Forensics Case Studies – Extraction of Deleted and Live Data from DJI Agras MG 1s Drone Through Chip-Off, Internal SD Card And Controller Chip-Off Extraction.

Ankit[1], Tarun Kumar[2], Harsh Kumar Singhal[3]
[1,2,3]*Digital Forensics and Incident Response Analyst*

***Abstract*—The increasing prevalence of drones, or Unmanned Aerial Vehicles (UAVs), has raised significant concerns regarding their potential for misuse in criminal activities. This research explores the forensic analysis of drones, focusing on the extraction and correlation of data from various sources, including the drone's internal storage, SD card and controllers, to establish links between the drone and illicit activity. Using advanced forensic tools such as FTK Imager, Cellebrite Inseyets PA, DatCon, and CsvView, we investigate methods for retrieving crucial data such as GPS coordinates, flight logs, user interactions, media files, and system logs from the drone and associated devices. Our methodology includes imaging data from the drone's microSD card, reconstructing flight paths, and analysing performance metrics like battery voltage to estimate speed and assess drone activity during different flight stages. The findings reveal how digital traces left by drones and their controllers can offer valuable forensic insights in criminal investigations. This study highlights the increasing relevance of drone forensics in law enforcement, providing a comprehensive framework for digital evidence analysis that can assist in the identification and prosecution of individuals involved in illegal drone activities.**

I. REVIEW STAGE: DRONE FORENSICS AND INVESTIGATIVE COMPONENTS

A. Drone Overview

Drones, or Unmanned Aerial Vehicles (UAVs), are complex devices composed of multiple integrated components that work together to ensure controlled flight and operational performance. These components, which include the SD card, internal storage, flight control system, sensors, controller, battery, and motor, all contribute to both the flight experience and the potential for forensic analysis. In criminal investigations, these elements can provide valuable digital evidence crucial for understanding drone operations and linking them to illicit activities.

B. SD Card and Internal Storage

The SD card and internal storage of a drone are integral to data collection during flight. Photos and videos captured by the drone during flight are typically stored on the SD card, providing visual evidence of the drone's activities. Flight logs, which include critical metadata such as GPS coordinates, timestamps, motor speeds, and other performance metrics, are typically stored in the internal storage in either TXT or DAT file formats. These files can be crucial for reconstructing flight paths and determining the geographical locations and activities of the drone.

C. Flight Control System

The flight control system plays a key role in managing the drone's operational settings and controls. It allows for the modification of parameters such as flight settings, Wi-Fi information, and the management of data storage. Through the flight control system, flight data files can be downloaded from the drone's SD card or internal storage, offering insights into flight parameters and aiding investigators in determining if the drone's settings were altered or tampered with. The ability to access and analyse these data files is essential for forensic analysis, especially in investigations where remote operation and data manipulation are suspected.

D. Sensors

Drones are equipped with a variety of sensors, such as gyroscopes, accelerometers, barometers, and GPS units, that ensure stability and precision during flight. These sensors work together to maintain the drone's

position and altitude, which is crucial for its navigation and performance. For forensic purposes, the data captured by these sensors can be invaluable in verifying the drone's trajectory, height, and location. GPS and barometric data, in particular, can be used to accurately map out the drone's flight path and provide critical evidence in criminal investigations.

E. Controller

The controller, or remote-control device, is used to guide the drone's direction and speed. It typically communicates with the drone via radio signals and may be connected to a mobile phone, which serves as the interface for controlling flight functions. The controller's role in forensic analysis includes tracking user interactions, identifying potential links between the operator and the drone, and determining whether the drone's flight was manually or autonomously controlled. Mobile phones can also be integral in forensics, as they often store metadata related to drone control, flight logs, and other crucial data associated with the drone's operation.

