Volume 9, Issue 9, September – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP960

Mobile Forensics: Extracting Geo-Location Data from Photos on Android Smartphones

Eman Daraghmi
Palestine Technical University - Kadoorie
Tulakrem, Palestine

Ahmed Hamoudi
Palestine Technical University - Kadoorie
Tulkarem, Palestine

Abstract:- With the rapid advancement of technology and communication, smartphones have become ubiquitous, offering functionalities such as geo-location-based photo capturing through GPS and navigation applications. Digital forensic examiners can retrieve location data from Exchangeable Image File Format (EXIF) metadata embedded in photos, commonly referred to as "geolocation," which is crucial in criminal investigations. Modern Android smartphones and digital cameras store GPS coordinates in every captured photo, allowing forensic analysts to leverage this information to solve cases. This paper demonstrates the process of manually extracting geographical identification data (latitude, longitude, altitude) from raw image files using Hex editor tools and validating the results with Google Maps. These methods aid forensic investigators and law enforcement agencies by providing evidence that can be presented in court.

Keywords:- *Geo-Location, GPS, Android, EXIF Meta- Data, Mobile Forensics, Longitude-Latitude – Height*

I. INTRODUCTION

The ability to determine our precise location on Earth has fascinated humankind for centuries. Ancient Greeks were among the first to triangulate their geographical position using the stars over 2,000 years ago [1]. This early curiosity has evolved into modern geolocation technologies that now allow us to pinpoint locations with extraordinary accuracy. Geolocation, in its current form, refers to the process of determining the physical geographic location (latitude, longitude, and altitude) of a device, such as a computer or smartphone, using various technological systems. In this digital age, where mobile devices play a central role in communication, navigation, and information sharing, geolocation has become an integral part of daily life.

With the widespread use of smartphones, particularly Android devices, the implementation of geolocation technology has grown exponentially. Android, being the market leader with a global market share of 87.7%, is the operating system of choice for millions of users, followed by iOS, which holds 12.1% of the market [2].

Other mobile operating systems make up only a fraction of the total market share, standing at 0.2%. This dominance makes Android smartphones a critical platform for studying and implementing geolocation technologies, especially within the field of mobile forensics.

Modern Android smartphones and digital cameras (see Fig 1) have the capability to save GPS coordinates within the metadata of every photo taken. This metadata, embedded within the Exchangeable Image File Format (EXIF), includes critical information such as the device's location, date, and time when the photo was captured. Forensic investigators can analyze this data to trace the physical movements of individuals or objects, making it invaluable in criminal investigations. The process of identifying the geographical origin of an item through its properties is referred to as forensic geolocation [3], [4], [5].

EXIF, which was developed by the Japan Electronic Industries Development Association (JEIDA), is now an international standard supported by both the Tagged Image File Format (TIFF) and JPEG formats [6], [7], [8]. The EXIF metadata contains not only geotagging information but also various other technical details such as camera settings (ISO speed, focal length, shutter speed), date and time, image orientation, and copyright information. The inclusion of geographic information (Geo-Tags) such as latitude, longitude, and altitude within an image is what transforms a regular photo into a geotagged image.

A geotagged image is a powerful resource in digital forensics, as it contains geographical identification data that can be used to track the location of where the image was taken. While numerous mobile forensic tools are available to extract geotag data from photos, understanding the underlying mechanisms of these tools is essential for forensic analysts. The ability to manually extract geolocation data from images provides a deeper understanding of how these tools function, and in some cases, can prove crucial when automated tools fail to perform. This paper explores the manual extraction of geotag data from images on Android smartphones by examining the byte-level information stored in the EXIF metadata using Hex editor tools.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP960

