been compromised [13]. You are better able to stop you may quickly recognize an incursion from an assault. You can save time and money even if it isn't possible by limiting the damage and hastening the response effort.

The following inquiries should be addressed when determining a security incident:

- Who found the opening?
- How much of a breach is there?
- Had an impact on our operations?
- Where did the compromise originate?

3.3 Containment

The third phase discusses the steps you should

take to minimize harm after being infiltrated. Depending on the circumstances, this can require taking action to remove the criminal hacker from your networks or to isolate the already compromised data [14].

During this stage, you should consider whether systems need to be shut down or removed as well as whether there are any rapid fixes for vulnerabilities.

3.4 Eradication

Fixing the fault that caused the data breach is the aim of phase four of a cyber incident response strategy. Again, the specifics will depend on the type of incident, but right now you need to determine how the information was disclosed and how to get rid of the threat [15].

For instance, you would remove the malicious software and isolate the affected areas if your firm had been compromised by malware. In the meantime, you would lock down a worker's account if the attack resulted from their login information being stolen by a malicious hacker.

3.5 Recovery

Getting your systems back online is the penultimate step in responding to a cyber incident once the threat has been eradicated. In some circumstances, this will be trickier to do than in others, but it's an important step that needs to be taken seriously. Without a strong recovery process, you might still be vulnerable to attacks, which would make the injury worse. As part of the recovery process, you should test and monitor the impacted systems after the

issue has been fixed. This guarantees that the measures you implement the function as planned and offers you the chance to fix any errors [16].

3.6 Lessons Learned

The final phase in the cyber incident response strategy is reviewing the occurrence and identifying potential areas for improvement. Your incident response team needs to meet to go over the parts of the plan that worked and any problems you encountered.

It is important to review the process at every stage. Discuss what happened, why it happened, what you tried to stop it, and what may have been done differently. For instance, was the documentation effective and clear, and did the plan include any gaps?

Before having this conversation, one to two weeks should have passed after the security incident; this will allow everyone to think about the incident in retrospect while still keeping it fresh in everyone's memory [17].

Instead of berating team members for prior mistakes, this stage's objective is to avoid inefficiencies from occurring again. Failures in the processed signal that the documentation was either unclear, the proper course of action wasn't specified, or staff training wasn't adequate.

4 Reverse engineering

The procedure of obtaining knowledge or designing blueprints from everything created by humans is known as reverse engineering. The idea has likely existed since the Industrial

Revolution, long before computers or other contemporary technology. It closely resembles scientific research, in which an investigator seeks to identify the "blueprint" of an atom or the human mind. Reverse engineering is different from a traditional scientific study in that the artifact under investigation is human-made, as opposed to a natural event in scientific research [18]. When such information is lacking, reverse engineering is typically used to fill in the gaps in knowledge, ideas, and design philosophy.

4.1 Resources Used in Reverse Engineering

Multiple tools are used to perform reverse engineering. These tools can help to debug, decompile and disassemble the application.

4.1.1 Debuggers

GDB is a debugger for programming that may also be used to decipher binary code. While the assembly code is running, you can view the information in memory and registers [19]. Additionally, breakpoints can be added anywhere in the application using debuggers.

4.1.2 Disassembler

Machine code is converted into a human-readable format using a disassembler. Because disassembled code lacks programmers' comments and annotations, reading it is more challenging than reading source code.

4.1.3 De compilers

Although IDA is difficult to use and needs extensive programming knowledge, its technical level accurately captures the fundamental nature of reverse engineering

(Seo et al., 2019). DE-compilation is the process of translating a compiled program into a higher-level symbolic language that humans can comprehend, and it particularly makes use of reverse engineering methods.

4.2 Stages in Reverse engineering

By creating models that describe the current program and the assumed goal, reverse engineering can be accomplished. Three main phases make up this process:

- Recovering from implementation. Prepare a preliminary model while learning about the application quickly.
- Adaptive design. Foreign key references should be resolved and the database's mechanics reversed.
- Retrieval of analysis. Eliminate any inaccuracies in the model and design artifacts.

4.2.1 Implementation Recovery

You prepare an early model for reverse engineering during implementation recovery. The first model should only reflect the implementation and contain no inferences because it will be used as a reference.

Reading through the most recent documentation and getting acquainted with a program is the first step. The resulting context makes it simpler to interact with application professionals and clarifies the developer's intention. This project ought to be finished in a few hours. Even though what you learn is unrelated to the actual reverse engineering, it is crucial since it enables you to make more

accurate observations as you go.

The database structure is then typed in manually or automatically into a modeling program. Some tools have can read an RDBMS's system tables and seed a model. If you utilize these tools, you ought to at the very least glance over the database architecture to get a sense of the development approach.

4.2.2 Design Recovery

You undo the database's mechanics during design recovery and just carry out simple operations. Conjecture and interpretation should wait until the analysis-recovery stage. In most cases, design recovery may be carried out independently, without assistance from application expertise. You fix three main problems at this stage.

Identity: For the prospective entity type keys, unique indexes will typically be defined. Otherwise, search for uncommon data combinations, which can point to a candidate key but not confirm it. You can also guess potential keys by looking at names and styling conventions. A suspected foreign key may imply a comparable candidate key.

Foreign keys: The most difficult aspect of design recovery is often identifying foreign keys or references between different tables. Foreign keys may be indicated by names and data types that match. Foreign keys and their referents can be declared by developers in some DBMSs, such as RDBMSs, but the majority of legacy applications do not use this feature.

Queries: When they are available, queries can be used to improve your understanding of

identity and foreign keys.

Design reclamation may result in optimizations and flaws, but it still reflects the DBMS paradigm in its ultimate form. The model will rarely be finished in practice. Some of the structure's components might be unclear.

4.2.3 Analysis Recovery

The last step is analysis and recovery. The model is interpreted, improved, and made more abstract. During this stage is when you should speak with any available application professionals. Recovery from analysis consists of four basic steps.

Clarification: Eliminate any existing design artifacts. For instance, file and database access keys do not include any essential information and are purely design options, thus they are not required to be included in an analytical model.

Redundancy: Remove derived data type if it improves database design or if it was included for the wrong reasons. You might need to examine the data to determine whether a data structure is a duplicate.

Errors: Resolve any leftover database problems. This phase of analysis recovery is necessary since you need to completely understand the database before you can say that the developer committed a mistake. An apparent error in the early stages might have been a fair procedure or the result of inadequate database understanding [20].

Integration of a model. Various information sources can result in various models. For instance, structure and data analysis is typically used to develop a reverse-engineered

model. A forward-engineered model could be created using a user manual. The final analysis model must incorporate all independent models.

5. Practical Demonstration

The following shown is the 32-bit executable file. The Alice ATM malware was discovered for the first time in November 2016 as part of an ATM malware research study with Europol EC3, however, researchers believe it has been present since 2014.

property	value
md5	F1478AA747A976FB2AD526FA71ECA853
sha1	4292DF415C11F4155E8910FBCDF8BD2DA24F4426
sha256	04F25013FB088D5E8A6E55BD8005C464123E6605897BD80AC245CE7CA12A7A70
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z
file-size	18432 bytes
entropy	3.724
imphash	43CB8BEA4CA8C4F791841893ADD4E86A
signature	n/a
tooling	Visual Studio 5.0 - 5.12
entry-point	53 56 57 33 FF 57 E8 A4 00 00 00 A3 17 10 40 00 6A 03 E8 EF F3 FF FF 57 68 E9 1A 40 00 57 68 D0 07
file-version	1.0.0.0
description	Project Alice
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x5431DF9B (Mon Oct 06 00:17:31 2014 UTC)
debugger-stamp	n/a
resources-stamp	0x00000000 (Thu Jan 01 00:00:00 1970 UTC)
import-stamp	0x00000000 (Thu Jan 01 00:00:00 1970 UTC)
exports-stamp	n/a

Figure 1: Executable file

This malware is detected on Virus total and 54 security vendors and 1 sandbox flagged this file as malicious on Virus Total.

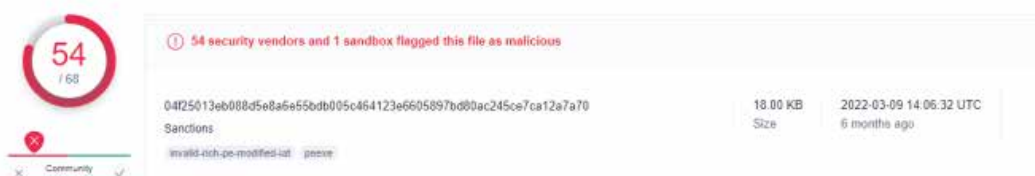


Figure 2: Results of Virus Total

These are the libraries that are used by this malware.

library (5)	blacklist (1)	type (1)	functions (36)	description
ntdll.dll	-	implicit	<u>6</u>	NT Layer DLL
user32.dll	-	implicit	<u>12</u>	Multi-User Windows USER API Client DLL
kernel32.dll	-	implicit	<u>7</u>	Windows NT BASE API Client DLL
comctl32.dll	-	implicit	<u>1</u>	Common Controls Library
msxfs.dll	x	implicit	<u>10</u>	Extension for Financial Services (XFS)

Figure 3: Libraries used by the malware

Ntdll.dll:

A module containing NT system functionality is called ntdll.dll. The NT kernel functions are

contained in the Microsoft-created file ntdll.dll, which is referred to as an "NT Layer DLL."

functions (36)	blacklist (3)	ordinal (0)	library (5)
RtlCaptureStackBackTrace	x	-	ntdll.dll
RtlMoveMemory	x	-	ntdll.dll
VerSetConditionMask	x	-	ntdll.dll
RtlUnwind		-	ntdll.dll
RtlZeroMemory		-	ntdll.dll
RtlFillMemory		-	ntdll.dll

Figure 4: Functions that are used from this library.

Comctl.dll:

A module called Comctl32.dll houses standard GUI elements used by Windows programs.

InitCommonControls		-	comctl32.dll
--------------------	--	---	------------------------------

Msxfs.dll:

Microsoft didn't provide much information on msxfs.dll.

WFSCleanUp		-	msxfs.dll
WFSOpen		-	msxfs.dll
WFSGetInfo		-	msxfs.dll
WFSExecute		-	msxfs.dll
WFSLock		-	msxfs.dll
WFSRegister		-	msxfs.dll
WFSFreeResult		-	msxfs.dll
WFSUnlock		-	msxfs.dll
WFSClose		-	msxfs.dll
WFSStartup		-	msxfs.dll

Malicious Strings:

encoding (2)	size (bytes)	location	blacklist (3)	hint (31)	value (190)
ascii	24	0x000013C2	✖	function	RtlCaptureStackBackTrace
ascii	13	0x000013DE	-	function	RtlFillMemory
ascii	13	0x000013EE	✖	function	RtlMoveMemory
ascii	9	0x000013FE	-	function	RtlUnwind
ascii	13	0x0000140A	-	function	RtlZeroMemory
ascii	19	0x0000141A	✖	function	VerSetConditionMask
ascii	13	0x00001446	-	function	AnimateWindow
ascii	9	0x00001468	-	function	EndDialog
ascii	10	0x00001474	-	function	GetDlgItem
ascii	8	0x0000149A	-	function	IsWindow
ascii	8	0x000014DA	-	function	SetFocus
ascii	11	0x00001504	-	function	ExitProcess
ascii	13	0x00001526	-	function	IsBadWritePtr
ascii	10	0x00001536	-	function	LocalAlloc
ascii	9	0x00001544	-	function	LocalFree
ascii	9	0x00001550	-	function	LocalSize
ascii	18	0x00001576	-	function	InitCommonControls
ascii	10	0x0000159A	-	function	WFSStartUp
ascii	8	0x000015A8	-	function	WFSClose
ascii	9	0x000015B4	-	function	WFSUnlock
ascii	13	0x000015C0	-	function	WFSFreeResult
ascii	11	0x000015D0	-	function	WFSRegister
ascii	10	0x000015E8	-	function	WFSExecute
ascii	10	0x000015F6	-	function	WFSGetInfo
ascii	10	0x0000160E	-	function	WFSCleanup

encoding (2)	size (bytes)	location	blacklist (3)	hint (31)	value (190)
ascii	713	0x000f8064	--	--	<?xml version="1.0" encoding="UTF-8" standalone="yes"?></?xml assembly xmlns="urn:schemas-microsoft-com:asm.v1" type="application/x-msi" />
ascii	2	0x000032A7	--	--	#AQ
ascii	2	0x00003098	--	--	IL
unicode	14	0x025F19CE	--	--	Operator panel
unicode	13	0x025F19F2	--	--	Times New Roman
unicode	9	0x025F1A30	--	--	Dispenser
unicode	13	0x025F1A60	--	--	Full Access
unicode	2	0x025F1A6C	--	--	LCS
unicode	14	0x025F1AB0	--	--	Dispense panel
unicode	3	0x025F1AE8	--	--	Go!
unicode	24	0x025F1AF8	--	--	Input cassette ID here:
unicode	27	0x025F43C8	--	--	Input PIN code for access
unicode	13	0x025F4404	--	--	MIS Servo Sent
unicode	18	0x025F441C	--	--	Authorize yourself
unicode	11	0x025F4480	--	--	Terminal ID
unicode	3	0x025F44C8	--	--	EI:
unicode	13	0x025F44D8	--	--	Your pin-code
unicode	3	0x025F4504	--	--	S&P
unicode	15	0x025F451E	--	--	V5 VERSION INFO
unicode	14	0x025F457A	--	--	StringFileIn
unicode	8	0x025F45B6	--	--	04004E
unicode	11	0x025F45B6	--	--	FileVersion
unicode	7	0x025F45D0	--	--	1.0.0.0
unicode	14	0x025F45E8	--	--	ProductVersion
unicode	7	0x025F4604	--	--	1.0.0.0

Figure 5: Malicious Strings

Dynamic Analysis:

When running this malware it asks for the pin and it only takes 123 as a pin. It didn't take any other number. When entering any other

number it wasn't proceeding and when you entered 123 as pin it automatically processes the next step [21].

