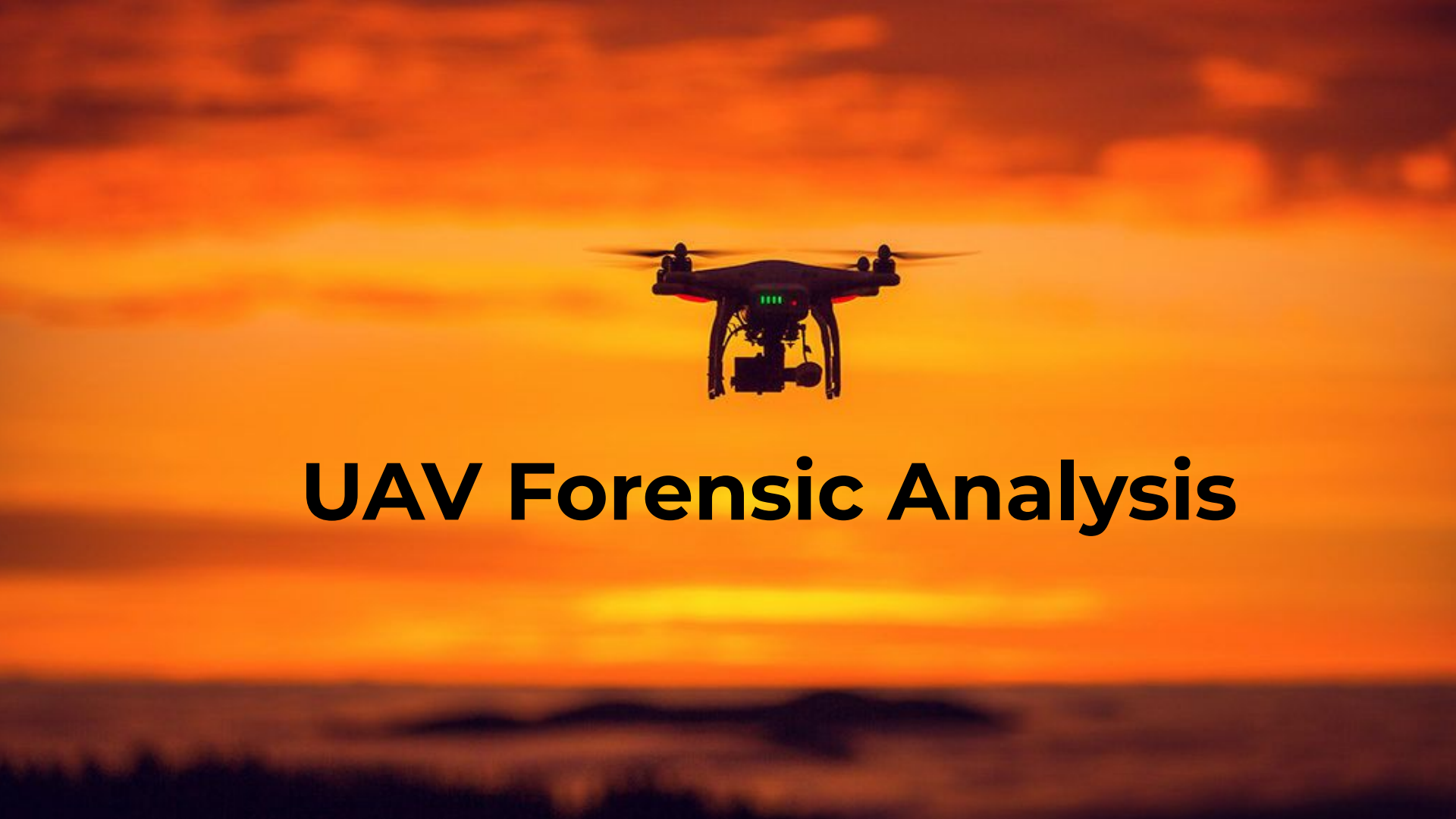

UAV Forensic Analysis

Echo ‘Whoami’

- 4th year Computer Engineering Student at NMIMS
- Interned with Deloitte in their Cyber Risk Department
- Currently volunteering as a Senior TA at Cybrary involved in beta testing, quiz question creation and much more
- Interested in all things relating to cybersecurity
- Email - navidkagalwalla27@gmail.com

DRONES - REPORTING FOR DUTY

WHAT IS COVERED

1) What are UAVs?
2) What is UAV Forensic Analysis?
3) Terminologies used in UAVs
4) UAV Forensic Challenges
5) Physical Evidence Available
6) Points to Consider while Conducting UAV Forensics
7) UAV Forensic Analysis Process

What are UAVs?

- Unmanned Aerial Vehicles (UAVs), also referred to as drones are aircraft piloted by remote control or by an on-board computer
- Designed for use in several environments such as security, disaster response, construction monitoring, agricultural mapping, and even recreation
- Wide range of UAVs, in terms of capabilities and prices
- According to a Gartner forecast, production and shipment of drones for personal and commercial use is growing rapidly with global market revenue from drones expected to grow more than $11.2 billion in 2020

What is UAV Forensic Analysis?

- Potential source of evidence in a digital investigation, due to their increasing popularity in our society
- Relating to recovery of digital evidence or data from a drone under forensically sound conditions.
- The security and prevention of exploitation of vulnerabilities present in UAVs by hackers have not been given the needed importance
- What Data is Recoverable
  - Serial number of the drone aircraft and some internal components such as MAC, IMEI, & IMSI
  - Version numbers for firmware
  - Metadata from operations such as launching, waypoint logs, GPS available or unavailable during flight
  - Geo location information for critical locations – launching, landing, and home or return location
  - Full flight path information
  - Wifi Data | SSID | MAC | I.P
  - Bluetooth | Paired devices | Timestamp

Terminologies Used in UAV

- UAS – Unmanned aircraft system means an unmanned aircraft and the equipment to control it remotely
- UAV – The aircraft portion of the system
- GCS – Ground Control Station – The flight control portion of the system. May include manual and automatic control features
- Data link – radio system to transmit data to and from the UAV. Often used for telemetry, sensor data, and FPV operation
- Drone – Common term for any UAV but most often used to describe quads and other multirotor UAVs
- FPV – First Person View – technology that enables the operator to fly the UAV from the perspective of the UAV

UAV Forensic Challenges

- Current tools provide limited data which isn't forensically sound and not admissible in a court of law
- Large number of drones available with different makes, models, features
- Digital evidence would include operating systems like the mobile OS, traditional OS, embedded Linux systems, a variety of file systems such as JFFS2, media storage, and firmware
- While NIST has built a dataset of the forensic images of 14 popular makes and models of drones in its Computer Forensic Reference Datasets there still isn't any published guideline for UAV Forensics

Physical Evidence Available

Points to Consider while Conducting UAV Forensics

- Problem - Crash, Theft, Privacy Abuse
- UAV Characteristics - Various capabilities, storage options, peripheral devices, and ports
- Evidence - Accurate representation of data

UAV Forensic Analysis Process

- Identify and determine the chain of command
- Have conventional forensic practices (DNA, fingerprints) already been implemented?
- Identify the role of the device in conducting the offence
- Identify the make and model
- Identify capabilities (Video/Audio recording, carrying capacity and technique)
- Identify potential modifications.
- Identify data storage locations and ports
- Extract removable data storage mediums
- Preserve evidence – Clone / forensic copy of storage medium