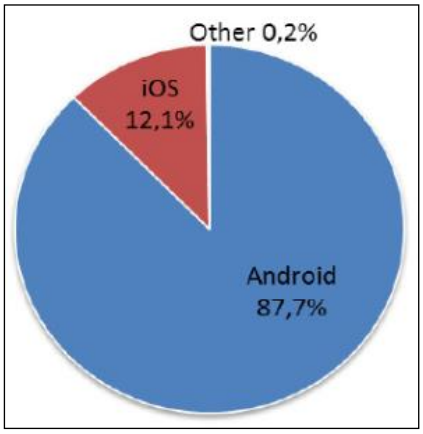


Fig. 1.Market Share of Mobile Operating Systems Globally

Android, being an open-source, Linux-based operating system, was developed by the Open Handset Alliance, led by Google. The first version of the Android code was released by Google in 2007, with the commercial version (Android 1.0) being launched in September 2008 [8], [9], [10], [11], [12], [13]. Since then, Android has rapidly evolved, with each version incorporating more advanced features, including those related to geolocation services. Its widespread adoption and versatility make it the ideal platform for implementing geolocation tracking systems.

Mobile forensics is the science of recovering digital evidence from mobile devices such as smartphones and tablets. This field has grown in significance due to the extensive use of mobile devices in communication and daily activities. Mobile forensics focuses on the extraction, preservation, and analysis of digital evidence from these devices, making it a crucial tool in criminal investigations.

In this paper, we focus on the manual parsing of image files to recover geolocation data when automated recovery methods fail or are unavailable. By using an Android smartphone, we demonstrate how to manually analyze raw image data to extract latitude, longitude, and altitude information. This manual approach highlights the importance of understanding the underlying structure of image files and provides a valuable skill set for forensic investigators when dealing with incomplete or corrupted data.

II. BACKGROUND

A. History of Global Navigation Satellite Systems (GNSS)

Global Navigation Satellite Systems (GNSS) refer to satellite constellations that transmit signals, allowing receivers virtually anywhere on Earth to determine their location. These systems have become integral to many aspects of modern life, including mobile device navigation, transportation, and even agriculture. GNSS has evolved over the decades, with the most notable systems being the Global Positioning System (GPS), developed by the United States Department of Defense, and the Global Orbiting Navigation System (GLONASS), operated by the Russian Federation. Both systems were fully operational by the mid-1990s. Other GNSS systems, such as Galileo (developed by the European Union) and BeiDou (developed by China), are in various stages of development and operation. These systems provide precise position coordinates, including longitude, latitude, and altitude, which are used in numerous applications, including mobile forensics (see Fig 2).

The history of positioning systems can be traced back over millennia, with early civilizations using celestial navigation techniques. The development of modern satellite-based navigation began in the mid-20th century. Key milestones include :

- **2,000+ years ago:** Ancient Greeks triangulated their geographical location using stars [1[14], [15], [16], [17], [18], [19], [20].
- **1933:** Radar was first used to detect aircraft and ships by the U.S. Navy [10].
- **1957:** The Soviet Union launched the first artificial satellite, Sputnik I, into space [12].
- **1973:** The GPS Navstar system was proposed by the Pentagon [13].
- **1978:** The first Navstar GPS satellites were launched into space by the U.S. [13].
- **1983:** President Ronald Reagan offered GPS technology to civilian aircraft for improved air navigation safety, though it was initially restricted [14].
- **1989:** Magellan introduced the first handheld navigation device, the NAV 1000 [15].
- **1995:** The GPS system achieved full operational status [16].
- **1999:** The Benefon Esc! became the first mobile phone to integrate GPS, primarily marketed in Europe [14].
- **2000:** President Bill Clinton authorized the removal of GPS restrictions for civilian use, vastly improving accuracy [17].
- **2005:** The first European experimental GPS satellite, GIOVE-A, was launched, marking the beginning of the Galileo system [18].
- **2005:** Google Maps made its debut, revolutionizing access to digital maps [19].
- **2015:** Facebook began integrating location-based data from geodata platforms, enhancing its location services [20].

These advancements have set the foundation for modern geolocation services, which are now commonplace in smartphones and digital cameras, allowing the seamless capture of GPS data along with photographs.

