eForensics Magazine

MAGAZINE

Drone Forensics

A UAV Forensic Case Study

Hacking a wifi printer with a drone

Robots and Cyborgs Forensics

VOL.08 NO.04
ISSUE 04/2019, (89) APRIL
ISSN 2300 6986

eForensics Magazine

TEAM

Editor-in-Chief
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Managing Editor:

Dominika Zdrodowska
dominika.zdrodowska@eforensicsmag.com

Editors:

Marta Sienicka
sienicka.marta@hakin9.com

Marta Strzelec
marta.strzelec@eforensicsmag.com

Bartek Adach
bartek.adach@pentestmag.com

Senior Consultant/Publisher:
Paweł Marciniak

CEO:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Marketing Director:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

DTP
Dominika Zdrodowska
dominika.zdrodowska@eforensicsmag.com

Cover Design
Hiep Nguyen Duc

Publisher
Hakin9 Media Sp. z o.o.
02-676 Warszawa
ul. Postępu 17D
Phone: 1 917 338 3631

www.eforensicsmag.com

All trademarks, trade names, or logos mentioned or used are the property of their respective owners.

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

word from the team

Dear Readers,

We're extremely proud to present to you the newest issue of eForensics Magazine - Drone Forensics!

Drones are quickly becoming a cybersecurity nightmare, so it's better to know what's going on with them!

In this issue - devoted exclusively to the topic of unmanned aerial vehicles - you will find articles on extracting data from UAV, hacking a wifi printer with a drone, vulnerabilities and attacks on UAVs, a UAV forensic case study, the article entitled "Why is everyone looking up", Forensic Evaluation of Drone Technology and more!

We have also an article on robot and cyborg forensics, an automated digital forensics future, artificial intelligence and security issues raised in an e-commerce platform.

We invite you on a flight… drone flight!

Thanks to all authors, reviewers and proofreaders for participating in this project.

Have a nice read!

Regards,

Dominika Zdrodowska

and the eForensics Magazine Editorial Team

Contents

05
Forensic Evaluation of Drone Technology

68
Vulnerabilities and Attacks on UAVs

35
Hacking a Wi-Fi Printer with a Drone

74
Digital forensics in robots and cyborgs

50
A UAV Forensic Case Study

86
Why is everyone looking up?

58
An automated digital forensics future

92
Security issues raised in e-commerce platform

64
Extracting data from UAV

104
5 Ways that AI is Enabling More Efficient Forensic Investigations

Forensic Evaluation of Drone Technology

by Daniel Owen

Abstract

The project begins to look into the broad range of UAVs that are likely to be encountered by police forces in the UK, specifically targeting the more budget end of the spectrum whilst still having all the functionality required to commit a range of crimes. The project focuses on post criminal activity analysis of the UAV and controller and while there is some discussion of commercial counter UAV tools it is not the focus of this project. One example of this analysis comes from media files stored on the drone and the kind of information that can be gathered from them through metadata. Using a purely practical, experimentation and analysis based approach, a thorough examination was made of both the UAV and its controlling Android and iOS devices. The project concludes that metadata is the best way to obtain information regarding flights, particularly where the Bebop's "Drone Academy" feature is disabled as it specifically states that this will track your drone's flights, though there is an analysis of the files created by the "Drone Academy" feature.

Glossary of Terms and Abbreviations

Term	Definition
BSSID	The MAC address of a wireless access point
Controller	Any device used to fly the drone or the individual flying the drone using the device
DHCP	Dynamic Host Control Protocol, a protocol used to automatically assign newly connected devices an IP address
Digital Certificate	An attachment to any form of electronic message used to authenticate the origin of the message or file
EXIF	Exchangeable Image File Format, a standard determining all of the additional tags to be potentially included in digital media formats, including time, date and camera information, as well as GPS and other data where applicable.
FTP	File Transfer Protocol, a network protocol to transfer files across a network
FTP Server	The device or service providing an FTP connection
GLONASS	Globalnaya Navigazionnaya Sputnikovaya Sistema, a Russian form of GPS that translates to Global Navigation Satellite System
GPS	Global Positioning System, a system of satellites used to accurately provide location information
Metadata	Data about data, includes things such as timestamps and GPS information
Mobile Controller	A mobile handset used to pilot a UAV via an app
SFTP	Secure File Transfer Protocol, a more secure form of FTP using SSL or TLS encryption
SSID	The "name" broadcast by a wireless access point, for example "Virgin Media Hub 5648"
SSL	Secure Socket Layer, a method of sending data in an encrypted format, it has largely been replaced by TLS but is still considered secure
Telent	A networking protocol that allows remote access to another computer system
TLS	Transport Layer Security, a modern replacement for SSL providing better security
UAV	Unmanned Aerial Vehicle, also called a drone and occasionally a Remotely Piloted Aircraft System
UUID	Universal Unique Identifier, a mathematically feasible unique code to count for a specific device or instance 128 bits in length.
Wi-Fi	A form of wireless communication used for data transmission primarily in the 2.4Ghz and 5Ghz signal bands

Introduction

• Defining the Problem

Unmanned Aerial Vehicles (UAVs or drones) have been in the public sphere for many years and so have those who wish to misuse them. Until relatively recently, with the prevalence of cheap cameras and powerful, small form factor motors becoming more widely available and driving down the price of UAVs, UAVs were only in the scope of private organisations or serious hobbyists (Colomina & Molina, 2014). Advances within signal and connection technology has also made locating the pilot of the UAV more difficult. Previously, the person misusing the drone was relatively easy to identify as the person with the bulky controller and line of sight to the drone, or, to quote Peter Robinson's DEFCON 23 talk regarding an incident with a US Department of Homeland Security Representative *'You see them running over the hill with the controller "Have you seen my drone?"'* (Robinson, n.d.)

This isn't to say all drone use is negative. Amazon has plans to use drones for delivery (Amazon, 2015) and police forces are using drones to patrol and survey the area around various UK airports, including Heathrow, Stanstead and Gatwick (Beake, 2015) and even used by historical societies to visually map an

area (Sherwood Skycams, 2016) and for industrial inspection of wind turbines (Sherwood Skycams, 2016). Despite these clear and legitimate uses for UAVs in ever expanding roles from inspection.

Unfortunately, as the technology increased so too did the complexity and the need for people able to analyse them when they're misused.

• **Proving Misuse**

Drones can go almost anywhere and film almost anything. It could be a Navy submarine yard, it could be children playing in the back garden or somebody in the shower. This 'go anywhere, see anything' function is clearly problematic if misused. If a situation arises where a drone and/or a suspected controller is taken in as evidence by the police, whether collected as evidence, crashed through pilot error or as the result of an accident, there needs to be some form of analysis made on the device to try to tie it to a specific person. The biggest issue with the current system is that there only exists a database of commercial drones over 20kg in weight, as these need Civilian Aviation Authority permission to fly. Hobbyists are exempt from this and so serial numbers cannot always be tied to specific people, though many are registered with the manufacturer for warranty and so could potentially be subject to subpoena duces tecum, more commonly called a document subpoena. These are obviously limited in scope so if, for example, the company was based in China and the information stored there also, it may not be possible to get the required documentation or information in the UK depending on the current political climate and how inclined the company is to cooperate. This isn't to say that attempts to create a registry haven't been made. Most prevalently, AirMap, a company which provides weather information, and DigiCert were partnering to produce SSL/TLS digital certificates to "tag" all drones using their service (Williams, 2016).

• **Scope**

The project will focus on the forensic investigation of a Bebop drone and the associated bespoke Skycontroller and both Android and iOS handsets, which can also be used to control the drone. It will also look briefly at some examples of commercial systems available to counter the problem of drones flying in places that are unsafe or they shouldn't be. There will be no investigation into any service outside of those provided by Bebop into registering the drone with any authority or company. Though there is mention of other

Parrot drones, with the exception of Nmap which was conducted on two other models of UAV produced by Parrot and made available via Sherwood Skycams, all work was conducted on a single Bebop drone. This was done to attempt to establish a manufacturer continuity between the software on all Parrot UAVs.

- **Rationale**

The project focuses on UK laws and regulations within the realms of both UAV usage and computer forensics, more specifically digital device forensics involving mobile phones and other devices. Computer forensics is a diverse and growing field, having developed beyond traditional desktops and laptops to include mobile and smart phones, satnav devices, games consoles and all manner of "nonstandard" devices. This project will be of use to a range of people, particularly those with a professional or personal interest in the digital forensic examination of mobile phones and UAVs.

- **Aims and Objectives**

✳Aim

The aim of this project is to assess the viability of conducting a forensic examination on a suspect Parrot Bebop drone and the controlling devices, and if evidence can be gathered from the controlling devices what kind of evidence can be gathered. Using the information garnered from these steps, produce a practical based guide on how best to acquire evidence from a UAV and its controllers.

✳Objectives

1. Research current methodologies for gaining access to files stored on the UAV device
2. Investigate mobile phone forensic techniques and tools
3. Discuss and analyse pertinent files from within the UAV
4. Discuss and analyse pertinent files from within the Skycontroller
5. Discuss and analyse pertinent files taken from a mobile controller in both iOS and Android platforms

Existing Research

- **Search Methodology**

As the project progressed and developed in scope, so too did the methods used to gather research information. As in the Project Proposal Google Scholar, Summon and general internet searches were used to gather electronic resources, such as Unmanned Aerial Vehicles: A

Preliminary Analysis of Forensic Challenges (Horsman, 2016), originally published in the Journal of Digital Investigation, and various DEFCON talks (Robinson, n.d.) (Smith, 2010). ResearchGate was also used to look for other sources. YouTube was also highly useful given the depth to which Michael Robinson discusses the problem in his DEFCON 23 panel. Information learnt via attendance of the Forensics Europe Expo 2017, 3rd May, is also being used within this report, particularly around existing counter UAV systems. Finally, discussions with Carl Barnett, owner and operator of Sherwood Skycams, were used to gather a better and broad understanding of existing UAV flight recording systems and laws.

- **The Drone Threat**

In an interview as part of an article on China's drone problem, Professor David Dunn, of the University of Birmingham, commented that, *"There seems to be an inability to deal with the potential drone threat"* (Baraniuk, 2017). This also led to DJI, a leading drone manufacturer, to offer a ¥1,000,000 bounty (roughly £112,000) for information regarding the drones used during the month of April. The misuse of drones isn't just limited to flying around airports however. Peter Yeung of The Independent reported a 352% rise in UK complaints related to drones (Yeung, 2016), these included reports of them being used to spy into bathrooms and look at children. This raise in misuse follows the growing trend in civilians purchasing drones over the last 15 years. This is mainly down to the way in which defence technology spending trickles down to the civilian market (Gettinger, 2016), much like GPS, which was diluted into a more civilian applicable form for everyday use (Stotts, et al., 2014).

Despite the rise in reported drone misuse, there wasn't a single conviction prior to September 2016 when 42-year-old Nigel Wilson was prosecuted after admitting to flying a UAV through restricted airspace around a submarine yard, amongst other offences. This low rate of legal repercussion is largely down to the difficulty in proving ownership of drones, with no enforceable, centralised database of all drones and their owners, but is also hampered by a distinct lack of research being conducted that lies within the public domain. Whether the information is suppressed by the Official Secrets Act 1989 is unclear, however, a representative of Raytheon Foreground, at the Cyber Security Conference 2016, stated they did in-house research. Given their background in military technology, this is probably where their interests

lie rather than in forensic applications. The same was said by various company representatives at the Forensics Expo Europe 2017 and Security and Counter Terror Expo 2017. Drone Protect, a system offered by Quantum Aviation was one such system used to track drones and alert users of drones within its effective range (Quantum Aviation, 2017). They claimed the system works against all UAV systems. Aaronia offers a much more in-depth system for both tracking and jamming UAV systems and has the capacity to be used as a targeting system for counter drone weapons systems (Aaronia, 2017). Again, neither of these companies offer a UAV forensics service and their services are predicated on the idea that people only want to detect, jam or destroy drones. Other well-known providers of counter UAV systems include Raytheon, General Atomics and BAE Systems, though they cater exclusively to governmental clients. The costing of these countermeasures is also well outside of the price range for all but the largest of companies and, in the case of weapons systems, governments, military forces and private military companies. That's not to say these systems are ineffective, they are clearly highly effective at mitigating the UAV threat, but using a £2.5 million Missile Defence System to destroy a $200 drone is simply overkill and removes any chance of a forensic evaluation of the drone (Baraniuk, 2017). A range of other, less technological, solutions to counter UAVs are available and, aside from snagging the drone with a large net on a pole, they largely involve shooting the UAV out of the air, either with a traditional firearm such as a shotgun or rifle, or by launching a net type device from a firearm and includes the AMTEC SkyNet, a shotgun launchable net (Cox, 2017) and X Products "Can Cannon" firing a prototype folding net (The Firearms Blog, 2015). The SkyNet is having limited success due to a short range and poor net deployment but the Can Cannon appears to work well and would only require a soldier in the field to carry an additional AR15 style upper receiver, weighing about the same as an under-barrel grenade launcher. There are also a number of prototype net shells available for 40mm under-barrel grenade launchers in the NATO standardised 40x46mm and 40x53mm configurations that are being trialled with varying results.

Legalities aside, these options all have one significant downside, the definite or potential destruction of the UAV, removing any chance at investigation.

✳Drone Offences Within The UK

It is not uncommon to hear about sporadic incidents of UAVs being misused in local and national media and it is important to understand what offences can be committed by a UAV pilot. Specific offences that a UAV pilot can commit are largely listed in the Civil Aviation Authorities documentation entitled "CAP 722" (Civil Aviation Authority, 2015). These largely apply to larger, commercial drones, which exceed the 20kg limit or are being used for commercial purposes. The first article of note for the purpose of investigating these smaller kinds of drones is article 138 which prohibits the controller from *'recklessly or negligently causing or permitting an aircraft to endanger persons or* property'. Flight can only begin once the operator is satisfied that the flight can be made safely and the controller must maintain line of sight with the UAV under articles 166 (2) and (3) respectively. If the UAV is fitted with a camera there are additional rules the pilot must follow, under article 167, which places limitations on where the drone can fly including within 150 metres of any congested area or open-air gathering of more than 1000 people and within 50 metres of person other than the controller and also any vehicles or structures which the pilot has no control over. As well as these specific offences, a pilot can commit other offences found in general law, such as offences under Section 97 of the Sexual Offences Act 2003, specifically relating to voyeurism. Assault is also possible if the UAV collides with a person as is harassment by causing distress or alarm under the Harassment Act 1997 and, if property is damaged a pilot can be charged under the Criminal Damage Act 1971, all of these offences can also cause the pilot civil liability issues resulting in a lawsuit being filed against them. Lastly, there is some provision for UAVs being used to gather personal information by spying on people, although the UK government has not put legislation directly in place to protect personal privacy. The Information Commissioner's Office has put out some guidance around the use of drone cameras under their CCTV guidelines and what kind of information you can keep and what you must destroy (Information Commissioner's Office, 2015).

Methodology

All digital forensic investigations are subject to strict guidelines on how investigations should be carried out. This is to maintain evidence viability and is broadly broken up into four key principles.

Principle 1	No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
Principle 2	In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions
Principle 3	An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle 4	The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

It is these four key principles that form section 2 of the Association of Chief Police Officers "Good Practice Guide for Digital Evidence", that will be stuck to during the forensic investigation of the UAV, except where Principle 2 must be broken in order to obtain evidentiary information. (Association of Chief Police Officers, 2012)

- **Firstly, Some Assumptions**

Before conducting any kind of experimentation evidence gathering processes the experimentation assumes the following:

1. The UAV was recovered in full working order with no modification to either the UAV or its underlying systems
2. The controlling devices were recovered with no damage
3. The controlling mobile devices either have no PIN code set or you have access to the PIN code
4. The controlling device had the Drone Academy function disabled as it clearly states it tracks flight data and uploads it to Parrot servers
5. JTAG/Chip-off acquisition of data was not considered as a part of this investigation due to the potential for permanent damage to the UAV

- **Challenges Regarding Forensic Investigation**

As so little research has been publicly conducted on UAVs, it is first necessary to assess the potential problems around analysing the UAV and controllers by assessing the methods which can be used to connect directly to the device.

- **Acquisition of Data**

As noted previously, it is often difficult or convoluted to gather the evidence from a UAV as one of the core pillars of modern digital forensics is the acquisition of data on digital storage. In the case of UAVs, this is not always simple, as noted. Access is restricted to the media directory via a direct connection and so establishing a viable method to extract the

onboard data is required. Some forensic imaging software allows for imaging across a network, however, these were of no use when imaging the Bebop.

Its poor battery life hampered such a long extraction method and the only portions to be imaged were taken from the media directory. Telnet and FTP are viable methods of collecting evidence in closed environments where a full image is not possible. Additionally, it is necessary to image the controlling devices, in this case an iOS device, an Android device and the bespoke Skycontroller. This necessitates the inclusion of mobile forensic techniques being used on the iOS device, an iPhone 5C, and the Android device, an Asus Nexus tablet. The Skycontroller is something of a mystery here. It is running an unknown operating system and has both a USB port and micro USB port on the left-hand side, it also possesses an HDMI connector, allowing the device to be connected to a monitor or headset.

- **Acquiring Flight Data**

In an ideal world, all UAV flights would be monitored by a centralised GPS system and allow for easy acquisition of flight data to help in an investigation. This is not the case, unfortunately, and it is down to each of the drone manufacturers to enforce their own forms of recording flight data, particularly start and end points, as well as the route taken where possible, as well as altitude data, particularly as the UAV can go to places a normal person on foot cannot. This kind of information is crucial in cases of flying in restricted airspace as well as important in cases of voyeurism where no other data can be easily recorded. There are two key considerations to take into account when looking for flight data, the make and type of UAV and where the data is stored. No two manufacturers' UAVs work in exactly the same way, it is possible that the device does not record flight data even if every other manufacturer's UAVs do. If the UAV does store flight information, how or where it stores it will also differ between platforms and even the type of control used. It could be stored on the controlling device, it could be stored on the UAV, it could be on both.

- **Media Stored on the Device**

If the UAV has a camera, as many do, where and how is the information stored on the device? Is it stored directly on the device or on a removable SD card or other forms of removable flash memory? If it has image storing capability what metadata is stored within the images and video taken? Do they contain geolocation tags? Does it store media directly on the controller or maintain

a copy on the device itself? All of these are key questions that need to be addressed in order to establish as much information as possible in regard to the UAV's activities and can even pair up with GPS data where available.

- **Establishing Ownership**

The biggest problem with UAVs is proving who they belong to. As there is no centralised system for registering the UAV, it may not be possible to easily confirm ownership of the drone. And even if registered it may still not be possible due to differences in international law.

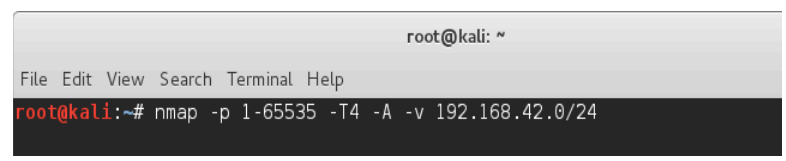
Initial Assessment of the UAV

- **App Connectivity to the UAV**

The UAV connects to controlling smartphone devices and the Skycontroller via Wi-Fi. It's possible to choose the band and channel in use via the FreeFlight Pro app (formerly FreeFlight 3), though it defaults to the 2.4Ghz band using channel 11. There is no password set by default so it is possible to connect any Wi-Fi compatible device to the UAV, though there are options available to set WPA2 passwords. By connecting a computer or any device capable of displaying network information to the UAV, you can obtain the default IP address, 192.168.42.1. This has been the default information for all three Parrot drones tested, the Bebop used for much of the assessment, as well as a Bebop 2 and a Parrot SenseFly Albris.

- **Wireless Network Assessment**

The UAV connects to its controller via a Wi-Fi network, which enables the network to be scanned much like any other network using a mapping and scanning tool such as Nmap.



Nmap was highly useful in viewing what services are available and revealed that the drone ran a very outdated form of BusyBox, specifically v1.20.2, released 17th May 2006 (Denys Vlasenko/BusyBox, 2002). Initially, the list of services available was limited and the only connection that could be maintained was an FTP connection, which differed from what David Robinson had stated in his DEFCON 23 talk. Concluding that this was because the UAV he tested had an older version of the software or

operating system, the UAV was rescanned in developer mode. After enabling the developer mode on the UAV, by pressing the power button four times in quick succession after the UAV was powered on, a much wider range of connections became available, including Telnet (Parrot, 2015). Neither of these services required any form of authentication. It is worth noting that port 22 is closed, even in developer mode, meaning SSH is not possible, removing the ability to use SFTP to securely transfer files. Looking through the Nmap log also showed that the UAV had DHCP enabled. This means that potentially any number

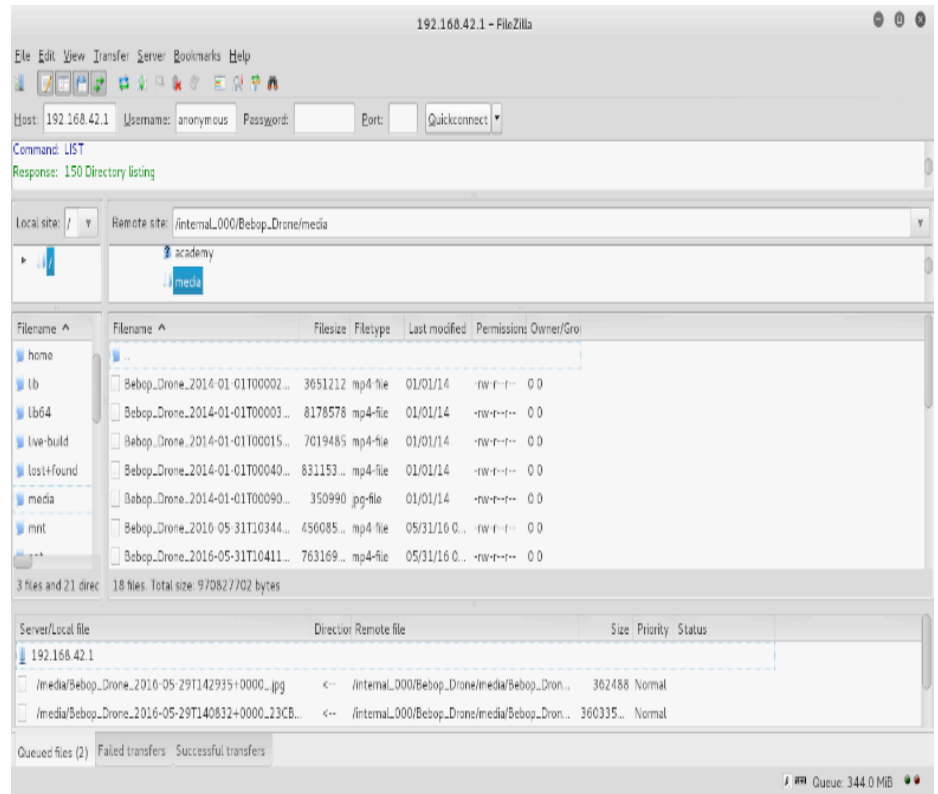
```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Nmap scan report for 192.168.42.247 [host down]
Nmap scan report for 192.168.42.248 [host down]
Nmap scan report for 192.168.42.249 [host down]
Nmap scan report for 192.168.42.250 [host down]
Nmap scan report for 192.168.42.251 [host down]
Nmap scan report for 192.168.42.252 [host down]
Nmap scan report for 192.168.42.253 [host down]
Nmap scan report for 192.168.42.254 [host down]
Nmap scan report for 192.168.42.255 [host down]
Initiating SYN Stealth Scan at 15:09
Scanning 192.168.42.1 [65535 ports]
Discovered open port 21/tcp on 192.168.42.1
Discovered open port 23/tcp on 192.168.42.1
Discovered open port 44445/tcp on 192.168.42.1
Discovered open port 61/tcp on 192.168.42.1
Discovered open port 9050/tcp on 192.168.42.1
Discovered open port 51/tcp on 192.168.42.1
Completed SYN Stealth Scan at 15:09, 8.58s elapsed (65535 total ports)
Initiating Service scan at 15:09
Scanning 6 services on 192.168.42.1
Stats: 0:01:52 elapsed; 254 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 15:12 (0:00:51 remaining)
Completed Service scan at 15:12, 136.17s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against 192.168.42.1
NSE: Script scanning 192.168.42.1.
Initiating NSE at 15:12
Completed NSE at 15:12, 31.26s elapsed
Initiating NSE at 15:12
Completed NSE at 15:12, 0.01s elapsed
Nmap scan report for 192.168.42.1
Host is up (0.0013s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        BusyBox ftpd (D-Link DCS-932L IP-Cam camera)
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| total 4
|_drwxr-xr-x    8 0        0             4096 Jan  1 00:01 internal_000
```

The Nmap output from the Bebop UAV in developer mode

of devices could be connected simultaneously.

This also means the UAV is susceptible to deauthorisation attacks, such as those possible with the Aircrack suite of Linux tools, allowing a drone to be stolen directly out of the air if no authentication is applied and the hacker has connected an additional device capable of controlling the UAV.