The "operator panel" is opened by entering a special PIN that is of 3 digits based on the terminal ID of the ATM.

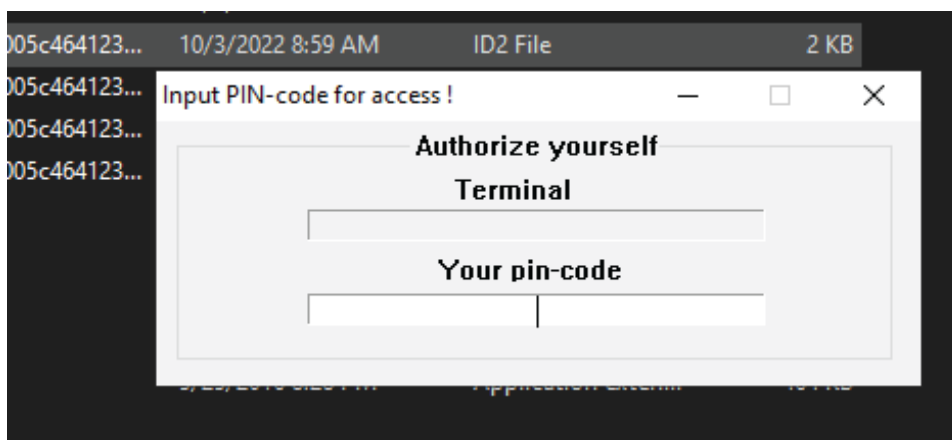


Figure 6: Running the malware

Maybe here it defines the password.

```
.text:00401031 ; int (__stdcall *dword_401031)(_DWORD)
.text:00401031 dword_401031 dd 0 ; DATA XREF: DialogFunc+185↓r
.text:00401031 ; sub_401AE9+36↓r
.text:00401035 align 4
.text:00401038 db 0
.text:00401039 dword_401039 dd 0 ; DATA XREF: DialogFunc+170↓r
.text:0040103D align 10h
.text:00401040 db 0
.text:00401041 ; CHAR a123[4]
.text:00401041 a123 db '123',0 ; DATA XREF: sub_401AE9+D5↓o
.text:00401045 ; CHAR String2[2]
.text:00401045 String2 db '0',0 ; DATA XREF: DialogFunc+13C↓o
.text:00401045 ; sub_401AE9:loc_401BF6↓o
```

```
lea ebx, [ebp+lParam]
push ebx ; lParam
push 104h ; wParam
push 0Dh ; Msg
push 7D5h ; nIDDlgItem
push [ebp+hDlg] ; hDlg
call SendDlgItemMessageA
push offset a123 ; "123"
push ebx ; lpString1
call lstrcmpiA
or eax, eax
jnz short loc_401BF6
```

Figure7: Password Defined

After entering the pin it asked to input the cassette id. The loaded cassettes holding the money are visible when the "operator panel" is opened. The values ID, Bills count, Bill value, Currency, and Result are shown. It displays all cassettes containing money in the machine.

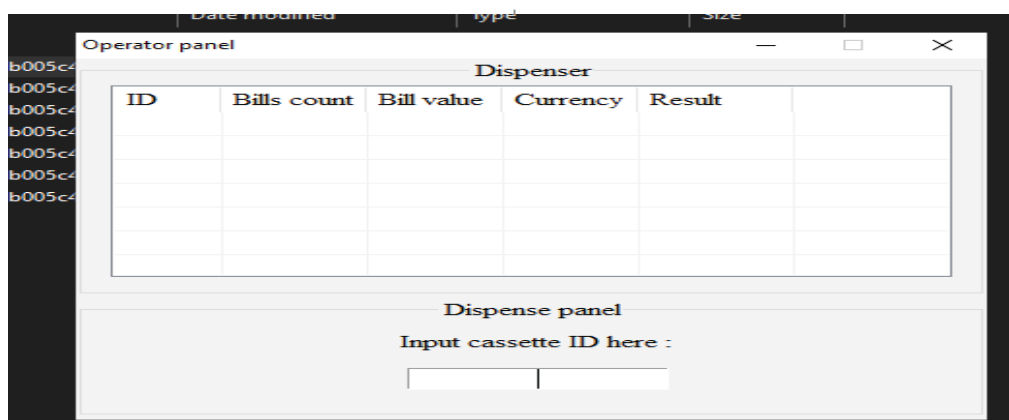


Figure 8: Entering the PIN

At this point, it detects that it is running on an ATM. When running on XFS (Extension for Financial Services)-based machines, it accepts

input. For Microsoft Windows-based financial applications, particularly those that use specialized peripherals like ATMs, XFS offers a client-server architecture.

```

push     esi
push     edi
xor      edi, edi
push     edi                ; lpModuleName
call     GetModuleHandleA
mov      hInstance, eax
push     3
call     sub_401047
push     edi                ; dwInitParam
push     offset sub_401AE9 ; lpDialogFunc
push     edi                ; hWndParent
push     7D0h              ; lpTemplateName
push     hInstance         ; hInstance
call     DialogBoxParamA
call     sub_401078
push     edi                ; uExitCode
call     ExitProcess
start endp

```

Figure 9: Second call

In the second call, it calls the **sub_401078** function. In this function it calls **WFSStartup**, a connection is made between an application and the XFS Manager by **WFSStartup**. It has

to be the first XFS API function a program calls. XFS functions cannot be supplied by an application until a successful **WFSStartup** has finished.

After that, it made calls to the

DialogBoxParamA

```

xor     edi, edi
push    edi                ; lpModuleName
call    GetModuleHandleA
mov     hInstance, eax
push    3
call    sub_401047
push    edi                ; dwInitParam
push    offset sub_401AE9 ; lpDialogFunc
push    edi                ; hWndParent
push    7D0h               ; lpTemplateName
push    hInstance          ; hInstance
call    DialogBoxParamA
call    sub_401078
push    edi                ; uExitCode
call    ExitProcess
start endp

```

Figure 10: DialogBoxParamA

This function takes five parameters. It takes one function as a parameter.

```

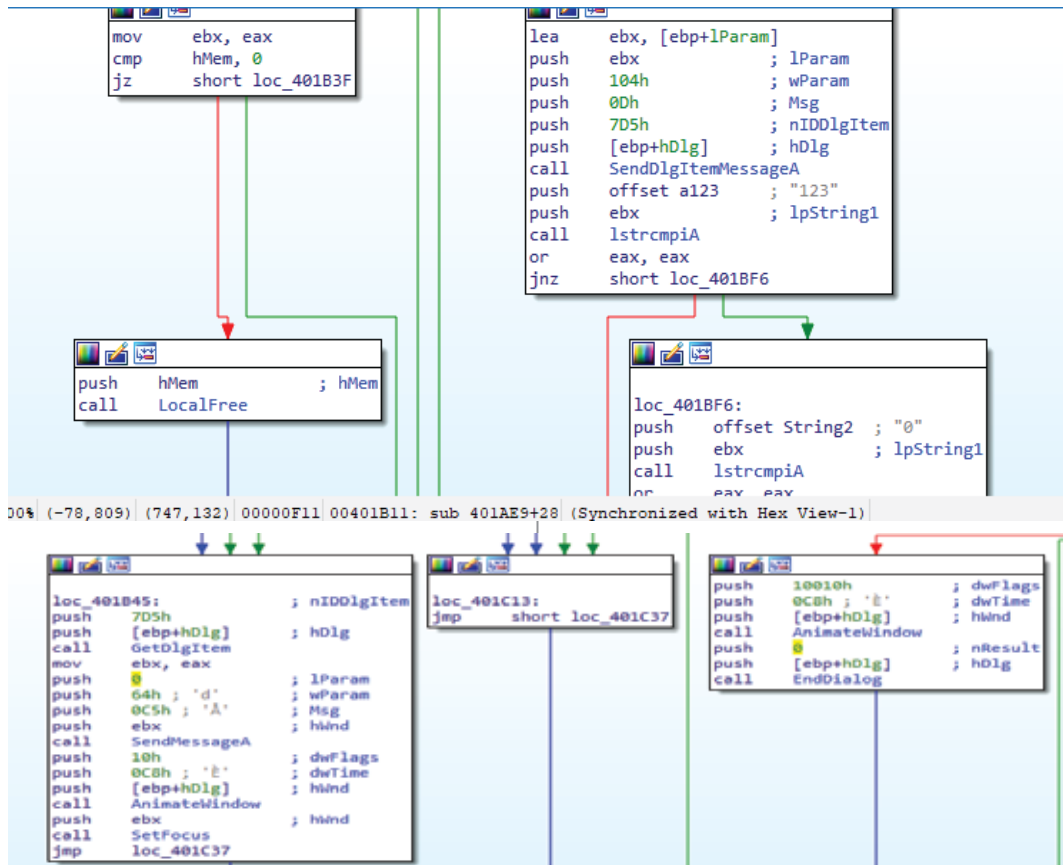
void __noreturn start()
{
    hInstance = GetModuleHandleA(0);
    sub_401047(3);
    DialogBoxParamA(hInstance, (LPCSTR)0x7D0, 0, sub_401AE9, 0);
    sub_401078();
    ExitProcess(0);
}

```

Figure 11: Function as parameter

run the program and it takes decisions based on provided data is correct or not.

This function that is going as a parameter is managed message box that appears when we



The highlighted function is responsible to

connect the dispenser1 of the ATM.

```

switch ( a2 )
{
case 0x110u:
    InitCommonControls();
    if ( sub_4011D1(byte_40102D, 0, 0) )
    {
        v4 = dword_401031(byte_40102D);
        if ( v4 )
        {
            v5 = (void *)v4;
            if ( hMem )
                LocalFree(hMem);
            hMem = v5;
        }
    }
    DlgItem = GetDlgItem(hDlg, 2005);
    SendMessageA(DlgItem, 0xC5u, 0x64u, 0);
    AnimateWindow(hDlg, 0xC8u, 0x10u);
    SetFocus(DlgItem);
    break;
}
  
```

Alice connects to ATM's CurrencyDispenser1 peripheral, and no other hardware; therefore

criminal does not need to issue any command via PIN pad.

```

mov     dword ptr [ebx], offset sub_40122F
mov     dword ptr [ebx+4], offset sub_4013F5
mov     dword ptr [ebx+8], offset sub_401483
mov     dword ptr [ebx+0Ch], offset sub_4012B7
push     0
push     [ebp+arg_8]
push     [ebp+arg_4]
push     30003h
push     offset aCurrencydispen ; "CurrencyDispenser1"
call     sub_401084
or       eax, eax
jz       short loc_401225

```

```

int __stdcall sub_4011D1(_DWORD *a1, int a2, int a3)
{
    int v3; // eax
    int v5; // [esp+214h] [ebp-4h]

    v5 = 0;
    if ( a1 )
    {
        *a1 = sub_40122F;
        a1[1] = sub_4013F5;
        a1[2] = sub_401483;
        a1[3] = sub_4012B7;
        v3 = sub_401084(aCurrencydispen, 196611, a2, a3, 0);
        if ( v3 )
        {
            a1[4] = v3;
            return 1;
        }
    }
    return v5;
}

