A ES
ISSN: 2096-3246
Volume 54, Issue 02, December, 2022
Special Issue

SIGNIFICANCE OF FORENSIC SCIENCE IN DAILY LIFE

Bhoopesh Kumar Sharma
SGT University, Gurugram, Haryana, India

Megha Walia
SGT University, Gurugram, Haryana, India

Deepika Dhillon
SGT University, Gurugram, Haryana, India

Vikas Rana
SGT University, Gurugram, Haryana, India

Amrita Yadav
Babu Banarasi Das University, Lucknow (U.P.), India

Abstract:
The use of scientific principles in relation to law for the benefit of justice is known as forensic science. Every time we use science to address a legal issue, we are engaging in forensic science. When a crime is being investigated, forensic science and forensic experts serve three main purposes i.e., Has a crime been committed? – To establish the Corpus Delicti, How and when was the crime committed? –To establish the Modus Operandi, and Who committed the crime? – To identify the Criminal. Forensic science is everywhere in our life, it may go unnoticed, but, since the beginning of our day till the end of it, we experience it in several ways. For instance: It begins from your driving car (keyless Car Entry), when you park your car/Toll Gates (License Plate Recognition, RFID Cards, Toll Tags, etc.), at login of your attendance in office or school (Biometrics), within your office/market/other places, within in your Mobile Phones as various security features, your ATM card PIN numbers/passwords/login id's etc. This chapter provides information on the use of forensic science and its practical applications in daily life of an individual.
Keywords: Forensic Science, Applications of Forensic Science, Mobile phone security, Forensic in daily life.

1. Introduction:

The use of scientific principles in relation to LAW for the benefit of justice is known as forensic science (Carracedo, 2007). Every time we use science to address a legal issue, we are engaging in forensic science. Say you came across a red stain on the carpet. Your initial thought is probably "Oh, is that blood?" Now, a variety of scientific techniques are needed to respond to this question:

- Whether it is Blood or Not?

- If it is blood, then whether an Animal blood or Human blood?
- If animal, then which species or which animal?
- If human, then what is the blood group, male or female, DNA identification etc.

In the aforementioned example, we need a little bit of biology like species origin test, antigen-antibody response, and DNA profiling, a little bit of chemistry to determine whether it is blood or not through certain chemical tests, and occasionally a little bit of physics to identify the source and impact force applied using specific tool or weapon.
The Latin term "Forum"—which refers to the group of people involved in the legal system is the root of the English word "Forensic." These individuals include detectives, forensic scientists, lawyers, judges, and police investigators (Pearson, 1983). None of their work is restricted to a single case or field; rather, they are all expected to offer sufficient results and judgments in a variety of situations.

1.1. Basic Principles of Forensic Science (Inman & Rudin, 2000):

In forensic science, certain principles are applied, including:

- Law of Individuality: Also referred to as the “Principle of Uniqueness”. This law asserts that nothing in the universe can ever be exactly like. No two persons can claim to have the same fingerprints, thus if one is found at the crime scene, it can only be matched to its real source, which is the same person and same finger.

- Law of Exchange: Also referred to as “Locard's Principle of Exchange”. This rule states that every contact leaves a trace. There is a mutual exchange of matter between two things whenever they come into contact with each other. As an illustration, if you touch a dusty table, you will leave your fingerprints on it and receive dust from the table in exchange. At the crime scene, the evidence is found in similar manner.

- Law of Progressive Change: Everything in the world is dynamic and undergoes gradual change through time. This law has a significant effect on forensic science since numerous pieces of information will be lost if the evidence is retained in place at the crime scene or left unattended for an extended period of time. There's a chance that some of the data won't be recognizable at all.

- Law of Probability: It states that an event could occur in multiple ways. The detectives may have a theory in mind as they approach the crime site that explains what transpired. However, in accordance with the law of probability, there might have been further events that led to the evidence in this specific manner. As a result, testing several hypotheses is advised.

- Law of Comparison: The comparison principle states that only like things can be compared. Meaning that the things that are similar in class and individual characteristics should be compared to one another. For example, a fingerprint should be compared with fingerprint impression, writing should be with writing, and so on. However, we can infer similar things from dissimilar evidence.

For instance, to compare DNA from various sources, blood from the crime scene can be used to extract DNA.