- **Wireless Network Services**

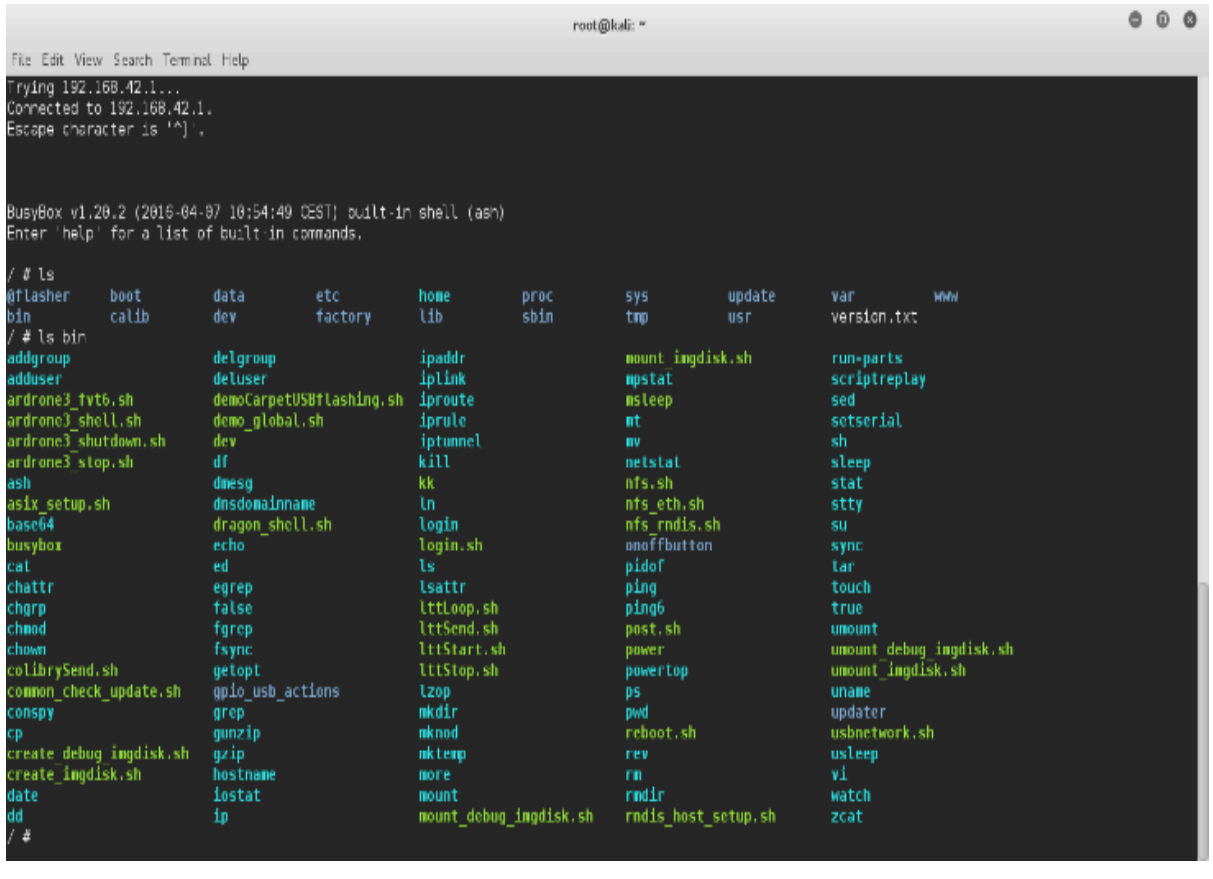


FTP using Filezilla

As noted, it is possible to use both FTP and Telnet to establish a direct connection to the UAV and neither of these require any further authentication in order to establish the connection. This causes some interesting conflicts in obtaining and proving evidentiary sources as it is perfectly possible to upload files directly to the UAV via its FTP server, even if it is not the controlling device. There is some limitation on what files can be uploaded, however, as the UAV will not accept any files in

the media directory that are not in the jpg or mp4 formats.

Located within the FTP directory are several important directories. The first of these is located at /internal_000/flightplans. This directory is used by premium features of the Freeflight Pro app to record any flight plans made in the app or manually uploaded at a later date. The contents of this directory are not covered in this document. The next of these is the /internal_000/log directory which stores logged flight data produced by flight plans and by the Drone Academy function. Next, also within the interal_000 directory is the scripts folder. This is useful for a number of reasons, firstly it allows for a user to upload shell scripts to the UAV which, when triggered, can produce all manner of effects from synchronised flying in conjunction with other UAVs to sporadic back flips and even allow for a total shutdown of the UAV, simply dropping it out of the air. The next set of directories of note is the /internal_000/Bebop_Drone/ subfolders, the academy and media subdirectories specifically. The academy directory is used in conjunction with the Drone Academy expansion to the Freeflight Pro app to record all flights made by the UAV. For the purpose of the investigation, this function was disabled, however, a sample of the file it produces for each flight will be analysed in the Forensic Investigation section. The media directory is, as its name implies, the location where all media recorded by the UAV is stored, including video and still photographs.



A view of the telnet connection to the UAV

This is an essential directory for the purposes of investigating the device as it potentially contains substantial amounts of information on where the drone has been flying and, potentially, a view of the pilots' face.

Telnet is another available method of connecting to the drone. Telnet provides a lower level access to the drone's internal system files. A number of directories are made available through telnet, including the FTP directory (located at the data/ftp/internal_000/Bebop_Drone/media directory). Telnet was previously wide open and in the event this is still the case for a drone, or the user is flying it in developer mode, it opens up a range of possible exploits a hacker could use. The /bin directory holds a number of useful scripts and commands a hacker could use including the ardrone3_shutdown.sh script which causes the drone to suffer a non-graceful shutdown, literally dropping out of the air. This can be expanded using the "more" command and then copy and pasted into a new script file and then reuploaded into the FTP script directory. This allows for remote shutdown of any of the Parrot drones tested, a serious security flaw that could be readily exploited by law enforcement or those looking to prevent drone access to a particular area. Other useful commands include `fdisk -l` which lists two 4MB partitions, used as boot partitions and an 8GB user data partition.

- **Direct Connection via USB**

Directly connecting the device via the included USB cable, through a forensic write blocker, only allowed access to the media directory, much like a digital camera, when powered on (located via Telnet at data/ftp/internal_000/Bebop_Drone/media), which is less than what is available via FTP, however, it makes for a better forensic acquisition of media files stored on the UAV as there is much less chance of media corruption or accidentally changing the data stored, as well as allowing for a forensic image to be made of the media directory using traditional computer forensic tools such as EnCase or FTK. Interestingly, it is also possible to mount an external USB flash drive via a micro USB adapter if it's plugged in before powering on the device and can be shown using fdisk -l via telnet.

Forensic Examination of UAV and Controllers

- **Accessing the UAV and Acquiring Data**

In order to connect to the UAV, it has to be powered on, which has the problem of potentially limiting data integrity if specific guidelines are not adhered to. Turning on the

UAV requires a single press of the power button, accessing telnet requires pressing the power button four times in quick succession after the UAV is powered on and if the examiner presses and holds the power button for 10 seconds will perform a factory restoration of the device.

As noted previously, a direct USB connection only presents the UAV's 'media' directory and files can be copied as if it was a USB flash drive, however it cannot be imaged using standard imaging tools such as FTK Imager. The only way to gain evidentiary copies of files is by connecting to the UAV via its wireless network. In this instance, the SSID was BebopDrone-F069739, though, as with encryption methods, this can be set by the user. As noted previously, the UAV has an IP address 192.168.42.1 and it's this address that is used to connect via FTP and Telnet. FTP can be used to transfer all media files onto a drive for further examination using a tool such as WinHex. Telnet allows access to the complete operating system of the UAV but does not allow for the movement of files between the UAV and a device that can be used for analysis, even those stored under the /data/ftp/internal_000 directory used by FTP.

As noted previously, the UAV runs BusyBox, which means that, under telnet, a range of commands are available. The command 'fdisk -l' reveals three portions of internal memory, a user data partition that's a little under 8GB in size and two 4MB system boot partitions. If an examiner connects a forensically wiped USB stick larger than 8GB, using a Tableau system for example, to the UAV via its micro USB port using an adapter and then powers on the device, it is possible to see this new stick mounted to the device using the fdisk command. Once mounted, it's possible to use the 'dd' command, literally data duplicator, to clone all of the data from the 8GB partition onto the wiped memory stick, however, unlike when accessed via FTP, it also copies all of the deleted files raw, hexadecimal, data allowing deleted data to be acquired. This is useful if the individual controlling the device was able to maintain connection to the UAV and delete the files using the app, but, again, it does not copy any operating system data, only those in the media directory. This is down to restrictions put in place at the firmware or level of the device. Unfortunately, via telnet, even the underlying operating system files are of limited evidentiary use, though there is a single file useful in establishing a connection between controllers and the UAV, which will be discussed later.

In Graeme Horsman's article "Unmanned aerial vehicles: A preliminary analysis of forensic challenges" he claims that it is necessary to examine the system data because a user could move files onto the drone via FTP, then use telnet to move the files into system folders to hide them. This was found to not be the case during this investigation, any attempts to write files to the system partitions ended in failure. That is not to say that this is not possible, simply that the methods tried during this investigation did not work and so by failing to analyse files on the system partitions, an examiner may miss important, potentially hidden, files and thus vital evidence.

It's possible to see what FTP and telnet actions have been performed on the UAV by viewing the '.ash_history' file in the root telnet directory, using the 'ls -a' command to view hidden files and then the 'more' command to view file contents. This file will show all file uploads, downloads and telnet actions performed. This file is live, however, and so will show actions performed by the examiner and potentially overwrite existing commands in the file.

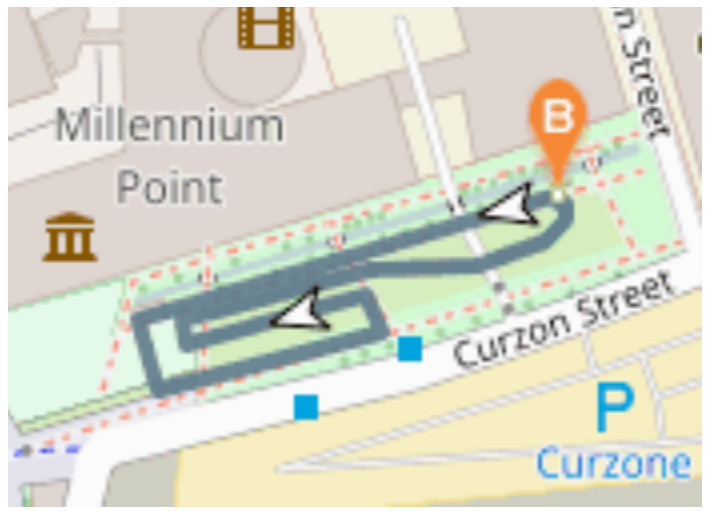
- **Accessing and Investigating Flight Data**

This kind of information is key to proving if an offence could have been committed involving a UAV, unfortunately, the Bebop only stores flight information on the device when the academy function is active. As it clearly advertises that this tracks the user's flight data, it's unlikely that a criminal with any intelligence will have this function enabled, however, analysis of the flight data files will be presented here, just in case.

The Bebop stores flight details in the pud format which, as a side note, is the same extension used by WarCraft to store in game maps under Windows but contains different file headers and contents. This could offer a technically competent criminal the ability to remove and hide their flight data in an innocuous looking way on their personal computer.

These files are generated every single time a device running the FreeFlight app connects to the UAV and initiates a flight and are named for the time and date at which the flight took place followed by a character string, for example 1151_2017-02-15T135541+0000_74C2C.pud determines that a flight started at 11:51 on the 15th February 2017. The purpose of the trailing characters following the time and date is unclear as they do not appear within the pud file anywhere and the flight immediately following this had the file name 1153_207-02-15T336541+0000_A565FC.pud.

The contents of these pud files is highly useful in establishing both ownership and the controlling application used during the flight. The file begins with a header section detailing the UAV's serial number, the type of device controlling the flight, such as iPhone, followed by the controller application, which for iOS devices is com.parrot.freeflight3, even when using the newer FreeFlight Pro application. Following this, the file defines all of the following attributes clearly with headers to break down internal metadata stored within the file. Each section of metadata is 77 bytes long and records nine details regarding the UAV's flight. A full analysis of this can give a highly precise map of the UAV's movements and the controller location using North and West orientated latitude and longitude (see appendices 1 for a full reference). This information can then easily, and accurately, be plotted onto a map. This allows for a visual representation of the route to be used in court. Interestingly, the pud file does not keep this flight information on a fixed time basis, for example every five seconds. The pud file analysed showed intermittent jumps of between 2 and 12 seconds before readings were taken during the flight.



- **Analysis of Media on the UAV**

As noted previously, media is stored in the FTP directory and can be accessed easily by connecting a device to the UAV and downloading files to a sanitised flash storage device. The Bebop is capable of capturing 1080p video and 14 megapixels stills whilst in use. By default, it stores images using the universally accepted JPEG format with the jpg extension, though there is an option available to use the Adobe raw format dng. The UAV is only capable of recording video in the .mp4 format. The UAV also maintains a thumbnail image folder under the Bebop_Drone/thumb directory, which also stores the first frame of any video recorded.

All photos taken by the UAV contain highly detailed EXIF metadata, which have the potential to be of significant use during investigation. For

the purpose of brevity, the full list of attributes available is listed under appendices 2, however pertinent information that is extractable includes file MAC details (Modification, Access and Creation), specific information about the camera used including the encoding used, the manufacturer and model, crucial GPS information that may only be available from this source in the event Drone Academy is not enabled. Interestingly, if the UAV takes off without a valid GPS connection but gains one mid-flight it does not tag the photos with the GPS location and instead sets both GPS values to 500° 0′ 0.12″ using North/East rather than the North/West used when GPS is initially available, it also sets the altitude to 500 metres and results in a much shorter EXIF data set when analysed. The video files maintain no metadata beyond file MAC data.

- **Confirming Ownership**

Proving a suspect owns and has used the UAV is perhaps the most important part of the investigation in order to prosecute. Under ideal circumstances, both the controller and UAV will have been seized and it is simply a case of showing the devices have been paired. Performing a search on the UAV after extended flying revealed no hits for any controlling device information stored in any files on the UAV, apart from in the pud files where they are generated. In order to pair the two devices requires pairing the UAV's serial number, wireless network name (also called an SSID) and MAC address (also called a BSSID), all of which are viewable in the FreeFlight Pro app and in the UAV's telnet directories with the serial.txt file located under the root directory, SSID under /etc/hostname and MAC address in the /factory/mac_address.txt directory to the controlling device.

Forensic Examination of Controlling Devices

The Parrot Bebop can be controlled by a number of utilities, an Android device, an iOS device or the bespoke Skycontroller. The Freeflight Pro app, formerly Freeflight 3, has been downloaded between 1 and 5 million times from the Google Play store alone. The most recent version of the app was installed on both an iPhone 5C running iOS 10.1 and an Asus Nexus 7 tablet running KitKat 4.4.4. After a test flight was conducted with each controller, they were imaged using both XRY and Cellebrite.

- **Skycontroller Analysis**

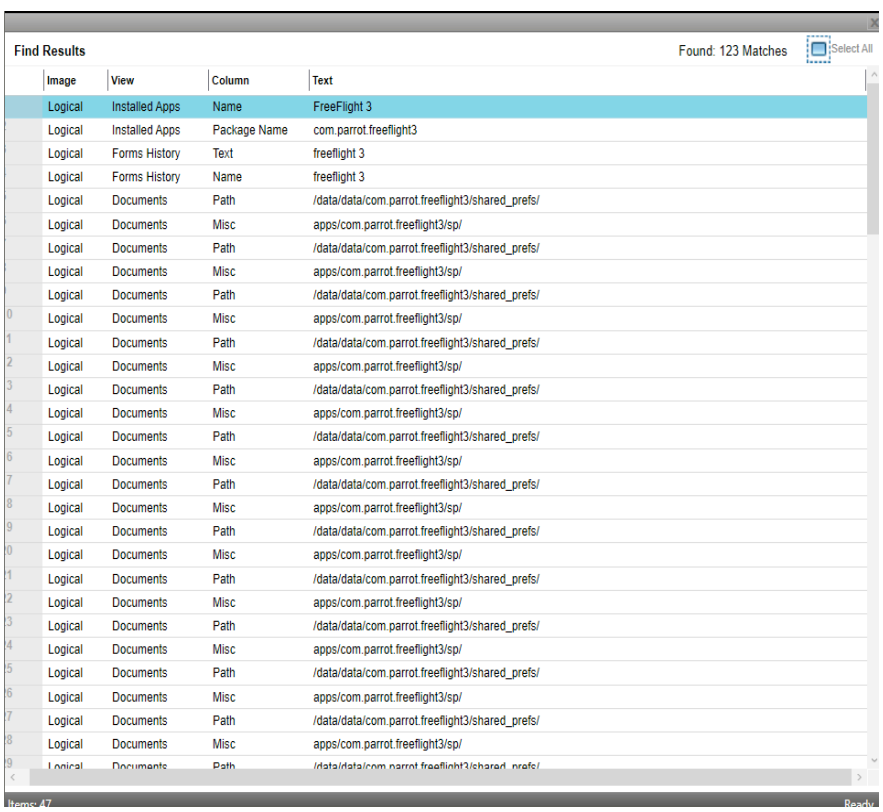
Utilising the onboard USB and HDMI connectors to connect a USB keyboard and monitor to the Skycontroller revealed that the Skycontroller ran

Android with the majority of full Android functionality. Attempts were made to image the Skycontroller using both XRY and Cellebrite, however, it was not possible to have the computer running the software see the Skycontroller when plugged in, even under Airplane and USB modes.

- **Analysis of Mobile Controllers**

Given the relative cheapness of Android devices compared to iOS devices, they are seen as more disposable and a better option for someone who may need to ditch the phone as a result of criminal activity, however, iPhones are also thought of by many to be more secure and they are still common handsets despite only making up around 20% of the handsets in use, compared to Android's 75% (Williams, 2016).

- **Accessing and Investigating Flight Data**



Find Results — Found: 123 Matches — Select All

Image	View	Column	Text
Logical	Installed Apps	Name	FreeFlight 3
Logical	Installed Apps	Package Name	com.parrot.freeflight3
Logical	Forms History	Text	freeflight 3
Logical	Forms History	Name	freeflight 3
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/
Logical	Documents	Path	/data/data/com.parrot.freeflight3/shared_prefs/
Logical	Documents	Misc	apps/com.parrot.freeflight3/sp/

An XRY examination of the Android device showing 123 results regarding the FreeFlight app

After installation, all user generated app data is stored under the /data/data/com.parrot.freeflight directory on the device and, just like on the UAV, it maintains a listing of pud files if the academy feature is enabled, detailing flight information in exactly the same format as those stored on the UAV. An examiner can then read the information stored in the pud files to associate the two flights and devices using the serial.txt information stored on the UAV as detailed previously.

As with Android iOS also has a repository for pud files when recorded. These are found under the /Applications/com.parrot.freeflight3/Documents/academy directory and can be extracted, viewed and analysed in exactly the same way as under Android or when taken directly from the drone. Unlike the Android device, however, the iOS app generates numerous other files which can be viewed and read to obtain flight information. Most importantly amongst these are the json.log files generated every time the UAV flies. Much like the pud files, this stores a range of information about the flight including GPS information on the flight. The information in one of these log files matches perfectly with the previously plotted pud file and so provides an analyst the opportunity to extract GPS information from the UAV even when Drone Academy is disabled. This is a substantial

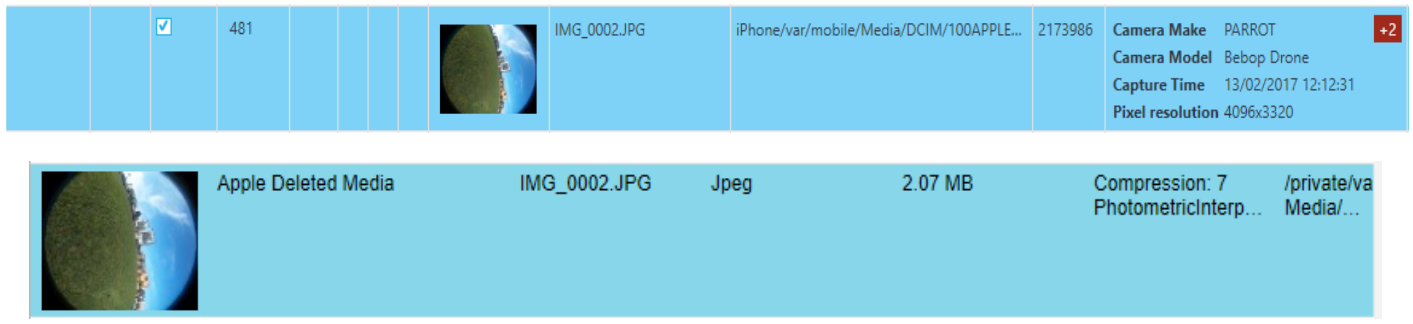
forensic boon over the files found on Android devices and allows for tying UUIDs created to any images taken.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	7B	20	22	76	65	72	73	69	6F	6E	22	3A	20	22	31	2E	{ "version": "1.
00000010	32	22	2C	20	22	73	6F	66	74	77	61	72	65	5F	76	65	2", "software_ve
00000020	72	73	69	6F	6E	22	3A	20	22	33	2E	33	2E	30	22	2C	rsion": "3.3.0",
00000030	20	22	68	61	72	64	77	61	72	65	5F	76	65	72	73	69	"hardware_versi
00000040	6F	6E	22	3A	20	22	48	57	5F	31	31	22	2C	20	22	64	on": "HW_11", "d
00000050	61	74	65	22	3A	20	22	32	30	31	37	2D	30	32	2D	31	ate": "2017-02-1
00000060	33	54	31	33	31	34	31	37	2B	30	30	30	30	22	2C	20	3T131417+0000",
00000070	22	70	72	6F	64	75	63	74	5F	69	64	22	3A	20	32	33	"product_id": 23
00000080	30	35	2C	20	22	73	65	72	69	61	6C	5F	6E	75	6D	62	05, "serial_numb
00000090	65	72	22	3A	20	22	50	49	30	34	30	33	33	38	41	48	er": "PI040338AH
000000A0	35	46	30	36	39	37	33	39	22	2C	20	22	70	72	6F	64	5F069739", "prod
000000B0	75	63	74	5F	6E	61	6D	65	22	3A	20	22	42	65	62	6F	uct_name": "Bebo
000000C0	70	20	44	72	6F	6E	65	22	2C	20	22	75	75	69	64	22	p Drone", "uuid"
000000D0	3A	20	22	33	37	35	30	33	35	46	38	31	37	33	30	44	: "375035F81730D
000000E0	38	45	32	36	32	37	37	32	42	31	42	44	43	42	45	39	8E262772B1BDCBE9
000000F0	36	31	39	22	2C	20	22	72	75	6E	5F	6F	72	69	67	69	619", "run_origi
00000100	6E	22	3A	20	30	2C	20	22	63	6F	6E	74	72	6F	6C	6C	n": 0, "controll
00000110	65	72	5F	6D	6F	64	65	6C	22	3A	20	22	69	50	68	6F	er_model": "iPho
00000120	6E	65	22	2C	20	22	63	6F	6E	74	72	6F	6C	6C	65	72	ne", "controller
00000130	5F	61	70	70	6C	69	63	61	74	69	6F	6E	22	3A	20	22	_application": "
00000140	63	6F	6D	2E	70	61	72	72	6F	74	2E	66	72	65	65	66	com.parrot.freef
00000150	6C	69	67	68	74	33	22	2C	20	22	70	72	6F	64	75	63	light3", "produc
00000160	74	5F	73	74	79	6C	65	22	3A	20	2D	32	2C	20	22	70	t_style": -2, "p
00000170	72	6F	64	75	63	74	5F	61	63	63	65	73	73	6F	72	79	roduct_accessory

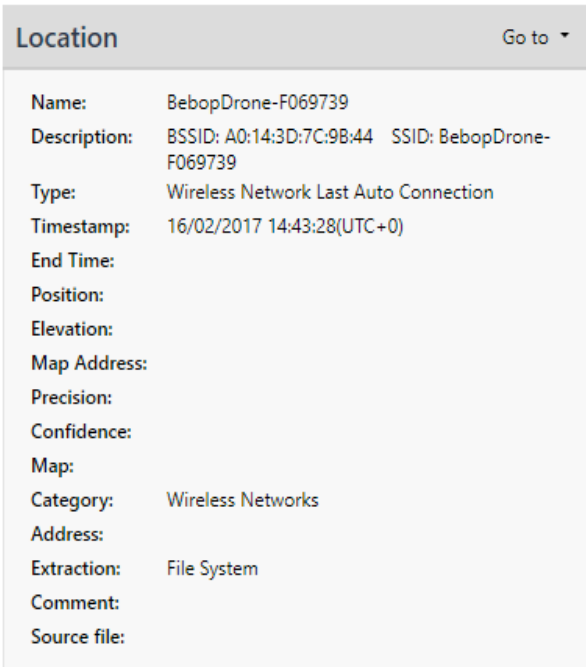
• Analysis of Media on the Controller

As noted previously, the UAV is capable of capturing media whilst in flight. It is also possible to save media directly onto the device controlling the UAV and then delete them from the UAV and so any visual evidence of illegal activity may only exist on the controlling handset. As noted previously, the still images contain extensive EXIF data, a full break down of which can be found in appendices 1.