B. Mobile Forensics

Mobile forensics is a critical field within digital forensics that focuses on recovering digital evidence from mobile devices. As smartphones have become central to personal and professional life, their increasing storage and computational capabilities present both opportunities and challenges for forensic investigators. The wealth of data stored on mobile devices—such as call logs, SMS messages, application data, GPS data, and locally stored files—can be instrumental in criminal investigations [21], [22], [23].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP960

Forensic investigators use specialized mobile forensic tools to extract and analyze data from smartphones. These tools can uncover various types of digital evidence, including metadata from photos that contain geolocation information, which is crucial for tracking the physical movements of suspects or victims. Table I lists some of the most commonly used mobile forensic tools in investigations.

The combination of mobile forensics and GNSS data allows forensic experts to map the locations of mobile device users over time, providing invaluable insights in legal cases, from locating missing persons to unraveling the movements of criminal suspects.

C. Related Work

Several research efforts have focused on the extraction and analysis of geolocation data for forensic purposes [24], [25], [26], [27], [28], [29], [30], [31], [32], [33]. In 2013, Stefan Sack, Knut Kröger, and Reiner Creutzburg conducted research on location tracking forensics using mobile devices. They explored three different procedures for extracting positional data from various devices and analyzed how these methods could be applied to different classes of devices. Another significant study, conducted in 2008 by Hsiang-Cheh, Yueh-Hong, and Shin-Chang, examined how EXIF data can be used as a binary watermark in images, further contributing to the understanding of geotagging in digital forensics [22].

A more recent study by Dr. Hamdi in 2016 focused on the forensic analysis of multimedia file signatures in smartphones. His research aimed to determine whether multimedia files, such as images and videos, were created locally on the smartphone or modified externally. The study also explored the detection of alterations made to these files, further enhancing forensic investigation techniques [23].

This growing body of work demonstrates the critical role of geolocation data and mobile forensics in contemporary digital investigations. By understanding the tools and techniques available, forensic analysts can more effectively recover and analyze evidence from mobile devices, supporting their investigative efforts.

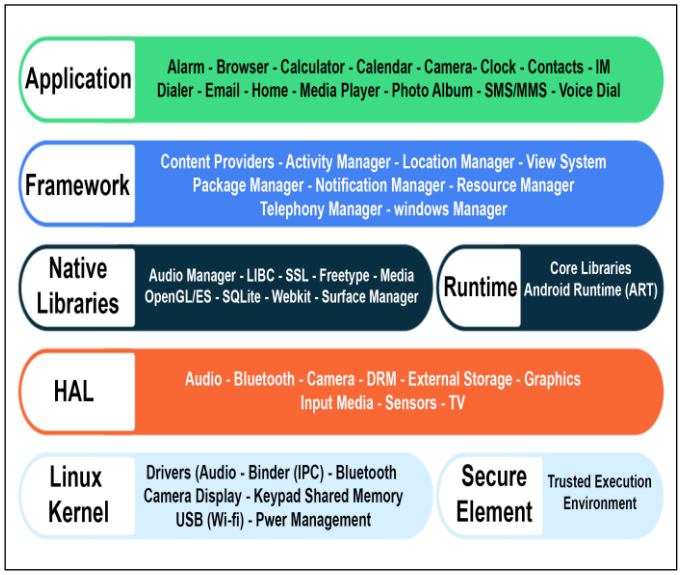


Fig. 2. Android System Architecture System [6]

Table 1: List of Mobile Forensic Tools

Mobile Forensics Tools
• FINALMobile Forensics4 • Cellebrite • Encase Forensics • Oxygen Forensic Suite • MailXaminer • MOBILedit! • Elcomsoft iOS Forensic Toolkit • Android Data Extractor Lite (ADEL) • WhatsApp Xtract • Skype Xtractor

III. METHODOLOGY AND CASE STUDY SETUP

This section outlines the methodology used to manually extract geographical identification data (latitude, longitude, and altitude) from an image using the HxD Hex Editor tool. The process involves capturing a geotagged image with an Android smartphone, transferring it to a workstation, and then manually parsing the image's EXIF metadata for location data.