F. Drone Crime Questions: Applying the 5W1H Framework in Drone Forensics

A well-structured crime investigation report follows the classic 5W1H formula—who, what, when, where, why, and how—to comprehensively address the core elements of the crime or incident. This method is essential in drone-related investigations, as it guides the forensic analysis and helps piece together the narrative of events surrounding the crime. By adapting the 5W1H framework to drone forensics, investigators can answer critical questions that shed light on the role of drones in criminal activities and establish connections between the drone, its operator, and the incident. The following outlines how the 5W1H approach applies to drone crime investigations:

G. Who:

1. Identifying the individuals involved is crucial in any criminal investigation. In the context of drone-related crimes, the primary focus is on identifying the drone operator and any other persons associated with the crime. This study utilizes flight data, including logs from the drone's internal storage and GPS information, to track the drone's movements and pinpoint the user or operator. By analysing interactions between the drone, controller, and connected mobile devices, investigators can establish a link between the drone and the suspect(s). Furthermore, forensic analysis of the controller or mobile phone may uncover identifying information such as user profiles, communications, or previously stored data that could point to the person responsible for operating the drone.
2. Where: Determining the locations involved in the crime is essential for understanding the geographical scope of the event. By examining GPS data retrieved from the drone's flight logs, investigators can reconstruct the flight path and accurately identify where the drone was during the crime. The GPS coordinates, timestamped in the flight logs, offer a precise location that may align with the crime scene. Additionally, by cross-referencing this information with other physical evidence, such as witness testimonies or surveillance footage, investigators can confirm the drone's proximity to key locations of interest during the event.
3. What: The "what" question pertains to the nature of the crime itself and the actions taken by the drone operator. This study aims to describe the specific facts surrounding the criminal activity, such as whether the drone was used for surveillance, smuggling, illegal photography, or any other unlawful actions. By analyzing the data collected from the drone, such as flight patterns, media files, and any recorded interactions, investigators can gain a clear understanding of the drone's involvement in the crime. The drone's internal storage, including photos, videos, and flight logs, may provide concrete evidence of the crime's nature and the drone's role in its execution.
4. When: The timing of the crime is another critical aspect of the investigation. To establish when the crime occurred, this study compares the timestamps recorded in the drone's flight logs with those on associated devices, such as the mobile phone or controller. This temporal analysis helps create a detailed timeline of events, enabling investigators to correlate the drone's activities with the crime's occurrence.

By establishing an accurate time frame, investigators can also identify patterns of behavior or determine if the crime was planned or opportunistic.

5. Why: Understanding the motivation behind the crime is a fundamental part of the investigation. While the “why” question is often more difficult to answer, forensic analysis of the drone’s flight data and user interactions may offer insights into the operator's intent. For example, examining the locations and timing of the drone’s flights may reveal patterns that indicate premeditation or a targeted approach to the crime. Additionally, communications from the controller or connected devices could provide further context about the operator’s motivations, whether they were related to personal, financial, or ideological reasons.
6. How: The “how” question addresses the methods used to carry out the crime. In drone-related incidents, this involves determining how the drone was employed in the commission of the crime. Was the drone used to access restricted areas, transport illegal goods, or capture sensitive information? By carefully analyzing the flight data, sensor readings, and media files, investigators can piece together how the drone functioned during the event. The flight control system and connected devices can reveal whether the drone was manually controlled or autonomously guided, offering insights into how the operator executed their plan.

II. CASE STUDY

A. The Growing Importance of Drone Forensic Analysis in Criminal Investigations

The demand for forensic analysis of drones has increased significantly, especially in criminal investigations. Drones, with their advanced cameras, sensors, and communication technologies, can provide crucial digital evidence that aids in identifying perpetrators and reconstructing criminal events. The data extracted from drone controllers, mobile phones, or the drones themselves can reveal valuable information about the suspect’s actions, flight path, and intentions. This evidence, when properly analysed, can be pivotal in solving crimes involving surveillance, smuggling, terrorism, and other illicit activities.

A foundational concept in forensic investigations, the Locard Exchange Principle, asserts that "with contact between two items, there is always a transfer of material." Originally a principle of physical forensics, this concept holds significant relevance in the digital forensics domain, particularly in the context of drone investigations. In drone-related incidents, the controller or mobile phone used to operate the drone is the primary interface for controlling the flight path. The Wi-Fi or radio signals connecting the drone to the controller or mobile device create a digital link, facilitating the transfer of data between the devices. This digital exchange leaves behind valuable evidence such as flight logs, GPS coordinates, video footage, and other metadata that are critical in forensic analysis.

Thus, the examination of data exchanged between drones and their controllers or mobile devices is integral to modern digital forensics. This paper will explore the methods for capturing, preserving, and analysing data related to drone activities, particularly focusing on Wi-Fi packet analysis using tools like Wireshark. Additionally, the paper will discuss the application of the Locard Exchange Principle in digital forensics, emphasizing how the interaction between drones and their operators creates digital traces that can link individuals to criminal behavior.