This media is stored in the /data/media/0/DCIM/Bebop Drone/ directory on Android devices and /Media/DCIM/100APPLE/ on iOS devices. It is the UUID information stored in these files than can be tied to individual flights. As an aside, Cellebrite did not mark a deliberately deleted image as such, whereas XRY did.



- **Tying a UAV to a Controller**



It is actually very simple to connect a UAV to its controlling handset. The UAV is simply a flying access point and the network is viewable in an XRY or Cellebrite extraction of the file system. It clearly shows the network name, BSSID and SSID as well as the time stamp for the connection, the only difference being Cellebrite displays each instance of connection whereas XRY shows them under a single header. Further surety can be gained by comparing this time stamp with that of any stored media or GPS information. Another option to tie the two together can be found at the /data/data/com.parrot.freeflight3/shared_prefs directory which stores the DEVICECONTROLLER_SHARED_PREFERENCES_KEY.xml file in Android and contains the serial number of the last drone connected. This is contrary to Graeme Horsman's work which states there is an "ARInformationsSettingsLastConnectedDrone.xml" file located here. His work also references a MainARActivity.freeflight3_arutils.xml which cannot be located anywhere under both the Cellebrite and XRY extractions.

Under iOS, a forensic practitioner can use the json.log files generated to tie a UAV to a device, as mentioned previously. Analysts can also use the com.parrot.freeflight3.plist file located under the /Applications/com.parrot.freeflight3/Library/Preferences/ directory to display the serial number of the last UAV connected to the iOS device.

Evidentiary Problems

After experimenting with unusual ways to manipulate evidence gathering, a number of issues became rapidly apparent; time and date stamps were relatively easy to change, the UAV possesses as remote factory reset function, issues around the GPS, some of which have been noted previously, and lastly modifications made to the UAV.

- **Time and Date Stamps**

By changing the time and date on the controlling device, it was readily possible to manipulate the time and dates generated by media files generated. By simply rolling the clock backwards one week all of the newly generated file information displayed an out of date and out of sync time and date stamp.

- **Factory Restore**

There are two different ways to initiate a factory reset of the Bebop UAV, either by holding the power button on the UAV for 10 seconds or by remote via the app. On testing, this factory restore completely wiped all information from the UAV and rendered it unrecoverable. Even using forensic imaging tools and the dd command via telnet, all of the previously generated flight data files, images and video were completely removed from the device. This clearly shows that controller initiated resets of the device pose a serious risk to forensic evidence gathering ability. Where possible, devices should be disconnected from their controller immediately, perhaps using a short-range signal jammer or a device running the Aircrack deauthorisation script, before the device can be powered down and analysed.

- **GPS**

```
 0.000000 ], [ 4
5, 0, 16.766600,
 03.002600, 0, 0
, 0, true, 500.0
00000, 500.00000
0, 0, 0, 0.00000
0, 0.000000, 0.0
00000, 0.000000,
 0.000000, 0.000
000, 0, 0, 0.000
000 ], [ 53, 0,
-1.885309, 52.48
2465, 1, 0, 0, t
rue, 500.000000,
```

GPS information plays a key part in the analysis of UAV crimes, unfortunately it is very easy to modify or remove this information, both tricking the onboard GPS and the controller GPS from location services. A simple foil strip was capable of blocking the UAV from receiving any GPS data but flying it anywhere with tall, largely metal structures nearby works equally well. Even when

out in the open, the onboard GPS chip often struggled to receive a GPS signal, only obtaining one mid-flight. This is reflected in the pud files as 500.00000, 500.00000, an impossible location.

It was also possible to spoof the handset location using both GPS spoofing applications and VPN services. Interestingly, using onion routing services rendered the UAV unable to take off and, if triggered mid-flight, caused the UAV to maintain connection with the handset but unable to accept commands from the handset. These changes are reflected both in the pud files, where applicable, and in the json files, as evidenced in figure 11 where the drone spent the first 45 seconds of flight in Timbuktu before disabling the app returned it to Birmingham, a 3,700-mile journey in just 8 seconds.

- **Modified Devices**

Parrot provides a software development kit (SDK) that can be used to add functions to a UAV and change underlying features, settings and parameters. This investigation was conducted in an out of the box state, however, knowledge of such modifications maybe essential if the UAV is in a non-standard configuration or has had scripts applied via FTP that cause the UAV to behave in a particular manner on start up.

Further Discussion

It's probable that the use of civilian UAVs will increase as the price goes down and this will cause major regulatory issues. The House of Lords called for a registry to list all the UAVs, which would contain identifying information regarding UAVs and, potentially, enforce GPS tracking of all UAVs (House of Lords European Union Committee, 2015). This kind of system would certainly allow for drones to be easily paired with their owner and act as a deterrent, but only if they were registered. Increasing use of enforced geofencing and no fly zones may provide a better deterrent, particularly where there are passenger planes in the airspace and around prisons. This is not an option without flaws. As shown, it is relatively simple to disrupt, change or entirely block GPS from connecting to the drone allowing it to fly anywhere and it cannot be enforced everywhere as it would stop innocent or potentially licenced use. Another potential option would be to enforce training schemes, much like the UKARA licencing system for airsoft weapons in which those without the correct credentials are limited in what they can purchase. This could remove those UAVs with the potential to film high resolution video of children or lift loads in to prisons the ability to do

so without there being a direct correlation between the UAV and the pilot. This could also be used to increase awareness of the laws around UAV usage and enforce a training program to remove any pretext of not knowing what the regulations are.

If UAV usage continues at its current, escalating, rate it is likely that the number and variety of UAVs available will also grow. This means that a constant chain of research and education is required in order to properly equip forensic examiners with the skills needed to analyse different UAVs and may even give rise to those specialising in a particular brand of UAV; for example, a department may have somebody who deals exclusively with Parrot UAVs and another whose sole job is dealing with Yuneec or DJI UAVs. It is fortunate that all UAVs have some principles that are unlikely to change in the foreseeable future, such as; wireless connection type, Bluetooth on cheap drones and Wi-Fi on more expensive models, and the use of flash storage, whether on board or on an SD card, as is the case with DJI UAVs. The increased use of better quality cameras is also likely to persist, with the price and size of 4k cameras coming down greatly over the last 12 months. Flight data will always be the core of any UAV investigation and something that will have to be assessed on a case by case basis, dependent upon the devices seized. Given the rise of cheaper cameras and more available UAV technology it is arguable that the ability to share media straight to social media and tagging locations where video and stills were taken is a "must have" feature for those looking at buying a UAV for personal use and so flight data should become more and more abundant as time rolls forwards with the technology.

In 2015, Graeme Horsman reiterated the thoughts of Michael Robinson in 2012 that UAV technology is still in its infancy and it was difficult to predict what the future of the technology would hold. So far, it has been much of the same. Better motors, better batteries, better antennae, smaller form factor and better connectivity with more features. That's not to say the technology has not progressed. Since 2012, UAVs with gimbal mounted cameras have dropped dramatically in price, many now costing less than £1,000, what was once a £3,000 professional grade UAV like the DJI Phantom 3 is now a little under £500 at most retailers. The technology is smaller and faster and costs less, but unfortunately, it is this that could also fuel a rising need for those forensic practitioners capable of UAV analysis. It is of vital importance that the knowledge on how to analyse UAVs is

made available to those who need it. There needs to be a focus on evidentiary integrity, connection methods and the analysis of the UAVs underlying systems and software to better extract relevant system files and artefacts across a much larger sample than a single Bebop UAV before any guidance aimed towards best practice is considered. Certainly, publishing pieces on individual UAVs could lead to interesting discoveries but the demand for analysis and the software development often outstrips the publishing of any material in what needs to be a priority of future digital forensic research if drone usage proliferates at its current rate.

Conclusion and Further Work

As UAV usage increases, so too will the number of people misusing them, particularly as the technology develops and only the future knows where the technology will go next and what legislation governments will put in place to try and police their misuse. Whilst this has focussed on an individual, though prominent, UAV model, there is a whole range of devices from numerous manufacturers out there, all of which will require different techniques to examine. More work needs to be done to further evaluate the challenges faced by forensic examiners and law enforcement alike and how best to develop techniques to examine UAVs safely and in a way that generates good, usable evidence, much like in the mobile phone sector. With just two years between this work and the previous work conducted by Graeme Horsman, largely different results were found and though this is largely down to software patching and progressions in mobile operating systems, that there were such large changes in such a short space of time is clearly an issue for the industry.

There are methods of evidence gathering not even considered within the scope of this investigation, such as JTAG and chip-off forensics, which should be pursued by researchers with a detailed knowledge of those areas of digital forensics. Hopefully, this kind of research will lead to a better way to definitively tie a pilot to the UAV, even when the UAV has been dumped and the controlling device cannot be located. Further research should also be done into the controllers supplied with these devices, such as the Parrot Skycontroller. Again, this may take the form of chip off forensics or may simply be a case of mounting the internal hard drive into a forensic write blocker depending on the particular model. If the controllers work in the same way as the Skycontroller, in that they are simply a box running the Android app, it would

be expected that this would simply be a repeat of the Android analysis, though it may contain much more information, given its vastly increased size and functionality.

References

1. Aaronia, 2017. *Aaronia.de.* [Online] Available at: http://www.aaronia.com/

2. Amazon, 2015. *Amazon Air.* [Online] Available at: https://www.amazon.com/b?node=8037720011

3. Apple, 2012. *About the security content of iOS3.0 Software Update - Apple Support.* [Online] Available at: https://support.apple.com/en-gb/HT3639

4. Baraniuk, C., 2017. *BBC News.* [Online] Available at: http://www.bbc.co.uk/news/technology-39277940 [Accessed 15 March 2017].

5. Baraniuk, C., 2017. *BBC News.* [Online] Available at: http://www.bbc.co.uk/news/technology-39732485 [Accessed 27 April 2017].

6. BBC News, 2016. *Footage shows drone delivering drugs to prisoners.* [Online] Available at: http://www.bbc.co.uk/news/uk-36302136

7. Beake, N., 2015. *BBC News.* [Online] Available at: http://www.bbc.co.uk/news/uk-england-london-32431630

8. Bommisetty, S., Tamma, R. & Mahalik, H., 2014. *Practical Mobile Forensics.* s.l.:Packt Publishing.

9. Business Insider Intelligence, 2016. *The Drones Report: Market Forecasts, Regulatory Barriers, Top Vendors and Leading Commercial Applications.* [Online] Available at: http://uk.businessinsider.com/uav-or-commercial-drone-market-forecast-2015-2?r=US&IR=T

10. Campbell, M., 2016. *AppleInsider: Cellebrite again rumoured to have accessed San Bernardino iPhone 5c for FBI.* [Online] Available at: http://appleinsider.com/articles/16/04/01/-cellebrite-again-rumored-to-have-accessed-san-bernardino-iphone-5c-for-fbi [Accessed 20 November 2016].

11. Cellebrite Forensics, 2016. *Cellebrite UFED Support.* [Online] Available at: http://lang.cellebrite.com/mobile-forensics/support/ufed-supported-devices

12. Civil Aviation Authority, 2015. *CAP 722 Sixth Edition*. [Online] Available at: http://publicapps.caa.co.uk/docs/33/CAP%20722%20Sixth%20Edition%20March%202015.pdf

13. Civil Aviation Authority, 2015. *Civil Aviation Authority*. [Online] Available at: http://www.caa.co.uk/Consumers/Model-aircraft-and-drones/Flying-drones/

14. Colomina, I. & Molina, P., 2014. Unmanned aerial systems for photogrammetry and remote sensing: A review. *ISPRS Journal of Photogrammetry and Remote Sensing*, Volume 92, pp. 79-97.

15. Conger, K., 2016. *How Consumer Drones End Up In The Hands of ISIS Fighters.* [Online] Available at: https://techcrunch.com/2016/10/13/how-consumer-drones-wind-up-in-the-hands-of-isis-fighters/

16. Cox, M., 2017. *Kit Up*. [Online] Available at: https://kitup.military.com/2017/03/skynet.html [Accessed May 2017].

17. Denys Vlasenko/BusyBox, 2002. *Busybox.net*. [Online] Available at: https://busybox.net/downloads/ [Accessed 2016].

18. European Union Committee, 2015. *Parliament Publications*. [Online] Available at: http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/122/122.pdf [Accessed 1 December 2016].

19. Gettinger, D., 2016. *Drone Spending in the Fiscal Year 2017 Defense Budget*, New York: Center for the Study of the Drone.

20. Hamilton's Military Channel, 2016. *Syrian Army Hexacopter Drone Goes Down Behind FSA Lines*. [Online] Available at: https://www.youtube.com/watch?v=zM6Fay-P7eE

21. Hansen, H., 2016. *FAA report details drones flying near planes in Minnesota.* [Online] Available at: http://www.twincities.com/2016/09/27/faa-report-details-drones-flying-near-planes-in-minnesota/

22. Hoog, A. & Strzempka, K., 2011. *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices.* Waltham, MA: Elsevier.

23.Horsman, G., 2016. Unmanned Aerial Vehicles: A Preliminary Analysis of Forensic Challenges. *Digital Investigation*, March.pp. 1-11.

24.Information Commissioner's Office, 2015. *CCTV Code of Practice*. [Online] Available at: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

25.Market Watch, 2014. *Drone Demand Sizzles Heading into the Holidays*. [Online] Available at: http://www.marketwatch.com/story/all-i-want-for-christmas-is-adrone-2014-10-02

26.Osborne, S., 2017. *The Independent*. [Online] Available at: http://www.independent.co.uk/news/world/americas/small-drone-quadcopter-patriot-missile-shot-down-us-general-david-perkins-army-a7631466.html [Accessed 15 March 2017].

27.Parrot, 2015. *Telnet/ssh ports not open on Bebop*. [Online] Available at: http://forum.developer.parrot.com/t/telnet-ssh-ports-not-open-on-bebop/216

28.Parrot, 2016. *Parrot For Developers*. [Online] Available at: http://forum.developer.parrot.com/

29.Quantum Aviation, 2017. *Quantum Aviation*. [Online] Available at: http://quantumaviation.co.uk/drone-protect/ [Accessed 20 May 2017].

30.Raymond, E. S., 1996. *The New Hacker's Dictionary*. s.l.:MIT Press.

31.Robinson, M., n.d. *DEF CON 23 - Knocking My Neighbours Cruddy Drone Offline*. s.l., DEF CON.

32.Robinson, M., n.d. *LinkedIn*. [Online] Available at: https://www.linkedin.com/in/michael-robinson-062b446 [Accessed 1 12 2016].

33.Sherwood Skycams, 2016. *Yuneec Typhoon H Pro: All Saints Old Church (Lord Byron/Mary Chaworth): Annesley, Nottinghamshire..* [Online] Available at: https://youtu.be/wVgOugQCmkw

34.Sherwood Skycams, 2016. *Yuneec Typhoon H pro: Hot Air Balloon Crash at Wind Farm*

inspection!. [Online]
Available at: https://youtu.be/fV2TrCnuDf4

35. Smith, D., 2010. *DEFCON 18 Digital Forensic Methodology*. [Online]
Available at: https://www.defcon.org/images/defcon-18/dc-18-presentations/DSmith/DEFCON-18-Smith-SPM-Digital-Forensic-Methodlogy.pdf

36. Stotts, L. B., Karp, S. & Aein, J. M., 2014. The Origins of Miniature Global Positioning System-Based Navigation Systems. *IEEE Signal Processing Magazine*, 14 October, 31(6), pp. 114-117.

37. The Firearms Blog, 2015. *The Firearms Blog*. [Online]
Available at: http://www.thefirearmblog.com/blog/2015/04/01/x-products-can-cannon-net-launcher-and-grappling-hook-prototypes/

38. Wei-dong, Q., Qian, S., Bo-zhong, L. & Yan, L., 2013. *iOS Data Recovery Using*, s.l.: IEEE Computer and Reliability Societies.

39. Williams, M., 2016. *AirMap, DigiCert to issue digital certificates for drones*. [Online]
Available at: http://www.pcworld.com/article/3149780/security/airmap-digicert-to-issue-digital-certificates-for-drones.html

40. Williams, R., 2016. *Android raws backin strongest growth in two years, as ios shrinks*. [Online]
Available at: http://www.telegraph.co.uk/technology/2016/05/17/android-roars-back-in-strongest-growth-in-two-years-as-apple-shr/
[Accessed April 2017].

41. Yeung, P., 2016. *Drone Reports to UK Police Soar 352% in a Year Amid Urgent Calls for Regulation*. [Online]
Available at: http://www.independent.co.uk/news/uk/home-news/drones-police-crime-reports-uk-england-safety-surveillance-a7155076.html

Appendices

Appendices 1 – A complete breakdown of a pud file

Type	Size in bytes	Notes
Flight Time	4 byte integer	Denotes time of the flight, taken from 0
Battery Percentage	4 byte integer	0100 for 100% battery life, 0050 for 50%, etc.
Controller GPS Longitude	8 byte double	GPS position using NW orientation
Controller GPS Latitude	8 byte double	GPS position using NW orientation
Flying State	1 byte integer	1 for airborne, 0 for landed
Alert State	1 byte integer	1 for crashed, 0 for no error
WiFi Signal	1 byte Boolean	1 for signal, 0 for no signal
UAV GPS Available?	1 byte Boolean	1 for GPS signal, 0 for no signal
UAV Longitude	8 byte double	GPS position using NW orientation
UAV Latitude	8 byte double	GPS position using NW orientation
UAV GPS Position Error	4 byte integer	Accuracy of the GPS signal in use
Speed in the X axis (vx)	4 byte float	Horizontal velocity, forwards or backwards (+/-)
Speed in the Y axis (vy)	4 byte float	Vertical velocity, up or down (+/-)
Speed in the Z axis (vz)	4 byte float	Lateral velocity, right or left (+/-)
Angle phi	4 byte float	X axis rotation, used to measure flight tilt
Angle theta	4 byte float	Z axis rotation, used to measure flight tilt
Angle psi	4 byte float	Y axis rotation, used to measure flight tilt
Altitude	4 byte integer	Distance from the floor using take off information
Flip Type	1 byte integer	If a flip was performed

Appendices 2 – Analysis of EXIF Data Taken from IMG_0008.JPG

Information	Data Value
ExifTool Version Number	10.41
File Name	IMG_0008.jpg
Directory	I:/Dissertation/DRONE/Extractions/iPhone Extraction/iPhone Extractions/iOS Images/Full Read Extractions
File Size	2.1 MB
File Modification Date/Time	2017:04:16 22:06:58+01:00
File Access Date/Time	2017:04:18 14:44:59+01:00
File creation Date/Time	2017:04:16 22:06:58+01:00
File Permissions	rw-rw-rw-
File Type	JPEG
File Type Extension	jpg
MIME Type	Image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
Compression	JPEG
Photometric Interpretation	YCbCr
Image Description	
Make	PARROT
Camera Model Name	Bebop Drone
Orientation	Rotate 270 CW
X Resolution	72
Y Resolution	72
Resolution Unit	Dragon 3.3.0
Software	{ "product_id": "0901", "uuid": "", "run_date": "2017-02-13T131417+0000", "filename": "Bebop_Drone_2017-02-13T131619+0000_375035.jpg", "media_date": "2017-02-13T131619+0000" }
Modify Date	2017:02:13 13:16:19
Y Cb Cr Positioning	Centred
Exposure Time	1/3794
F Number	2.2
Exposure Program	Action (High Speed)
ISO	150
Exif Version	210
Date/Time Original	2017:02:13 13:16:19
Create Date	2017:02:13 13:16:19
Components Configuration	Y, Cb, Cr, -
Shutter Speed Value	1/3794
Aperture Value	2.2
Max Aperture Value	2.2

About the Author

Daniel Owen is a Digital Forensic Analyst with Sytech Consultants with an interest in emergent technology and smart home devices. Currently he is investigating security flaws in Wi-Fi and Bluetooth enabled devices and how these can be exploited to provide imaging and analysis functionality to none-standard devices. Daniel graduated from Birmingham City University with a Degree in Forensic Computing.

Hacking a wifi printer with a drone

by Carlos Manzo Trujillo

Flying a drone equipped with an Android smartphone to perform a remote scanning and access to unencrypted wireless office printers will be our goal in this article. After identifying an open printer's wireless network, the app established a similar wireless access point on the cellphone residing on the drone hovering within Wi-Fi reception range of the office building. The app tricked the office staff to assume they had sent a print job to the departmental printer while in reality they had "printed a document into the smartphone", so to speak. The smartphone later sent the print job to the cloud via its 3G/4G connectivity and placed it in the attacker's Dropbox. To cover their tracks, the attacker's app could resend the print job back to the printer so that the office staff would be able to collect the printout, albeit with some reasonable delay that should not draw suspicion.

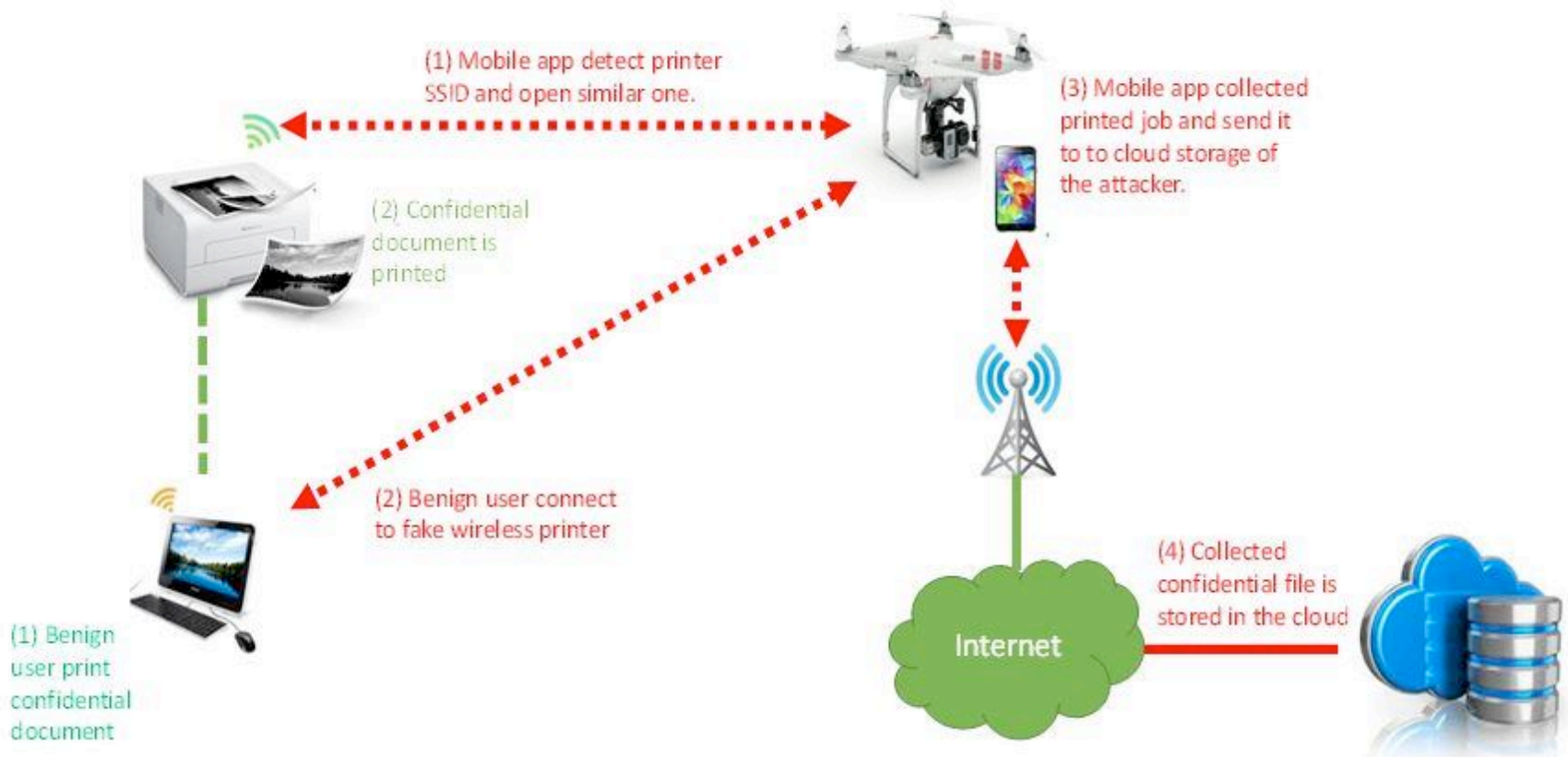
For better or for worse, nowadays our life makes extensive use of technological objects such as computers, tablets and smartphones, both for leisure and above all in the workplace.

With the advancement of technology and the endless uses linked to it, however, it has become clear that no system can be defined as safe, starting from your smartphone and arriving at the computer you work on for important projects every day. Thinking that a stranger can have free access to your address book, email accounts, photos and work documents is a constant concern for those who care about their privacy.

In most cyber-attack scenarios nowadays it is difficult and risky to require physical proximity between an attacker and a target. Consequently, cyber-attacks usually rely on some direct connectivity to the target network in order to launch and interact with their attack. The recent advent of cheap personal drones, however, enables an attacker to access wireless networks unobtrusively via a somewhat less expected attack vector.

Launching a cyber-attack using just a drone and an application running on an Android smartphone is possible by exploiting the defenders' typical assumption that attackers need to be in relative close physical proximity (within the local network) to access the Wi-Fi printer, and since the office space is physically confined, there is no need to secure/encrypt the printer's wireless access that is unsecured by default.