A. Research Tools

The following tools were used in this experiment:

➢ *Mi 9T Pro Smartphone*

- Model: M1903F11G
- Android version: 10 (QKQ1.190825.002)
- MIUI version: Global 12.0.3 Stable
- Kernel version: 4.14.117-perf-g7428a5b

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP960

➢ *Original Type-C Cable for Xiaomi Mi 9T Pro*
- Used for fast charging and data transfer between the mobile device and the investigation workstation.

➢ *Workstation*
- Asus Computer (i7, 6th generation)
- Operating System: Windows 10 Pro

➢ *HxD Hex Editor*
- Version: 2.4.0.0 (Mh-nexus, 2020)

➢ *The Hex Editor was used to manually analyze the image's hexadecimal content for geotagging information embedded within the EXIF metadata.*

B. Research Data Setup

➢ *Enabling Geolocation Services*

For the purpose of this experiment, the geolocation (GPS) service on the Mi 9T Pro smartphone was enabled. This ensures that any image captured using the camera app would be tagged with geolocation metadata, including latitude, longitude, and altitude.

➢ *Image Capture*

After enabling the geolocation service, an image was captured using the Mi 9T Pro's native camera application. This image was automatically tagged with geolocation data as part of the EXIF metadata embedded in the file.

➢ *Data Transfer*

The captured image was transferred from the Mi 9T Pro smartphone to the workstation via th …….e original Type-C cable. The cable ensured fast and secure data transfer, necessary for preserving the integrity of the image file and its metadata.

➢ *Hexadecimal Analysis*

Once the image was successfully transferred to the workstation, the HxD Hex Editor tool was used to open the image file. By examining the hexadecimal representation of the image, we manually extracted the geotagging information. This involves identifying specific patterns within the EXIF metadata that correspond to geographical data such as latitude, longitude, and altitude, as outlined in the **Data Analysis and Findings** section.

Fig 4 illustrates a hexadecimal view of the image file as displayed by the HxD Hex Editor.

IV. DATA ANALYSIS AND FINDINGS

To verify the geolocation data embedded in an image on a Windows operating system, a simple method is to right-click on the image, choose "Properties," and navigate to the "Details" tab, where the EXIF metadata, including geotagging information, can be viewed (as shown in Fig 3).

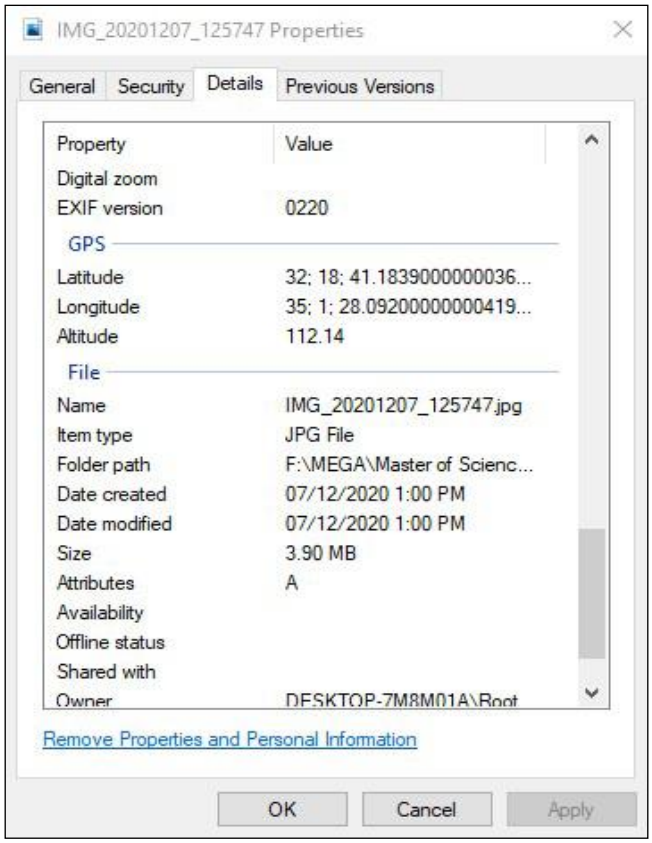
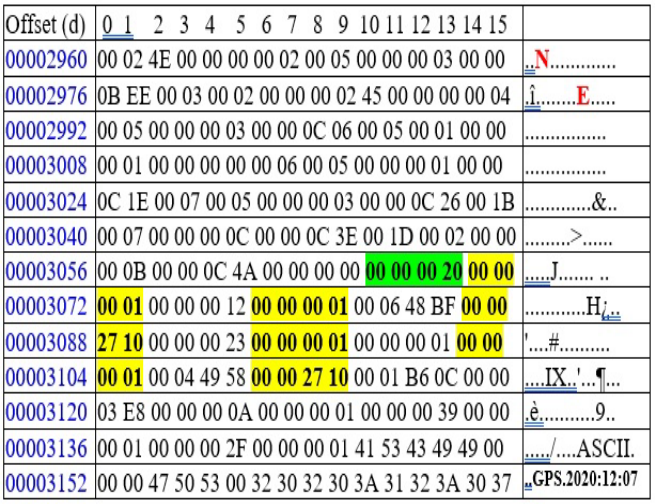