By utilizing advanced digital forensics techniques, investigators can gain a deeper understanding of drone-related incidents, enabling them to identify perpetrators and resolve criminal cases more effectively. This research aims to underline the growing importance of drone forensics in law enforcement and demonstrate how digital evidence from drones can be systematically leveraged to support criminal investigations.

Hardware

- Drone
- SD Card
- Laptop
- Chip-off station
- Software
- FTK Imager
- DatCon
- Cellebrite Inseyets PA

Data we get.

III. METHODOLOGY

This research outlines a forensic process for extracting and analyzing data from a drone's internal microSD card. The process follows industry-standard practices to ensure the integrity of the data throughout the acquisition and analysis stages. Below are the detailed steps involved in the methodology:

A. Removal of the Internal microSD Card from the Drone

The first step is to safely power off the drone and carefully remove the internal microSD card. This procedure must be done with caution to prevent physical damage to the card. Depending on the drone model, accessing the microSD card may require disassembling the drone's outer casing or accessing a specific compartment designed for the storage device.

B. Connecting the microSD Card to a Laptop with a Write-Blocker

Once the microSD card is removed, it is connected to a laptop through a write-blocker. The purpose of the write-blocker is to prevent any data modification during the extraction process. It ensures that the data on the microSD card is only read, preserving the integrity of the evidence. The write-blocker is crucial for maintaining the forensic soundness of the process, preventing accidental writes or data corruption.

C. Creating a Forensic Image with FTK Imager

The next step is to create a bit-by-bit forensic image of the microSD card using FTK Imager. FTK Imager is a widely recognized tool in the field of digital forensics and provides a reliable method for creating an exact copy of the data from the original storage device.

D. Steps in FTK Imager:

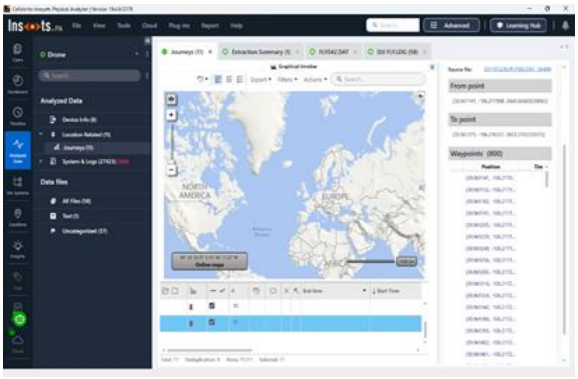
- Launch FTK Imager and select the option to create a new disk image.
- Choose the microSD card as the source device.
- Specify the destination for the image file, which is typically saved in an E01 format, ensuring the image is created with a proper hash value (such as MD5 or SHA-1) for verification purposes.
- Start the imaging process. The software will produce a forensic copy of the microSD card, which includes both visible and hidden data, along with any deleted or fragmented files that may exist on the card.

E. Ingesting the Image into Cellebrite Insights PA

After creating a complete forensic image of the microSD card, the next step is to ingest this image into Cellebrite Insights PA for further analysis. Cellebrite Insights PA is a digital forensics platform designed to decode data from a variety of devices, including drones. The software is used to extract, decode, and display the data stored on the microSD card.

F. Process in Cellebrite Insights PA:

- Open Cellebrite Insights PA and select the “Ingest” option to import the image file created with FTK Imager.
- The software processes the image, automatically identifying and categorizing the types of data stored on the microSD card. This includes system logs, GPS data, and other relevant files.
- Cellebrite Insights PA decodes and makes the raw data readable, preparing it for analysis.



G. Decoding the .DAT Files and Extracting the Data
The core data stored on the microSD card is typically found in .dat files. These files contain various types of data, such as flight logs, system logs, and GPS records, all of which are critical for understanding the drone's operations.

H. Types of Data Extracted:

- Flight Logs: These logs provide details on the drone's operational events, such as power-ups, shutdowns, flight sequences, and system warnings or errors.
- GPS Data: The GPS records stored in the .dat files include precise location information, capturing the drone's movement, altitude, and flight path at different times.
- System Data: Additional data, such as battery levels, temperature readings, and error messages, may also be stored in .dat files, offering a comprehensive overview of the drone's performance.
- Once the .dat files are decoded, the extracted data is made available in a user-friendly format, ready for analysis. This data is then parsed for further examination and to draw conclusions about the drone's flight history and operational status.