```

```

.text:00401000 _text          segment para public 'CODE' use32
.text:00401000                assume cs:_text
.text:00401000                ;org 401000h
.text:00401000                assume es:nothing, ss:nothing, ds:_text, fs:nothing, gs:nothing
.text:00401000 aCurrencydispen db 'CurrencyDispenser1',0
.text:00401000                ; DATA XREF: sub_4011D1+4010
.text:00401013 aPtr          db 'PTR',0
.text:00401017 ; HINSTANCE hInstance
.text:00401017 hInstance      dd 0
.text:00401017                ; DATA XREF: sub_401AE9+10010
.text:00401017                ; start+84w ...
.text:0040101B dword_40101B  dd 0
.text:0040101B                ; DATA XREF: DialogFunc+324w
.text:0040101F ; CHAR Caption[]
.text:0040101F Caption       db 'Project Alice',0
.text:0040101F                ; DATA XREF: sub_401084+4210
.text:0040101F                ; sub_4012B7+10810 ...
.text:0040102D byte_40102D  db 3 dup(0)
.text:0040102D                ; DATA XREF: DialogFunc+16B40
.text:0040102D                ; DialogFunc+10010 ...
.text:00401030                db 0

```

From here we can see the malware name

Project Alice

```
int __stdcall sub_4011AE(int a1)
{
    WFSClose(a1);
    return 0;
}
```

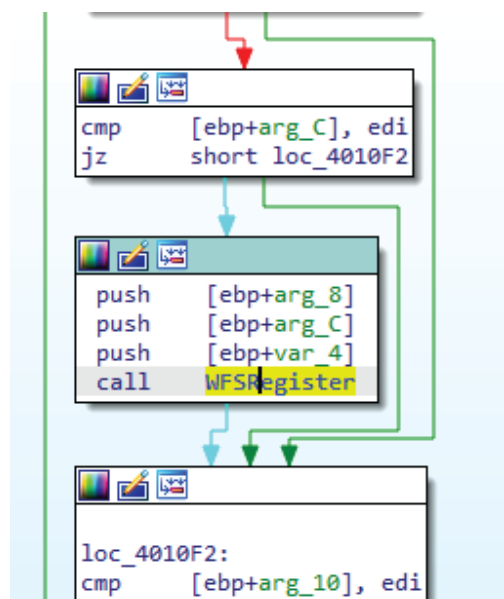
WFSClose is used to end a session or a series of service requests between the application and

the designated service that was started using WFSOpen.

Then it calls WFSFreeResult, which informs the XFS manager that a memory buffer that was dynamically allocated by a service provider is ready to be released. An application uses this function to deallocate the memory.

```
    v10 = v4;
    v5 = v4;
    v6 = *(unsigned __int16 **)(v2 + 4);
    do
    {
        v7 = *v6;
        *v5 = **v6;
        v5[1] = v7[6];
        v5[2] = v7[4];
        RtlMoveMemory(v5 + 3, (char *)v7 + 13, 3u);
        v5 += 4;
        ++v6;
        --v3;
    }
    while ( v3 );
}
WFSFreeResult(v9);
}
}
return v10;
}
```

A second call was placed. All messages of the defined classes are forwarded to the window indicated in the hWndReg argument by WFSRegister, which enables event monitoring for the specified service via the specified window. For instance, the application can call WFSRegister with the parameters SYSTEM EVENT and USER EVENT to receive data for both system and user events.



```

v15 = v5;
if ( *((_DWORD *)v4 + 1) >= 0x14u )
    v6 = 20;
else
    v6 = *((_DWORD *)v4 + 1);
*((_DWORD *)v5 + a3 - 1) = v6;
v11 = 1;
v12 = v13;
result = sub_40111F(*(_DWORD *)(a1 + 16), 302, Destination);
if ( !result || *((_DWORD *)(result + 22) )
{
    if ( result )
        v8 = *((_DWORD *)(result + 22));
    else
        v8 = -55;
    sprintfA(Text, "Can't dispense requested amount. Error %d occurred!", v8);
    MessageBoxA(hwnd, Text, Caption, 0x30u);
    LocalFree(v15);
    return v17;
}
return result;

```

At this point, it decides to see if input caste is available or not if available it calls the highlighted function if not then it moves on else part and displays an error.

WFSLock Establishes the application's sole authority over the designated service. Before beginning the transaction, the application needs to make sure that it has access to all the devices and that no other program will be able to utilize them until the transaction is finished.

Utilizing the WFSLock function and its companion WFSUnlock allows for this.

WFSExecute communicates a command specified by the service to a service provider. To run commands supplied by the service, use this function.

A service that has been locked by a previous WFSLOCK FUNCTION is released by **WFSUnlock**.

```

int __stdcall sub_40111F(int a1, int a2, int a3)
{
    int v4; // [esp+Ch] [ebp-8h] BYREF
    int v5; // [esp+10h] [ebp-4h]

    v5 = 0;
    WFSLock(a1, 0, &v4);
    if ( v4 )
        WFSFreeResult(v4);
    v4 = 0;
    WFSExecute(a1, a2, a3, 0, &v4);
    v5 = v4;
    WFSUnlock(a1);
    return v5;
}

```

So here before starting the transaction, the application ensures that it has access to all devices and until a transaction is made, no other program can use them. For this, it uses

WFSLock & WFSUnlock. After calling the function WFSLock it will call the next command for execution.

Examining the next function, it monitors if the selected caste is available or not. It gives an

error if the input caste is unavailable

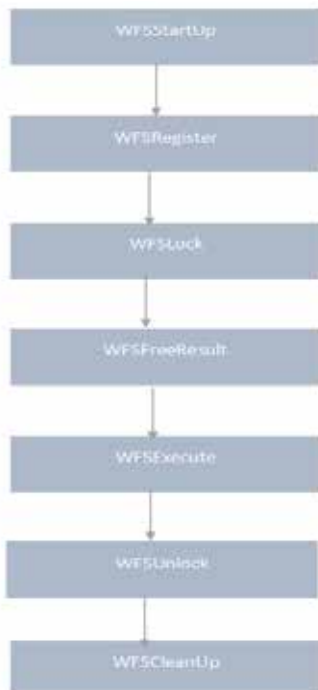
```
.text:00401260 ; CHAR Text[]
.text:00401260 Text db 'Selected cassette is unavailable !',0
; DATA XREF: sub_4012B7+1274o
.text:00401260
.text:00401283 ; CHAR aCanTDispenseRe[]
.text:00401283 aCanTDispenseRe db 'Can',27h,'t dispense requested amount. Error %d occurred !',0
; DATA XREF: sub_4012B7+F84o
.text:00401283
.text:004012B7
```

Before exiting the process it calls the function.

```
void __noreturn start()
{
    hInstance = GetModuleHandleA(0);
    sub_401047(3);
    DialogBoxParamA(hInstance, (LPCSTR)0x7D0, 0, sub_401AE9, 0);
    sub_401078();
    ExitProcess(0);
}
```

In this function, it calls the **WFSCleanUp** function. An application is unplugged from the XFS manager via **WFSCleanUp**.

The Flow of XFS APIs used:



Key Points:

This executable file, when provided is not named when I start reverse engineering I found a titled 'Project Alice'. Alice ATM first asks for a pin after entering a pin opening the operator panel reveals the loaded cassettes that hold the money. While malware has one main function that it uses to connect to the currency dispenser peripheral in the ATM. During the reverse engineering process, I didn't see that if it attempts to connect to other ATM hardware such as a PIN pad. So one thing is clear at this point it is not controlled by commands issued via Pin pad.

How exactly it works:

1. It first calls **WFSStartup** API to connect the application with the **XFS** manager.
2. After that it calls **WFSRegister** to enable event monitoring for the specified service.

3. Next, it makes a call to the **WFSLock** API to make sure that the application has access to all the devices before beginning the transaction and that no other application can use them until the transaction is finished. Utilizing the **WFSLock** function and its companion **WFSUnlock** allows for this.
4. Next, a call to **WFSFreeResult** alerts the XFS manager that a dynamically allocated memory buffer from a service provider has to be freed. An application uses this function to deallocate the memory.
5. Next, it calls **WFSExecute** to transmit a command specific to the service to a service provider. To run commands supplied by the service, use this function. Then it calls **WFSUnlock** to release a service that has been locked by a previous **WFSLOCK** function.
6. To disconnect the application from the XFS manager, it makes a final call to **WFSCleanUp**.

6. Conclusion

The globe has suddenly become a global village as a result of the extraordinary rise of information technology. As it happens, it has made the world smaller and knowledge flow more freely. Additionally, it has increased internet vulnerabilities, threats, scams, and criminal activity. The privacy of people, organizations, and states has been violated by the accessibility, user-friendly hacking tools, and complexity of cyberattacks. A good computer and network security life cycle, which comprises countermeasures, detection,

and reaction, now includes incident response as a crucial component. An organization's information security policy should contain the necessary provisions, and from there, planning and organization are essential for a successful incident response effort. The planning and organizing for the incident response also includes developing a suitable incident response architecture, planning resource requirements, planning the use of technology, developing incident response procedures, cooperating with other teams and organizations, and developing appropriate metrics. Moreover, Reverse engineering encompasses a wide range of tasks, such as system data analysis and the DE compilation and disassembly of executable files and libraries. Reverse engineering is a technique used in computer security to analyze malware activities and develop solutions to stop them.

7. References

- [1]. A. Javaid, "Incident Response Planning for Data Protection". SSRN Electronic Journal. Vol. 3, no.4. pp. 21-32. 2013.
- [2]. A. Ahmad, J. Hadgkiss, and A. B. Ruighaver. "Incident response teams—Challenges in supporting the organisational security function." *Computers & Security*. Vol. 31, no. 5. pp. 643-652. 2012.
- [3]. M. Kevin, C. Prosis, and M. Pepe. "Incident response & computer forensics". New York: McGraw-Hill, vol, 2. 2003.

- [4]. M. Hausi. "Reverse engineering: a roadmap." Proceedings of the Conference on the Future of Software Engineering. 2000.
- [5]. E. Eldad. "Reversing: secrets of reverse engineering". John Wiley & Sons, 2011.
- [6]. U. K. Sharath, K. Saumya and M. Madou. "Deobfuscation: Reverse engineering obfuscated code." 12th Working Conference on Reverse Engineering (WCRE'05). IEEE, 2005.
- [7]. W. Wego. "Reverse engineering: Technology of reinvention". Crc Press, 2010.
- [8]. S. Bruce. "The future of incident response." IEEE Security & Privacy. Vol. 12, no.5, pp. 96-96. 2014.
- [9]. W. Brown and J. Molra. Handbook for computer security incident response teams (CSIRTs). Carnegie-mellon univ pittsburgh pa software engineering inst, 2003.
- [10]. R. Werlinger, K. Muldner, K. Hawkey and K. Beznosov. "Preparation, detection, and analysis: the diagnostic work of IT security incident response". Information Management & Computer Security.vol.3, pp.13-56, 2010.
- [11]. C. Rui. "Design principles for critical incident response systems." Information Systems and E-Business Management. Vol. 5, no. 3. Pp. 201-227. 2007.
- [12]. W. Rodrigo. "Preparation, detection, and analysis: the diagnostic work of IT security incident response." Information Management & Computer Security. 2010.
- [13]. G. George, W. B. Glisson, and T. Storer. "Rethinking security incident response: The integration of agile principles." arXiv preprint arXiv. Vol.3. pp. 1408.2431.2014.
- [14]. F. Felix and B. Schwittay. "A common process model for incident response and digital forensics." Proceedings of the IMF2007. 2007.
- [15]. L. Trevor. "A forensic approach to incident response". Information Security Curriculum Development Conference. 2010.
- [16]. S. Alexander. "A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems." International Journal of Critical Infrastructure Protection. Vol. 37 . pp.100-105. 2022.
- [17]. S. Daniel, M. Caselli, and G. Pernul. "A comparative study on cyber threat intelligence: the security incident response perspective." IEEE Communications Surveys & Tutorials. vol. 23, no. 4. Pp. 2525-2556. 2021.
- [18]. H. A. Müller, J. H. Jahnke, D. B. Smith, and M. A. Storey. "Reverse engineering: a roadmap. InProceedings of the Conference on the Future of Software Engineering". pp. 47-60. 2000.

- [19]. H. Nikhil. "Where is the debugger for my software-defined network?." Proceedings of the first workshop on Hot topics in software defined networks. 2012.
- [20]. E. Stroulia and T. Systä. Dynamic analysis for reverse engineering and program understanding. ACM SIGAPP Applied Computing Review, vol.10, no. 1. pp. 8-17. 2002.
- [21]. S. Eleni, and T. Systä. "Dynamic analysis for reverse engineering and program understanding." ACM SIGAPP Applied Computing Review. Vol. 10, no.1. pp. 8-17. 2002.



Analysis of Packet to Detect Malware Files

Muhammad Shairoze Malik, Arooj Fatima and Saad Waqas

School of Electrical engineering and computer Sciences, National University of Science and Technology, Islamabad.