- Law of Analysis: Law of analysis states that only properly gathered and packed evidence may be accurately analyzed. Analysis and results of an evidence depends upon several factors like condition in which it is encountered, environmental situations, state of matter, quantity, quality, and sophistication of techniques used for analysis.

2. Functions of Forensic Science:

When a crime is being investigated, forensic science and forensic experts serve three main purposes (Risinger, 2017):

1. Has a crime been committed? – To establish the Corpus Delicti
2. How and when was the crime committed? –To establish the Modus Operandi
3. Who committed the crime? – To identify the Criminal

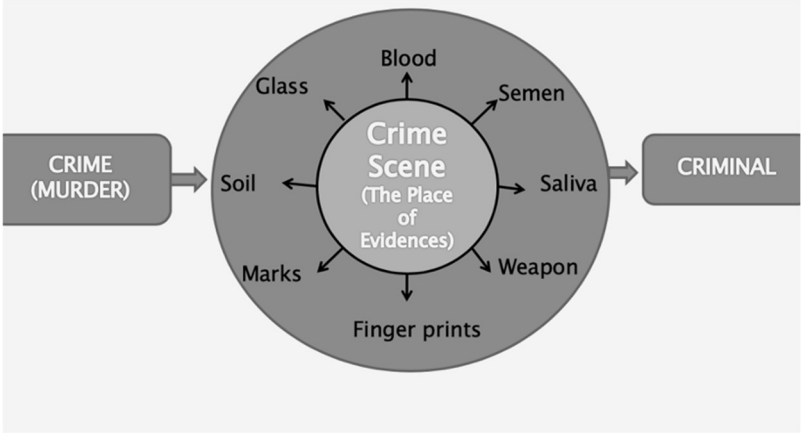

Figure 1: Showing how the evidence encountered at the scene of crime can be linked to crime and the criminal.

To determine if a crime scene is real or phony, undamaged or staged, forensic scientists or other professionals must first analyze the evidence and the crime scene. Many times, an incident that appears to be a homicide is actually a suicide, and vice versa (Tilley & Ford 1996). It must be determined whether the crime scene the investigator is working with is real or phony because it could also be constructed by criminals or witnesses to mislead the investigators (Ludwig & Fraser 2014).

Next, how was the crime committed? What did the mode of operation mean? or a criminal act. One can make a strong case for this truth by considering the sequence of events and the available data. In forensic identification, modus operandi is helpful in a variety of ways (Ribaux, Walsh & Margot, 2006).

Identification of the criminal is the third step. This involves looking over the evidence found at the crime scene, analyzing it, and comparing it to the samples taken from the suspects. There are several instruments and strategies that must be used in this lengthy process (Ainsworth, 2011).

There are several branches of forensic science including Fingerprinting, DNA Profiling, Forensic

Ballistics, Forensic Toxicology, Forensic Biology, Forensic Chemistry, Forensic Physics, Cyber Forensics, etc., they all deal with the identification, and analysis, of the evidence encountered at the scene of crime and their comparison with the control samples.

3. Forensic Science in Daily Life:

Forensic science is everywhere in our life, it may go unnoticed, but in reality, since the beginning of our day till the end of it, we experience it in several ways. For instance: It begins from your driving car (keyless Car Entry), when you park your car/Toll Gates (License Plate Recognition, RFID Cards, Toll Tags, etc.), at login of your attendance in office or school (Biometrics), within your office/market/other places, within in your Mobile Phones as various security features, your ATM card PIN numbers/passwords/login id's, while buying vegetables/meat/groceries we can tell the freshness of it either by viewing it or smelling it or by reading the manufacturing and the expiry dates. Also, when we suspect that someone has entered our living room from the misarranged articles (O'Hara & O'Hara, 2003).
If, as a general population, we will observe our daily activities, we will find that we all are investigators in one way or the other. For example:

a. What should we do if we receive a questionable email, message, note, or letter? Most likely, we start by looking at the envelope, including its origin, stamp, writing, type of paper, and who gave it to us. Even if it can be challenging to read emails, analyse email addresses, retrieve information, and other things, we nevertheless do our best.

b. When we discover a dent or scratch on our car, our first thought is to try to identify where it came from? We may have encountered a little or severe mishap, or it may be suspicious. In this instance, we once more do our utmost to pinpoint the origin and type of scratch. Sometimes, we could play detective to keep an eye on the one who is torturing you. Are we not?