I. Analysis of Extracted Data
The extracted data can be analyzed to reconstruct the flight path, assess the drone's operational history, and investigate any technical issues or anomalies. The analysis of GPS data allows for the mapping of the drone's flight path over time, while log files provide insights into any system errors or irregularities.

J. Analysis Techniques:

- Reconstructing Flight Paths: Using GPS data, the movement of the drone can be traced and visualized on a map. This allows forensic investigators to determine where the drone was flown and when, providing critical information for investigations.
- Identifying System Issues: By reviewing the flight and system logs, errors or malfunctions during flight can be identified. This includes detecting system failures, low battery alerts, or any other abnormal events recorded during operation.
- Tracking Performance: A detailed performance analysis can be conducted by reviewing system logs, which provide data on battery usage, temperature, and other critical performance metrics.

K. Results and Discussion
The forensic process described above successfully extracted and decoded multiple data types from the microSD card of the drone. The key findings include:

- Flight Path Data: GPS coordinates extracted from the .dat files provided precise location data, which was used to map the flight paths of the drone. The data allowed the reconstruction of the drone's movement and location over time, helping to establish where the drone was flown and the areas it visited.
- Log Data: The flight logs provided critical insights into the drone's operational status. These logs included start-up and shutdown sequences, flight warnings, and system errors that occurred during operations. The logs were essential for understanding the performance and behavior of the drone during the investigation period.
- System Performance: Analyzing the extracted system data revealed important information about the drone's operational health, including battery life, temperature readings, and the occurrence of any mechanical issues. This data can be used to assess whether the drone was functioning optimally or encountered any difficulties during flight.

IV. METHODOLOGY

This section outlines the step-by-step process used to extract and analyse data from a drone's internal microSD card, focusing on the use of forensic tools to obtain critical information, such as the drone's flight path, motor performance, frequencies, and health status. The entire methodology is designed to ensure the integrity of the data and maximize the accuracy of the findings. The following steps were followed:

A. Removal of the Internal microSD Card from the Drone

The process begins with the careful removal of the internal microSD card from the drone. The drone is powered off before extracting the microSD card to prevent any possible damage to the data. Depending on the drone's design, the microSD card may be accessible through the removal of a compartment cover or require partial disassembly of the device.

B. Connecting the microSD Card to a Laptop Using a Write-Blocker

To prevent any accidental modification or overwriting of data on the microSD card, a write-blocker is used when connecting the card to a laptop. The write-blocker ensures that the card is only readable and prevents any write operations. This step is essential for maintaining the integrity of the original data during forensic acquisition and analysis.

C. Creating a Forensic Image with FTK Imager

Once the microSD card is connected to the laptop via the write-blocker, a forensic image is created using FTK Imager, a widely used tool in digital forensics. FTK Imager creates a bit-by-bit copy of the microSD card, ensuring that all files, including deleted or hidden data, are preserved.

D. Process in FTK Imager:

- Launch FTK Imager and select "Create Disk Image."
- Choose the microSD card as the source device.
- Specify the destination to save the forensic image, usually in E01 format to ensure the integrity and reliability of the data.
- Generate hash values (e.g., MD5 or SHA-1) to verify the image integrity during later analysis.
- Start the imaging process, allowing FTK Imager to create an exact copy of the microSD card.

E. Ingesting the Image into Cellebrite Insights PA

After creating a forensic image, the next step involves ingesting the image into Cellebrite Insights PA, a powerful tool designed for decoding and analysing data from various devices, including drones. This software provides an efficient way to parse and identify different data types stored on the microSD card, including log files, GPS data, and system performance data.

F. Process in Cellebrite Insights PA:

- Open Cellebrite Insights PA and import the created forensic image.
- The software processes the image and automatically identifies the data structure, including file systems, logs, and other relevant data.
- After decoding, the extracted data is displayed in a readable format, allowing for easy navigation and further analysis.

G. Exporting the .DAT Files and Importing into DatCon

Once the data is decoded and extracted from the microSD card, the .dat files are exported from Cellebrite Insights PA. These files contain valuable operational data collected by the drone during flight, such as motor performance, health status, and flight path.

