Drone Forensics
An update on a U.S. Department of Homeland Security R&D Project

Steve Watson, Principal Investigator
Acknowledgement & Disclaimer

This material is based on research sponsored by the United States Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD) via contract number HHSP233201700017C.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Department of Homeland Security.
Team Profile

• VTO is a recent technology startup focused digital forensics, data recovery, and cyber security.

• Small team of industry veterans with deep experience in hardware analysis and hardware deconstruction to access data.

• Principal Investigator chairs SWGDE Forensic Committee and NIST OSAC Working group on Mobile and Embedded Device Forensics.
Customer Need

• At the time of project proposal, no industry tools existed to retrieve data from consumer and professional drones.

• Limited research focused on logical data acquisition.

• Drones continue to fly and land in places they should not with no processes to identify evidentiary data.
Approach

Device Analysis

• Complete physical analysis of interrogated consumer and professional drones including teardown.

• Identification and consolidation of existing technical information online.
Approach

Data Acquisition

• Identification of data acquisition methodologies available against interrogated devices.

• Logical acquisition methods. Serial/JTAG/debug acquisition. Chip-off acquisition against flash storage and microcontrollers on devices.

• Acquisition methods and sample data will be made available to community for further research.
Goals

1. Establish base scientific research regarding the application of existing digital forensics techniques against consumer and professional level drones.

2. Identify procedures and practices that can be utilized by digital forensics service providers (gvt/le/mil/pvt) for the successful extraction of data from drone/suas systems.

3. Share results with the community to support and strengthen law enforcement efforts against these devices.
Scope

Twenty 30 consumer and professional drones. Available to anyone for purchase.

- Identify data artifacts of evidentiary value.
- Identify methods and process to extract data.
- Share results with digfor community.
<table>
<thead>
<tr>
<th></th>
<th>Manufacturer</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DJI</td>
<td>Phantom 3</td>
</tr>
<tr>
<td>2</td>
<td>DJI</td>
<td>Phantom 4</td>
</tr>
<tr>
<td>3</td>
<td>DJI</td>
<td>Spark</td>
</tr>
<tr>
<td>4</td>
<td>DJI</td>
<td>Inspire 1</td>
</tr>
<tr>
<td>5</td>
<td>Yuneec</td>
<td>Typhoon</td>
</tr>
<tr>
<td>6</td>
<td>Parrot</td>
<td>Disco</td>
</tr>
<tr>
<td>7</td>
<td>DJI</td>
<td>Mavic Pro</td>
</tr>
<tr>
<td>8</td>
<td>Parrot</td>
<td>Bebop 2</td>
</tr>
<tr>
<td>9</td>
<td>DJI</td>
<td>Inspire 2</td>
</tr>
<tr>
<td>10</td>
<td>Yuneec</td>
<td>Q500 4K</td>
</tr>
<tr>
<td>11</td>
<td>Yuneec</td>
<td>H520</td>
</tr>
<tr>
<td>12</td>
<td>DJI</td>
<td>Matrice 600</td>
</tr>
<tr>
<td>13</td>
<td>DJI</td>
<td>Agras MG-1</td>
</tr>
<tr>
<td>14</td>
<td>DJI</td>
<td>S1000</td>
</tr>
<tr>
<td>15</td>
<td>SenseFly</td>
<td>eBee</td>
</tr>
<tr>
<td>16</td>
<td>SenseFly</td>
<td>Albris</td>
</tr>
<tr>
<td>17</td>
<td>DJI</td>
<td>Mavic Air</td>
</tr>
<tr>
<td>18</td>
<td>Ryze</td>
<td>Telo</td>
</tr>
<tr>
<td>19</td>
<td>DJI</td>
<td>Phantom 4 Pro V. 2.0</td>
</tr>
<tr>
<td>20</td>
<td>Aion Robots</td>
<td>R1 Rover</td>
</tr>
<tr>
<td>21</td>
<td>Skydio</td>
<td>R1</td>
</tr>
<tr>
<td>22</td>
<td>Handbuilt</td>
<td>Ardupilot</td>
</tr>
<tr>
<td>23</td>
<td>Skyviper</td>
<td>V2450 GPS</td>
</tr>
</tbody>
</table>
Process

1. Procure devices
2. Salt devices with data
3. Interrogate devices in lab
4. Apply digital forensics techniques against devices
5. Publish results
6. Support DigFor community
Process - Procure Devices

• Identify industry penetration of consumer and professional level drones.

• Procure devices.

• Twenty (20) Thirty (30) device models in scope for program.

• Three (3) devices of each model

• Sixty (60) Ninety (90) drones total
Process - Salt Devices

Control the variables

• All 60 devices are flown at same location
  • 1,800 acre ranch in the mountains of Colorado
• Geofenced location
• Time/date identified

• Geolocation/time/date variables critical for parsing unknown data systems.
Process - Lab Interrogation

1. Documented teardown of each device.
   - DSLR and microscope photographs

2. Identification of data storage areas on device.

3. Investigation of every integrated circuit package.
Process - Application of Digital Forensic Techniques

Logical and physical acquisitions attempted against every drone.

1. Logical acquisitions of file systems
2. Physical acquisitions of intact media and integrated circuit packages
3. Serial attempts against devices for data acquisition and device compromise.
Process - Publish Results


2. Publication of papers to journals to establish baseline scientific research.
NIST CFReDS Project

CFReDS – computer forensic reference data sets

Drone datasets added as an official reference set by NIST.
Process - Reports

Complete reports will be available on each model.

Three reports completed.

Eight more to drop soon.
Slick Sheets

1. Non-Technical First Responder
2. Technical First Responder
3. Digital Forensics Lab Team
Interesting Information So Far

Successful data acquisitions on all devices attempted so far

- 23 models, 69 drones
- Over 1.3TB of data acquired so far.

Interesting data on drones, controllers, connected mobile devices.

1 security vulnerability discovered.
microSD Cards
Glued onto Circuit Board

• DJI Models typically have an internal microSD card glued onto the circuit board
• Carefully remove the glue to loosen the microSD card
• Image the microSD per normal physical acquisitions processes
Conformal Coatings

- Immature conformal coatings identified on drones manufactured by Chinese companies
- Obfuscates and complicates chip removal
- Industry standard - IPC-7711/7721
Custom Asics

• Custom integrated circuit packages designed specifically for the manufacturer for this purpose.

• Difficult to identify adapters to read data.

• Will be challenges to parse unknown structures.
Parrot SkyController 2
Further Research Questions

• More drones.

• Different firmware versions – future and historical.

• Drone swarms.