Corresponding author: aroorfatima72315@yahoo.com, saadwaqas832@gmail.com

Received: 18 September, 2022; Accepted: 18 November, 2022; Published: 20 December, 2022

Abstract:

The article covers the procedure of detecting malicious files from a packet which was responsible to make the system infected, this paper will highlight all the key elements that plays a pivotal role in detecting those files. The primary motivation behind this work is to provide information about those malware files and the detection of those files. This article also describes the use of perfect packet analysis software as well as its key features which can make our analysis simpler. Moreover, this article concludes with the author's perspective regarding the malware analysis.

Keywords: Malware files, Packet analysis software, Malware analysis, Detection

1. Introduction

Malware is the most common attack in the Cyber Security field. Most of the attackers use different malware techniques to gain benefit, it can be in terms of money or can be anything else. Malware can cause a huge damage to the user without his consent. In today's world, it is becoming the most damageable attack. It can affect your system, hardware, data loss and mostly data theft, your network and many other. So, to survive in this world, to control the number of attacks and to investigate malware cases, malware analyst showed their existence. They provide many of the detection procedures or techniques of malware which we can be used to investigate

these cases and to protect our system. Some questions that are being asked in this field are:

- What behavioral changes a malware can cause?
- How to detect the malware?
- What are the procedures of malware analysis?
- How to capture packets?
- What tool should we use to do the analysis?

The word malware is derived from words **MAL**icious **softWARE**. Whereas the word software means the program that targets the safety and integrity of the system is called malware. So, the Malware Analysis is the field

of inspecting malware tests to attempt to extricate important data about their starting point, conduct, and effect. There are many techniques that are used by malware analysts, a person who perform these activities, like Static Analysis and Dynamic Analysis [1]. Static Analysis include analysis of the malicious code without running it i.e., the File Headers, Strings, Hashes whereas the Dynamic Analysis include the analysis of the malicious code in a sandbox or safe environment.

2. IOC's:

IOC's stands for **Indication of Compromise**. These are the forensics evidence of a potential intrusion on a system network. These clues allow security professionals to determine the tactic of an occurred or impending attack IOCs are not always easy to detect, they can be as simple as metadata elements or incredibly complex malicious code and content samples. There are several IOC's which are listed below:

A. IP ADDRESS:

The word IP stands for "Internet Protocol", which can be regard as the set of rules governing the form of data sent via the internet or local network [3]. IP addresses are the unique addresses which can be used to identify the device.

B. DOMAIN NAME:

A domain name is a part of a URL. It is a string of text that maps to a numeric IP address, used to access a website from client servers [4].

C. USER AGENT:

The User-Agent request header is a characteristic string that let servers and network peers

identify the application, operating system, vendor, and version of requesting user-agent [5]. The syntax of use-agent is **User-Agent: <product> / <product-version> <comment>**.

D. HOSTNAME:

A hostname is a label that is assigned to a device connected to a computer network and that is used to identify the device in the various forms of electronic communication such as World Wide Web [4].

E. FILE HASHES:

File hashing is also used for file verification.

3. Tools For Analysis:

There are many tools that we can use to do analysis on the malware like PeStudio, Process Hacker, Process Monitor (ProcMon), ProcDot, Autoruns, Fiddler, IDA PRO, Ghidra. Wireshark is mainly used for the analysis because of its simplicity.



4. Wireshark:

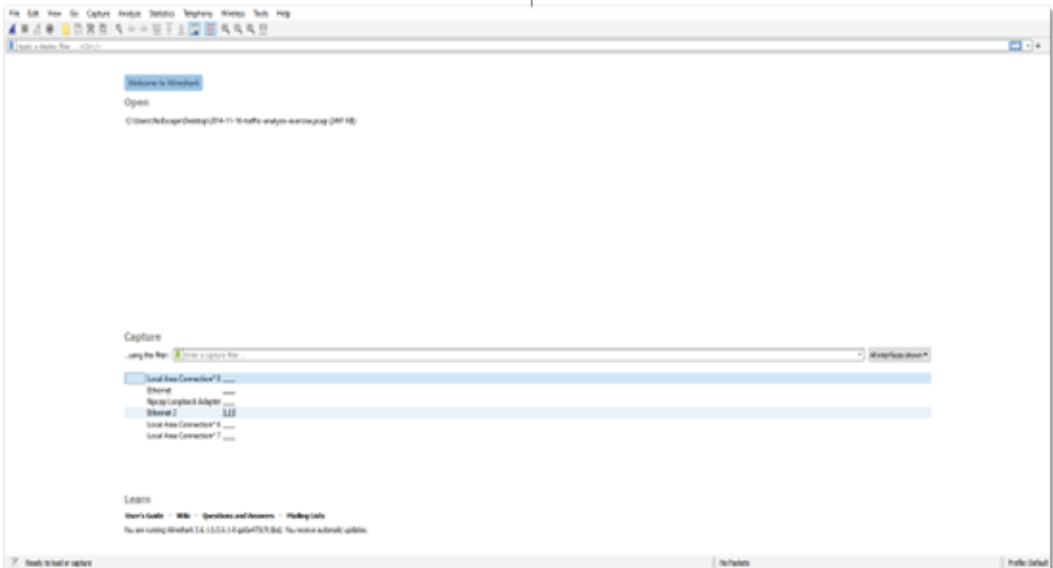
Wireshark is a free and open-source packet analyzer. Wireshark is a tool used for capturing and analyzing PCAPs files. It is used for **network troubleshooting, analysis, software and communication, protocol development and education**. The working of Wireshark is like tcpdump but has a graphical front and integrated sorting and filtering options. All the packet traffic is visible on the interface including uni-cast traffic. Wireshark is a data capturing program that understand the structure of different network protocol and it uses PCAPs to capture packets so it can only capture packets on the type of network that PCAP support. It can also color packets based on

rules that match fields in packets to help the user identify the type of traffic at a glance. Users can change the interface according to their choice [2].

4.1 Wireshark Default View

When you open the Wireshark, you will see this interface. To open a packet, just go to the file in the menu bar. Click open and select your

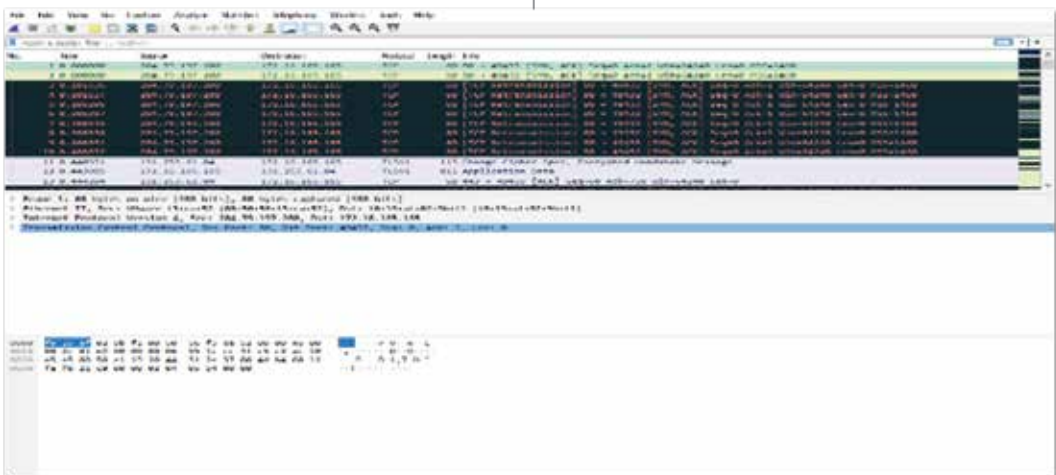
file. From Wireshark, you can also analyze the packets of your machine. All you need to do is choose the Local Area Connection. Another way to capture the local packets is to choose the Start Capturing Packets option with a symbol  on the top left side of the page. And to stop the capturing, click on the option named as Stop Capturing Packets with the  symbol.



4.2 Starting With Wireshark:

Now have a look on Wireshark user interface. The main window shows Wireshark as you

would usually see it after some packets are captured or loaded.



4.3 Wireshark Display Parts

The Wireshark Display has 4 parts as shown in the figure. These parts are also described below [7]:

- a) Filter Box (1): It is used to filter the packets displayed.
- b) Packet Listing (2): It shows all packets that satisfied the display filter.
- c) Packet Detail Windows (3): Display the contents of the currently selected packet.
- d) Hex Window (4): It displays the hex content of the current packet. The hex window is linked with the packets detail window and with highlight any field selected.

4.4 Changing The Default View:

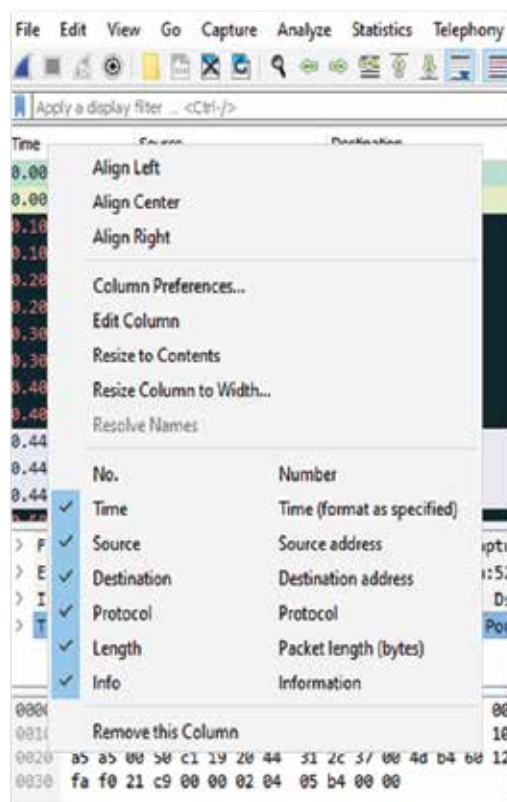
The Default view of Wireshark is not very friendly to every user, so Wireshark gives a functionality to the user to customize the interface of the Wireshark according to their choice or need. The default column in the Wireshark is not ideal in every case. Here comes the need to modify the columns. The default columns are:

- No: It is the frame number from the beginning of the PCAP.
- Time: Seconds are broken down into Nanoseconds.
- Source: Source address.
- Destination: Destination address.
- Protocol: Used in Ethernet Frame, IP Packet, or TCP segment.
- Length: Length of Frame in Bytes.

So, following are the ways to customize the columns in the interface:

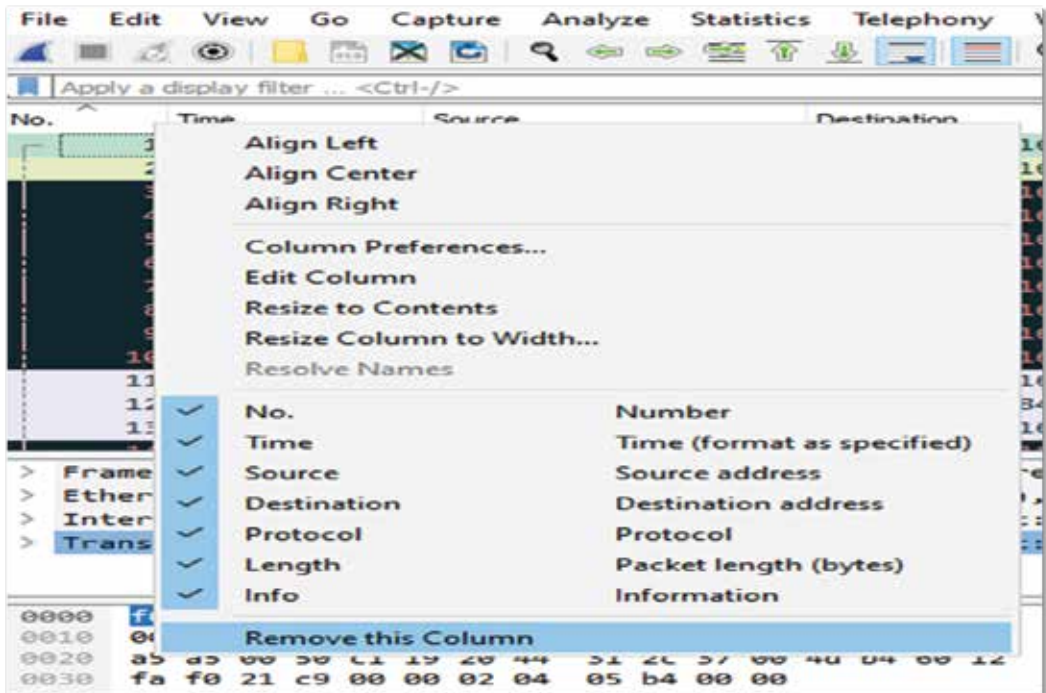
a. Hiding Columns:

We can easily hide the columns in the interface, we can also unhide the columns when there is a need to use the columns. First Right-Click on the Column which you want to hide and then uncheck the column name. And to unhide the column, you just need to check the column name again. Following Figures shows the way how to hide the columns:



b. Removing Columns:

There are some of the columns in the interface which are not required for the analysis like the **NO column** and the **Length column**. We can also remove these columns. For this we just need to Right Click on that column and then Select **Remove this Column** option from the drop-down menu.