c. What would we think if our partner arrived home from work early or late? For the majority of us, that occurs. Regardless of whether it is entirely psychological—which depends on our nature—it could also have a sinister undertone. Then, we start our inquiry by examining the time, mobile, phone logs, talk times, messages, getting in touch with friends and coworkers, among other things. So, in a sense, we are applying our investigative thinking to this situation.

d. All of a sudden, we get a message stating you've won $100,000. The majority of us have experienced the recent situation where we unexpectedly receive a message or email revealing the prize amount. Yes, we might fall victim to "Cyber Crime" or "Phishing," however many of us are too attentive and choose to disregard these warnings, while others react to them and fall victim.

e. If we learn that our credit card has been used to make a certain amount of purchases, we immediately notify the banks to block our credit card, which is a proactive forensics step, and we start an independent inquiry as well. Depending on which retailer or ATM sent the notice, our account may have been compromised.

f. Verifying the drug expiration dates - As of right now, we are all aware that every food item and every pharmaceutical is required by the FDA or FSSAI to have an expiration date related to the date of manufacture. We frequently encounter situations where products that have an expiration date are being sold, or when the manufacturing date and the expiration date are different (see the figure for reference). As investigators, we must be more cautious in these circumstances and know where to file complaints and what to do next.

Below are some examples, which shows the use of forensic science in our day-to-day activities:

3.1 Remote keyless system in cars:

A lock that employs an electronic remote control as a key that is activated by a portable device or automatically by proximity is referred to as a remote keyless system (RKS), also known as a keyless entry or remote central locking. The most typical method of achieving keyless entry into a car is by sending a radio frequency signal from a distant transmitter to a control module or receiver in the vehicle as shown in fig.2. This radio frequency signal is transmitted as an encrypted data stream directly to the vehicle. The transmitter is a tiny silver can that is roughly the size of a split pea, and a tiny chip that generates the code that is transmitted. A hopping code or rolling code is used by the controller chip in every modern controller to offer security. The current 40-bit code is stored in a memory location on the transmitter's controller chip. Our key fob delivers the 40-bit code when you press a button, along with a function code that instructs the vehicle what you want it to do (lock the doors, unlock the doors, open the trunk, etc.).

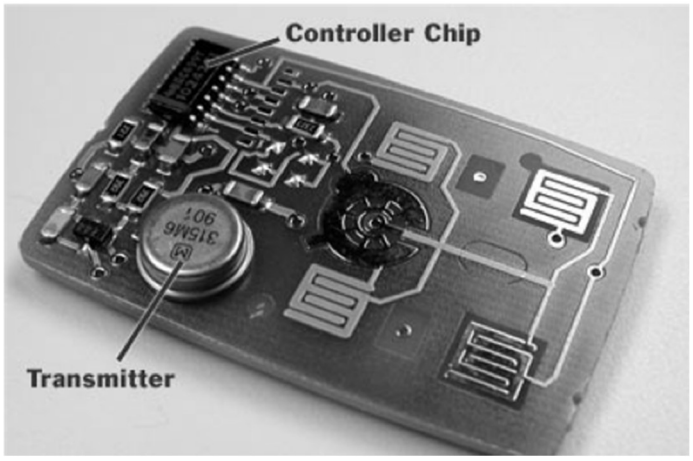

Figure 2: Showing the integrated circuit diagram of a keyless entry system

The 40-bit code is kept in a memory location on the receiver's controller chip as well. The receiver executes the requested function if it receives the 40-bit code it anticipates. If not, it has no effect. The same pseudo-random number generator is utilised by both the transmitter and the receiver. The transmitter chooses a new code each time it delivers a 40-bit code, which it then saves in memory using a pseudo-random number generator. On the other hand, the receiver chooses a fresh one using the same pseudo-random number generator after receiving a valid code. The transmitter and receiver

are synced in this manner (fig.3). If the receiver receives the expected code, it will only unlock the door (MuraliKrishna & Mallikarjuna Reddy, 2012).