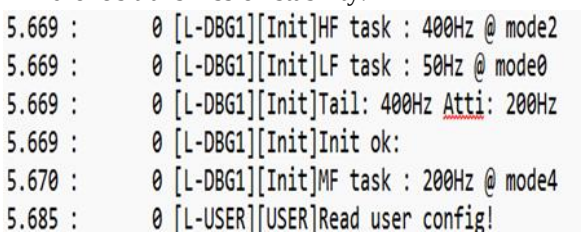
H. Process in DatCon:

- The exported .dat files are individually added to DatCon, a tool specifically designed for processing and interpreting drone flight logs.
- DatCon decodes the .dat files, revealing valuable information embedded within the data.

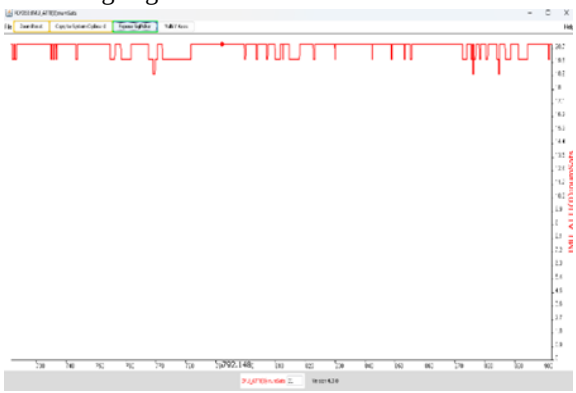
I. Analyzing the Data

DatCon decodes the data into multiple types of information that are crucial for understanding the drone's operations. The primary data points extracted from the .dat files include:

- Drone Frequencies: The first type of data obtained is the frequencies used by the drone during operation. These frequencies are vital for understanding communication and signal strength, and may be critical in analysing the drone's transmission stability.

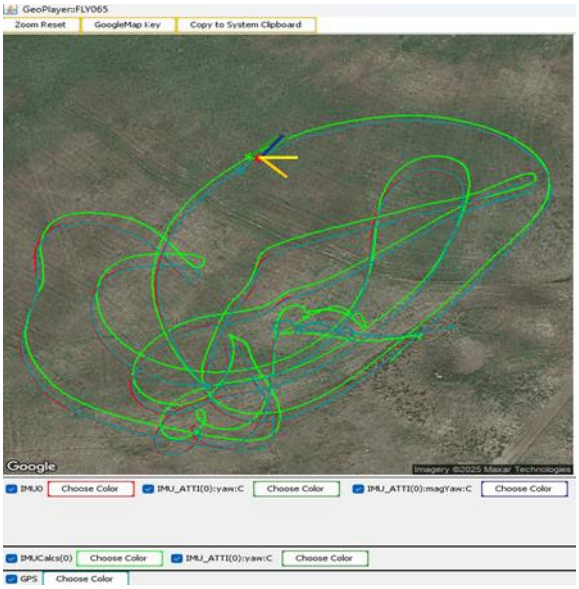


- Drone Health States: The second data type consists of the health states of the drone. This data includes critical system parameters such as battery health, temperature readings, sensor statuses, and any system errors or warnings. Health state data helps assess the overall operational reliability of the drone and any potential malfunctions that may have occurred during flight.

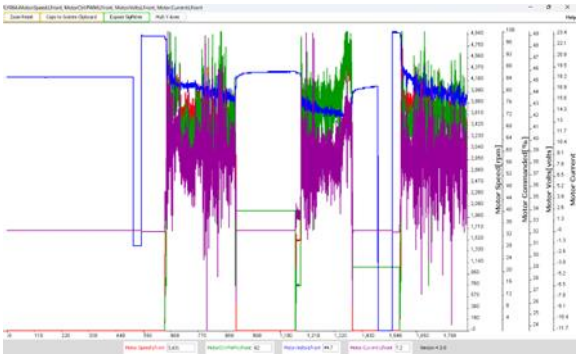


- Drone Motor Performance: The third type of data includes motor performance metrics such as motor speed and current. These data points are essential for evaluating the drone's motor function during flight. By analysing motor speed and current, investigators can determine if the motors were functioning within normal parameters or if any irregularities were present.