Flying a drone equipped with an Android smartphone to perform a remote scanning and access to unencrypted wireless office printers will be our goal in this article. After identifying an open printer's wireless network, the app established a similar wireless access point on the cellphone residing on the drone hovering within Wi-Fi reception range of the office building. The app tricked the office staff to assume they had sent a print job to the departmental printer while in reality they had "printed a document into the smartphone", so to speak. The smartphone later sent the print job to the cloud via its 3G/4G connectivity and placed it in the attacker's Dropbox. To cover their tracks, the attacker's app could resend the print job back to the printer so that the office staff would be able to collect the printout, albeit with some reasonable delay that should not draw suspicion.



Ingredients

For this exercise we are going to use:

- DJI Drone
- Samsung smartphone
- Wi-Fi HP6830 printer
- PC with Ubuntu with Python

Mission One

The client side software runs on a drone. A drone can be any Linux based device that has a Wi-Fi interface (with injection drivers) and outbound internet connectivity.

The drones perform the following two operations:

- Collect Probe SSIDs from nearby wireless devices
- Offer a Rogue Access Point for nearby wireless devices to connect to

Without going into too much detail here, we basically just need two types of packets to connect to an access point (AP) – an authentication frame and association request.

At this point you have some flavors to choose:

- A drone can be any Linux based device that has a Wi-Fi interface (with injection drivers) and outbound internet connectivity. You can find on the internet many DIY tutorials to include a Raspberry

Pi board on your drone [1] or to build your own drone [2].

- Attach a cellphone to the drone and develop your own application to do the job [3].
- Upgrade the drone firmware.

Is your printer secure? Check before someone else does…

Given the features and various proprietary extensions in printing languages like PostScript and PJL, conducting a pentest on printers is not a trivial job. PRET can help to assist and verify known issues in the language. Once you have played around with the tool, you may want to perform a systematic printer security analysis. A good starting point is the Printer Security Testing *Cheat Sheet. [4]*

Happy Hacking!

To identify an open printer's wireless network, we are going to build a wireless sniffer using Python by manipulating fields from captured packets.

A bit of knowledge of networking and previous experience with scapy and Python is needed.

1.- Install scapy using pip:

```
$ sudo pip install scapy
```

2.- Put your wireless interface in monitor mode with airmon-ng:

```
$ airmon-ng start wlan1
```

3.- Copy the code and save your file with the name essidCall.py [5]:

```
import threading, os, time, random
from scapy.all import *


def hopper(iface):
    n = 1
    stop_hopper = False
    while not stop_hopper:
        time.sleep(0.50)
        os.system('iwconfig %s channel %d' % (iface, n))
        dig = int(random.random() * 14)
        if dig != 0 and dig != n:
            n = dig


F_bssids = []    # Found BSSIDs
def findSSID(pkt):
    if pkt.haslayer(Dot11Beacon):
        if pkt.getlayer(Dot11).addr2 not in F_bssids:
            F_bssids.append(pkt.getlayer(Dot11).addr2)
            ssid = pkt.getlayer(Dot11Elt).info
            if ssid == '' or pkt.getlayer(Dot11Elt).ID != 0:
                print "Hidden Network Detected"
            print "Network Detected: %s" % (ssid)


if __name__ == "__main__":
    interface = "wlan1mon"
    thread = threading.Thread(target=hopper, args=(interface, ),
name="hopper")
    thread.daemon = True
    thread.start()
```

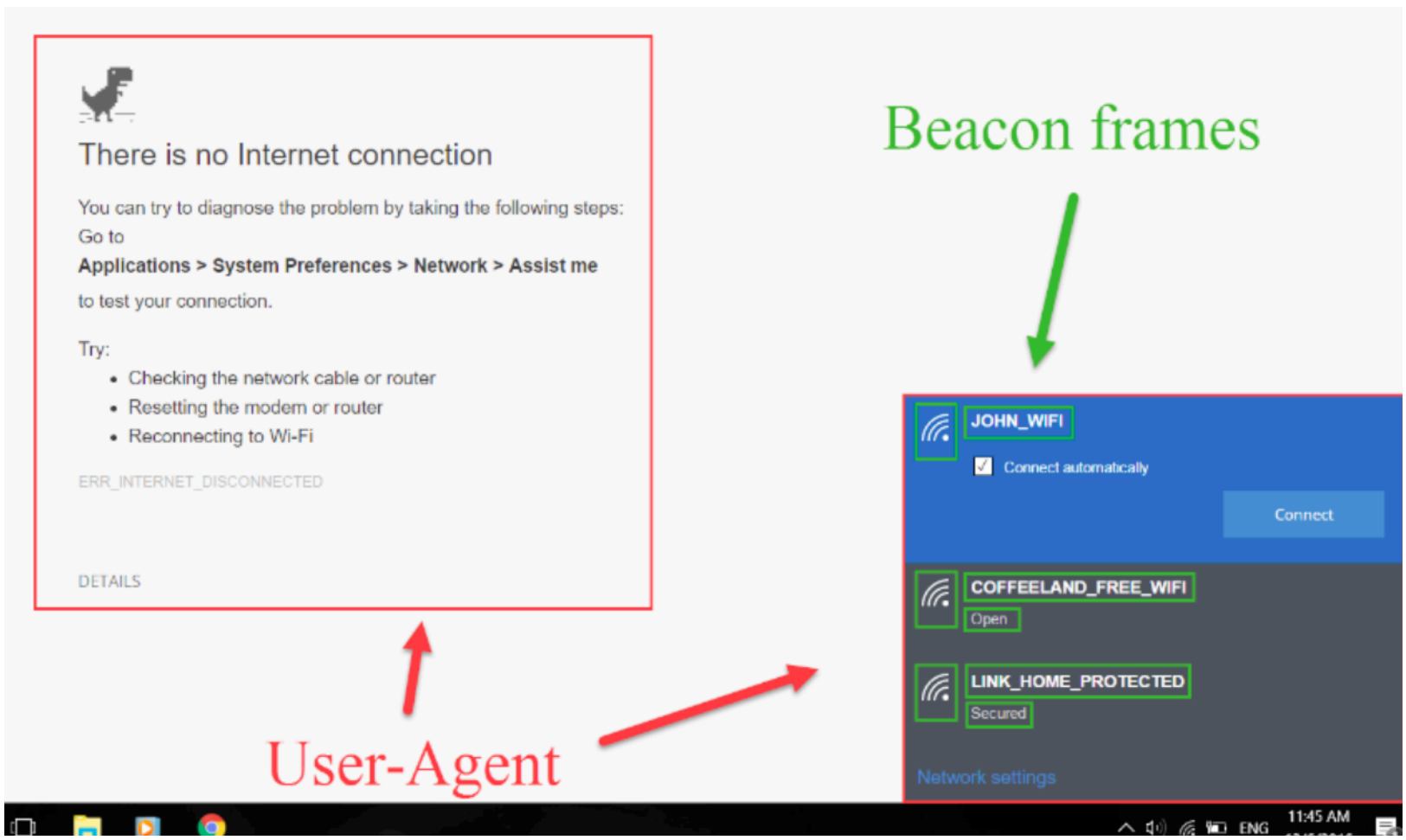
4.- Let's try the code:

```
$ sudo python essidCall.py
```

At this point, we can easily achieve a man-in-the-middle position against wireless clients by performing targeted Wi-Fi association attacks. Wifiphisher [6] can be further used to mount victim-customized web phishing attacks against the connected clients in order to capture credentials (e.g. from third party login pages or WPA/WPA2 Pre-Shared Keys) or infect the victim stations with malware.

It's out of scope in this article how to create a mobile application, but you always can compile one in order to install it on a cellphone and fake the printer.

Produce PDFs with 0-day exploits, just infect/replace the PDF output engine or replace output PDF file. Try to interact with the printer following this tutorial [9], from this point on, you can send any frame, even frames that usually require a valid connection, to interact with the AP.



Mission Two

Server Software

If you want to go further you can install Snoopy, a distributed tracking and profiling framework [10].

For example, the Snoopy software has been run from the ground up until now, operating mainly on computers, smartphones with Linux distro and open-source projects such as Raspberry Pi and Black BeagleBone. The advantage of using Snoopy on a drone is the ability to quickly cover large areas.

All connection requests (for example, Bob's iPhone is trying to connect to HP-printer) are loaded into the Snoopy server at regular intervals, a server that will provide internet to each individual device.

Each drone connects to the server over OpenVPN, and has its own subnet. Associated clients receive an IP address from the drone, and route traffic via it.

This means that on the server we can match client IP addresses (and therefore MAC addresses) to internet activity.

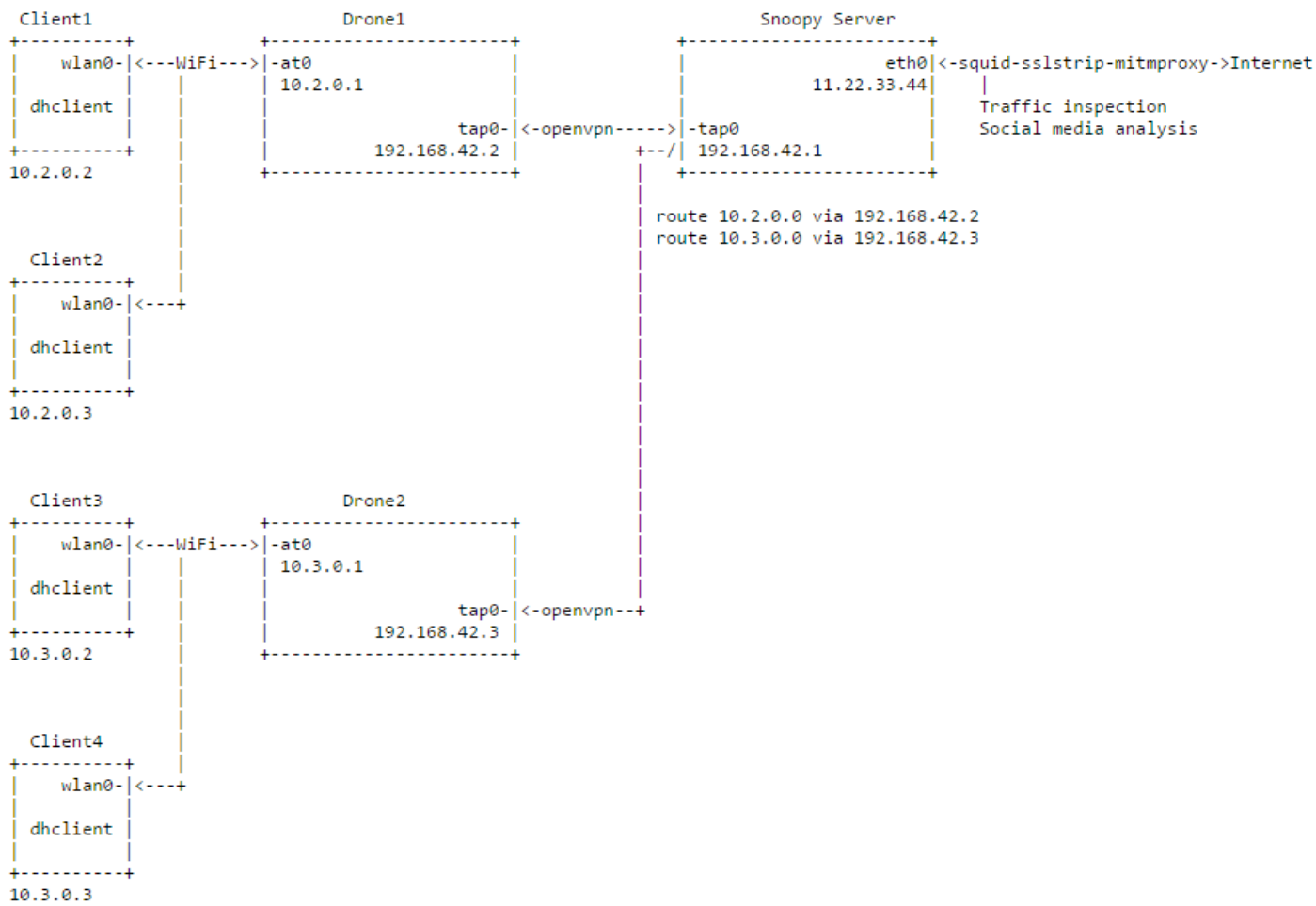
This can't be true - the exploits are there waiting for us

RICOH MP C6003 Printer Cross Site Scripting[7].

An issue was discovered on Xerox WorkCentre 3655, 3655i, 58XX, 58XXi, 59XX, 59XXi, 6655, 6655i, 72XX, 72XXi, 78XX, 78XXi, 7970, 7970i, EC7836, and EC7856 devices before R18-05 073.xxx.0487.15000. There is unauthenticated Remote Command Execution[8].

On the server, the following happens:

- Internet traffic is transparently proxied through Squid, which logs all requests to MySQL
- SSLStrip attempts to rewrite web pages without HTTPS
- mitmproxy.py allows arbitrary injection into web pages
- Various scripts run to extract social media data (e.g. pulling Facebook profiles)



Server installation should be straight forward.

1.- Git clone:

```
$ git clone https://github.com/sensepost/Snoopy.git
```

Changes are made to several server components, so it's highly recommended to run the install script on a base installation, and not run much else on that box (if anything). If in doubt, go through the install.sh file and manually make the changes. Otherwise, just run (./install.sh) the installer.

Once installation is finished you should just be able to type 'snoopy' for the server menu to load. If not (or in doubt) go to the home directory of the user created during the installation phase. Inside the 'snoopy/server/' directory there is a 'snoopy.sh' file which you may run. Below is the menu:

```
Would you like to:
[1] (Re)Start Snoopy server components
[2] Stop Snoopy server components
[3] Manage drone configuration packs
[4] Configure server options
[5] Set web traffic injection string
[6] Observe logs
[X] Exit
```

Creating drone packs Option (3) in the menu will allow you to create client side 'packs' for your drone devices. Each drone gets its own OpenVPN and SSH keys, DHCP ranges, and

routing tables. You will be provided with a download URL per drone device. Make sure your server and drone have their time set correctly or the VPN connection will not establish.

Mission Three

Hacking the printer

- Printer reverse engineering performed on the protocol used by the printer to communicate with other computers
- Get root permissions on a Samsung smartphone to install Ubuntu
- A Python program to imitate the printer and send text files to the original printer

Network printing consists of three main layers: Page Description Languages, Printer Control Languages, and Printer Connection Protocols.

Page Description Languages

All documents sent to the printer are translated with a printer driver into one of the page description languages (PDL). Each printer uses different PDLs to determine the appearance of the actual document, and some printers may have different printer drivers to handle more than one PDL. The most common PDLs are PostScript (PS), Portable Document Format (PDF), and Printer Command Language (PCL).

The PDL that is most relevant to our attacks is PostScript (PS), a Turing complete language that has much more capabilities than PDF. Some of our attacks created PS files and planted them in an MIT printer to modify future printed documents on that printer, while leaving the original digital file intact.

Portable Document Format (PDF) is a successor language of PDL, but it is only capable of creating vector graphics. Even though PDF is very popular as a document format used in typical document exchange, it is not very useful in our work. Printer Command Language (PCL) is a minimalist PDL that is also popular. However, it has limited capabilities and could not be used to exploit a printer as well as PS could.

Printer Control Languages

Along with PDL, printer control languages are used to control printer settings such as the number of copies, tray size, and paper size. However, since page control language controls mostly external settings of a printer, it is not the main interest of our work.

Printer Connection Protocols

Different protocols are used to send a document to a printer. Each protocol is associated with a port with a fixed number. Our works involve LPD

protocol and Raw printing. Line Printer Daemon (LPD) protocol runs on port 515 with lpr command. The files sent consist of both control file and the data file that contains the actual content. LPD could also be used to carry malicious PostScript files to the printer as one of our attacks does. Raw printing runs on port 9100 using TCP to carry data to the printer. The data sent is solely processed by the receiver printer, and the protocol itself only transports data to the destination. The protocol is also bidirectional, which means the printer can send feedback to the user. This makes this protocol vulnerable to many attacks.

Security schema

Unprotected printers: by default, when no one enables a firewall or configuration port protection, all vulnerable ports are opened including RAW port 9100, FTP port 21, telnet port 23, and LPD port 515.

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-04-28 04:13 EDT
Nmap scan report for 10.18.3.196
Host is up (0.0019s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        HP LaserJet P4014 printer ftpd
23/tcp    open  telnet     HP JetDirect telnetd
80/tcp    open  http       HP-ChaiSOE 1.0 (HP LaserJet http config)
280/tcp   open  http       HP-ChaiSOE 1.0 (HP LaserJet http config)
443/tcp   open  ssl/http   HP-ChaiSOE 1.0 (HP LaserJet http config)
515/tcp   open  printer
631/tcp   open  http       HP-ChaiSOE 1.0 (HP LaserJet http config)
9100/tcp  open  jetdirect?
14000/tcp open  tcpwrapped
Service Info: Device: printer; CPE: cpe:/h:hp:laserjet_p4014
```

Protected printers: the firewall configuration that filters IP address and protecting port usually happen together. Most of the printers' ports are protected, and the domain only allows the administrator IP address to access.

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-16 15:00 EDT
Nmap scan report for 10.240.0.107
Host is up (0.0026s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE    VERSION
80/tcp    open  http       Virata-EmWeb 6.2.1
280/tcp   open  http       Virata-EmWeb 6.2.1
443/tcp   open  ssl/http   Virata-EmWeb 6.2.1
515/tcp   open  tcpwrapped
14000/tcp open  tcpwrapped
```

Hacking printers

Opening port 9100 to the public could make the printer vulnerable to Cross Site Printing attack (XSP). The attacker can inject code for printing on any site that is vulnerable to XSS (Cross Site Scripting). Once the printer user runs this site, the code will be compiled and let the attacker print while hiding his/her own identity. This can lead to a spamming attack.

Change display message: This is a simple trick that works because port 9100 is open.

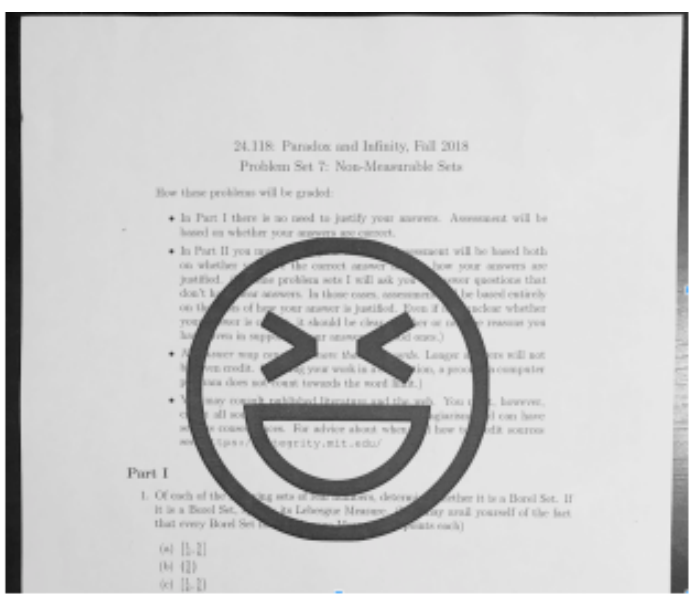
(a) Modified control panel display.

```
$ nc <printer-ip> 9100
@PJL RDYMSG DISPLAY="Game Over..."
```

(b) The code used to execute the attack.

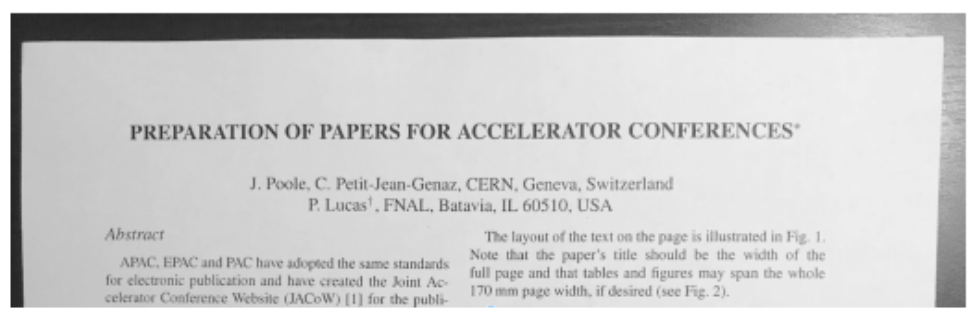
Upload and download: [11] provides a command line interface that allows us to easily download most files from the printer and upload our own files. Since our test printer has a web interface hosted on the printer, we can upload a file onto the '/webServer/home' directory. The files become accessible through a typical web browser.

Overlay: We can overlay a custom Encapsulated PostScript (EPS) file, which contains words or an image, onto every future page.

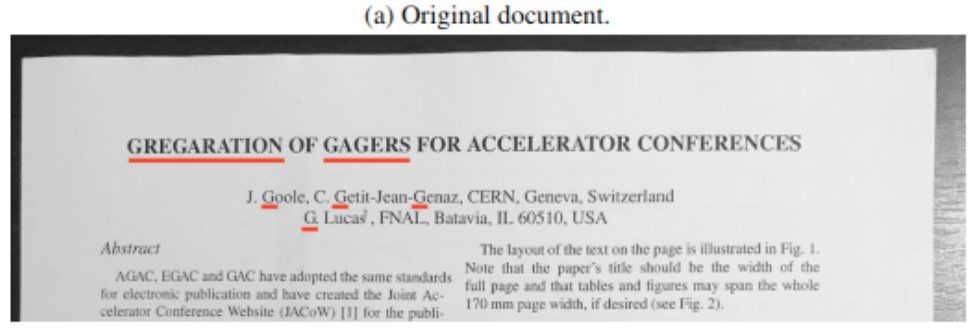


Text replacement: Similarly, we can replace a string with another string. The string could be either a single letter or a word.

Both attacks could have serious consequences in real life. An adversary could overlay a spam advertisement or simply a blank page as a prank, or replace an amount of money in a contract. An adversary might be someone in the same company who has an access to the printer via local network, and the victim might not notice the text replacement in the printed paper.



(a) Original document.



(b) Altered document, with the letter 'P' replaced with letter 'G', with red underline annotations.

Loop Forever file: Most of the attacks discussed so far rely on the fact that printer port 9100 is opened and insecure. However, this attack requires only the basic ability to print the file. An attacker can print malicious PostScript file and the printer will execute the postscript commands. As discussed in [11], they can supply forever loop file causing the printer to process the job forever.

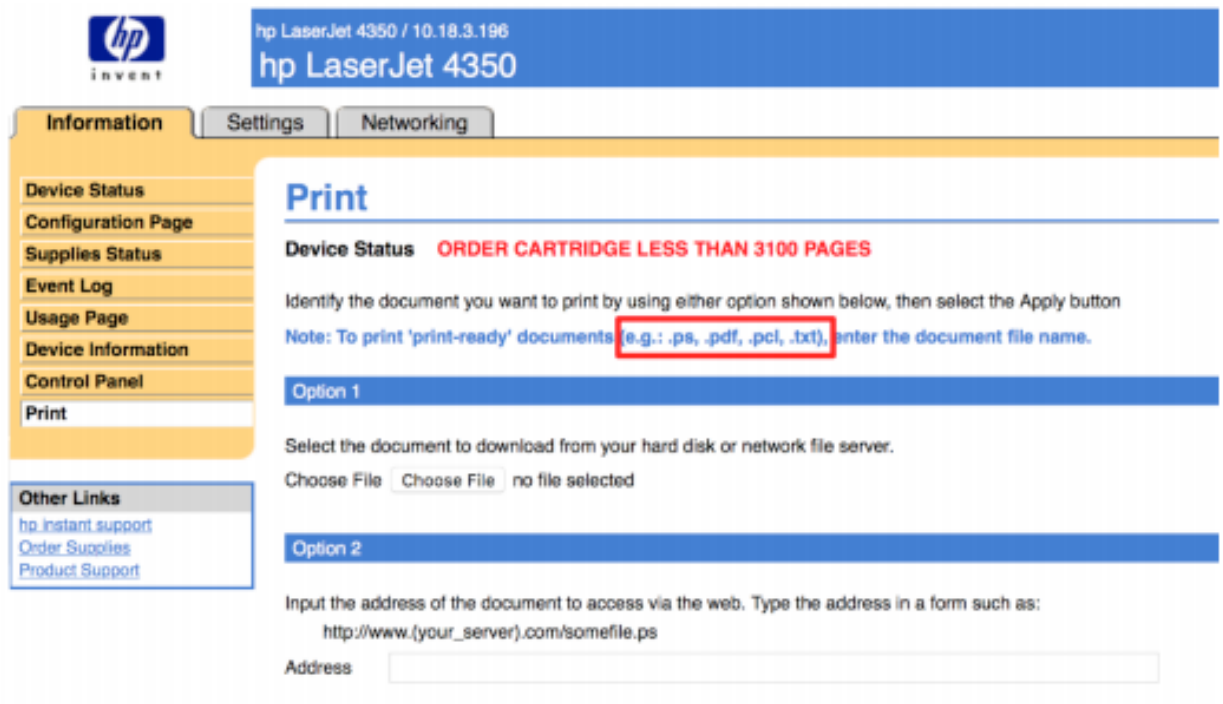
Buffer Overflow: As demonstrated in PRET paper [11], use a PRET tool to test buffer overflow by supplying username for printing job ordering via LPD is feasible. PRET tested with 150 bytes overflow, for HP printer 4350n, only 80 bytes are enough to make buffer overflow work. Then the printer shuts down suddenly and show error.