Fig. 3. Image Properties in Windows OS

Alternatively, several tools can extract geotag and other relevant information from images, such as ExifTool GUI, Metadata++, or various free online services [24]. For this study, we opted to manually extract the geolocation data embedded in an image using the HxD Hex Editor tool. The manual extraction process ensures a deeper understanding of the underlying structure of EXIF metadata and helps in cases where automated tools might fail.

To achieve this, the following steps were followed:
- Capture a geo-tagged image using a Mi 9T smartphone.
- Use the HxD Hex Editor tool to examine the image and locate direction letters (N, S, E, W).
- Identify the patterns in the hexadecimal values, such as "0x00 00 00 01" and "0x00 00 27 10."
- Perform calculations on the extracted values to convert them into meaningful geographic coordinates.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP960



Offset (d)	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	
00002960	00 02 4E 00 00 00 00 02 00 05 00 00 00 03 00 00	..N.....
00002976	0B EE 00 03 00 02 00 00 00 02 45 00 00 00 00 04	.î.....E.....
00002992	00 05 00 00 00 03 00 00 0C 06 00 05 00 01 00 00	.....
00003008	00 01 00 00 00 00 00 06 00 05 00 00 00 01 00 00	.....
00003024	0C 1E 00 07 00 05 00 00 00 03 00 00 0C 26 00 1B	.....&..
00003040	00 07 00 00 00 0C 00 00 0C 3E 00 1D 00 02 00 00	.....>.....
00003056	00 0B 00 00 0C 4A 00 00 00 00 00 00 00 20 00 00	.....J..... ..
00003072	00 01 00 00 00 12 00 00 00 01 00 06 48 BF 00 00	.....H¿..
00003088	27 10 00 00 00 23 00 00 00 01 00 00 00 01 00 00	'....#.....
00003104	00 01 00 04 49 58 00 00 27 10 00 01 B6 0C 00 00	....IX..'...¶...
00003120	03 E8 00 00 00 0A 00 00 00 01 00 00 00 39 00 00	.è.....9..
00003136	00 01 00 00 00 2F 00 00 00 01 41 53 43 49 49 00	...../....ASCII.
00003152	00 00 47 50 53 00 32 30 32 30 3A 31 32 3A 30 37	..GPS.2020:12:07

Fig. 4.Hexadecimal View of an Image from Mi 9T Smartphone using the HxD Hex Editor Tool

00 00 00 01	00 00 00 12	00 00 00 01	00 06 48 BF
00 00 27 10	00 00 00 23	00 00 00 01	00 00 00 01
00 00 00 01	00 04 49 58	00 00 27 10	00 01 B6 0C
00 00 03 E8			

Fig. 5.Hexadecimal View Showing Specific Patterns in the EXIF Data

A. Finding Direction Letters (N, S, E, W)

The first step in manually extracting geolocation data involves opening the image file in the HxD Hex Editor. After the image is loaded, search for direction letters such as "N" (North), "S" (South), "E" (East), or "W" (West) within the hex code (as shown in Fig 4). These letters indicate the latitude and longitude orientation and will help guide further calculations.