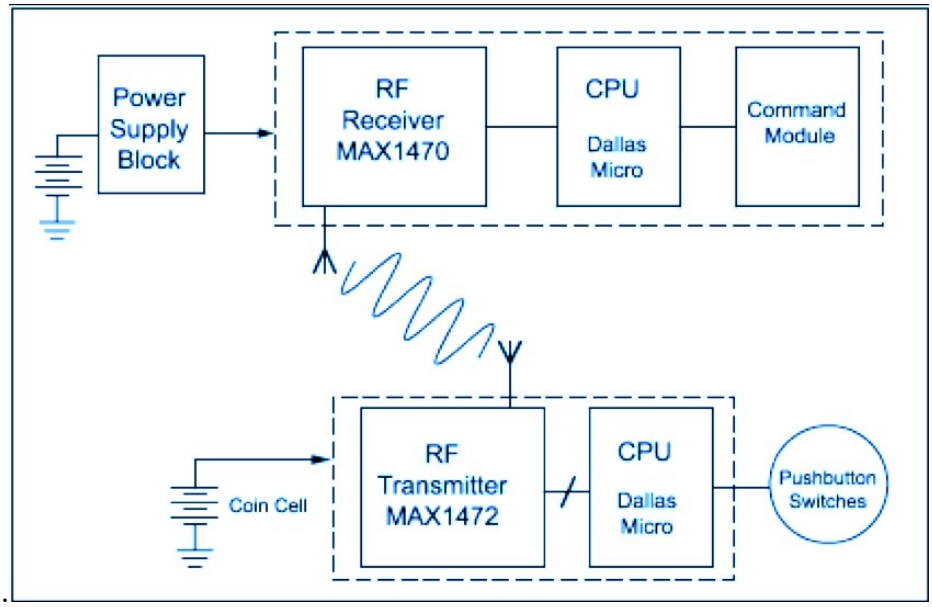

Figure 3: Showing the functioning of remote keyless car entry system.

Here, a question may arise that whether someone can breach the keyless entry system? And the answer to this is 'Yes'. It's relatively simple for thieves to steal a vehicle using relay theft, commonly referred to as keyless theft. Perpetrators usually buy a relay transmitter and an amplifier for this act. Such technological gadgets can be bought from the shabbier parts of the internet (Van de Beek & Leferink, 2016). In order to steal a car, a person must first recognize a house with a fine car parked outside. Then, using special equipment, they must determine whether the car has keyless entry and exit. The second burglar waves his amplifier around the outside of the home as the first one waits by the car with his transmitter. If the car key is close enough, the amplifier picks up the signal from it, amplifies it, and sends it to the accomplice's transmitter. The transmitter then effectively serves as the key, deceiving the vehicle into believing the genuine key is nearby, allowing the thieves to unlock the vehicle, enter, and drive away. The complete procedure might only take 60 seconds.

3.2. Biometric Technologies:

There are several biometric technologies we use in our daily life ranging from Biometric Fingerprints, Hand/Finger geometry, Voiceprint, Digital Signature Devices, Facial Recognition, Iris Recognition, Retina Scans, and others. Utilizing a system like this involves two distinct steps (Molenberghs, 2005). We must first go through a procedure called enrollment through which the system gathers information on all of the users it will need to identify every day. Each person's fingerprints are scanned, examined, and then saved in a coded form on a safe database after enrollment. Once enrollment is complete, which is the second phase, or verification, the system is prepared for usage. Anyone who wants to enter must place their finger on a scanner. The scanner takes their fingerprint and determines whether or not they are authorised to access the database by

comparing it to all of the prints that were registered during enrolment. Up to 40,000 prints per second can be verified and matched by sophisticated fingerprint technologies! During registration or authentication, when the lines in your fingerprint finish or split into two, each print is examined for highly specific characteristics, known as minutiae (Woodward, Orlans & Higgins, 2003). The device computes the angles and distances between these features, then applies a mathematical method (algorithm) to convert this information into a particular numerical code as demonstrated in fig. 4.

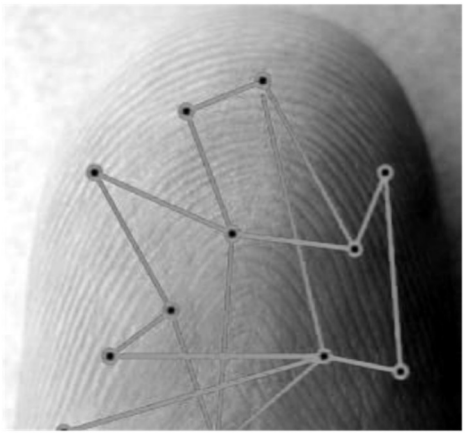

Figure 4: Showing the functioning and minutiae pattern generation in a biometric fingerprint device.