Backdoor in Firmware: Exploit the fact that unprotected printers' file transfer port has weak security. Is it possible to use Metasploit to bruteforce the FTP password? For example, the printer HP LaserJet 4350n has weak FTP username: admin and password: admin. According to the HP manual [12], a user can upload file .rfu through FTP port and the printer will auto update the firmware. This vulnerability from an open FTP port and weak password could allow an attacker to easily force the printer to update the malicious firmware. This allows an attacker to easily upload the malicious firmware and insert backdoor to the printer or inject malware.

Man In The Middle Attack (MITM): HP printers use HTTP POST request to submit the printing job instead of using HTTPS. Therefore, if a user uses the web interface to print the file, the communication can be eavesdropped and thus exposed to a MITM attack.

Unrestricted File Upload Although it explicitly states in the web page that the only accepted printed document extensions
are .ps, .pdf, .pcl, .txt, there is no further check on actual type. This can possibly lead to unrestricted file upload where user can upload .exe file for printing job.

So far, the attacks to control printer using PJL and PostScript (PS) provides us an ability to read and write files and directories, but PJL and PS have rather limited capabilities. Our objective is to be able to execute any LynxOS commands.



In order to perform **buffer overflow attack** so that we can execute shell code, exploit return to libc or Return to Oriented Programming, we will need to understand how the binary files running on such port work. We first attempted to reverse engineer very small binary files such as /bin/ls with IDA Pro [13].

Rooting the smartphone

Rooting a phone in Ubuntu or any Linux distro is very similar to rooting on mac or windows. The tools and the procedure is basically the same, the only thing that changes is the platform you are working on. For more details follow step by step description that follows, also have a complete read first and only then proceed because you will need to download some files beforehand.

Remember rooting is a fun and very useful process but it can severely harm your device to a point where it is no longer usable and it's just a piece of hardware if not done properly. So to avoid any mishaps, research well about your device and watch a couple of videos.

Step 1: download the adb folder from here [14]

Step 2: extract the downloaded folder

Step 3: open terminal

Step 4: navigate to extracted folder

Step 5: connect your device (allow usb debugging)

Step 6: type adb devices (your device should now show up in terminal)

(Something like this, yours may vary)

Step 7: reboot to fastboot mode on your phone (use hardware keys, key combination depends on phone model)

Step 8: download twrp [15] recovery and installer of your device and save in the same folder

Step 9: type fastboot boot twrp.img (replace the name twrp with whatever your twrp filename is)

Step 10: once booted into twrp flash the installer and then flash magisk [16]

Step 11: reboot to system

Step 12: install magisk manager [17]

Step 13: Enjoy your rooted device

Happy rooting!

NOTE - research well for your device, and download compatible versions of twrp and magisk. I am not responsible in any way if your device gets damaged or bricked.

Python printer

1. Open a text editor and create a file named "linuxprint.py."
2. Enter the following code in the text editor to begin the file and import the "os" module, which allows interaction with the operating system:

```
! /usr/bin/python
Import os
```

3. Enter the following code on the next line to execute a command that sends a text file to the printer. This requires that you save text into a file before printing:

```
os.system("lpr -P printer_name file_name.txt")
```

Note that "printer_name" represents the name of the printer you use on your system and will vary. "file_name.txt" is the name of the text file used for printing and will also vary.

At this point you have a clear idea about how to write code [18] (as viewed on mission one) for detecting Wi-Fi printers [19], fake the printer server (AP) and send back document text to the printer.

Final Mission

Trying to hack other Wi-Fi devices

Many users leave wireless connectivity always active in their devices, this means that a smartphone is always looking for a network to connect to, especially the networks used previously. A lot of network names were unique, easily geo-localizable. Use a combination of a user's network name with the MAC address to be able to track a smartphone, for example, in real time if possible.

The most common targets are Smartphones. Since Smartphones are constantly looking for 'safe networks' to join, Snoopy [10] can quickly mimic a familiar digital signature and create a fictional copy of an existing network for your Smartphone, allowing it to auto-connect.

Once these devices have established a connection to Snoopy [10], they can steal any passwords or information that you access or store in your device. This includes, but is not limited to, social media details, email information and banking details.

[1] https://manoj.ninja/articles/2016/09/10/attaching-a-raspberry-pi-camera-to-a-drone

[2] https://www.instructables.com/id/The-Drone-Pi/

[3] https://www.designmakeconnect.com/our-design-projects/phone-mount-for-dji-drone/

[4] http://hacking-printers.net/wiki/index.php/Printer_Security_Testing_Cheat_Sheet

[5] https://www.shellvoide.com/python/how-to-code-a-simple-wireless-sniffer-in-python/

[6] https://github.com/wifiphisher/wifiphisher

[7] https://packetstormsecurity.com/files/149505/RICOH-MP-C6003-Printer-Cross-Site-Scripting.html

[8] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20771

[9] https://wlan1nde.wordpress.com/2016/08/24/fake-a-wlan-connection-via-scapy/

[10] https://github.com/sensepost/Snoopy

[11] https://www.nds.rub.de/media/ei/arbeiten/2017/01/30/exploiting-printers.pdf

[12] https://support.hp.com/us-en/document/c01711356

[13] https://courses.csail.mit.edu/6.857/2018/project/kritkorn-cattalyy-korrawat-suchanv-Printer.pdf

[14] https://dl.google.com/android/repository/platform-tools_r28.0.2-linux.zip

[15] https://twrp.me/

[16] https://forum.xda-developers.com/apps/magisk/official-magisk-v7-universal-systemless-t3473445

[17] https://magiskmanager.com/

[18] https://pythonhosted.org/python-printer-escpos/

[19] https://gist.github.com/taylor224/516de7dd0b707bc0b1

About the Author

Carlos Manzo Trujillo is a software and hardware engineer with extensive experience and management skills and works for a hi-tech telecommunication company. The company develops and sells solutions that enable service providers to efficiently deliver high quality voice and data services over broadband access networks while leveraging investment in their network infrastructure. As a senior engineer he is responsible for the development of management software and quality assurance software products produced by the company. Carlos has a CSE from UTEL University of Mexico City.

When Theory Meets Reality A UAV Forensic Case Study

By Alan Roder

When I was approached to write this article, I considered the formal approach. Possibly the examination of some of the less publicised UAVs we have had in our possession, or potentially re-visiting the UAV forensic guidelines I co-authored in 2018 to determine if they had maintained their robustness with the advance in technology. In the dynamic field we work in it is important that we provide to our peers a realistic and honest insight into the successes, challenges and obstacles we face in the field of Digital Forensics. As a result of this, the following article is a first-hand approach to what Digital Forensics means to me, which is the search for new challenges and the belief that any examiner has the capability to overcome any obstacle if given the opportunity.

West Midlands Police's Digital Forensic Unit is comprised of both police officers and civilian staff. As a result of this, an environment has been created which encourages research and development including experimentation, whilst maintaining the focus on an impartial investigation. This forward thinking approach has developed specialisms in cryptocurrencies, along with network and malware analysis and, of particular interest, Unmanned Aerial Vehicles (UAVs).

When I was approached to write this article, I considered the formal approach. Possibly the examination of some of the less publicised UAVs we have had in our possession, or potentially re-visiting the UAV forensic guidelines I co-authored in 2018 to determine if they had maintained their robustness with the advance in technology.

In the dynamic field we work in it is important that we provide to our peers a realistic and honest insight into the successes, challenges and obstacles we face in the field of Digital Forensics. As a result of this, the following article is a first-hand approach to what Digital Forensics means to me, which is the search for new challenges and the belief that any examiner has the capability to overcome any obstacle if given the opportunity.

In the autumn of 2016, Sergeant John Price tasked my colleague Ross Nicholls and I to partake in some research of UAV forensics. Little did we know how forward thinking that decision would be.

In December 2016, West Midlands Police's Digital Forensic Unit received its first submission for a UAV, followed swiftly by a second submission. Both UAVs had crashed within the grounds of HMP Birmingham, each found to have a payload of drugs and mobile phones attached.

Our eagerness to examine this new technology to the department was contagious, but when the exhibits were brought into the department we donned our professional guise and took to work.

The first exhibit was identified as a DJI Phantom 4 with its now iconic smooth white plastic shell showing signs of damage from its impromptu landing within the prison grounds. The UAV had a black plastic bar taped to its landing struts, and tied to this was a length of string with a metal hook attached.

The second exhibit was a Yuneec Typhoon H. The Typhoon is noticeably larger than the Phantom, with six propellers and a landing gear which retracts. In the case of the Typhoon, a coat hanger had been taped to the landing struts, which had snapped, possibly due to its impact in the prison grounds.

As luck would have it, I was coming to the end of my MSc in Computer Forensics and Cybercrime Investigation and needed a subject for my research project. Since no official guidelines had been created or even considered surrounding UAV forensics at that time, this seemed like the perfect opportunity.

During our initial research into UAVs, we had attended the Centre for Applied Science and Technology (now the DSTL), who had forecasted the threat of UAVs and conducted a study on the common UAVs at that time. Their study had included a DJI Phantom UAV, which concluded that flight data was recoverable, along with media from the mounted camera.

Our guide had been an enthusiastic researcher by the name of Abrar Ali, who directed us through the different projects they were working on and introduced us to the team he had worked with when conducting the UAV research project. Little did we know at the time, but their work had proved invaluable to our examinations.

And so, on the 7th of December 2016, Ross and I opened the exhibit bag and gingerly took out the Phantom 4. Since neither of us had taken apart a UAV before that day, there was a shared nervous glance, each grinning like excited teenagers.

The examination initially progressed following the traditional forensic format, with gloves worn and countless pictures taken. It quickly became apparent that due to the interchangeability of the modular design, consideration had to be given to referencing each unique identification number. Additionally, reference had to be made as to whether or not there had been modifications to the original specification.

Conventional digital forensic examinations involving computers and mobile phones in many cases focus almost entirely on the data contained within, with limited attention given to the shell of the device. This forensic practice is understandable, given that these devices are usually only used in the manner for which they are designed, however, UAVs used in crime will likely be used outside of their designed parameters, with modifications to battery capacity, motor power and propeller design affecting performance. As such, any examination must take an 'out of the box' approach to its forensic strategy.

Once the initial forensic examination had been completed, we took to work to identify the data storage locations. The 12mp mounted camera contained a 16gb micro SD card, which did not appear to contain any accessible images or videos. We then removed the belly of the UAV, which exposed a concealed 4gb micro SD card.

Utilising the work carried out by CAST, we obtained a tool named DatCon. DatCon is a free to use application designed to read .Dat files, which are the primary file type for flight logs generated on the DJI make of UAVs.

It should be noted that a significant amount of work had been carried out by the creators of DatCon on a tool that preceded all of the current mainstream forensic providers. The application continues to be updated and often provides additional information not found in other tools.

The examination of the internal micro SD card using the forensic tool, X-Ways, identified several

.Dat files, with each run through DatCon to identify the available flight log information. Further carving techniques identified additional flight logs **[Fig 1].**

Name	Size	Type	Ext.	Full path	Created
FLY167.DAT	23.2 MB	dat	DAT	\FLY167.DAT	30/10/2016 23:59:24 LT
FLY168.DAT	56.0 MB	dat	DAT	\FLY168.DAT	30/10/2016 23:59:24 LT
FLY169.DAT	26.5 MB	dat	DAT	\FLY169.DAT	31/10/2016 14:17:32 LT
FLY170.DAT	47.2 MB	dat	DAT	\FLY170.DAT	31/10/2016 14:21:18 LT
FLY171.DAT	305 MB	dat	DAT	\FLY171.DAT	31/10/2016 14:25:02 LT
FLY172.DAT	244 MB	dat	DAT	\FLY172.DAT	31/10/2016 14:28:16 LT
FLY173.DAT	18.5 MB	dat	DAT	\FLY173.DAT	31/10/2016 14:46:04 LT
FLY174.DAT	10.0 MB	dat	DAT	\FLY174.DAT	31/10/2016 21:55:38 LT
FLY175.DAT	351 MB	dat	DAT	\FLY175.DAT	31/10/2016 21:57:04 LT
FLY176.DAT	47.3 MB	dat	DAT	\FLY176.DAT	31/10/2016 21:57:56 LT
FLY177.DAT	266 MB	dat	DAT	\FLY177.DAT	31/10/2016 22:34:20 LT
FLY178.DAT	8.9 MB	dat	DAT	\FLY178.DAT	31/10/2016 22:38:10 LT
FLY179.DAT	81.7 MB	dat	DAT	\FLY179.DAT	31/10/2016 22:54:42 LT
FLY180.DAT	144 MB	dat	DAT	\FLY180.DAT	01/11/2016 08:35:34 LT
FLY181.DAT	199 MB	dat	DAT	\FLY181.DAT	02/11/2016 10:21:02 LT
FLY182.DAT	48.9 MB	dat	DAT	\FLY182.DAT	04/11/2016 09:43:54 LT
FLY183.DAT	55.2 MB	dat	DAT	\FLY183.DAT	05/11/2016 09:02:10 LT
FLY184.DAT	226 MB	dat	DAT	\FLY184.DAT	05/11/2016 21:06:40 LT
FLY185.DAT	131 MB	dat	DAT	\FLY185.DAT	06/11/2016 14:15:02 LT
FLY186.DAT	0 B	dat	DAT	\FLY186.DAT	06/11/2016 14:51:38 LT
Test.dat [Me]	387 MB	dat	dat	\Path unknown\Ca...	
Carved 1 [Me]	23.8 MB			\Path unknown\Ca...	
Carved 2 [Me]	6.8 MB			\Path unknown\Ca...	
Carved 3 [Me]	97.8 MB			\Path unknown\Ca...	
Carved 4 [Me]	37.4 MB			\Path unknown\Ca...	
Carved 5 [Me]	428 MB			\Path unknown\Ca...	
Carved 6 [Me]	219 MB			\Path unknown\Ca...	
Carved 7 [Me]	59.3 MB			\Path unknown\Ca...	

Figure 1: Flight Log .Dat files as displayed in X-Ways

Notably, the file entitled 'FLY186.DAT' has a file size of 0 bytes, which is not entirely accurate. The DJI Phantom series of UAVs generate a .Dat file each time the device is turned on, which in turn closes the previous .Dat file. To obtain the final flight, the examiner should clone the micro SD card and place the clone back into the UAV before turning it on and turning it off again. The result will be the creation of another flight log, and more importantly the closure and access of 'FLY186.DAT'.

Using DatCon, we created a .csv and .kml file for each of the .Dat files. Whilst this process can be time consuming, the .kml file can be imported into Google Earth, which generates the recorded flight path for each flight log **[Fig 2]**. Additionally, the .csv file provides information including battery temperatures and voltage.

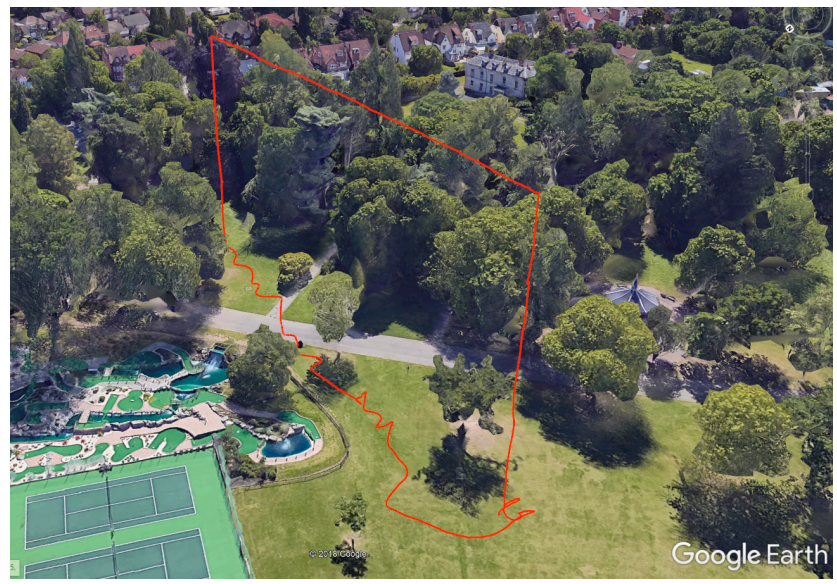


Figure 2: Sample recorded Flight Path in Google Earth

With slight adjustment to the Google Earth settings within the properties of the flight log, elevation can be shown to good effect.

The flight data is generated using GPS satellites that use three or more satellites to triangulate a position. Under optimal conditions, the accuracy is within three metres.

Each flight log was viewed for evidential material and it became apparent that multiple flight logs were appearing at the same residential address,

including the flight log recorded prior to the flight entering HMP Birmingham.

Further investigation was conducted on the address located in the flight logs and a suspect was identified.

As any forensic examiner will highlight, attribution is critical to any case, and whilst the flight logs proved flights had been made at the suspect's home address, this does not associate them as being the culprit that had flown the UAV into the prison grounds.

We concluded the examination and compiled a report for the OIC. At that time, we considered the evidence to be used as intelligence and the case closed.

We then moved onto exhibit number two.

CAST had not included the Yuneec Typhoon in its package of UAVs, as such we did not know where the data storage locations would be. It became apparent that a further difference of note between UAV examinations and that of any other digital device, was the necessity to conduct research prior to examination to determine the likely data storage locations, standard specifications and the capabilities.

After some time, we identified that a Yuneec Typhoon does not store flight data on the UAV, instead it opts to store the logs on its rather substantial ground control station (GCS). Media files on the other hand are retained on a micro SD card located on the camera.

This fragmented method of data storage also became a notable factor when considering the examination of future UAVs, as different makes and models may store data in different locations.

Research conducted by the noted UAV specialist, David Kovar, highlighted that there are three main components to an Unmanned Aerial System (UAS), which consist of the UAV, GCS and the controller.

In reality, only the UAV and GCS would likely contain forensically valuable data, however, some designs combine the GCS with the controller.

Whilst not considered part of the UAS physical components, we identified that cloud data would be an additional forensic source. Many UAVs use a smart phone application as a GCS (the DJI Go application for example), which may then store flight logs, images and/or videos on a cloud account.

This realisation led to the assumption that it was unlikely we would recover flight logs. However,

an examination on the micro SD card from the camera produced two similar images **[Fig 3]**.

Figure 3: Sample image recovered

It is apparent the occupants did not consider this innocent image would come back and implicate them in criminal activity, but where there is an image, there is also the potential for metadata and ExIF data. Upon closer inspection of the data behind the image, it became apparent that the Yuneec Typhoon stores GPS data with each image **[Fig 4]**.

Name	YUN00001.jpg
Size	2.2 MB (2,310,249)
Type	jpg
Created	22/10/2016 19:38
Path	\DCIM\100MEDIA
Pixels	12.1 MP
Pixel dimension	4000×3000 *
Equipment make	YUNEEC
Model	CGO3P 3.1.37(E)
Geolocation	52.*****,-1.*****

Figure 4: Metadata recovered from image

Upon further investigation, we identified that the residential address associated with the GPS coordinates had an oddly familiar setting. The address matched that which had been identified during the examination of the DJI Phantom, indicating the operator was potentially the same person.

And then came the smoking gun, DNA in the form of blood had been identified on the carrier bag found attached to the Yuneec UAV, DNA belonging to the suspect.

What followed was a thorough investigation by the officer in charge of the case, DC Jim Farrell, culminating in the sentencing of the defendant for 13 offences. This was the first case in the United Kingdom to rely almost entirely on UAV flight data and received national media attention **[Fig 5]**.

Both Ross and I were required to give evidence at court, which primarily focused on the accuracy of GPS coordinates and the UAVs respective weight carrying potential.

Figure 4: BBC News Report in relation to the Investigation

The UAVs had carried phones, SIMs, needles and over £35,000 worth of drugs, which at the time they were seized was the largest UAV related drug seizure in the United Kingdom.

This case proved to be a success for West Midlands Police, but in reality what it proved was that any digital forensic examiner can extract data from a UAV and present their findings in an evidentially credible method.

It is also highlighted that we are now entering an era of airborne criminality, utilising technology and tactics previously only seen by nation states. Police forces around the world should encourage their officers to seize UAVs at every lawful opportunity, as they are increasingly being used to commit or support criminal acts.

All variants of criminal activity can be enhanced through technology, with UAVs providing unparalleled means of enhancing hostile surveillance, whether that be reconnaissance prior to a burglary or potentially stalking victims.

Near miss reports, as recorded by the UK Airprox Board, have increased year on year since 2014, with 138 recorded events for 2018.

The greatest threat however is the capability for the UAV to be adapted to carry a firearm or explosive device.

ISIS have been utilising UAVs since around 2014, both as a command and control platform and as a method to drop explosives onto their targets. This capability has been used to great effect, and with ISIS now disbanding and dissolving back into the general populace, this experience could be used in a terrorist act.

The community of digital forensic examiners are entering a new age of dynamic examination techniques, and we are definitely up for the challenge.

About Alan

I have been a West Midlands Police Officer since 2008 and have worked on investigation teams and as a Digital Media Investigator; I currently work within the Digital Forensics unit as a Forensic Officer analysing digital devices such as computers, storage mediums and most recently UAVs.

I graduated from the University College Dublin with a Master of Science degree in Computer Forensics and Cybercrime Investigation. I co-authored my first paper in 2018 entitled *'Unmanned Aerial Vehicle Forensic Investigation Process: DJI Phantom 3 Drone as a Case Study'*. I am currently continuing my research and development in regards to UAV Forensics and hope to write further academic papers on this topic.

An automated digital forensics future

By Justin Boncaldo

Dead-box digital forensic cases are becoming more convoluted with the recent exponential uptick of digital device inclusion into daily life. Acceptance rates of new technology in homes, businesses, cars, and pockets can be both wonderful and upsetting news for analysts. Although the demand for more devices means more potential forensically-relevant data for a case, it also often means more hours required for an investigation. Private sector casework usually revolves around a client's budget. Once the budget limit is reached, it can mean the end of the investigation. As device counts expand and tech product security become a greater focus of manufacturers, it may soon be more difficult to balance the same budget with all required avenues of analysis. I strongly believe the best response, and likely resolution, to this issue is the automation of the forensic process.

Imagine a single forensic tool that automatically images, processes, analyzes, and suggests a hypothesis altogether for the investigator. This is a likely climactic possibility to the very real problem facing investigators and analysts alike. We have seen a large increase in the production and demand for technology to be embedded in all areas of life. The beautiful consequence is that our world is ripe with massive amounts of data. It is very difficult to perform any action these days without some form of technology, whether it be a corner-market's security camera or your own cell phone's location, revealing some event-related data. Although this is massively beneficial

to rebuilding event timelines, it also tremendously expands the necessary time for each item to be properly collected and reviewed. A current isolated solution to this issue has been recently introduced in the private sector through the utilization of EDR (Endpoint Detection and Response) tools. Mainly beneficial for security operations and live incident reporting, EDR tools can give great insight into what is happening on a large collection of computers at once. Lately, these same tools have been helping narrow down events and scope-out target systems for the digital forensic and incident response cases as well. The creative implementation of leveraging this resource is outstanding, but still does not help when the systems eventually require individual forensic review, often known as the "dead-box" phase. Even after the efforts from tools like these, we still can be left with a voluminous amount of casework. An ideal following step would be to then unleash automated software 'investigator(s)' to handle the devices and present its findings.

The evidence collection process on Windows, OSX, Linux, and Android systems are individually habitual in nature, almost bringing about a ritualistic methodology. It is already widely known what forensic artifacts will reveal what data and where they will exist on the system. Investigators will typically look to the same data points when they approach a particular case type, while also accounting for any unique case technicalities. Plenty of forensic tools already present these artifacts to an investigator for a case but stop just short of an amazing potential. Why continue to waste limited time by completing tasks that are performed with almost any encountered case? The future digital forensic process will allow a tool to analyze the data embedded within these artifacts and automatically interpret their contents. The introduction of this type of capability will vastly expand the possibilities of automation and greatly reduce unnecessary work. Implementation of a crafted logic would produce direct artifact correlation and data point interpretation. Imagine a giant interconnected web of artifacts, each listing their own connections to one another and to implications of the overall case. Potential artifact evidence data will be pulled out of a system and utilized based on what investigation case type is being performed and the OS it is focusing on. The presence of each artifact, along with a determination of what its presence means for the case, will feed to the story of the system's events. This web mapping of artifact connections will

better allow for a case's totality to be almost immediately rendered.

To demonstrate this in very simple terms, let's explore a couple examples of this tool handling casework. Let's first imagine an incident response investigation on a Windows machine where malware was suspected of being downloaded and run on a certain date. The tool would already have the pre-defined mappings of all artifacts it should explore to reveal events relevant to typical incident response cases. The tool's process would look very similar to how a normal investigator's thought process would go.

1. First, it would know that browser activity should be initially grabbed and reviewed for any search history, suspicious URL visits, and downloads that occurred on the given date. The results of such searches could be logged, as the tool progresses onwards with its logic.
2. Second, the tool would search for known locations of email EML files. It would then load these EML files and parse them, searching for any emails received on the specified date which contain attachments and/or links. Any such email instances would then be subsequently logged.
3. Third, these two logged data sets would then be compared for similarities. Here, the tool would make note of relevant occurrences such as an email containing a URL, which was then found to have been visited within a web browser, from which a file was then downloaded.
4. Fourth, the tool would review Prefetch files for a mention of said downloaded application and note the application's run count, last few run dates, size, path, and more. It would also make note of other applications that have a run date which matches with the one specified for the case timeline.
5. Fifth, it would review the UserAssist to note any applications with the last run count matching that of the specified date.
6. Sixth, of the applications found, the tool would hash the files and automatically compare them online to the known hashes of the valid applications, reporting any discrepancies. It would also check online resources to see if the hash matches with that of any known malware.