B. Locating the Hexadecimal Pattern

The next step is to identify the specific hex pattern associated with the geotagged information. Search for the pattern "00 00 00 01 ... 00 00 00 27" and locate the values four bytes before the first occurrence of "00 00 00 01." In this case, the value is "00 00 00 20," and its corresponding offset is 3066–3069.

C. Identification and Calculations

➢ *Latitude Calculation:*

- **Converting Hexadecimal to Decimal:** The value "00 00 00 20" is converted from hexadecimal (base 16) to decimal (base 10). This gives:

$(0000\ 00\ 20)_{16} = (32)_{10}$

- **Next Bytes for Division:** The next four bytes are "00 00 00 01," which equals 1. The division is then performed as:

Value of degrees: 32 / 1 = 32

- **Minutes:** The next four bytes are "00 00 00 12" (offset: 3074–3077), which equals 18 in decimal, followed by "00 00 00 01." Thus, the value of minutes is:

Value of minutes: 18 / 1 = 18

- **Seconds:** The subsequent four bytes are "00 06 48 BF" (offset: 3082–3085), which equals 411,839 in decimal, followed by "00 00 27 10" (offset: 3086–3089), which equals 10,000 in decimal. Therefore, the value of seconds is:

Value of seconds: 411,839 / 10,000 = 41.1839

The latitude is then calculated as:

Latitude = 32° 18' 41.1839" N

➢ *Longitude Calculation:*

- **Degrees:** The four bytes following "00 00 27 10" are "00 00 00 23" (offset: 3090–3093), which equals 35 in decimal. Therefore:

Value of degrees: 35 / 1 = 35

- **Minutes:** The next four bytes are "00 00 00 01" (offset: 3098–3101), followed by a divisor of "00 00 00 01," giving:

Value of minutes: 1 / 1 = 1

- **Seconds:** The following four bytes are "00 04 49 58" (offset: 3106–3109), which equals 280,920 in decimal, followed by "00 00 27 10" (offset: 3110–3113), which equals 10,000 in decimal. Therefore:

Value of seconds: 280,920 / 10,000 = 28.092

The longitude is then calculated as:

Longitude = 35° 1' 28.092" E

➢ *Altitude Calculation:*

The four bytes after "00 00 00 27" are "00 01 B6 0C" (offset: 3114–3117), which equals 112,140 in decimal. The next four bytes are "00 00 03 E8" (offset: 3118–3121), which equals 1,000 in decimal. Therefore:

Altitude = 112,140 / 1,000 = 112.14 meters above sea level

Based on the extracted and calculated coordinates (Table II), the precise geographic location can be determined. These coordinates can then be entered into Google Maps for verification (as shown in Fig 6 and Fig 7).

Table 2. Coordinates Calculated in the Case Study

Latitude	Longitude	Altitude
32°18'41.1839" N	35°1'28.092" E	112.14 m

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP960

Fig. 6.Coordinates Entered into Google Maps

Fig. 7.Location Displayed on Google Maps

V. CONCLUSION AND FUTURE WORK

The analysis presented in this paper demonstrates that, in the absence of professional tools capable of automatically parsing geolocation data and extracting artifacts, manual extraction through hex analysis is a viable alternative. By carefully identifying and calculating key patterns in the EXIF metadata, we can retrieve essential geolocation information (latitude, longitude, and altitude) embedded within an image. This manual approach proves beneficial not only when dealing with fully intact images but also in scenarios where files are partially corrupted or recovered. In such cases, the patterns discussed in the Data Analysis and Findings section can guide investigators to extract partial geolocation data or confirm suspicions that the file in question is an image.