3.3. CCTV (Closed Circuit Television):

CCTV refers to the use of video cameras to convey a signal to a certain location and display it on a constrained number of displays. The signal is not openly broadcasted, unlike broadcast television, even though point-to-point (P2P), point-to-multipoint (P2MP), or mesh wireless networks may be used. Nowadays, CCTV cameras are present almost everywhere, including on the road traffic system. Do you not consider it to be forensics? Yes, without a doubt, it is a component of proactive forensics, in which our readiness is used to pinpoint the offender and the crime (Courtney, 2011). A CCTV system would be ideal for enhancing the security of your commercial space and providing constant monitoring of important areas. This would be especially helpful for large facilities or those that house expensive equipment, goods, or data. A CCTV system can be used to monitor activities on the premises both during and outside of business hours, but it can also be used to identify wanted criminals and discourage possible attackers.

In order to transmit video and conduct video surveillance, wired security cameras need cables, however the signal can deteriorate once it is farther than 300 meters. To solve this issue, the proper networking connections, switches, and signal boosters should be used. One monitor in a security room can display images from multiple cameras that are attached to it. Since they have been around for so long, analogue cameras continue to be the most often used type of CCTV camera installed today. They are functionally simple and include on-site video storage.

Despite having significantly more capabilities than their analogue equivalents, IP (Internet protocol) cameras perform the same tasks. IP cameras offer more versatile options like remote zoom and repositioning along with better, higher resolution images. You can also choose to view the video on a web browser, which they also offer. This allows you to view it live from anywhere using a computer or smartphone and receive notifications for anything odd your cameras record, like movement within your business at 3 in the morning. The primary disadvantage of IP cameras is their increased cost.

CCTV cameras have a variety of applications, including monitoring activity both inside and outside of a building, for safety reasons, to prevent shoplifting, for industrial purposes, crime management, disaster management, medical monitoring, etc. (Stedmon, 2011).

3.4 Body Scanners:

When used for security screening, a full-body scanner can identify objects on a person's body without having to touch or remove clothing. Depending on the technology used, the operator might view a cartoonish portrayal of the subject with an indicator telling where any suspicious objects were found, or an alternate-wavelength image of the subject's nude body. The display is typically hidden from other passengers for privacy and security reasons, and in some situations, it may even be placed in a separate room where the operator cannot see the individual being screened (Elster, 2011). Millimeter Wave (MMW) body scanners and Backscatter body scanners are the two main types of body scanners that are now on the market. These two are crucial components of both proactive and reactive forensics.

3.5 Proactive and Reactive Forensics in Mobile Phones:

The word "mobile devices" refers to a broad range of devices, including wearables, PDAs, smartphones, tablets, and mobile phones (Induruwa, 2009). They all share the ability to hold a significant amount of user data as a common feature. The primary objective of mobile device security is to prevent unauthorized users from entering the corporate network. It is a portion of a comprehensive enterprise security strategy (Curran, Robinson, Peacocke & Cassidy, 2010). We daily encounter several cases where mobile data has been stolen, passwords have been compromised, online fraud took place through mobile devices and much more. Though we apply our level best to find out what has happened and how it has happened? And hence, we apply lot of forensics there.

Given that more than half of business PCs are now portable, network security must take into account all of the locations and usage that employees require of the corporate network. Malicious mobile apps, phishing scams, data leaks, malware, and insecure Wi-Fi networks are a few potential hazards to smartphones. Investment in enterprise solutions and a multi-layered strategy are necessary for mobile device security. Mobile device security has some essential components, but each firm must choose which ones work best for their network. As a precautionary measure we must try to secure our data through password protection and password policies, incorporating biometric features in our smart devices, avoiding public Wi-Fi, beware of malicious apps etc. (Gan, 2018).