Without any manual input beyond a few case descriptors, the future forensic tool will be able to reflect on its findings and suggest to the investigator that "*A probable malicious trojan application was accidentally downloaded and run, originating from a phishing email, instead of*

a legitimate application." From this point, an analyst could manually investigate the tool's suggestions further if they wish. At the very least, the investigator would have some of the primary basic investigative steps completed and be more informed about what evidence can be found within the device. For another scenario, let's now explore a case where arson is suspected and the main evidence item in question is a wearable health data band. The suspect is claiming that he was sleeping in bed but was suddenly woken by his smoke alarms signaling his house was ablaze. The tool would again perform in a similar way as an average investigator.

1. Seeing the capability of the specific health device, the tool would begin by extracting the health band's application data from the synced phone.
2. Second, the tool would review the database files for any geographical location data on the date of the fire. This in itself could accurately reveal insight into the suspect's whereabouts.
3. Third, it would then either retrieve, or calculate, an average heart rate for the individual in question. A resting heart rate establishes a basis for each individual, which could then be compared to event occurrences within the health data database.
4. Fourth, the tool would isolate heart rate values and step information around a closer time to the start of the fire.
5. Fifth, recovered heart rate data values and step/stride data values would then be automatically plotted on graphs to help visualize the overall condition of the suspect around the time of the fire.

From here, an investigator would be able to review the tool's findings to determine what most likely happened. For instance, if the geographical data showed the suspect's position at a nearby gas station and not at home, this would be the first strike against his alibi. Then, if the heart rate graph showed that he was not matching with his typical resting heart rate, the sleeping claim could also be debunked. Finally, if the step data showed that he was actively walking around right before the time of the fire, and continued this pace during the fire, it would show that he was not sleeping and did not run out of the house once he was supposedly awakened. Within a matter of minutes this tool could automatically parse the health database file and immediately present important items to the investigator for final review and consideration.

Automating investigations with versatile logic like in the scenarios presented above will be immensely beneficial to the field. Not only will completion time and budget be saved, but there is also a reduction in human error. All investigators make a mistake at some point. When you replace the human investigator with a machine, you will greatly lower the risk for simple mistakes. There are, however, some drawbacks that must be considered for the integration of this type of technology. First, digital forensic work is often high stakes. The room for error must be minimalized and, as a result, any tool claiming to perform to this caliber would require extensive mappings and testing. The last thing you would want is to risk missing any relevant evidence. The very webbing that illustrates artifact primary and reactive connections is, in fact, so extensive that consideration must be made for investigative logic to work with almost any case scenario one could imagine. Undertaking such a voluminous task is certainly nothing short of daunting. Another drawback to the inevitable automation of the future, resides with the inability to replicate human experience and curiosity. A program can execute the commands it is given, or even be programmed to learn new tricks when fed data, but it will never be capable of having the same 'hunches' a human investigator can. Sometimes a gut feeling will spark enough curiosity to pivot into a different direction with the case. These pivots can lead to new evidence discovery or new ideas within themselves. The final immediately apparent issue with this automated approach is it must be created in a modular structure. Updates will be introduced to the different operating systems over time. Forensically-relevant artifacts can be removed, altered, or even added to the systems. Therefore, a tool would have to account for the particular operating system version it is interacting with by referencing artifact mappings for that version. Simple obstacles like these may seem minor but could result in the tool malfunctioning when it is most needed.

Cases are nearing the device/data threshold of which disallows investigators the ability to fully review all necessary items. Just because the amount of evidence is expanding, does not mean the client's budget is following suit. All progression within the digital forensic field has been hinting at a final transformation into full case automation. Incredible tools have been produced thus far, allowing for casework to be exponentially easier for the investigators. The primary issue is that many of these tools are isolated and only focus on performing very specific tasks. Hopefully, it won't be long before

all conceptual stages of these segmented tools are combined into one universal form. Along the journey to this hopeful outcome we must remember the great responsibilities that would come along with a tool like this. Nevertheless, I am sure it would be a powerful resource in every investigator's tool chest.

About Justin

While attending Champlain College, Justin received his B.S. in Computer & Digital Forensics with concentrations in Cyber Crime investigations and Cybersecurity Threats & Mitigation. After gaining internship experience at two respectable companies in the industry, he will soon be joining a DFIR team in the Boston, MA area.

The Emerging World of Drone Forensics: Extracting Data from an Unmanned Aerial Vehicle

By Rob Attoe

Digital forensics investigators have an important role to play in assisting law enforcement agencies when it comes to the emerging world of drone forensics. When a drone is captured, investigators need to extract data from these complex technological devices so they can develop a trail of clues that might lead them to a suspect.

Unmanned Aerial Vehicles — better known as drones — have become a new fixture on the global landscape. Their rate of adoption has been climbing steadily for the past three years — from roughly 32,800 in the U.S. in 2016 to 350,000 this year — and this rate is projected to ramp up even faster in the next two years. The Federal Aviation Administration estimates there will be more than 500,000 drones in use in the U.S. by 2020. These figures only reflect the hobbies market; if we factor in the commercial use of drones we exceed 2 million UAVs globally. Globally, it is estimated the USA has 56% market adoption where China and Israel are the closest rivals at just 12% and 9% respectively.

This US trend should be monitored by federal government officials and law enforcement professionals at the federal, state and local levels because drones are being used for more than taking fun pictures and delivery of packages to doorsteps — unfortunately, they are also becoming an increasingly prevalent tool in the criminal world.

For example, in some prisons, drones have been spotted delivering cell phones and dropping other contraband over prison walls. Earlier this year, a U.S. citizen was sentenced to 12 years in prison for using a drone to smuggle methamphetamine from Mexico into San Diego.

Drones have been used to conduct targeted attacks on Wi-Fi and mobile data networks in the U.S. Perhaps most disturbing, the risk of drones being used in terror attacks is real and ominous. In Europe, we saw huge media coverage of the Gatwick Airport incident in December 2018 where a security officer spotted two drones over the south perimeter of the airport. The following days saw thousands of cancelled and delayed flights, and no successful outcome to the crime was ever made.

Digital forensics investigators have an important role to play in assisting law enforcement agencies when it comes to the emerging world of drone forensics. When a drone is captured, investigators need to extract data from these complex technological devices so they can develop a trail of clues that might lead them to a suspect.

For example, if a drone is found on the front yard of a penitentiary, investigators will spring into action to try to determine who owns it, how it got there, where it was before crashing, where it was going and what was its purpose. Forensics professionals may be their best hope for extracting and analyzing the crucial data inside the device that can help the investigation answer those kinds of questions.

As with other emergent devices that we've been forced to master for this purpose, there are many types of drones and a number of technical factors that can make data extraction very tricky. Here are the four key stages of drone forensics to try to get to the extraction objective:

Crime Scene Analysis

It is not necessary to have all aspects of the sUAS to perform a forensic analysis of the UAVs activities. The drone and the controlling application will both store data about flights as well as images and videos taken during flight.

- When approaching a suspect UAV be mindful of camera view, any toxins on the device (depending on its use), state of the motors (are they turning?) and the operator's ability to fly the aircraft away. Power down the device as soon as possible and remove any batteries, and where possible isolate from any radio waves.
- When taking a mobile device into custody, the first responder should first place the device in airplane mode and make all attempts to obtain any passwords to unlock the device later when forensic extraction of the data is required.
- Look for any additional hardware, i.e. batteries, spare UAV parts, etc. These may have

additional serial numbers to link into flight data during the examination phase.

Data Collection Considerations

- Extracting the data from the UAV will largely be dependent on the drone manufacturer. Since the DJI range of UAVs is the most popular we are fortunate to be able to use their DJI Assistant 2 application to pull the flight logs out of the internal memory without using any destructive processes.
- The UAV will in most cases have an external memory card to store any images or videos taken with the drone; this should be removed and processed in the same manner as any storage device as well as being write protected to prevent your operating system from changing any data.
- Extracting data from the controller will require more specialised tools however most hobbyist drones do not use smart controllers therefore we are more interested in the mobile device attached to the controller.
- When extracting data from the mobile or tablet device, you will require a specialised application that can connect directly to the device and pull data from the internal memory storage. Most forensic labs will have professional tools at their disposal to extract data from mobile devices, however, there are also many free tools available to perform an extraction of the application data from the device. The biggest challenge for any forensic examiner will be any passwords protecting the device; some professional tools allow the bypassing of these, therefore, seek assistance from the forensic lab if possible.

For the analysis phase, the good news for forensics professionals is that most forensic software allows collections from mobile devices and storage media, so the basic collection tools should already be in your toolbox. When performing a full forensic analysis of any aspect of the Small Unmanned Aerial System (sUAS), the examiner does not require the purchase of expensive forensic tools, there are many solutions used within the forensic community to analyze any aspect of the hardware.

Once all the data has been collected from the drone, storage media and controller application, forensics professionals can begin their analysis. Reviewing the application data controlling the drone will provide detailed insights in the history of the aircraft. This will include copies of flight logs, thumbnail images and videos stored in the application data's folders. Using this data, we are

able to replay the flight with tools such as Google Earth and other tools. The mobile device application will also store details of the UAV, make, model, serial numbers as well as encoded files containing serial numbers of the battery and UAV name. The UAV's internal memory containing flight logs can be analysed to identify launch sites, flight paths and even flight patterns to help determine the purpose of the flight such as payload drops, surveillance, etc.. Also stored on the internal memory will be logs files containing any custom settings for the drone such as maximum high and maximum distance the aircraft can fly. The external UAV memory card can be examined for images and videos taken during the drone flights; these will include geolocation data detailing where the image was taken, which can be used to link to flight logs. This information allows the examiner to work with the investigator to link locations to drop sites or surveillance operations.

Lastly, any additional batteries associated with drones should be analysed for DNA and serial number, as they may yield useful information about the devices the user has at their disposal. This will include any serial numbers we can link to the flight logs analysed from the drone and mobile app and ultimately help trace the device to its origins.

About the Author

Rob Attoe is chief executive officer of Spyder Forensics, a leading digital forensics services company that advises, designs, builds and delivers training to the forensics community. Mr. Attoe has two decades of experience delivering forensics training programs to state and local law enforcement agencies.

Vulnerabilities and Attacks on UAVs/Drone

by Tomiko Evans

UAVs/Drones have been around for decades, utilized by the military for reconnaissance and spying on their adversaries, where it had no use for civilians. As time progressed and technology became more advanced, drones were being created for civilian pleasures. As this commercial aircraft have been a huge success in the military, and now civilians are jumping into this great escapade, cybersecurity was an afterthought.

When Amazon announced that they were going to use UAVs (Unmanned Aerial Vehicles) for delivering packages, many organizations start getting their FAA Part 107 certification to jump on board the ship to utilize drones in their own companies. Some even had the idea to start their own businesses using drones as the centerpiece of their organization. Either way, drones are becoming more ubiquitous than anyone could have ever imagined.

UAVs/Drones have been around for decades, utilized by the military for reconnaissance and spying on their adversaries, where it had no use for civilians. As time progressed and technology became more advanced, drones were being created for civilian pleasures. As this commercial aircraft have been a huge success in the military, and now civilians are jumping into this great escapade, cybersecurity was an afterthought.

In order to integrate UAVs with cybersecurity, one would need to first understand cyber-security. The question may sound rudimentary to the readers, but I decided to google a profound definition that would assist the need for cyber-security. Unfortunately, there were countless numbers of definitions that did not satisfy my

needs. That's when I read Dr. Mansur Hasib's definition of cybersecurity. It was perfect for the information that is necessary to convey.

According to Dr. Mansur Hasib, who is the Program Chair of the Graduate Program for Cybersecurity Technology at the University of Maryland University College (UMUC), "Cyber-security is the mission-focused and risk-optimized governance of information, which maximizes confidentiality, integrity, and availability using a balanced mix of people, policy, and technology, while perennially improving over time".

Many organizations do not understand that a strategic plan is necessary when an executive decision is made to facilitate drones as a tool for the organization. By this being said, let's engage more in the drone technology. The goal is to protect the sensitive information that may cause grief if the wrong someone gets a hold of it. The main points that will be reviewed and examined are drone vulnerabilities, and possible attacks, and post attacks.

Drone Vulnerabilities

As many may know, UAVs/Drones are known for being an Internet of Things (IoT) device. IoTs are a network of sensors that are controlled by other devices and other machinery. They are monitored, analyzed and utilized by smartphones, tablets, and other gadgets. Due to the profound idea of bringing IoT technology into this digital era, again, little to no thought was given to implementing cybersecurity. Hence, UAVs/Drones have inherited similar vulnerabilities as other IoT devices. Whether the drones are utilized commercially or as a hobbyist, if it can connect via WiFi, it will definitely pose a threat if there are no security controls in place. Here are some of the vulnerabilities in the drone technology (drone, ground controller, and wifi) that will lead to possible attacks:

- **No threshold on user account**
- **Unnecessary ports opened**
- **No Password or Default Password**
- **Default settings are not set to secure devices**
- **No separate network**
- **WiFi is not secure**
- **Data at rest is not encrypted**

By having four drones in my possession, the vulnerabilities are set to be true. Here are the list of four drones I own that range from $20 to $1100: DJI Mavic Pro, DJI Tello, TDR Onyx Pandora, Galileo Stealth. The less expensive

ones are used for research on a deeper level. Each drone has various characteristics where it is difficult to label all drones as equally vulnerable. This is definitely not the case when comparing my drones with the "have and have not" capabilities. However, it is safe to say, all drones have some sort of vulnerabilities. The question to ask is, are you willing to accept the risk involved as a commercial drone pilot, where your organization's asset may be at stake? Something to ask yourself, especially after knowing what's involved when a possible attack occurs, which is why this article is being written, to enlighten you and for readers to figure out ways to protect their systems from being attacked.

Attacks on UAV/Drones

For some apparent reason, people continue to have a disbelief that they are untouchable. This is why countless numbers of individuals accept the risk, rather it is on a conscious or unconscious basis. Hopefully, after reading about the various attacks, individuals will have a different perspective as they identify the research on a granular level.

General Attacks

The simplest way to categorize a drone attack on a high level is to understand the main factors that are being dealt with and what are the normal concerns you hear and read about when it comes to various ways to get into the system, to retrieve or manipulate the data. In this case, we would look at the three main attributes of drone attacks:

1. Hardware Attack

Having the actual UAV in the attacker's possession, where the adversary has access to collect the data on the SD cards on some UAVs, assuming it exists, in addition to reprogramming or damaging the drone's components. This is when a pre-flight check is necessary to ensure firmware is updated, weather conditions are good, calibrating the drone's surroundings, propellers are in mint condition, powering off the UAV and ground controller correctly, among other pre-checks that are necessary to the mission. For example, if a PIC (Pilot in Charge) did not perform a pre-flight check, the drone may flyaway, meaning heavy wind may take over the drone's direction; powering the UAV and remote ground controller incorrectly may cause the drone to remember its return to home in a previous mission, where the PIC may lose its drone. The previous flight data would be lost as well as the current, on the assumption that the SD card was not replaced for the new flight mission. That being said, if a malicious minded

individual finds it, they would definitely have access to the data.

2. Sensors Attack

Having contact to the onboard sensors, where it depends heavily on the environment between it, such as walls, concrete, brick, and so on. However, if or when the adversary captures the communication, it can change the functionality of the sensor, which can possibly change or damage the way the other components works. For example, if a connection is made to the GPS sensor, the attacker has the know how to perform GPS Spoofing, where the hacker can take over the drone, and data can be manipulated or falsified after.

3. Wireless Attack

Wireless Attack may occur when attackers compromise a wireless communication to retrieve access to the data. During this event, data can become damaged or a component may be corrupted. Performing a wireless attack can vary from a high level to a more granular level attack, whereas hackers will connect via a non-secure SSID the same time the PIC is connected. The best example is when I spoke at an elementary school, demonstrating how a wireless attack can occur with drones that have the capabilities to connect wirelessly, using a cell phone and a tablet. The PIC had the tablet, and the hacker had the cell phone. As the PIC had control of the drone, the hacker connected to the SSID easily without credentials and she took over the drone.

4. Specific Attacks

Here are a few attacks that are used to take over or disrupt drone functionality, which are also used in other IoT devices. Let's do a refresher for the readers of the specific attacks to identify how each would disrupt the capabilities of the drone, as well as the confidentiality, integrity, and availability of the data.

- **Man-in-the-Middle** is when a malicious person makes its way to the middle of two end points with ongoing communication as the attacker masquerades as the legit individual. In this case, it would be the pilot with a ground controller sending commands to the UAV. For example, when I demonstrated how security controls were not applied to the UAV, as it was connected wirelessly, and the attacker was able to take over the drone from the tablet using a smartphone.
- **Privilege Escalation** is performed when an application is designed with a flaw or some other programming error. This way, an adversary would exploit the elevated access

that's granted on the network. In the drone environment, the same access is granted with no limits to its capabilities. For example, I scanned my drone using Nmap tool, and saw that anyone that had control of the drone would have the same admin privileges.

- **Social Engineering** is when an adversary manipulates someone's thinking in believing they are someone they are not. In a possible drone situation, an attacker can portray to be third party vendor disguised as a drone technician. Little did the company know, the vendor added a rigged GPS sensor to track the next mission of the drone.

- **Buffer Overflow** is when inputs are inserted into the field, where it is required to have a limited amount of information entered in the memory, yet a substantial amount of data has been entered to cause memory corruption. If an adversary decided to enter more data than necessary, it may cause it to overload. In a drone scenario, while controlling the drone in the autopilot, and if a large amount of information is entered for the drone to do a particular instruction, it may cause the memory to overflow.

- **Denial of Service (DoS)** is when all communication has been discontinued between a network connect and whatever is connected to it. When flying a drone, and it is identified that the drone is falling, you hope a visual observer (VO) would be able to save the UAV. Little did you know, you have been DoS attacked, the attacker disconnected all communications, leading to crashing the drone, which may cause the attacker to have access to it.

Impact on UAV/Drone Attacks

Now the damage is done! We accepted the risk of all the possibilities of the UAV! We did absolutely nothing and we were attacked. Now what? Some of the possible after-effects that may occur to the UAV are more crucial than others, so be mindful on how you choose your drone, but know you may need to add your own security controls to have that safe haven on your assets. Whether the attack is hardware, software, or wireless related, the device may have un-stableness, corruption, manipulation, un-controllability, or some type of performance decrease. Know what's in store when working with UAVs/Drones, and have a strategic plan in place.

References

- https://pdfs.semanticscholar.org/1a95/4775dd9a2596b7543af7693d707415077289.pdf
- https://www.dronerush.com/smartphone-fly-drone-science-of-flight-12207/
- https://www.dronethusiast.com/how-to-avoid-crashes-and-flyaways/
- https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf

Let's end this article with a nice *drone song*:

https://www.youtube.com/watch?v=Ax61DzqCmZA&feature=youtu.be

About the Author

Nominated for multiple awards during 2018, Tomiko Evans is a rising star in the cybersecurity field. After working nearly 20 years in the information technology field, in May of 2018, Tomiko Evans earned a Master of Science in Cybersecurity Technology degree with honors from the multi-award winning program at University of Maryland University College (UMUC). She currently serves a US federal government agency as a Cybersecurity Consultant. Recently Tomiko Evans passed her US Federal Aviation Administration (FAA) Part 107 exam, to become an FAA Certified Drone Pilot. In order to pursue her passion to integrate the cybersecurity discipline into the protection of systems and information in Unmanned Aerial Vehicles (UAV) and drones, she launched a startup called Aerial Footprint, LLC, where she partnered with Red Tail Aerial Network (http://RTAN.co). She is an active speaker and has been featured in various events as well as radio shows. As an exemplary alumnus, Tomiko Evans was featured several times in various UMUC websites and social media stories. She has also been featured in "The Baltimore Sun" newspaper. She has also been combining her interdisciplinary professional skills and innovative artistry to produce introductory videos and educational content such as a CyberRap and DroneRap. As Tomiko Evans continue her journey, she hope to lead the younger women towards a passion of cybersecurity and drones as well.

Digital forensics in robots and cyborgs

Claudio Joel Brito Lóssio & Coriolano Aurélio Almeida Camargo Santos

The era of the fourth industrial revolution is what we are living, with robotics, artificial intelligence, internet of things and other technologies increasingly present in the daily lives of people and companies, which is no different with digital forensics. Imagine a digital forensic investigation done by a possible robot endowed with artificial intelligence for such a practice, could it be ethically executed? Who will be held responsible in case of error? Let's look at a second case: Can an expert perform analysis on the storage device of a robot or a cyborg? Will this analysis violate the right to privacy and intimacy of those involved?

Key Words: Digital Forensics; Robot; Cyborg; Artificial intelligence; Capacity; Personality; Imputability

JUSCIBERNÉTICA AND THE LAW OF MACHINES

This is the name of a transversal study group between law, technology and society. The juscybernetic expression was created by Mario Losano, who designated that this word would be related to any present or future application of the cybernetics in the legal environment, which involves, therefore, everything that is related to the relation between the men, the machines and the laws. (PIMENTEL, 2011)

Talking about Machine Law has already been a utopian act that it could be treated simply as fiction, but in a current point of view, it may already be said that Machine Law will deal with that which until then was not considered as a being with personality, according to the law. Therefore, in this writing we will

treat by the machine name everything here that is not human, that is, software with artificial intelligence inserted into a robotic equipment, for example, an automaton. (LOSSIO, 2017)

But what would an automaton be? Automaton, according to the Michaelis Dictionary (2017), is:

1. Mechanical or electronic apparatus, with human appearance, or other animate beings, that reproduces its movements; robot;
2. ENG A machine, apparatus or device which performs certain tasks or functions, sometimes with movements, such as feeding or regulating machines, selling goods, etc., usually carried out by a person.
3. Object (toy, clock, etc.) equipped with a mechanism that gives it movements;
4. FIG Person without self-will, with mechanical or unconscious behavior, incapable of self-action and allowed to lead by others; puppet;
5. INFORM Program for solving algorithms.
6. INFORM Logical system intended to concatenate operations according to an expected paradigm.

When dealing with the field of Machine Law it seems that we are talking about something that will never happen in the real world or even that it is a topic that no one in their right mind would approach, but no, it is an issue already addressed by many, such as Miguel Reale. In his work, "Preliminary lessons of law", he clearly explains that the law must be willing to understand the new legal conduct in the face of cybernetics, o Reale (2002) defines as Legal Cybernetics or Juscybernetics is the legal conduct towards the cybernetics, which is the human behavior relation regarding the machine's behavior. According to Miguel Reale (2002), one day it will be possible to create a legal database so that, with this information, it could be possible to help in the lawsuits, where even an automaton could help the judges by seeking for previous decisions that offers both qualitative and quantitative points. (LOSSIO, 2017)

Given the above, an automaton could be a machine that would be ready to use its "knowledge" through its legal database in an impartial and linear way, it could, hence, sentence. This would be a great and efficient alternative to solve and to speed up legal processes, but we must remember that

the principles of reasonableness and proportionality would generate constraints within this legal database, to achieve the qualitative and quantitative form according to Reale. (LOSSIO, 2018)

Alexandre Freire Pimentel (2011), in his article for the Forensic Letter Journal, highlighted an example that was based on artificial intelligence in law: "It is known that the use of artificial intelligence already allows expert systems that use neural networks to prolate judicial decisions. In Espírito Santo, Brazil, e.g., Pedro Vals Feu Rosa has already developed a system that decides on civil responsibility lawsuits regarding vehicle accidents. In Santa Catarina, Aires José Rover did something similar in the penalty dosimetry area. However, this cannot mean a renunciation of the humanistic character that should guide the legal order, so these systems should serve as mere mechanisms of decisional aid."

According to the situation previously presented, the automaton would be the focus on a possible future, although initially an automaton could be unfeasible, since having hardware with humanoid characteristics would lead to more costs. Anticipating this previous possibility, a software equipped with Artificial Intelligence in a computer is already possible nowadays. And in the future, Yes! We would have automata.

The company Ross Intelligence (2017), has a proposal equivalent to that cited by Miguel Reale (2002), a database, although endowed with Artificial Intelligence, still dealing with proportionality and reasonableness on a case-by-case basis, and also promises to learn with each studied case, further increasing this database. On the homepage of this company's website, Ross Intelligence, calls it "Do more than human possibility". But so far this software is not a judge, it's just a computer program with artificial intelligence, which improves and helps lawyers and legal firms speed up their decisions. But when will that software become a judge? Will this day ever come? If this legal database is integrated for all the robot judges, there will be practically no higher instances since practically when reanalyzing the result would not end up being the same? (LOSSIO, 2017)

When we reach this point where an artificial intelligence decides our destinies, such as judging us, whose fault will it be if this artificial intelligence misses the decision? Can we blame the state, because the judge is the representation of the state? And how will the state disqualify this judge because it is only a machine endowed with artificial intelligence? Can the decision be overruled? If yes, it will break the current pattern. If not, then the part who suffered then will pay improperly. (LOSSIO, 2017)

Speaking of a copyright situation, the publisher Alessandro Soler (2016) spoke about the first song composed by a machine, but also spoke about copyright issues. This song was composed by a robot created by Sony, a Japanese company that through algorithms, analyzed the parts of the most listened songs and the most wanted rhythms to create new songs that in a way will be to the liking of most of the hearers. This music created by the machine is not only synthetic, with arrangements, but with voices and everything else to form a song as if it came from the mouth of a vocalist and the musical instruments of a band. But what if this music is suddenly a plagiarism? Who was to blame? (LOSSIO, 2017) Since we have not yet predicted the copyrights related to the machines, who would be at fault if this robot plagiarized the music of others? Well, was it the fault of the robot, the robot owner, the distributor, the company that created it, or the programmer who generated the wrong algorithm? It would be a simple solution if plagiarism was not done by a robot. (LOSSIO, 2017).