- Drone Flight Path: The final type of data extracted is the drone's flight path, derived from the GPS coordinates stored in the .dat files. The flight path provides a detailed record of the drone’s movements, including altitude, direction, and geographic location during the flight. This data can be visualized to recreate the drone’s trajectory and to identify specific areas of interest or potential incidents during the flight.
- Visualization and Interpretation of Data
  After extracting and decoding the data, it is analyzed to understand the drone's operational history. The following techniques are employed to interpret the data:
- Flight Path Visualization: The GPS data can be plotted on a map, allowing for the reconstruction of the drone's flight path. The analysis provides a visual representation of where the drone flew, helping to determine its movement across different geographic regions.



- Health and Performance Evaluation: By examining the motor speed, current, and health state data, the drone's performance can be assessed. Any anomalies, such as abnormal motor speeds or temperature spikes, may indicate mechanical or operational issues that require attention.



- Signal Integrity Assessment: Analyzing the drone's frequency data allows investigators to

evaluate the stability of communication during the flight, helping to identify potential communication failures or signal disruptions that could have affected the flight.

V. RESULTS

The data extracted from the drone's microSD card provided critical insights into the operational performance and behavior of the drone during flight. The analysis of the .dat files revealed several key findings:

- Drone Frequencies: The frequencies used by the drone were recorded and analyzed. These frequencies are important for understanding the communication protocols between the drone and its control system, as well as any potential interference or signal disruptions.
- Health States: The health state data provided detailed information on the drone's system status, including battery life, temperature, and sensor health. No significant errors or malfunctions were detected, but the data helped verify that the drone was functioning within expected parameters during the flight.
- Motor Performance: The motor speed and current data revealed the operational efficiency of the drone's motors. The motors were operating within the expected speed ranges, with no indication of overloading or underperformance.
- Flight Path: The reconstructed flight path accurately depicted the drone's trajectory, showing its movements across various locations and altitudes. This data was essential in understanding the drone's operational history and its potential interaction with specific environments or areas of interest.

VI. CONCLUSION

The forensic extraction and analysis of data from a drone's internal microSD card using FTK Imager and Cellebrite Insights PA proved to be an effective methodology for retrieving valuable data such as flight logs, GPS coordinates, and system records. By employing a write-blocker during the acquisition phase and creating a physical image of the microSD card, the process maintained the integrity of the original data, ensuring that no modifications occurred during the extraction.

The results demonstrated that drone data, including critical flight information and system performance logs, could be successfully decoded and analysed to provide important insights into the drone's operations. This methodology is a valuable tool for forensic investigators and researchers seeking to analyse drone data for purposes such as criminal investigations, incident reconstruction, and operational performance reviews.

Future work could further refine the process by incorporating automated tools for data analysis, potentially improving the efficiency of extracting and interpreting large datasets from drones. Additionally, as drone technology advances, forensic methodologies will need to evolve to handle new data formats and storage solutions used in next-generation drones.

The forensic extraction and analysis of data from the drone's internal microSD card, utilizing FTK Imager, Cellebrite Insights PA, and DatCon, successfully provided a detailed picture of the drone's operations. The extracted data revealed valuable insights into the drone's frequencies, health states, motor performance, and flight path, offering a comprehensive understanding of its functionality during flight.

This methodology can serve as a standard approach for drone data recovery in forensic investigations, providing a reliable framework for extracting, decoding, and interpreting various types of operational data. It ensures that the integrity of the original data is preserved and enables a thorough analysis of the drone's performance, which can be used for legal investigations, system troubleshooting, or operational assessments.

Future research could focus on refining these methods to handle larger datasets and incorporate new data analysis techniques, such as machine learning models for automated anomaly detection, to further enhance drone forensics and operational insights.

REFERENCES

[1] DatCon https://datfile.net/DatCon/downloads.html
[2] FTK Imager-

[3] https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81
[4] OpenAI
[5] Drone https://www.dji.com/mg-1s
[6] cellebrite inseyets
[7] https://cellebrite.com/en/cellebrite-inseyets/
[8] (IJIRT 171846) Forensics Case studies – Extraction of deleted and live data from DJI Drone Matrix 600 Pro Through Chip-off, Internal SD Card and Mobile Phone Extraction. (Ankit, Harsh Kumar Singhal)