Conclusion:

There are many other things which we apply as an investigator in our everyday life like analyzing gait pattern (walking style) of a person, using face recognition on our mobile phones, fingerprint scanners on mobile phones, unique identification codes, one-time passwords, and other parameters to avoid the fraudulent activity or data theft. Hence, forensic science is not only meant for investigators or forensic experts, but also, we can apply it to our daily routine life. If we go much deeper into Forensic Science, we can witness the cutting-edge technology and methods to solve any legal or even biological issues. For instance, Human microbiome aids in race differentiation and individualization of an unknown dead body encountered at the scene of crime and within the race it can differentiate between the pregnant women from non-pregnant women through urine analysis. Besides, metagenome is highly differentiable among Human mother's milk, mother's feces, and infant feces (Walia, et al., 2022). Hence, Forensic Science is all around, just what we need to see and realize is the investigator within as well as the science of criminal identification we are using daily in thousands of civil and criminal cases.

References:

Carracedo, A. (2007). Applications in forensic science. Forensic Science International, 169, S22-S23. doi: 10.1016/j.forsciint.2007.04.135

Pearson, E. (1983). Forensic Science Handbook. Forensic Science International, 21(1), 93-94. doi: 10.1016/0379-0738(83)90096-8

Inman, K., & Rudin, N. (2000). Principles and practice of criminalistics: the profession of forensic science. CRC Press.

Risinger, D. M. (2017). The five functions of forensic science and the validation issues they raise: a piece to incite discussion on validation. Seton Hall L. Rev., 48, 719.

Tilley, N., & Ford, A. (1996). Forensic science and crime investigation (No. 73). London: Home Office, Police Research Group.

Ludwig, A., & Fraser, J. (2014). Effective use of forensic science in volume crime investigations: Identifying recurring themes in the literature. Science & Justice, 54(1), 81-88.

Ribaux, O., Walsh, S., & Margot, P. (2006). The contribution of forensic science to crime analysis and investigation: Forensic intelligence. Forensic Science International, 156(2-3), 171-181. doi: 10.1016/j.forsciint.2004.12.028

Ainsworth, P. (2011). Offender profiling and crime analysis (pp. 33-44). New York: Routledge.

O'Hara, C., & O'Hara, G. (2003). Fundamentals of criminal investigation. Springfield, Ill.: C.C. Thomas.

MuraliKrishna, V., & Mallikarjuna Reddy, Y. (2012). A Novel Method for Identifying the Keyless Authentication Entry System using Mobile for Auto Mobiles (CAR). International Journal Of Computer Applications, 51(7), 6-12. doi: 10.5120/8052-1398

Van de Beek, S., & Leferink, F. (2016). Vulnerability of Remote Keyless-Entry Systems Against Pulsed Electromagnetic Interference and Possible Improvements. IEEE Transactions On Electromagnetic Compatibility, 58(4), 1259-1265. doi: 10.1109/temc.2016.2570303

Molenberghs, G. (2005). Biometry, Biometrics, Biostatistics, Bioinformatics, ... , Bio-X. Biometrics, 61(1), 1-9. doi: 10.1111/j.0006-341x.2005.040831.x

Woodward, J., Orlans, N., & Higgins, P. (2003). Biometrics. Emeryville, USA: McGraw-Hill Professional Publishing.

Courtney, M. (2011). Public eyes get smart [CCTV camera]. Engineering &Amp; Technology, 6(1), 38-41. doi: 10.1049/et.2011.0103

Stedmon, A. (2011). The camera never lies, or does it? The dangers of taking CCTV surveillance at face value. Surveillance &Amp; Society, 8(4), 527-534. doi: 10.24908/ss.v8i4.4192

Elster, A. (2011). Airport Full-Body Scanners. Yearbook Of Diagnostic Radiology, 2011, 173-176. doi: 10.1016/j.yrad.2010.12.007

Induruwa, A. (2009). Mobile phone forensics: an overview of technical and legal aspects. International Journal Of Electronic Security And Digital Forensics, 2(2), 169. doi: 10.1504/ijesdf.2009.024901

Curran, K., Robinson, A., Peacocke, S., & Cassidy, S. (2010). Mobile Phone Forensic Analysis. International Journal Of Digital Crime And Forensics, 2(3), 15-27. doi: 10.4018/jdcf.2010070102

Gan, S. (2018). The history and future of scientific phone apps and mobile devices. Scientific Phone Apps And Mobile Devices, 4(1). doi: 10.1186/s41070-018-0022-8

Walia, M., Sharma, B. K., & Verma, P. (2022). Application of human microbiome in forensic investigations. International Journal of Health Sciences, 6(S1), 7545–7551.