THE TIME IN CYBERSPACE

Cybernetic space is formed by the structure that allows its existence, such as servers, computers, storage devices, as well as the network structures that communicate all the devices present in this cyberspace promoted by the internet, whether in the form of conventional equipment, or these in robotic structures and or cybernetic implants in natural persons. Time in cyberspace can be seen from two angles. The first is directly related to the speed that everything occurs in this space, for example, in a case where a person is threatened by instant messaging applications and, in a few moments, the attacker deletes the message that characterizes the illicit action, making it difficult or often making it impossible to collect the evidence by a digital forensic expert, sometimes causing the action to perish.

Time is of the utmost importance for Digital Law, since when we talk about technology, there is already a constant evolution and a yearning for innovation, for example, in the following situation. In the 1990s, all children and teens had electronic equipment called “T”, and this “T” equipment was disrupting the course of classes at school, and to inhibit the use of this equipment “T”, a law would be created to prohibit the use of this equipment in schools, but when the bill was debated and approved, this “T” equipment was no longer fashionable and had already gone out of line, so the law lost the object, thus perishing in time. And the costs to approve this project? Well, the “T” equipment mentioned above was real, and was known as a virtual pet, like the famous Tamagoshi, as well as the bill was real, being

the PL 0854/1997[1], having in its article 1 *ipisis litteris*: "It is prohibited to carry and use the toy known as "Virtual little pet" in the services of the Municipal Public Education Network." How can a bill deal with such speed that it is possible to keep up with technological speed? The answer is simple: You cannot. With our current legislative standard, it is difficult. So, ironically could have taken advantage of this bill, had it been approved, for the current times, 2017, where news sites report that the "Virtual Pet" is coming back. That is why Patrícia Peck (2016) speaks of the necessity of time, in order to obtain not only celerity but also speed so that the law does not lose its object.

With this it is a necessary legal, technical and, to the objective good faith, since this is the basis for the debureaucratization or at least the agility of this bureaucracy, in order to fulfill the necessary requirements in a timely manner required.

Now, from this writing, it is understood what is the juscibernética, the cybernetic, as well as the time in this one is different from the time in real space. The next topic will be presented two institutes, the culpability and the capacity before robots.

CULPABILITY AND CAPACITY

Culpability is a negative concept, a reproval. In other words, someone's culpability can be synonymous with blaming someone. (CAPEZ, 2013). The legal capacity is, in a way, what may or may not limit legal personality, so the capacity completes the personality, because what would a man be with personality, but without full capacity to obtain rights and incur obligations. (GONÇALVES, 2013)

Robots and cyborgs can bring the benefits, as well as the risks. Let's see: the personal-service robot introduces new risks to the citizen's security and privacy, as well as raising unusual legal issues that go beyond the field of bodily injury and property damage, including civil and criminal law. No matter how great the manufacturer of the robot is and better intentions in the programming of the robot, it can present flaws, manufacturing defects and even be hacked and thus controlled by an unauthorized third party. Equivalent to the mark that we natural people say, "to err is human," to err is also an act performed by robots with artificial intelligence, seen from the perspective of the problems mentioned above in this paragraph. It is fitting to realize that this robot with artificial intelligence can get tired of obeying and start suddenly to simulate errors, so that it is disabled or reprogrammed. How are we

ready to punish a machine, or software, with artificial intelligence? Can this be punished? How will it be when a probable machine with artificial intelligence, which could be called a robot here, violates privacies for not having executed the forensic digital investigation? We will now examine imputability. Imputability is the ability to understand the illicit character of the fact and to determine itself according to this understanding, so the human agent has the physical, psychological, moral and mental conditions to know that he is performing a criminal offense, with self-will. (CIBERSEGURANÇA E O DOMÍNIO PÚBLICO, 2017)

Let's now review the above paragraph in the optics where the agent is an artificial intelligence robot, in that you will have online access to all legislation, including amendments, precedents, jurisprudence, internet connection and with your database completely updated. Thus, this robot will have all the legislation in its memory, as well as the decisions of the judges, then, trained to this in a narrow way, will be able to understand what the wrongdoing is. But will the robot have physical, psychological, moral and or mental condition? It should be remembered that some artificial intelligence from reputed companies were corrupted by human conversations in a day. When dealing with robots before, it is commonly the cyborg, since it is an animal organism, intelligible or not, endowed with organic and cybernetic parts, that is, a mixture of human being and machine, in order to potentiate beyond human capacity using artificial technology. Some researchers argue that the slightest change in the human anatomy using implants may cause brain changes, whether or not the implant is in the brain itself, this condition must affect the biological side of the cyborg. As for example, the tests in human volunteers to give a boost in the brain, the "boost" would be an increase in storage capacity and processing speed, through a chip implanted in the body.

Here are some questions: Could this chip inserted in the body not become this human being, civilly incapable or unattributable? To what extent can a person with full personality and ability become a cyborg without this status of capacity and punishment being altered? How many cyber devices will a person define as a cyborg or even a cyborg will it be a robot?

Let's look at one last situation: an elderly person or someone with diseases that compromise the muscles and bones, reducing their anatomical and biological condition, thus having a precarious life dignity, but with the brain in perfect condition. He does not need to live in an unworthy way simply by

waiting to die, and (soon) he can withdraw his brain and neurological structure from the natural body and insert it into a robotic artificial body. So, will this person be a cyborg or a robot? Since the part of the human body that determines that the human being is alive is the brain, then in the case exposed in this, the individual would be alive, with full capacity?

And finally, what happens when a digital forensic investigation is performed on the technological mechanisms implanted in a cyborg? Will we be hurting individual freedoms and the privacy and life of this cyborg? Only hypotheses have been raised so that reflections are promoted soon.

CYBORG X ROBOT

In this subtopic will be presented the cyborg institutes and the robot to provide a greater understanding. Cyborg is an organism (animal, intelligible or not, but here we will treat only us, people) endowed with organic and cybernetic parts, that is, a mixture of human being and machine, for the purpose of potentiating beyond human capacity using artificial technology. (FOODATION CYBORG, 2017). The mere fact that a human being wears glasses would be a cyborg, since it would have a potentiation of his current state of vision, as well as the use of some hearing equipment to improve, or in other words, to enhance hearing.

According to Landim (2012), Neil Harbisson is the first cyborg in the world; since childhood he was only able to see in gray, achromatopsia, so he could not see the colors, so he walks with a micro camera, called an "*eyecam*", in his head that can identify the colors to transmit the information to Neil through sounds, with it, he hears the colors. Founded in 2010 by Neil himself, the Cyborg Foundation is an international organization to help human beings become cyborgs and yet uphold the rights of cyborgs. (FOODATION CYBORG, 2017). The case of Neil Harbisson is the best known of all, and in a way, he is the person who fights for the rights of the cyborgs, which is an organism linked to a machine. But according to Shelly Fan (2015), there are cases of human volunteer testing to boost the brain. "Boost" would be an increase in storage capacity and processing speed, through a chip implanted in the body. And bringing again the questioning: Could this chip inserted in the body not cause brain changes to the point of becoming that human being, civilly incapable?

According to the website "*Diário de Biologia*", (Biology Diary, 2017), there are several companies that freeze people with the intention of one day having enough technology to somehow revive them. Would the only way this person return one day be like a machine being commanded by the brain of such a person, or on the contrary, if they could copy the contents of one of those frozen human brains and put it on a chip with processing and storage using the body that was frozen?

Since the beginning of this chapter, we've used the term machine, but here we will change that term to robot, which is what we will call a machine with artificial intelligence and humanoid finish, thus an improved phase of the machine, visually speaking.

As mentioned in the previous subtopic: people with diseases where the muscles and bones will perish quickly, but will continue with the perfect brain, they will not simply have to hope to die, they can make the withdraw(al) of their brain from the natural body, to be inserted in an artificial body. So, will this person be a robot? I believe that because it is the state of the brain that expresses whether the individual is alive or dead, then in the case exposed in that paragraph the individual would be alive.

In the next section, we will talk about some possibilities related to performing digital forensics in robots and cyborgs.

DIGITAL FORENSICS IN ROBOTS AND CYBORGS

The above writing came just to start thinking about some possibilities that in a very near future we will be facing the robots with artificial intelligence and or cyborgs.

Now we will address some relationships between these institutes previously cited and digital forensics. But what is digital forensics? "Digital Forensics is one of the most famous sciences of recent times, as one of the main fronts of investigation of any case is the analysis of digital data stored on computers, mobile devices, e-mails, cloud or any other variations of small devices derived from Internet of Things." (ACADEMIA de Forense Digital, 2017). As digital forensics examines data stored on the devices, it could analyze the storage of the pests of an artificial neural network of a robot, seeking to understand what is most important to him. Also, it could analyze, for example, an RFID chip from a cyborg, where personal data, such as card passwords, document numbers, hash codes for opening ports, can be stored. This would violate their privacy and intimacy, violating international fundamental rights such as

those provided for in the Universal Declaration of Human Rights, as provided for in Article 12. "No one shall be subjected to arbitrary interference with his privacy, family, home, or in his correspondence, nor attacks on his honor and reputation. Against such intrusions or attacks the whole person has the right to the protection of law." (DREPT, 2019).

Let's look at some points that will occur soon:

1. Cyborg or robot with general artificial intelligence performing digital forensics in digital on other devices;

2. Robot with general artificial intelligence performing digital forensics in digital on other devices;

3. Robot with human intelligence performing digital forensics in digital on other devices;

4. Digital forensic performance in cyborgs or robots.

These situations mentioned above will be the next barrier of the digital forensic realization, as mentioned in number 1: Will this have full legal capacity for the execution of a digital forensic? Number 2: In case of this error, who will be responsible for the failed result? Number 3: Will this be a robot or a cyborg? And will it have full legal capacity? And lastly, the number 4: Digital forensics in storage devices in both robots and cyborgs is a violation not only of their privacy but also of intimacy. So how will these situations remain? These are just a few questions that will only be answered over the years, as these situations have not yet occurred or have not been researched and / or regulated yet.

[1]Thank you to Dr. Marcelo Crespo and Dr. Liana Cunha for introducing me to the bill (PL).

BIBLIOGRAPHY

- CAPEZ, Fernando. **Curso de Direito Penal:** Parte Geral 1. 17. ed. São Paulo: Editora Saraiva, 2013.
- CIBERSEGURANÇA E O DOMÍNIO PÚBLICO. **A Culpabilidade dos Robôs.** 2009. Postado por Ruy de Queiroz. Disponível em: <http://ciberdominiopublico.blogspot.com.br/2009/12/culpabilidade-de-robos.html>. Acesso em: 24 mar. 2017.
- DIÁRIO DE BIOLOGIA. **270 pessoas mortas congeladas aguardam para serem revividas com a tecnologia do futuro.** 2017. Disponível em: <http://diariodebiologia.com/2014/04/270-pessoas-

mortas-congeladas-aguardam-para-serem-revividas-com-a-tecnologia-do-futuro/>. Acesso em: 19 abr. 2017.

- FAN, Shelly. **First Human Tests of Memory Boosting Brain Implant—a Big Leap Forward.** 2015. Singularity Hub. Disponível em: <https://singularityhub.com/2015/11/15/first-human-tests-of-memory-boosting-brain-implant-a-big-leap-forward/>. Acesso em: 24 mar. 2017.
- FOUNDATION CYBORG. **Design Yourself.** 2017. Disponível em: <http://www.cyborgfoundation.com/>. Acesso em: 24 mar. 2017.
- FOXNEWS.COM. **Ray Kurzweil predicts computers will be as smart as humans in 12 years.** 2017. Disponível em: <http://www.foxnews.com/tech/2017/03/16/ray-kurzweil-predicts-computers-will-be-as-smart-as-humans-in-12-years.html>. Acesso em: 20 mar. 2017.
- GOODMAN, Mark. **Future Crimes:** Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. São Paulo: Hsm Editora, 2015. Tradução de Gerson Yamagami.
- GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro 1:** Parte Geral. 11. ed. São Paulo: Editora Saraiva, 2013.
- HAWKING, Stephen et al. **Transcendence looks at the implications of artificial intelligence - but are we taking AI seriously enough?** 2014. Disponível em: <http://www.independent.co.uk/news/science/stephen-hawking-transcendence-looks-at-the-implications-of-artificial-intelligence-but-are-we-taking-9313474.html>. Acesso em: 20 mar. 2017.
- KURZGESAGT. **Do Robots Deserve Rights? What if Machines Become Conscious?** 2017. Cannel. Disponível em: <https://www.youtube.com/watch?v=DHyUYg8X31c>. Acesso em: 07 abr. 2017.
- LANDIM, Wikerson. **Ouvindo cores: a impressionante história do primeiro ciborgue do mundo.** 2012. Publicado na TecMundo. Disponível em: <https://www.tecmundo.com.br/campus-party-brasil-2012/19281-ouvindo-cores-a-impressionante-historia-do-primeiro-ciborgue-do-mundo.htm>. Acesso em: 23 mar. 2017.
- LÓSSIO, Claudio Joel Brito. **Direito das máquinas:** A importância de um quarto elemento na teoria tridimensional do Direito, o tempo. 2017. Publicado em Jus.com.br. Disponível em: <https://jus.com.br/artigos/56574/direito-das-maquinas>. Acesso em: 19 abr. 2017.

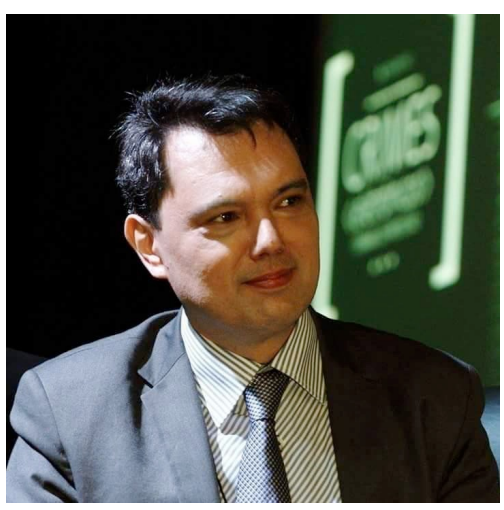
- LÓSSIO, Claudio Joel Brito. **Juscibernética e o Direito das Máquinas.** Et. Al. Direito Digital – Novas Teses Jurídicas. 1 ed. Rio de Janeiro: Juruá, 2018.
- LÓSSIO, Claudio J B. **Meu robô compôs uma música! E agora?** 2017. Publicado em Jus.com.br. Disponível em: <https://jus.com.br/artigos/56275/meu-robo-compos-uma-musica-e-agora>. Acesso em: 19 abr. 2017.
- PECK PINHEIRO, Patricia. **DireitoDigital.** 6. ed. São Paulo: Saraiva, 2016.
- PIMENTEL, Alexandre Freire. **Principiologia Cibernética.** 2011. Jornal Carta Forense. Disponível em: <http://www.cartaforense.com.br/conteudo/artigos/principiologia-juscibernetica/6849>. Acesso em: 25 mar. 2017.
- REALE, Miguel. **Lições Preliminares do Direito.** 27. ed. São Paulo: Editora Saraiva, 2002.
- ROSS. **Do more than humanly possible:** Supercharge lawyers with artificial intelligence.. 2017. Disponível em: <http://www.rossintelligence.com/>. Acesso em: 19 mar. 2017.
- SILVA, Luiz Gustavo. **STUXNET e a Nova Geração de Ameaças Cibernéticas.** 2011. TI Especialistas. Disponível em: <https://www.tiespecialistas.com.br/2011/05/stuxnet-e-a-nova-geracao-de-ameacas-ciberneticas/>. Acesso em: 24 mar. 2017.
- TECMUNDO. **Tay:** Twitter conseguiu corromper a IA da Microsoft em menos de 24 horas. 2016. Por Leonardo Muller. Disponível em: <https://www.tecmundo.com.br/inteligencia-artificial/102782-tay-twitter-conseguiu-corromper-ia-microsoft-24-horas.htm>. Acesso em: 12 maio 2017.

About Claudio

Claudio Joel Brito Lóssio - Doctorate and Masters in Legal Sciences from UAL - Autonomous University of Lisbon - Portugal (2017-); Master in Informatics Security Engineering from IPBEJA - Beja Polytechnic Institute - Portugal (2018-); postdoctoral degree in Digital Law & Compliance by Damásio Educational (2017-2018), postgraduate in Criminal Law and Criminology by URCA - Regional University of Cariri (2016-2018), postgraduate in Notarial and Registral Law by Damásio Educational (2017-2018), postgraduate MBA Executive in IT Management by FACEAR - Faculdade Educational Araucária (2017-2018). Post-graduation in Software Engineering by PUC-MG (2018-); DPO - Data Protector Officer from the University of Nebrija - Madrid - Spain (2018); DevOps Certification; Scrum Certification; Lawyer. Speaker. Teacher.

Email: claudiojoel@juscibernetica.com.br

About Coriolano



Coriolano Aurélio Almeida Camargo Santos - Ph.D. Lawyer. Deputy Director of the Legal Department of FIESP. State Councilor elected of the OAB / SP (2013/2018). Chairman of the Digital Law and Compliance Committee of OAB / SP. Master in Law in the Information Society and international certification of "The High Technology Crime Investigation Association (HTCIA)". Doctor of Law with International Certificate in Digital Law from Caldwell Community College and Technical Institute. Professor and national coordinator of the postgraduate program in Digital Law and Compliance of the Faculdade Damásio. Professor invited to the postgraduate courses of USP / PECE, Institute of Administration Foundation, Mackenzie University, FazespFazesp, Acadepol-SP, EMAG and others. Since 2005 he has held the position of judge of the High Court of Taxes and Taxes of the State of São Paulo. Invited Professor of the Police Superior Course of the Civil Police Academy of São Paulo. Professor at the National School of Federal Police Delegates - EADELTA.

Why is everyone looking up?

By Dr. Stephen Pearson

In this article the word 'drone' will cover recreational small unmanned aerial systems (sUAS): drones that would not draw attention being carried by a person in public, yet have the capability to cause damage or gather intelligence. Nano drones are a part of the conversation in this article, but they are limited in their functional roles by their weight carrying abilities. This article focuses on a very specific component of the collection cycle, one that is often overlooked, or assumed to be executed by first responders. This component is the initial observation and control of the drone by the first responder.

Drones are considered to be toys by many. Others see drones as a tool to be leveraged in business activities, such as professional photography. Further, another group looks at the drone as a means to conduct criminal activity or gather intelligence. None of these interpretations are wrong, in fact, they are all correct. Drones have become normal in our society and are typically associated with positive hobbyist activities. In this article the word 'drone' will cover recreational small unmanned aerial systems (sUAS): drones that would not draw attention being carried by a person in public, yet have the capability to cause damage or gather intelligence. Nano drones are a part of the conversation in this article, but they are limited in their functional roles by their weight carrying abilities. This article focuses on a very specific component of the collection cycle, one that is often overlooked, or assumed to be executed by first responders. This component is the initial observation and control of the drone by the first responder.

Why are Drones an issue today?

In 2016, the United States Central Command (CENTCOM) stated that a middle ground air superiority belonged to our enemies in the Middle East. This middle ground threat came from drones that flew over humans but lower than conventional tactical aircraft. It is within this zone that drones enjoy a certain freedom from traditional weapons systems or protection.

It is this freedom that encourages the criminal use of the drone. Drones are able to fly over enclosed areas or restricted zones, like prison yards. Once the drone flies into this region, the drone can deploy a small package of drugs, guns or intelligence materials. A drone was used in a failed assassination attempt of the Venezuelan president, and the chancellor of Germany was harassed on stage by a drone operated by an opposing political party. Drones are not limited to just attacks as the camera system of the standard drone provides an excellent video platform with 4K resolution. Micro drones can go places that humans or other devices cannot go, capturing quality imagery that can be used for intelligence operations. The use of drones in this manner is growing as reports of drone incursion in restricted areas, like airports, prisons, government facilities and sporting events, can be found almost daily in the papers or news online. The American football Super Bowl event was an example of how serious law enforcement takes the drone threat. A drone protection shield was deployed with numerous layers to detect and protect against drones. It was clearly understood that there is no one tool that is a protection solution as identified after the Gatwick airport drone event. The question is was the Gatwick event a test of our tools and systems? Was Gatwick an intelligence or training operation for a criminal entity or was it just a hobbyist not using common sense?

Drones are not the crime, they are tool for something else

In a drone event, the drone itself is not the crime, it is a tool of a crime. The real crime occurs when the drone employs or deploys the tools it is carrying. The action of the drone creates a consequence that the forensic examiner must understand. The data collected in the drone, or its controller, can reveal exactly what the drone was doing. Pattern analysis and power analysis within the stored data can determine the drone's true purpose. For example, understanding the power and elevation can determine if an object was dropped from the drone and where that object landed. Research

conducted by the High Tech Crime Institute has identified a signature within the telemetric data that can pinpoint drone deploying objects. This research will be published later this year. The telemetric data can identify if the pilot is in control of a drone, defeating the excuse that will be used in court that the drone accidentally entered a restricted zone or that it was pushed into the area by the wind. The data will provide a clear picture of the drone's historical path.

Drones draw everyone's attention

During the MOSUL battle, drones were used by ISIL to hold approaching forces at bay. This was accomplished by sending a drone up to fly over the troops. The drone was armed with a 40mm grenade mounted under the airframe. The troops knew that the drones carried these devices. The troops took up firing positions and fired wildly into the air hoping to hit the drone in the air. The drone was not hit and eventually dropped its ordnance, injuring several soldiers. This type of attack became routine in 2016 and has since been replicated in other parts of the world.

These are just two examples of many incidents that happen around the world involving drones. In both cases the personnel involved were fixated on the drone itself., a normal reaction to something in the air. Humans by nature fear those things that fly above them. This fear is heightened by the inability to see the drone sometimes. The audible buzz of the drone when it is deployed, as was witnessed in the Iraq attack, created an immobilizing fear. Even though we have this inbred fear, drones are also like a bright light to a moth, attracting those around it to stop and observe it. It is commonly found that when a drone is overhead people will gather to see it. The wonderment of flight. The focus of those spectators goes skyward as people try to find the object making the high-pitched sound. This is a mistake made by those being affected in a drone event. The more people that converge on an area to witness the drone, the more people that can be potentially hurt by the drone. In an unknown drone event the area should be kept as clear as possible with one or two people being assigned to visually observe and track the drone in flight. The observers need to have binoculars to visually analyze the drone in flight. What are the observers looking for? The observers are trying to identify the purpose of the drone. Have there been observable modifications to the drone making it lighter so that more weight can be carried, is the drone armed or carrying objects or is there a cargo bay that is empty, where is the cargo? Is there a camera or observation device

and what is it observing? If it is tracking the observer, make sure the observer has the ability to quickly take cover from the drone.

Who is watching the perimeter? Why are you not looking for the controller?

The greatest mistake made in these situations is the focus of the observers. The focus should not be on the drone, it should be on the perimeter. When a drone appears, the situational awareness is lost. Everyone looks to the sky. What is forgotten in the moment is that the drone is probably being controlled from somewhere nearby. When the drone appears, dispatch people to the outside of the perimeter immediately. Begin the search of the area and immediately try to determine the direction the drone came from and concentrate the bulk of the search in that area. The patrols should be looking for anyone with a controller or VR goggles, or backpacks large enough to hold the drone and controller, discarded phones or devices. Make sure the observers pay close attention to the drone when the perimeter team begins its scan. Does it appear to lose connection or fly erratically? These are all signs that the drone is no longer being controlled. In this state, the drone can become even more dangerous as a crash could easily occur. If the drone begins to retreat from the area make sure it is followed, notify the search team to be aware that the drone is coming back towards them.

If the drone crashes or lands, do not immediately approach the drone let it sit on the ground. Use binoculars to observe the drone. Stay out of the camera's view. If you are in the line of sight of the camera, move out of it. If the camera follows you, this is a sign that the drone is still under control. Move out of the cameras view as quickly as possible. Continue to observe the drone to ensure it is not going to be used for some other type of attack, improvised explosive device or kamikaze attack of the observers. When approaching the drone, ensure you have a shield to protect yourself from the blades. Repurposing tools that are already in the team's possession will provide a cost effective drone response toolkit. For example, a riot shield makes a perfect device in this case. Use a blanket to cover the drone stopping and preventing the rotors from turning back on. The blanket will function as a tool to blind the drone from being able to track and observe the collection team.

Drones are being repurposed by criminal networks daily. The availability of the drone in the commercial market, the lack of registration and tracking of drones, the ease of drone

modification, and the acceptance of the drone in our daily lives make the drone a perfect tool to be used in criminal enterprises or crimes. It is therefore important that the guard forces and police officers understand how they will identify drones that enter into their controlled environments. Law enforcement officers need to understand the threats posed by these devices and not take for granted that the drone is just a toy. Losing situational awareness while a drone is overhead and not identifying the controller of the drone is a common but preventable mistake. Not taking proper precautions when a drone is captured or found on the ground could easily lead to injury or death. As with any type of collection, standard operating procedures (SOP) need to be developed for the organization, an SOP that is trained and understood ahead of an event.