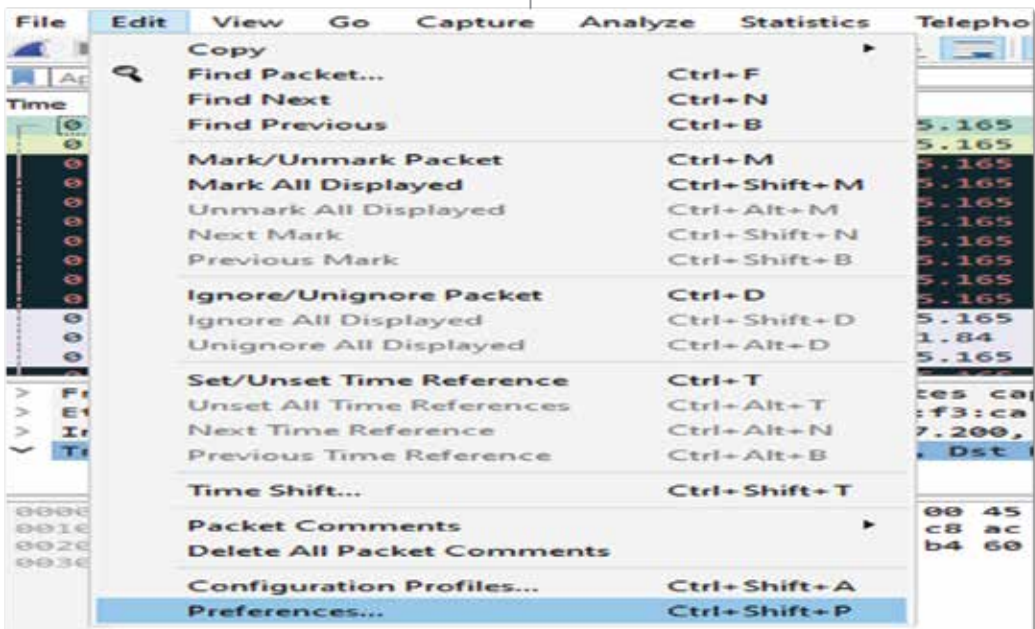


c. Adding Columns:

Wireshark also provide us with the feature which allows us to add the column of our own choice. For Adding the column, you must go through from the number of steps listed below:

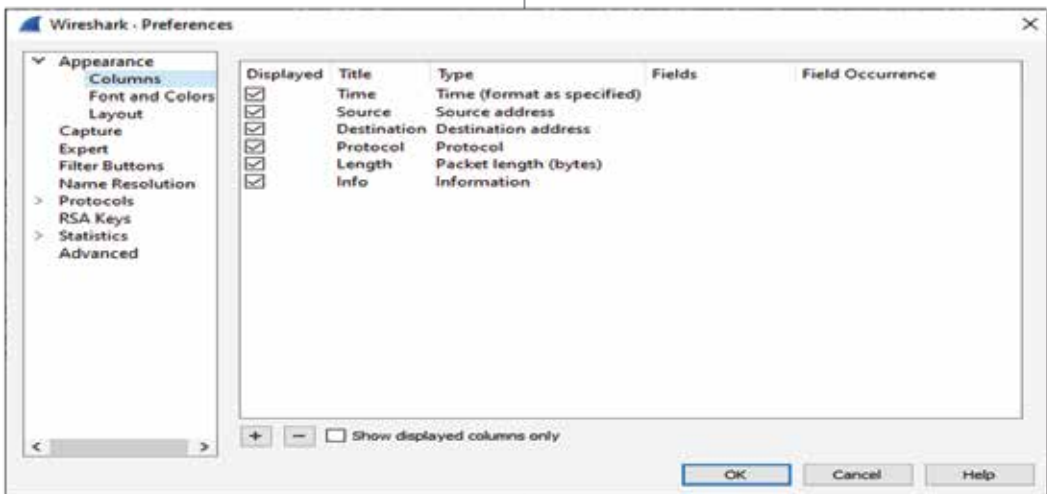
STEP 01:

Go to the **Edit** on the menu and then select **Column Preference** option from the drop-down menu.



The Column Preference Menu List all columns, viewed or hidden at the bottom of the menu there are two buttons **plus (+)** and **minus**

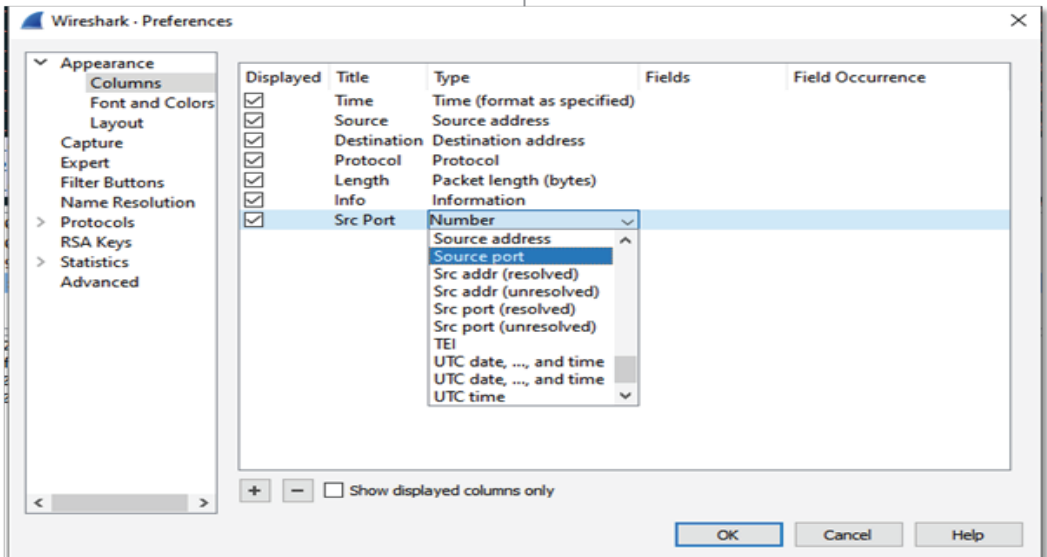
(-) which are used to add or remove the column respectively.



STEP 02:

If you want to add a column, you just need to click on the plus sign, a new row will appear

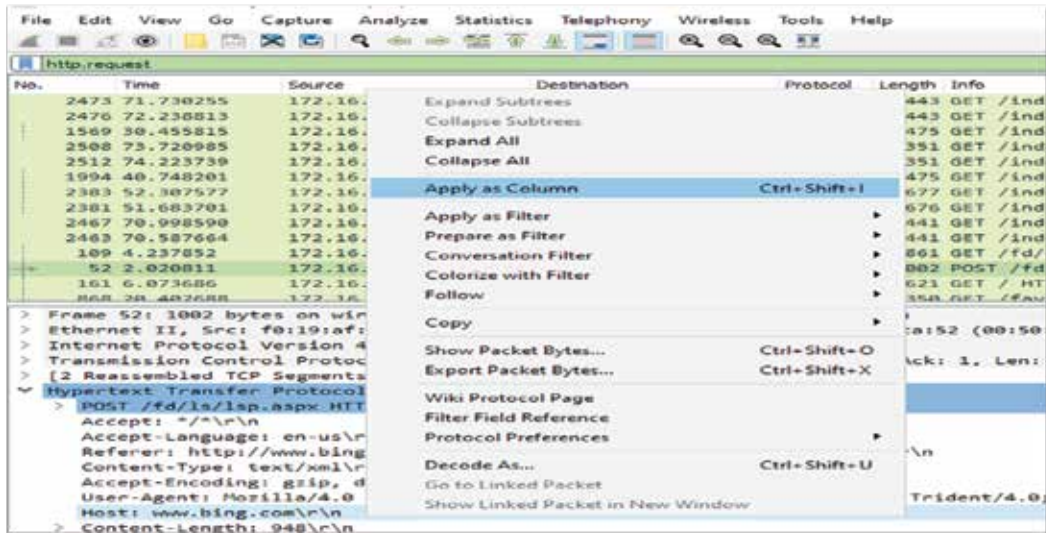
and then rename the Column and select the type of your column.



Same case goes with the removing column. After setting up this click on **OK**. Now, you have successfully changed the columns of the Wireshark interface.

d. Apply As Column:

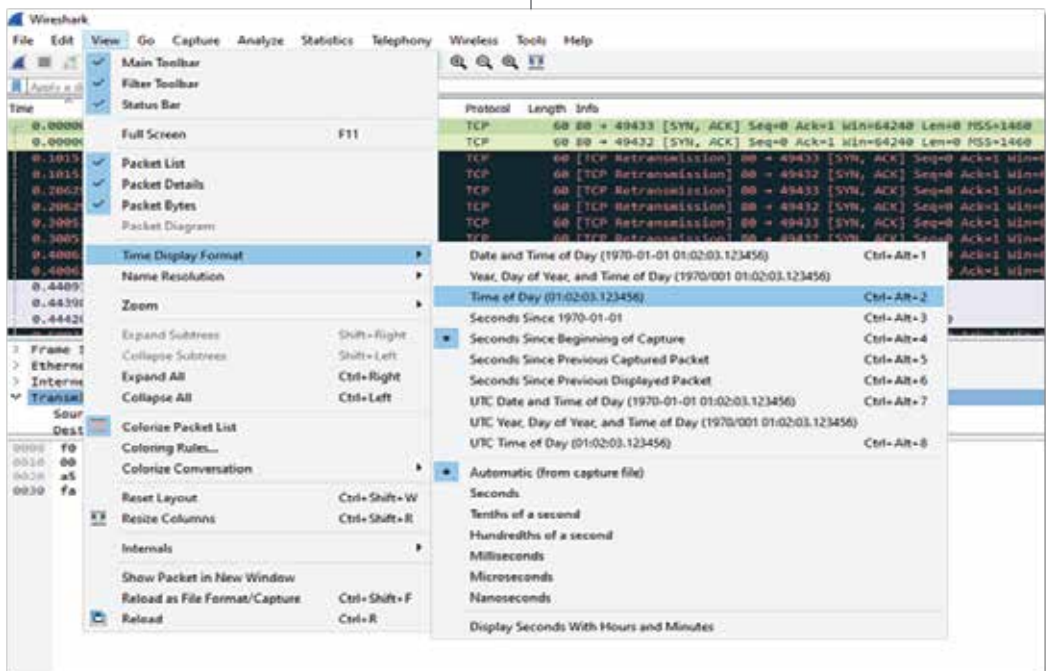
If you want to apply any field from the Packet Window Detail as a column, you need to Right-Click on that field. Choose Apply as Column option and then it will be displayed as column.



e. Time Display:

We can also change the format of the displayed time. The default syntax of the time is seconds broken down into Nanoseconds which in real is like 0.101536. You can also change this

syntax into readable syntax. First Go to the **View** from the **Menu** and then choose **Time Display Format**, now choose the format of your own choice.



5. Detection Of Malware:

Initially, we will check the traffic, if they were

sent in continuous packets, then they will be exportable through Wireshark itself or if not then we have to manually analyze the streams

and packets. Detection of malware includes number of steps:

- Analyze the network traffic present in the packet through protocol hierarchy.
- Check the greater percentage of network protocol i.e., HTTP/HTTPS, SMB etc.
- Analyze all the packets present in the traffic.
- Sort the objects with the Content-Type.
- Locate suspicious files and take hashes of those files by using hashmyfile [8].
- Cross Check the hashes of suspicious files by putting those hashes in Virus Total [9].

Sometimes malicious traffic can also be detected through different destination port for example: victim is connecting through port:80 and attacker is connecting through port:143 sounds malicious.

6. Case Study:

Let's consider a case study [10]. Here we have a packet which contains the logs of malicious files. These files are responsible to make the machine infected. Now we must do some

investigation in that packet to give the answers to some questions listed below. This section of the document covers that how and where to get the information in in the packet.