Additionally, this method can assist in rebuilding missing file headers or other essential metadata, allowing for further recovery of the image. The ability to manually parse and interpret image files enhances the investigator's toolkit, offering more flexibility and precision in scenarios where automated tools might fail or be unavailable.

Future research is needed to explore whether modern mobile forensic tools can extend their capabilities to handle partially recovered image files more effectively. Investigating how these tools can improve the automated extraction of geolocation data from fragmented or incomplete images would be an invaluable addition to the field. Moreover, research into optimizing manual methods for quicker analysis and more complex cases involving image modification would further enhance forensic practices.

ACKNOWLEDGMENT

The authors would like to thank Palestine Technical University – Kadoorie for their support.

REFERENCES

[1]. I. Amato, Pushing the Horizon: Seventy-Five Years of High Stakes Science and Technology at the Naval Research Laboratory. 2001. [Online]. Available: http://www.nrl.navy.mil/content%7B%5C%7Dimages/horizon.pdf
[2]. K. Curran, A. Robinson, S. Peacocke, and S. Cassidy, "Mobile phone forensic analysis," Int. J. Digit. Crime Forensics, vol. 2, no. 3, pp. 15–27, 2010, doi: 10.4018/jdcf.2010070102.
[3]. J. Fan, "Image forensics on exchangeable image file format header." [Online]. Available: https://doi.org/10.32657%2F10356%2F61970
[4]. Geopointe.com, "The History of Geolocation: Modern Technology Born from Ancient Human Interest." [Online]. Available: https://www.geopointe.com/2017/07/11/geolocation-history/
[5]. N. S. Grantham et al., "Global forensic geolocation with deep neural networks," J. R. Stat. Soc. Ser. C Appl. Stat., vol. 69, no. 4, pp. 909–929, 2020, doi: 10.1111/rssc.12427.
[6]. M. S. Grewal, "Global navigation satellite systems," Wiley Interdiscip. Rev. Comput. Stat., vol. 3, no. 4, pp. 383–384, 2011, doi: 10.1002/wics.158.
[7]. D. Hamdi, F. Iqbal, T. Baker, and B. Shah, "Multimedia File Signature Analysis for Smartphone Forensics," in Proceedings of the 9th International Conference on Developments in eSystems Engineering (DeSE), 2016, pp. 130–137. doi: 10.1109/DeSE.2016.22.
[8]. H.-C. Huang, Y.-H. Chen, and S.-C. Chen, "Copyright protection for images with EXIF metadata," in 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, 2008, pp. 239–242.
[9]. D. A. M. Maradin, "The Market Structure of the Smartphone Operating Systems Industry in the EU." [Online]. Available: https://www.researchgate.net/publication/343362173_The_Market_Structure_of_the_Smartphone_Operating_Systems_Industry_in_the_EU

