NIST
National Institute of Standards and Technology
U.S. Department of Commerce

FORENSICS @ NIST | #NISTForensics

Drone Forensics and other new additions to CFReDS

Ben Livelsberger

Information Technology Laboratory

Computer Forensics Reference Datasets (CFReDS) Overview

- The CFReDS project provides documented sets of simulated digital evidence.
- Uses for Data Sets
  - Tool Testing
  - Training
  - Proficiency Testing
- Sourced from
  - NIST
  - Non-NIST (LE, forensic labs, conferences)

Types of Datasets

- Tool Testing / Computer Forensics Tool Testing
  - Windows Registry Forensics
  - String Search
  - Metadata-based Deleted File Recovery
  - File Carving (graphic and video files)

Types of Datasets

- Multi-skill sets of simulated digital evidence
  - Hacking Case – Law Enforcement
  - Data Leakage Case - NIST
  - Rhino Hunt - DFRWS

Types of Datasets

- Misc. special purpose sets
  - Create a reference drive - NIST
  - DCFL control image - DCFL
  - Container Files - NIST
  - Mobile Device Images - NIST
  - Memory Images – ManTech
  - Basic Mac Images - NIST
  - Russian Tea Room - NIST

New and Coming Soon

- Drone Images - VTO Labs - **NEW**
- JTAG & Chip Off images of smart phones - NIST+LE - **COMING SOON**
- More multi-skill sets - DFRWS - **COMING SOON**

Drone Forensics

- Drone – unmanned areal vehicle
  - Crop dusting
  - Photo/videography
  - Mapping/surveying
- What do you do when it's part of your crime scene?

Photos courtesy of www.drone-world.com, www.pobonline.com, www.suasnews.com, & www.wellbots.com

VTO Labs Drone Dataset

- 63 drones, 25 models
  - DJI, Parrot, SenseFly, Yuneec, Skydio, Ryze, Sky Viper, ArduPilot & Aion
- Forensic images
- VTO Labs, funded by Department of Homeland Security Science and Technology Directorate

Creating the Dataset

- ~3 drones of each model
- Establish baseline data
- Acquire contents of:
  - Drone storage areas
  - Controller
  - Mobile devices and computers

Photo courtesy of VTO Labs

Dataset Contents

- Images for each drone
- Drone research results reports:
  - Where and when drone was flown
  - Data storage areas
  - Instructions & photos for disassembly
  - Data acquisition methods

Photo courtesy of VTO Labs

What Data Can You Retrieve?

- Serial numbers
- Flight paths
- Flight speed and bearing
- Launch and landing locations
- Photos, videos
- Log of actions user made from the drone controller

Applications

- Practice recovering data
- Training
- Proficiency testing
- Research
- Forensic tool development

Contacts

Ben Livelsberger
benjamin.livelsberger@nist.gov

www.cfreds.nist.gov
cftt@nist.gov

Jim Lyle, CFReDS Project Leader
James.lyle@nist.gov