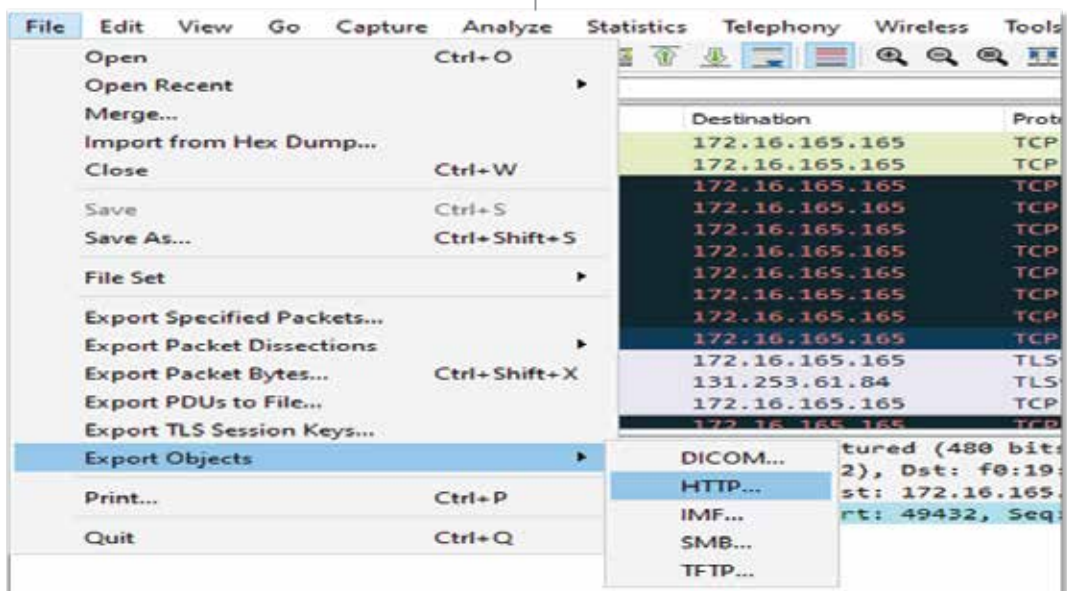
Questions

- What is the infected file(s) downloaded and their hashes?
- What is URL/Domain of the infected site?
- What is the IP address of the infected site?
- What is the IP address of the infected machine?
- What is the hostname of the infected machine?
- What is the mac address of the infected machine?

Question No. 01:

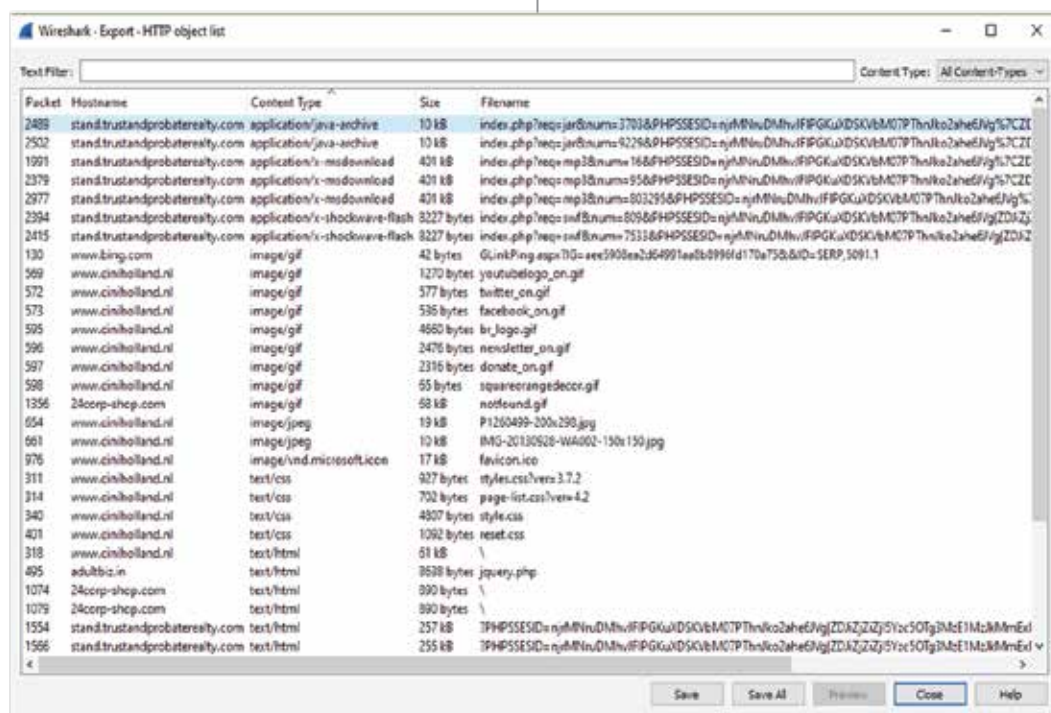
STEP 01:

Go to the file drop-down in the menu bar and then choose Export Objects. Then another drop-down will appear which will show some of the options like HTTP. As most of the traffic in the packet logs were of HTTP, so we will choose HTTP option from the menu.



After doing the above step, a window will appear with the name Wireshark – Export – HTTP object list. It will describe the information of every downloadable material. We can

sort the Content Type alphabetically just by clicking the Content Type. Now save every file.



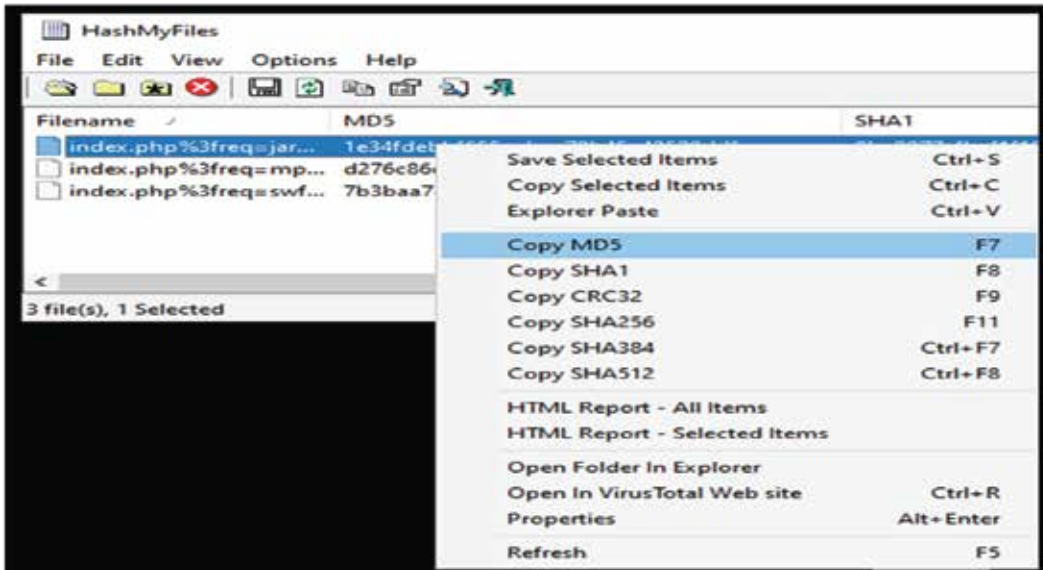
Take hashes of every file you downloaded from the list with the help of *hashmyfiles*

software.



After getting the hashes, copy those hashes of any type one by one and then put those hashes

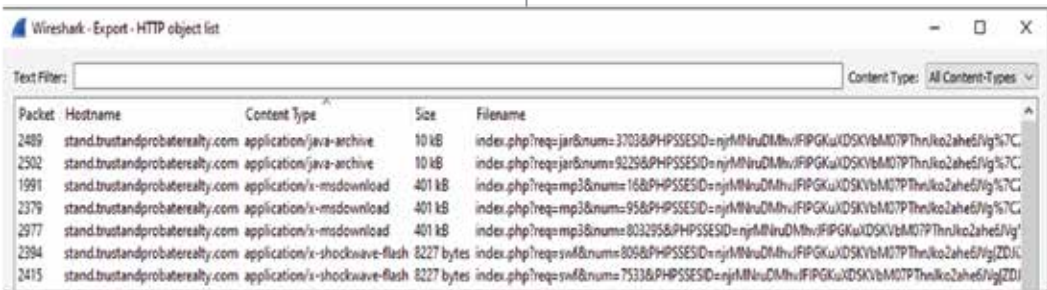
in the virus total that will show if these hashes are infected or not.

**Question No. 02:**

Solution of Question no. 01 shows the infected files. Now the question is to get the URL/Domain of the infected site. Again, follow the steps mentioned in the Question No. 01 till the window appear with the name Wireshark – Export – HTTP object list. In this window, there is a column named as hostname. This column will give us the answer of Question No. 02.

Question No. 03:

We have already found the infected site hostname. Now we are going to find the IP address of that infected site. For this, just put the filter *http.request*. It will only show the logs requested by the user. In the Destination Column, we can easily find the IP address of the infected site.

Question No. 04:

With the same filter, we can find the IP address of the infected machine. The Source Column shows the IP address of the infected machine.

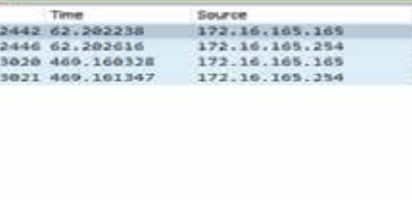
Question No. 05:

There is more than one way to get the

hostname of the infected machine. Some of them are described below:

WAY 01:

Put the DHCP filter in the filter box. Some of the packets will be shown. Click any of the



No.	Time	Source	Destination
2442	62.202238	172.16.165.165	255.255.255.255
2446	62.202616	172.16.165.254	172.16.165.165
3020	469.160328	172.16.165.165	172.16.165.165
3021	469.161347	172.16.165.254	172.16.165.165

Relay agent IP address: 0.0.0.0
 Client MAC address: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
 Client hardware address padding: 000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: DHCP
 > Option: (53) DHCP Message Type (Inform)
 > Option: (61) Client identifier
 ✓ Option: (12) Host Name
 Length: 12
 Host Name: K34EN6u3N-PC
 > Option: (60) Vendor class identifier
 > Option: (55) Parameter Request List
 ✓ Option: (255) End

name of the infected machine.

Question No. 06:

No.	Time	Source	Destination	Protocol	Length	Host	Info
2400	53.160900	172.16.165.165	172.16.165.2	HTTP	118		Refresh NB K342H6U0N-PC(00)
2430	54.660204	172.16.165.165	172.16.165.2	HTTP	118		Refresh NB K342H6U0N-PC(00)
2439	56.160211	172.16.165.165	172.16.165.2	HTTP	118		Refresh NB K342H6U0N-PC(00)
2449	62.502002	172.16.165.165	172.16.165.2	HTTP	92		Name query NB SPAD(00)
2491	64.002559	172.16.165.165	172.16.165.2	HTTP	92		Name query NB SPAD(00)
2493	65.502640	172.16.165.165	172.16.165.2	HTTP	92		Name query NB SPAD(00)

The image shows a Wireshark packet capture of an HTTP GET request. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for various functions. The packet list pane on the left shows a single packet, #1, selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP GET request. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Full request URI
570	11.202403	172.16.165.165	82.150.140.30	HTTP	457	http://www.ciniholland.nl/wp-
579	11.202596	172.16.165.165	82.150.140.30	HTTP	448	http://www.ciniholland.nl/wp-
650	12.073745	172.16.165.165	74.125.233.96	HTTP	602	http://www.youtube.com/embed-
868	28.402688	172.16.165.165	82.150.140.30	HTTP	358	http://www.ciniholland.nl/fav-
981	21.787861	172.16.165.165	188.225.73.100	HTTP	505	http://24corp-shop.com/
982	21.787964	172.16.165.165	188.225.73.100	HTTP	585	http://24corp-shop.com/
1076	22.631140	172.16.165.165	188.225.73.100	HTTP	413	http://24corp-shop.com/source
1212	23.664535	172.16.165.165	37.200.69.143	HTTP	695	http://stand.trustandprobat
1213	23.664644	172.16.165.165	37.200.69.143	HTTP	695	http://stand.trustandprobat
1509	30.455615	172.16.165.165	37.200.69.143	HTTP	473	http://stand.trustandprobat
1994	40.748201	172.16.165.165	37.200.69.143	HTTP	475	http://stand.trustandprobat
2381	51.683701	172.16.165.165	37.200.69.143	HTTP	677	http://stand.trustandprobat
2488	52.308727	172.16.165.165	37.200.69.143	HTTP	677	http://stand.trustandprobat

Packet #1 details:

- Frame 578: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits)
- Ethernet II, Src: fo:19:af:02:9b:f1 (fo:19:af:02:9b:f1), Dst: VMware_f3:ca:52 (00:50:56:f3:ca:52)
- Destination: VMware_f3:ca:52 (00:50:56:f3:ca:52)
- Source: fo:19:af:02:9b:f1 (fo:19:af:02:9b:f1)
- Type: IPv4 (0x0800)

35

7. Conclusion

According to the author and the co-author, detection of malware in a packet is an interesting activity in investigating it. The above-mentioned ways to detect the malware was related to the HTTP traffic. The reader can have a basic understanding of malware analysis in traffic.