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP960

[10]. N. Rahimi, J. Nolen, and B. Gupta, "Android Security and Its Rooting—A Possible Improvement of Its Security Architecture," J. Inf. Secur., vol. 10, no. 02, pp. 91–102, 2019, doi: 10.4236/jis.2019.102005.
[11]. S. Sack, K. Kröger, and R. Creutzburg, "Location tracking forensics on mobile devices," in Multimedia Content and Mobile Devices, 2013, p. 866712. doi: 10.1117/12.2003952.
[12]. W. Sturdevant, "NAVSTAR, the Global Positioning System: A Sampling of Its Military, Civil, and Commercial Impact," Hist. Backgr., vol. 5, no. September, pp. 32–45, 1994.
[13]. "Google Maps' biggest moments." [Online]. Available: https://blog.google/products/maps/look-back-15-years-mapping-world/
[14]. "Naval Radar Systems." [Online]. Available: https://www.nrl.navy.mil/accomplishments/systems/naval-radar-systems/
[15]. "SOS in Computer Science and Applications Jiwaji University (II) Advantages, features, API levels."
[16]. "Sputnik." [Online]. Available: https://history.nasa.gov/sputnik.html
[17]. "What is Galileo?" [Online]. Available: http://www.esa.int/Applications/Navigation/Galileo/What_is_Galileo
[18]. "Celebrating 10 years of GPS for the masses." [Online]. Available: https://www.cnet.com/tech/mobile/celebrating-10-years-of-gps-for-the-masses/
[19]. "A brief history of GPS." [Online]. Available: https://www.pcworld.com/article/2000276/a-brief-history-of-gps.html
[20]. "Magellan NAV 1000 GPS Receiver, 1988." [Online]. Available: https://timeandnavigation.si.edu/multimedia-asset/magellan-nav-1000-gps-receiver-1988
[21]. "Facebook And Factual Expand Global Geo-Data Alliance." [Online]. Available: https://geomarketing.com/facebook-and-factual-expand-global-geo-data-alliance
[22]. "Navstar: GPS Satellite Network." [Online]. Available: https://www.space.com/19794-navstar.html
[23]. "Best Exif viewers and editors." [Online]. Available: https://www.techgenyz.com/2020/02/25/best-exif-viewers-to-scan-photo-details/
[24]. Z. Alsaed et al., "Role of Blockchain Technology in Combating COVID-19 Crisis," Appl. Sci., vol. 11, no. 24, p. 12063, Dec. 2021, doi: 10.3390/app112412063.
[25]. E. Daraghmi, "Augmented Reality Based Mobile App for a University Campus," 2017, doi: 10.13140/RG.2.2.36356.24962.
[26]. E. Daraghmi, Z. Qaroush, M. Hamdi, and O. Cheikhrouhou, "Forensic Operations for Recognizing SQLite Content (FORC): An Automated Forensic Tool for Efficient SQLite Evidence Extraction on Android Devices," Appl. Sci., vol. 13, no. 19, p. 10736, Sep. 2023, doi: 10.3390/app131910736.
[27]. E. Y. Daraghmi, C. H. Hsiao, and S. M. Yuan, "A New Cloud Storage Support and Facebook Enabled Moodle Module," in 2014 7th International Conference on Ubi-Media Computing and Workshops, Ulaanbaatar, Mongolia: IEEE, Jul. 2014, pp. 78–83. doi: 10.1109/u-media.2014.12.
[28]. E. Y. Daraghmi, C.-F. Lin, and S. M. Yuan, "Mobile Phone Enabled Barcode Recognition for Preferences Monitoring," in Advances in Computer Science and Education Applications, vol. 202, M. Zhou and H. Tan, Eds., in Communications in Computer and Information Science, vol. 202. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 297–302. doi: 10.1007/978-3-642-22456-0_43.
[29]. E. Y. Daraghmi and Y. S. Ming, "Using graph theory to re-verify the small world theory in an online social network word," in Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services, Bali Indonesia: ACM, Dec. 2012, pp. 407–410. doi: 10.1145/2428736.2428811.
[30]. E. Daraghmi, C.-P. Zhang, and S.-M. Yuan, "Enhancing Saga Pattern for Distributed Transactions within a Microservices Architecture," Appl. Sci., vol. 12, no. 12, p. 6242, Jun. 2022, doi: 10.3390/app12126242.
[31]. E.-Y. Daraghmi, M.-C. Wu, and S.-M. Yuan, "A Multilayer Data Processing and Aggregating Fog-Based Framework for Latency-Sensitive IoT Services," Appl. Sci., vol. 11, no. 4, p. 1374, Feb. 2021, doi: 10.3390/app11041374.
[32]. E.-Y. Daraghmi and A. Hamoudi, "THE DEVELOPMENT OF A BLOCKCHAIN-BASED SYSTEM FOR ELECTRONIC VOTING," . Vol., no. 17.
[33]. Y. Salem and E.-Y. Daraghmi, "GDPR-BLOCKCHAIN COMPLIANCE FOR PERSONAL DATA: REVIEW PAPER," . Vol., no. 23, 2021.

.