8. References:

- [1] I. Ahmed and K. suk Lhee, "Classification of packet contents for malware detection," *Journal in Computer Virology*, vol. 7, no. 4, 2011.
- [2] N. Dutta, N. Jadav, S. Tanwar, H. K. D. Sarma, and E. Pricop, "Introduction to Malware Analysis," in *Studies in Computational Intelligence*, vol. 995, 2022.
- [3] R. S. Kunwar and P. Sharma, "Malware analysis: Tools and techniques," in *ACM International Conference Proceeding Series*, 2016, vol. 04, March-2016.
- [4] B. Dodiya and U. K. Singh, "Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise," *Int J Comput Appl*, vol. 183, no. 53, 2022.
- [5] T. Moore and R. Clayton, "Which malware lures work best? Measurements from a large instant messaging worm," in *eCrime Researchers Summit, eCrime*, vol.5, 2015.
- [6] V. Jain, "Getting Familiar with Wireshark," in *Wireshark Fundamentals*, 2022.
- [7] N. Pachhala, S. Jothilakshmi, and B. P. Battula, "A Comprehensive Survey on Identification of Malware Types and Malware Classification Using Machine Learning Techniques," in *Proceedings - 2nd International Conference on Smart Electronics and Communication, ICOSEC 2021*, 2021.
- [8] X. Zhong, Y. Fu, L. Yu, R. Brooks, and G. K. Venayagamoorthy, "Stealthy malware traffic - Not as innocent as it looks," in *2015 10th International Conference on Malicious and Unwanted Software, MALWARE 2015*, 2016.
- [9] B. A. Mah, "Empirical model of HTTP network traffic," in *Proceedings - IEEE INFOCOM*, 1997, vol. 2.1997.
- [10] M. Yaibuates and R. Chaisricharoen, "A Combination of ICMP and ARP for DHCP Malicious Attack Identification," in *2020 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering, ECTI DAMT and NCON 2020*, 2020.



Role of Analytical Techniques in Crime Investigation

Asif Ibrahim¹ and Syed Khurram Hassan²

¹ Department of Mathematics, FC College University, Lahore.

² Institute of Quality and Technology Management, University of the Punjab, Lahore, Pakistan.

Corresponding author: khuramshah6515@gmail.com

Received: 21 September, 2022; Accepted: 25 November, 2022; Published: 20 December, 2022

Abstract

Forensic science is becoming a growing discipline in crime scene investigation. The field of rhetorical science has recently undergone an intriguing evolution and significantly raised its public visibility. Advances in science and technology, increased dependence on law enforcement and court systems science, and media exposure have all contributed to the importance of forensic. Several completely unrelated fields have been associated with the name "forensics". Among the topics that commonly make the headlines are acts of terrorism, a rise in gun ownership, drug misuse, and driving while under the influence of narcotics. The forensic scientist must rely on chemical analysis of trace amounts of materials such as drugs, explosives, discharge residues, toxicological specimens, paints, glass, fibres, soil, etc. to establish or rule out links between suspect and victim and scene in the absence of fingerprints and of material that could lead to the recovery of DNA. This instructional overview outlines the analytical issues that forensic chemists must deal with, as well as the current approaches and strategies used to solve them.

Keywords: Techniques, forensics, DNA, Toxicology, fingerprints

1. Introduction

Now, the public in general has grown more awareness of how science is used to solve crimes, as a result of the rise in both fictional and documentary television shows [1]. Among the topics that commonly make the headlines are acts of terrorism, a growth in the illicit use of guns, drug trafficking, and driving while under the influence of narcotics [2]. Since the identification of person-specific human DNA "fingerprints" and the subsequent

forensic use of DNA fingerprints in 1985, forensic science laboratories have invested a significant amount of money in the creation of DNA profiling techniques. Evidence makes it as advanced tool for identification [3]. According to Forensic Technology Survey's findings and related case studies, there is an urgent need for more advanced forensic science technology, as well as for qualified people to utilize it and communicate its findings [4]. Major conclusions include that numerous crime laboratories have a sizable

backlog of evidence that has not been analyzed or otherwise processed [5]. No matter how careful a criminal tries to avoid leaving his fingerprints, he may still accidentally touch other areas of his body and leave bodily fluids or tissue behind, each of which will contain his DNA. In crime scenes, fingerprints are also person-specific [6]. However, forensics experts should indeed focus solely on chemical evaluation of trace quantities of materials such as explosive devices, stimulants, glass, soil, etc. to develop links between victim and suspect [7]. This study will look at the most recent approaches to forensic analytical chemistry for the categories of evidence mentioned above. The case become more prompt if effective forensic scientific skills are available.

2. Process Used By a Toxicologist

Three steps may be identified in the procedure toxicologists use. In the first, the medicines, metabolites, and other relevant analytes are tentatively identified using qualitative analysis. These are identified through screening tests, same like with narcotic examination of confiscated goods. But the narcotics chemist who was apprehended has fewer alternatives. There are two reasons for this restriction. The sample matrices come first and are more significant [8].

3. Drug Analysis

The most often abused narcotics amphetamines, heroin, benzodiazepines, cannabis, cocaine are the substances that a forensic drugs analyst is most likely to come across [9]. They can be found in small amounts

in the hands of individual users as so-called "street seizures," in greater amounts in the hands of local drug traffickers, and in kilogramme quantities as imported substances. The basic objectives of the forensic scientist's analysis are to: (a) establish if a prohibited substance is present, (b) establish the quantity of the substance, and (c) occasionally establish the link between drug samples by comparison or "profiling" [10]. For quick screening and straightforward comparison, thin layer chromatography (TLC) is used on ethanol extracts of the resin, herbal material and oil [11]. Profiling can be done using GC-MS or HPLC. Reversed-phase HPLC will establish if the resin blocks came from the same batch based on the results of the preliminary TLC screen. HPLC is helpful since, unlike GC-MS, it does not call for derivatizing the materials. Because they are thermally labile, tetrahydrocannabinolic acids would break down under GC-MS conditions. The drug profile is shown by the chromatogram [12].

4. Explosives

The removal of explosive residues or traces can be done using sticky tape, solvent cleaning of objects, vacuum sampling, or swabbing (dry or with a solvent) [13]. Ion mobility spectrometry is a quick and practical screening procedure at the crime scene or in the lab (IMS) [14]. Explosive remnants from questionable surfaces are collected using a suction using a portable IMS device. [15]. Prior to colour spot tests and chromatographic analysis, residues submitted to the lab are first inspected under a microscope. They are then dissolved in a solvent such ethanol or acetone. The most popular analytical system combines

mass spectrometry's (MS) identification capabilities with HPLC's separation capacity [16].

Based on Locard's Exchange Principle, forensic investigation of any trace evidence, including textile fibres, is performed [17]. According to this, "every contact leaves a trail." In reality, even though there has been a movement of material (in one or both ways), it might not be feasible to tell because of how little was really moved. Additionally, some surfaces may swiftly and readily lose transferred material due to their nature and texture. As a result, it's critical to gather clothes from suspects and victims as quickly as possible after an alleged crime since recent transfers are frequently involved in proof of touch (and hence affiliation) discovered by comparison of fibres.

When fibres are readily visible, forceps, lifts with sticky tape, or suction are used to recover or retrieve them from a crime scene [18]. Microscope comparison, fibre identification, and colour analysis are all steps in the study and analysis of fibres. UV/visible comparison microscopy is used to compare known or control fibres to extraneous (suspect) fibres that have been collected loosely or from tape lifts [19]. It is possible to identify whether a fibre is synthetic or natural using morphological information from optical microscopy, whereas synthetic fibres may be identified using pyrolysis gas chromatography (PGC) and pyrolysis mass spectrometry (PyMS). Visible light microspectrophotometry is used to check known and suspicious fibres for similarities following comparison microscopy [20]. If the resultant spectra are comparable, an FTIR analysis is performed,

which provides a clear identification of the fibre polymer as well as some information on the dyes. The procedures utilised for dye extraction will vary on the kind of fibre and colour being employed. Visually like colours could really be made up of many component dyes (a so-called "metameric match") that are easily distinguishable by TLC, HPLC and Surface Enhanced Resonance Raman Scattering (SERRS) have been successfully employed [21].

5. Paint

Paint can be found as an evidence in a variety of situations. It may appear as tiny peels on the clothing of someone who has vandalised a building and damaged the paintwork, as paint streaks transmitted from one car to the other in a collision, or from a car to a victim in a hit-and-run accident [22]. Beginning with a microscopic inspection of control paint, such as that from the place of entry in the instance of a break-in, the analytical method to such evidence is used (found on the garments of the suspect). In addition to visible light microscopy, polarised light microscopy are used because they can provide a wealth of information about the general appearance of the samples. This also includes the existence of a layer structure, the texture and color of the layers, information on particle size. Since single-layer forensic paint specimens are the norm, it is necessary to identify the chemical makeup of the extenders, binders and pigments after comparing colours [23]. X-ray powder diffraction (XRD), X-ray fluorescence (XRF), and scanning electron microscopy/energy dispersive spectroscopy (SEM/EDS) are used to analyse paint pigments and extenders. Because it can do elemental

analysis and offers a magnified view of the paint flake specimen, scanning electron microscopy is very helpful. An elemental analysis can be accomplished by focusing the electron beam directly on certain paint layers and individual particles. It is possible to infer the quality of pigments present in the material, however SEM/EDS by itself cannot identify the pigments with certainty. Although multilayer paints require layer separation before examination, XRD is a good non-destructive method for analysing paint since it does offer conclusive identification of the pigments (organic or inorganic) and extenders [24]. Its relative insensitivity in compare to the other approaches is its main flaw. Elements have also been analysed using laser ablation inductively coupled plasma-mass spectrometry (LA-ICP-MS). Prior to ICP-MS analysis, the laser ablation method can concurrently sample numerous layers in order to identify and quantify trace elements that are present in various layers of the sample. A new method of discriminating is added via trace element analysis. Pyrolysis techniques like Pyrolysis Gas Chromatography (PGC) and Pyrolysis Mass Spectrometry are used to analyse the binders in a paint material [25].

6. Fibres

Target fibre investigations demonstrate that practically all fibres only sometimes appear in the environment, as was previously noted. Indigo-dyed cotton would be the most notable exception. This suggests that the degree of linkage is likely to be high if well-known and unknown fibres are comparable overall in physical and chemical properties. This may not

be the same as personalising the evidence. Only a tear match can differentiate between fibres. In addition to the previously mentioned, fibres (and hairs, too) have the shared characteristic of being easily transferred from one substance to another or from a material to a different surface, like a chair seat. The transmitted fibres may stay on the destination item or may just be transferred again [26].

7. Fingerprints

The finger markings, which are the impressions made by the friction ridges of the finger. These fingerprints not only show that the surface or object was touched, but they also help to identify the individual. Latent, patent, and plastic fingerprints are the three types that are most frequently discovered [27]. Almost all crime scenes contain latent prints, which must be processed since they are difficult to see with the human eye [28]. A wide range of physical and chemical techniques have been developed to decode the latent fingermarks. The most popular technique for creating latent fingermarks is powder. The best fingerprint powder will attach to the finger sweat residues, which produce the distinctive patterns that transform latent prints into coloured or fluorescent visible prints depending on the type of powder used. It is much more difficult to make a definite identification since many common materials stick to the backdrop [29]. In order to solve these issues and increase precision, nanotechnology is being employed to build fingerprint. The fingerprint pattern has been deciphered using tiny particles. Numerous research have shown that nanopowders may be used to decode fingerprints, and most recently, one of these

studies found that zinc oxide powders with a 20 nm particle size produce superior prints and UV fluorescence than other powders. Additionally, their newly created techniques operate in moist conditions where conventional powders cannot [30].

8. Glass

Globally, Glass has potential applications. As a result, it frequently occurs in violent crimes including murder, robbery, planned car accidents, and reckless driving. When glass breaks, tiny pieces might become stuck to the offender's clothing or weapons. These pieces can be used as significant evidence in court proceedings if they are gathered, examined, and compared. It has also been done to analyse glass samples using both elemental analysis and RI determination. The majority of these investigations have come to the conclusion that these analyses are complementing rather than rival. Metals in glass samples may be analysed using inductively coupled plasma-atomic emission spectroscopy (ICP-AES) and inductively coupled plasma-mass spectrometry (ICP-MS). However, their primary drawback is their destructive nature, which has led to Laser Ablation-ICP-MS largely replacing them (LA-ICP-MS) [31]. Glass samples may quickly be directly analysed using a quasi-non-destructive approach. Other studies have using X-Ray Fluorescence (XRF) methods. XRF has a non-destructive nature, is simpler to operate, and costs less than ICP-MS. Due to its speed, lack of sample preparation requirements, and similar sensitivity to LA-ICP-MS, Laser Induced Breakdown Spectroscopy (LIBS) has recently gained popularity. Although to a lesser degree, glass

examination has also been performed using the scanning electron microscope energy dispersive X-ray spectroscopy (SEM-EDX), particle free induced X-ray emission (PIXE), and the electron probe micro-analyzer (EPMA) [32][33].

9. Arson

The most common accelerants used in arson assaults are gasoline (also known as gasoline), paraffin (also known as kerosene), and occasionally paint strippers. After the flame has been extinguished, any remnants of these substances may quickly vanish. The method that is most frequently used to analyse evidence of accelerants found at fire sites is gas chromatography (GC) [34]. The bags or jars containing the trash and garments are sampled from headspace to begin the examination. Any volatile residue is driven into the container's atmosphere by heating it. A syringe containing an absorbent material, like the resin Tenax, is used to pull the air comprising volatile compounds through the resin [35]. The absorbent substance is forced through the storage container into the surrounding air. Volatiles that have been absorbed are thermally exfoliated from the Tenax when the cuvette is inserted in the GC. As a result of the heating action of the fire, A mixture of peaks from the accelerants and any pyrolysis byproducts from the heat degradation of polymers and natural materials will appear in the resulting chromatogram. When residues are retrieved from a fire scene, the more volatile parts of petrol are not present, which at first may make identification more difficult. However, comparison with chromatograms of conventional paraffin, diesel, white spirit and

diesel will typically identify the accelerants [36].

10. Conclusion

Forensic science applications can lead to distinct identifications in different ways. In situ trace analysis using Surface Enhanced Resonance Raman Scattering Spectroscopy (SERRS), which is practically non-destructive, also has a lot of promise. SIRMS and SERRS will undoubtedly advance, becoming important analytical techniques for determining, respectively, the source and composition of materials such as drugs, dyes, glass, fuels, soils, inks, glass explosives, and many others. This is similar to how DNA profiling will undoubtedly continue to advance.

11. References

- [1]. M. Storksdieck. "Critical information literacy as core skill for lifelong STEM learning in the 21st century: reflections on the desirability and feasibility for widespread science media education". *Cultural studies of science education*, vol. 11, no. 1, pp. 167-182. 2016.
- [2]. M. Sarkar and R. Amin, "Globalization, Local Crimes and National Security: The Case of Bangladesh" (Doctoral dissertation, University of Dhaka). 2019.
- [3]. C. W. Hunt. "Agent based evidence marshaling: Agent-based creative processes for discovering and forming emergent scenarios and hypotheses". George Mason University. 2001.
- [4]. J. M. Anderson, C. Matthies, S. Greathouse and A. Chari. "The Unrealized Promise of Forensic Science-A Study of Its Production and Use". *Berkeley J. Crim. L.*, vol. 26, pp. 121-127. 2021.
- [5]. A. Shaw and A. Browne. "A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. *Digital Investigation*", vol. 10, no. 2, pp. 116-128. 2013.
- [6]. M. Ulker, B. Arslan and S. Sagiroglu. "Evaluation of Fingerprint Enhancement Techniques Used by Crime Scene Investigation. In 10th. International Conference on Information Security And Cryptology". pp. 29-37. 2017.
- [7]. E. Mistek, M. A. Fikiet, S. R. Khandasammy and I. K. Lednev. "Toward locard's exchange principle: recent developments in forensic trace evidence analysis". *Analytical chemistry*, 91(1), 637-654. 2018.
- [8]. M. R. Meyer, J. Wilhelm, F. T. Peters, and H. H. Maurer. "Beta-keto amphetamines: studies on the metabolism of the designer drug mephedrone and toxicological detection of mephedrone, butylone, and methylone in urine using gas chromatography-mass spectrometry". *Analytical and bioanalytical chemistry*. vol 397, no. 3. Pp. 1225-1233. 2010.
- [9]. A. Al-Matrouk, M. Al-Hasan, H. Naqi, N. Al-Abkal, H. Mohammed, M. Haider and H. Bojbarah. "Snapshot of narcotic drugs and psychoactive substances in Kuwait: analysis of illicit drugs use in Kuwait from 2015 to 2018". *BMC public health*, vol. 21, no. 1, pp. 1-14. 2021.

- [10]. H. C. Lee, and E. M. Pagliaro. "Forensic evidence and crime scene investigation". *Journal of Forensic Investigation*, vol. 1, no. 2, pp. 1-5. 2013.
- [11]. Sherma, J., & Rabel, F. (2019). Thin layer chromatography in the analysis of cannabis and its components and synthetic cannabinoids. *Journal of Liquid Chromatography & Related Technologies*, 42(19-20), 613-628.
- [12]. Lee, H. Z. S., Ong, M. C., Lim, J. L. W., & Yap, T. W. A. (2017). Challenges in GC–MS analysis: Case studies on phenibut and ethylphenidate. *Forensic science international*, 277, 166-178.
- [13]. Dalby, O., Butler, D., & Birkett, J. W. (2010). Analysis of gunshot residue and associated materials—a review. *Journal of forensic sciences*, 55(4), 924-943.
- [14]. Staymates, J. L., Orandi, S., Staymates, M. E., & Gillen, G. (2014). Method for combined biometric and chemical analysis of human fingerprints. *International Journal for Ion Mobility Spectrometry*, 17(2), 69-72.
- [15]. I. A. Buryakov. "Detection of explosives by ion mobility spectrometry". *Journal of Analytical Chemistry*, vol. 66, no. 8, pp. 674-694. 2011.
- [16]. T. D. Schachel, A. Stork, R. Schulte-Ladbeck, T. Vielhaber and U. Karst. "Identification and differentiation of commercial and military explosives via high performance liquid chromatography–high resolution mass spectrometry (HPLC-HRMS), X-ray diffractometry (XRD) and X-ray fluorescence spectroscopy (XRF): Towards a forensic substance database on explosives". *Forensic science international*, vol. 8, 110-118. 2020
- [17]. D. Sumad-on. "The Methods of Extracting Trace Evidence in Criminal Investigation". Available at SSRN 3832502. 2021
- [18]. J. Robertson, and C. Roux. "From crime scene to laboratory. In *Forensic Examination of Fibres*". CRC Press. pp. 99-144. 2017.
- [19]. C. Gwinnett. "The Use of Trace Evidence in Missing Persons Investigations. In *Handbook of Missing Persons*". Springer, Cham. pp. 463-489. 2016
- [20]. J. Was-Gubala and R. Starczak. "Non-destructive identification of dye mixtures in polyester and cotton fibers using Raman spectroscopy and ultraviolet-visible (UV-Vis) microspectrophotometry". *Applied spectroscopy*, vol. 69, no. 2, pp. 296-303. 2015
- [21]. M. Gładysz, M. Król and P. Kościelniak. "Current analytical methodologies used for examination of lipsticks and its traces for forensic purposes". *Microchemical Journal*, 164, 106002. 2021.
- [22]. S. Ryland and E.M. Suzuki. "Analysis of paint evidence. *Forensic chemistry handbook*", 131-224. 2012.
- [23]. Janssens, K., Van der Snickt, G., Vanmeert, F., Legrand, S., Nuyts, G., Alfeld, M., ... & De Wael, K. (2017). "Non-invasive and non-destructive examination of artistic pigments, paints, and paintings by means of X-ray methods". *Analytical chemistry for cultural heritage*, 77-128.
- [24]. J. Almirall, and T. Trejos. "Interpol review of paint, tape, and glass evidence 2019–2022". *Forensic Science International: Synergy*, 6, 100306. 2023.

- [25]. T. H. Chen and S. P. Wu. "Forensic applications of direct analysis in real time (DART) coupled to Q-orbitrap tandem mass spectrometry for the in situ analysis of pigments from paint evidence". *Forensic Science International*, vol. 277, pp. 179-187. 2017.
- [26]. J. A. Siegel and K. Mirakovits. "Fibers, Paints and Other Polymers. In *Forensic Science*". CRC Press. pp. 557-583. 2021.
- [27]. P. K. Bose, P. K. and M. J. Kabir. "Fingerprint: a unique and reliable method for identification". *Journal of Enam Medical College*. Vol. 7, no. 1, pp. 29-34. 2017
- [28]. A. Makrushin, T. Kiertscher, M. Hildebrandt, J. Dittmann and C. Vielhauer. "Visibility enhancement and validation of segmented latent fingerprints in crime scene forensics". In *Media Watermarking, Security, and Forensics 2013*. Vol. 8665, pp. 61-72. 2013.
- [29]. C. Yuan, M. Li, M. Wang, and L. Zhang, L. "Cationic dye-diatomite composites: novel dusting powders for developing latent fingerprints". *Dyes and Pigments*, vol. 153, pp. 18-25. 2018.
- [30]. A. Pandya and R. K. Shukla. "New perspective of nanotechnology: role in preventive forensic". *Egyptian Journal of Forensic Sciences*, vol 8, no. 1, pp. 1-11. 2018
- [31]. F. A. Orellana, C. G. Galvez, M.T. Roldán, and C. García-Ruiz. "Applications of laser-ablation-inductively-coupled plasma-mass spectrometry in chemical analysis of forensic evidence". *TrAC Trends in Analytical Chemistry*, vol.42, pp. 1-34. 2013.
- [32]. T. Trejos, R. Koons, S. Becker, T. Berman, J. Buscaglia, M. Duecking, and J. Almirall. "Cross-validation and evaluation of the performance of methods for the elemental analysis of forensic glass by μ -XRF, ICP-MS, and LA-ICP-MS". *Analytical and bioanalytical chemistry*, vol. 405, no. 16, pp. 5393-5409. 2013.
- [33]. D. F. Rendle. "Advances in chemistry applied to forensic science". *Chemical Society Reviews*, vol. 34, no. 12, pp. 1021-1030. 2005.
- [34]. B. Gruber, B. A. Weggler, R. Jaramillo, K. A. Murrell, P. K. Piotrowski and F. L. Dorman. "Comprehensive two-dimensional gas chromatography in forensic science: A critical review of recent trends". *TrAC Trends in Analytical Chemistry*. VOL. 105, PP. 292-301. 2018.
- [35]. L. Chu, S. Deng, R. Zhao, J. Deng, and X. Kang. Comparison of adsorption/desorption of volatile organic compounds (VOCs) on electrospun nanofibers with tenax TA for potential application in sampling. *PLoS One*, vol. 11, no. 10. 163-168. 2016
- [36]. V. K. Yadav, T. Das, A. Harshey, M.M. Yadav, K. Nigam and A. Srivastava. A Forensic Approach to Evaluate the Effect of Different Matrices and Extraction Solvents for the Identification of Diesel Residue in Simulated Arson by GC-MS. *Chromatographia*, vol. 84, no. 5, pp. 413-423. 2003.

Editorial Policy and Guidelines for Authors

IJECEI is an open access, peer reviewed quarterly Journal published by LGU. The Journal publishes original research articles and high quality review papers covering all aspects of crime investigation.

The following note set out some general editorial principles. All queries regarding publications should be addressed to editor at email IJECEI@lgu.edu.pk. The document must be in word format, other format like pdf or any other shall not be accepted.

The format of paper should be as follows:

- Title of the study (center aligned, font size 14)
- Full name of author(s) (center aligned, font size 10)
- Name of Department
- Name of Institution
- Corresponding author email address.
- Abstract
- Keywords
- Introduction
- Literature Review
- Theoretical Model/Framework and Methodology
- Data analysis/Implementation/Simulation
- Results/ Discussion and Conclusion
- References.

Heading and sub-heading should be differentiated by numbering sequences like, 1. HEADING (Bold, Capitals) 1.1 Subheading (Italic, bold) etc. The article must be typed in Times New Roman with 12 font size 1.5 space, and should have margin 1 inches on the left and right. Length of paper should not be longer than 15 pages, including figures, tables, exhibits and bibliography. Table must have standard caption at the top while figures below with. Figure and table should be in continues numbering. Citation must be in according to the IEEE style.

LAHORE GARRISON UNIVERSITY

*L*ahore Garrison University has been established to achieve the goal of excellence and quality education in minimum possible time. Lahore Garrison University in the Punjab metropolis city of Lahore is an important milestone in the history of higher education in Pakistan. In order to meet the global challenges, it is necessary to touch the highest literacy rates while producing skillful and productive graduates in all fields of knowledge.

VISION

*O*ur vision is to prepare a generation that can take the lead and put this nation on the path to progress and prosperity through applying their knowledge, skills and dedication. We are committed to help individuals and organizations in discovering their God-gifted potentials to achieve ultimate success actualizing the highest standards of efficiency, effectiveness, excellence, equity, trusteeship and sustainable development of global human society.

MISSION

*A*t present, LGU is running Undergraduate, Graduate, Masters, M.Phil. and Ph.D. programs in various disciplines. Our mission is to serve the society by equipping the upcoming generations with valuable knowledge and latest professional skills through education and research. We also aim to evolve new realities and foresight by unfolding new possibilities. We intend to promote the ethical, cultural and human values in our participants to make them educated and civilized members of society.

Contact: For all inquiries, regarding call for papers, submission of research articles and correspondence, kindly contact at this address:

Sector C, DHA Phase-VI Lahore, Pakistan

Phone: +92- 042-37181823

Email: ijeci@lgu.edu.pk