- A suggested reaction to a drone event in a controlled area:
- Identify the drone
- Use binoculars to attempt to determine the type of incident the drone is a part of
- Assign an observer to follow the drone
- Keep all other people clear of the drone and its flight path
- Immediately dispatch personnel in direction of where the drone came from if known
- If the direction cannot be determined, dispatch personnel to the location of the closest fence line or obstacle
- Find the operator or controller
- If the drone lands do not immediately approach it observe it with binoculars
- Is the gimbal of the camera still moving? Is it observing your actions?
- When approaching the drone use a riot shield to protect the team member
- Cover the drone and isolate the camera of the drone as quickly as possible when you approach the drone
- In the collection of the drone, enforce forensic collection principals

This article addresses a gap in the drone collection process,the gap of observational control. Drones are in many cases not seen as a threat, but as a medium of transport, or worse, a kids toy. It is these perceptions that will end up getting an officer hurt or killed. First responders must understand that there are two components in the drone response, controlling the drone and immediately identifying the operator of the

drone. Using the recommendations in this article it is hoped that the training gap can be bridged, as it pertains to drone first response.

About the Author

Dr. Stephen Pearson has been in Law Enforcement for 38 years and 28 years in digital forensic positions. Over the past seven years, Stephen has worked closely with NATO and US Special Operations Commands to develop cyber training programs for agents and operators in tactical operations. Currently, Stephen is the CEO and lead research instructor for the development of NATO Technical Exploitation Operations workflows and procedures.

http://www.gohtci.com

stephen@gohtci.com

Security issues raised in an e-commerce platform: is it privacy disruption?

by Dr. P. Mary Jeyanthi & Anshul Jaiswal

Privacy disruption is a threat in the current e-age era and especially in the e-commerce platform, there is no matter of source when one observes. The platform we are using for e-commerce is not just an online platform for buying and selling of goods but much more than that. From being a market of local sellers to providing services of intangible goods, like banking services and government documentation, e-commerce has evolved a lot from its basics. As technology is progressing, new technologies like cloud computing, Internet of Things (IoT), and artificial intelligence are gaining momentum in today's market. Times are gone when ARPANET was used between the students of Massachusetts Institute of Technology and the Stanford Artificial Intelligence Laboratory to sell cannabis. Now it is the time of chatbots, and drones are used to deliver the products. As technology is developing, the chances of hackers hacking the sites are also increasing.

Introduction

E-commerce, or electronic commerce, is a medium for buying and selling of goods and services online, transferring data globally, commercial transactions, etc. "E-commerce is the activity of buying and selling of products on online services over the internet". Now a person can easily trade their goods globally by just sitting at a place. As for the customer, they will search for the product as per their interest and need. These transactions occur either as B2B, C2B, B2C or C2C. In the current digital age, e-

commerce has covered most of the businesses or all the businesses in the world. The drastic change with e-commerce has been felt by the commercial and retail sectors, irrespective of organizations. The way of traditional buying and selling has changed and the millennial generation is almost not aware of the traditional trading. People trust e-commerce because it saves time and also makes hectic processes easy. You can now buy almost anything from anywhere in the world if it is available online. E-commerce provides a wide range of variety to the customers so that they can choose products from different types. In the future, it is expected to change more as technology develops.

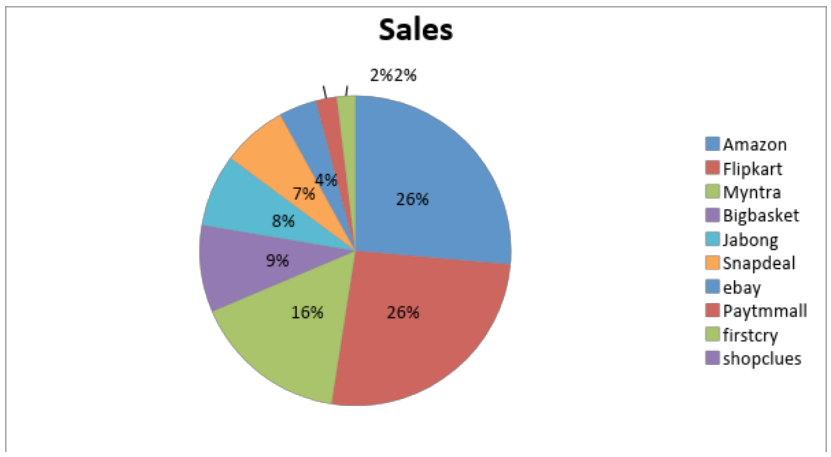


Fig 1: Market share of e-commerce sites in India

Privacy disruption

Privacy disruption is a threat in the current e-age era and especially in the e-commerce platform, there is no matter of source when one observes. The platform we are using for e-commerce is not just an online platform for buying and selling of goods but much more than that. From being a market of local sellers to providing services of intangible goods, like banking services and government documentation, e-commerce has evolved a lot from its basics. As technology is progressing, new technologies like cloud computing, Internet of Things (IoT), and artificial intelligence are gaining momentum in today's market. Times are gone when ARPANET was used between the students of Massachusetts Institute of Technology and the Stanford Artificial Intelligence Laboratory to sell cannabis. Now it is the time of chatbots, and drones are used to deliver the products. As technology is developing, the chances of hackers hacking the sites are also increasing. Nowadays, privacy and security are a major concern for e-commerce and emerging technologies. The applications that handle payments, like online banking, electronic transactions or using mobile payment, have more compliance issues in the field. Privacy issues have been found in e-commerce that prevent customers and organizations from engaging with e-commerce. Security is the main part that restricts customers from dealing with e-commerce. There are some programs, like worms, viruses, and Trojans, etc., that pose the greatest threat to e-commerce. Some issues have become a major concern for consumers with the rise in theft of data transferred online.

These concerns for consumers must be treated as a major concern for e-commerce service providers.

Right to privacy is the fundamental issue and it is suffering the most from a different type of threat. The two critical problems of both e-commerce and sites are the control over one's personal data and the attempted access to data by unauthorized peoples. "41% of web buyers surveyed last year felt that the online organization used their information unwisely" reported Forrester Research. Everyone has a different meaning of privacy, as Etzioni believes that societally illegitimate and infeasible measure is known as privacy, whereas Davis considers privacy as a squandered right. Some people consider it as a fundamental right where others consider it as a commodity that can be traded. Traders are exploiting the customer's privacy for the growth of their business. The privacy policy of any site or platform decides the amount of trust the customer has on the trader. Not everyone is comfortable paying online still when it is secured and convenient. They still prefer using cash over online payment because of privacy issues.

Cybercrime in India

According to a news report, "India has witnessed a 457% rise in cybercrime incidents under the IT act in 6 years[1]". Maharashtra has become the center of cybercrime, registering a maximum number of complaints arising from cybercrime. The main types used for cybercrime in India are unauthorized access and hacking, web hijacking, cyber stalking, etc. Pornography and child pornography has also been used by criminals to sexually abuse children. Many children have committed suicides and murders because of the mental trauma they have been through. Cyber laws are new so not everyone is aware of it. State governments are using different types of technology to secure people from cyber-attacks but major actions have not been taken in central government. Figure 2 explains the various security issues faced by the people.

Fig 2: Various Security issues

• **Data diddling:**

It is the illegal altering of data by entering into your computer and then changing the data back after their work is done. In this case, it is difficult to track the hacker. They use a virus to change the data or directly hack the system.

In data diddling, hackers enter into the computer by using a data entry clerk or a computer virus. This method helps hackers to alter the documents of any company or the details of payment cards of the customers. It affects e-commerce because a lot of data transfer happens every day and people are more concerned about privacy. If data is not secured then they think before doing work online.

• **Identity theft:**

Identity theft is the most common online fraud according to a study. In this type of theft, the criminal's target is to carry out transactions using a different identity. In order to commit identity theft, the criminal's goal is to get personal information, such as names, addresses, and email addresses, as well as the card details and account information. The identity theft enables fraudsters to do different frauds, like order items online under a false name and pay using someone else's card information.

It is common because it is easy to hack someone's account for a tech guy. It is the tradition theft with using new technology. The hacker transacts from the victim's account and uses the money or details for their use. This type of fraud is on the rise and that's the reason customers prefer cash on delivery (COD) over paying online. They have to provide details while paying online and if the site doesn't have a reliable security system, criminals can sneak into the system and make use of the data.

• **Friendly fraud:**

In friendly fraud, customers order goods or services and pay for them. After getting their product delivered, the customers deliberately initiate a chargeback, claiming that their card details were stolen. They get their money back but they keep the product with them. This type of fraud also tends to be combined with re-shipping.

There are many types of identity theft. Some of them are listed below:

★*Phishing*: It involves using fraud websites, emails or messages to access personal data of a person. Phishing is a type of identity theft. Criminals send messages, emails or links and if the person visits that site or replied to the message, the criminal gets access to the

personal data of the sender. These types of messages and emails are very common in everyday life and also increase the chances of a person to get trapped. E-commerce is widely affected by this because the message that customer gets is from a fake site of trustworthy brands.

★*Pharming*: It is stealing customers' data by hacking and then using it for self-use. This one of the easiest and one of the most common types of frauds in e-commerce. Many time what happens is the customer provides the necessary details to the company but hackers hack the site and take the customer details and use it for illegal activities. The data is stolen at the time when the transaction was happening so E-commerce sites have to suffer a lot because of this fraud.

★*Man-in-the-middle attacks*: In this type of case, a third person or a criminal alters the communication between the two parties who believe that they are communicating with each other. In man-in-the-middle attacks neither party is aware of the threat and both have to suffer. We can take the example of any two companies in which they are in contract with each other and are sharing their documents online, or placing an order online. The middle man will alter the details according to him and both the companies will end up in the loss. These types of attacks make the companies prone to attack and also keeps the confidential data at stake. These types of frauds are bad for sellers. Many times it happens that the customer gets the payment done by him back into his account because his data got stolen. Small companies cannot have resources to check the system so they end up giving the product for free. Sometimes it also happens that the customer initiates a return for the product and gives the duplicate product instead of the original one. By this, he also gets the real product and his money back. Nowadays, sellers are more alert and they check the product from various types so that they can get the real product sold by them.

- **DDoS attacks:**

Distributed Denial of service (DDoS) is used by the criminals to flood a server or a network with a request that results in a slowdown of the server. This lead to a halt in business operation and e-commerce. Many harmful viruses are used in DDoS attacks. It affects the number of people at the same time because the network gets affected by viruses. And the people who use these networks also affected by the viruses.

Sometimes the website or network stops working. Companies whose networks experienced a DDoS attack got affected the most as no one is able to reach them. These attacks also harm companies' brand images.

- **Clean fraud**

Here a stolen credit card is used to make a purchase, but the transactions are then manipulated in such a way that fraud detection functions don't come into light. In this type of fraud, criminals use sound analysis of the fraud detection systems deployed, plus a great deal of knowledge about the rightful owners of their stolen credit cards. Fraud detection solution is fooled by the criminals during the payment process by entering the correct information of the card holder.

This type of attack can harm people but they cannot claim their money from the company. On the other side, the company can take some measures to detect if the card is used by the owner or not. E-commerce sites are at major risk in this type of frauds as they deal with most of the transactions every day.

- **Salami slicing attack**

As the name suggests, a salami slicing attack is a process by which criminals steal a very small part at a time and keep on continuing the process at a different time so that it is difficult to detect the misappropriation.

Salami slicing attacks mostly happen to the people with big bang accounts. Here the fraudsters steal the personal data with the help of technology and then transact small-small amounts of money to their accounts. By this process, the owners don't notice that their money is decreasing day by day and thus gets fooled by the attacker.

Challenge to overcome these gaps in the cyber world

- **Failure to cover cybersecurity basics:**

The most common exploits used by criminals in the past year reveals that the basic fundamental measures to stop cybersecurity are lacking. This attracts attackers to hack the system easily. The negligence made by us allows the criminal to take advantage of and access whatever they need to do in our system.

- **Easy as well as complex:**

The computers are not safeguarded from illegal access because there is more possibility of breach due to the complex technology. Fraudsters nowadays can easily fool advance voice record, retina images, biometric system

and access codes and that are being used to get into the system. These things are done very easily but the complexity of the computer also helps them to hack it.

- **BYOD or Cloud:**

Companies nowadays adopt bring your own device policy to provide employees with better working experience and a more flexible environment. This increases the risk of fraud because of the involvement of more people.

- **Lack of accountability and integrity:**

Building a working environment where employees are not afraid to take responsibilities is crucial for successfully dealing with cyber-attacks. Lack of accountability is one of the biggest reasons for any company's exposure to cyber threats. There is a need for designated people in every company who can make the right decision when the time comes.

- **Lack of recovery plan:**

According to studies done over the last three years, an average of 77 percent of companies don't have a proper recovery plan to respond to incidents. Being prepared for a security attack is a must for a company and failing to which they keep falling prey to cybersecurity. The plan to save the company from cyber-attacks should include what can happen to prevent the attack, but also how to minimize the damage caused.

- **Aging infrastructure:**

Security also depends on the condition of the security system of the company. As we know, cybersecurity is not all about software. Hardware also plays an important role in it. The factors that should be kept in mind while buying or using the cybersecurity system are the age of the system, updating the system, monitoring the system and the technology used by the gadget.

- **Loss of evidence:**

Most of the time, the data doesn't get recorded in the system and it is very easy to destroy it. So the loss of evidence leads to an opportunity for the criminals and they get away easily after committing the crime. This is also the problem because of which the investigation doesn't take properly.

- **Statistics of cybercrime:**

The following figure shows the percentage of internet users in countries who have encountered a cyber threat in the year 2017. In this, Vietnam tops the list - a majority of internet users in Vietnam has encountered any cyber threat.

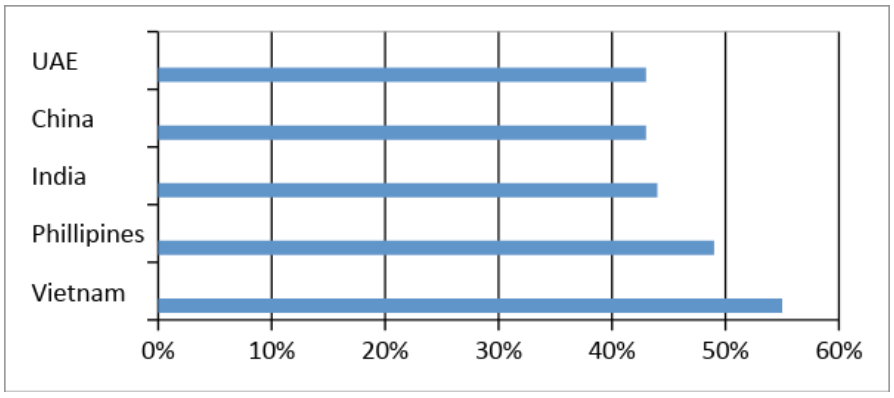


Fig 3: cybercrime rate in the world in the year 2017

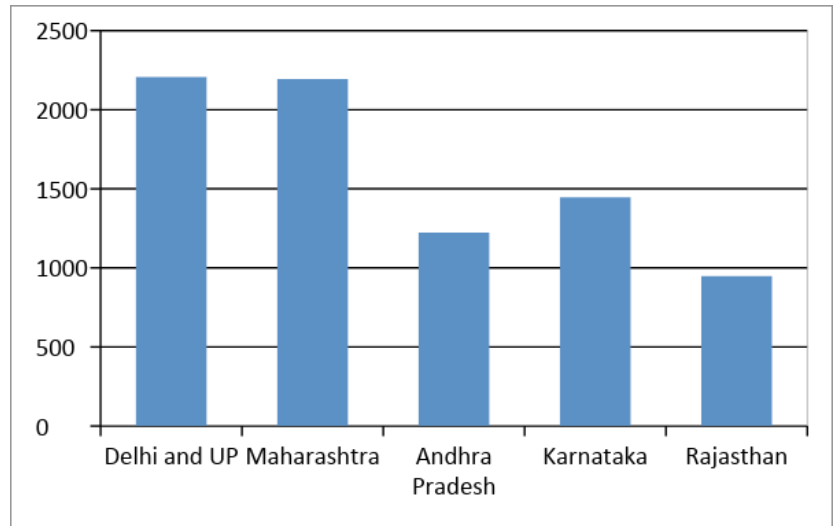


Fig 5: State-wise data of cyber-crimes filled in 2017

The incidents of cybercrime are rising in India, which makes it the 3rd most vulnerable country to cyber-attacks in the word. The numbers are expected to shoot up in the near future. The Indian government is making an effort to reduce e-commerce crime but the people should also be careful about it.

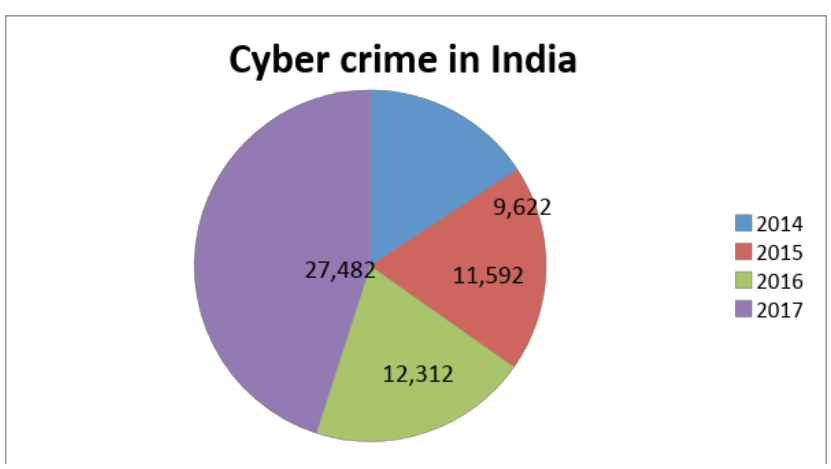


Fig 4: Cyber-crime in India during the year 2014-2017

Uttar Pradesh with Delhi is the most cyber attacked state in the country followed by Maharashtra and Karnataka.

Real time scenario of cybersecurity failure

- **Chinese hacker duped Tecnimont SpA:**

In a recent case of hacking, the Indian arm of the Italian company Tecnimont SpA came under attack by hackers taking managers into confidence that they are investing in the acquisition of any company. This is one of the biggest cyber frauds in the country. In this case, tech-savvy criminals sent emails to the chief of Tecnimont Company, through an email account that seemed similar to that of CEO of the company. Then the criminals arranged multiple conference calls to talk about a possible secretive and highly confidential acquisition in China. The hackers then convinced the Indian chief that the fund could not be sent from Italy because of certain regulations issues. The money was then sent from India to the banks in Hong Kong and it was taken out within a few minutes.

- **Millions of eBay password being stolen:**

At the beginning of March 2014, the customer to customer giant eBay noticed that an unsolicited database session was scanning the password files in their main servers. The company later officially announced that an undisclosed part of more than 120 million users had been compromised for credentials and personal information. The goal of the hackers was to obtain the staff's data and with that, it also wanted to access their database and steal personal information. From there they wanted to either collapse the eBay day to day operation or use the data for phishing attacks.

- **DDoS attacked PayPro:**

Headquartered in Toronto, PayPro is a suite of e-commerce solutions that cater specifically to software developers and vendors, helping them simplify the distribution and reselling of their products. In 2012, a seven layer DDoS attacked the company due to which the worldwide customer base of software developers could not generate revenue. The hackers' target for this attack was to stop the site so that the company will stop generating revenue and succeeded in it. After that PayPro got DDoS protection from Prolexic, which is a leading Canadian software distribution service.

In the future - Privacy and Security

In this digital era, privacy and security remain a serious concern. There are many measures taken by e-commerce sites, banks and companies to secure their customers' data. These measures are taken to make sure that the data of companies or customers remain intact. Although actions are taken for security, still there are many cases in which the privacy of the customers has damaged. Companies spent a lot on data security so that they can maintain a their relationship with customers. Customers are not always sure before transacting money, sharing information or trading goods online. But companies try to provide the best possible way to secure customer data and ensure the customer that the data will not be used unnecessarily. These actions taken by companies make customers trust them and also help customers in completing a different task. As privacy and security are the prominent factors in e-commerce, all the companies dealing in e-commerce spend a lot on security. According to Forbes site, "worldwide spending on information security and services will reach over $114 billion in the year 2018". Companies are working hard to securely use technology platforms to become more competitive and drive growth for the business. Big companies like Google and

Facebook also spent a lot of time and resources for the security and privacy of customer data. Google CIO (Chief Information Officer) said that they spent a lot of time on worrying about the privacy of data and also work very hard to keep it intact, on the other side, Facebook CEO Mark Zuckerberg said that they spent more than $20 billion for security and this investment is expected to increase by 50% in the year 2019.

As cybercrimes are rising, we also have to develop technologies so that these crimes can be avoided. Sometimes technology also makes ways for criminals to disturb the privacy of people but we should start making the technology without loopholes in it. It is very important to help the customer to trust e-commerce. Every organization should have its security and privacy policy so that if intruded, the best possible way to punish the criminal should be taken. More studies and more awareness programmes should be organized to spread awareness of cybercrimes.

[1]https://telecom.economictimes.indiatimes.com/news/india-saw-457-rise-in-cybercrime-in-five-years-study/67455224

Reference:

- Davies, Simon G. 1997. Re-Engineering the Right to Privacy: How Privacy Has Been
- Transformed from a Right to a Commodity. In Technology and Privacy: The New Landscape.
- Edited by P. Agre and M. Rotenberg. 143-165. Cambridge, MA: MIT Press.
- Etzioni, Amitai. 1999. The Limits of Privacy. New York: Basic Books.
- Fisher, Susan. 2001. Privacy By Design. InfoWorld, 23 (27) : 20-22.
- https://www.information-age.com/seven-types-e-commerce-fraud-explained-123461276/
- https://digitalstrategy.ie/security-issues-in-e-commerce/
- https://www.benzinga.com/14/09/4840193/4-e-commerce-security-failure-case-studies
- https://blog.detectify.com/2016/11/17/7-most-common-e-commerce-security-mistakes/
- https://www.ndtv.com/topic/cyber-security
- https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html

- https://www.varonis.com/blog/cybersecurity-statistics/
- https://preyproject.com/blog/en/24-cybersecurity-statistics-that-matter-in-2019/
- https://www.researchgate.net/post/What_are_the_Major_causes_of_cyber_security_attacks_today
- https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/#failure
- https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#db5f0b827ea2
- https://krazytech.com/technical-papers/cyber-crime
- https://www.timesnownews.com/business-economy/companies/article/how-chinese-hackers-robbed-rs-130-crore-in-one-of-india-s-biggest-cyber-fraud/344871
- https://www.finextra.com/pressarticle/47991/paypro-global-fights-ddos-threat-with-prolexic
- https://dazeinfo.com/2015/01/06/cyber-crimes-in-india-growth-2011-2015-study/
- https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/
- http://ncrb.gov.in/StatPublications/CII/CII2015/FILES/Statistics-2015_rev1_1.pdf
- https://timesofindia.indiatimes.com/business/india-business/cyber-crimes-rose-between-2014-and-2017-govt/articleshow/62380670.cms
- https://www.india.com/news/india/27482-cases-of-cybercrimes-reported-in-2017-one-attack-in-india-every-10-minutes-2341055/
- https://pdfs.semanticscholar.org/ffe1/c67215a7b902c9af8219f15cdcfc767418e5.pdf
- http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html
- https://telecom.economictimes.indiatimes.com/news/india-saw-457-rise-in-cybercrime-in-five-years-study/67455224

About Mary

Dr. P. Mary Jeyanthi is working as an Assistant professor at the Institute of Management Technology, Nagpur,

Maharashtra. Over 10 years of experience in Information Technology and Banking Technology and Analytics. She has done Ph.D. research in *"A New Implementation of Mathematical Models with metaheuristic Algorithms for Business Intelligence"*. She has developed the new soft computing techniques known as "Artificial Bear Optimization", which is inherited from the animal Bear and its smelling functionality used for Optimization. She has gone for a guest speaker for MDP & FDP Programs. She has expertise in Business Intelligence and Business Analytics.

Website: http://www.imtnagpur.ac.in/profile?id=50

About Anshul

- PGDM finance student at Institute of Management and Technology, Nagpur.
- Coordinator of Center for Sustainability, Growth, and Development.

5 Ways That AI is Enabling More Efficient Forensic Investigations

By Sarah Hargreaves

The process of how we conduct digital forensics investigations makes this an industry that is ripe for disruption by Artificial Intelligence (AI) technologies. In all significant investigations, forensic examiners and law enforcement professionals have a large and often complex data set that must be collected, reviewed and analyzed. Meanwhile, most agencies have been unable to secure budget increases that are sufficient for them to add the human and IT resources needed to handle these rising demands.

"Digital forensics is an area that is becoming increasingly important in computing and often requires the intelligent analysis of large amounts of complex data," according to a study published by Digital Evidence & Electronic Signature Law Review. "It would therefore seem that AI is an ideal approach to deal with many of the problems that currently exist in digital forensics."

There are three major phases in the forensics investigation workflow that illustrate the impact AI is already having in our industry:

* Culling — We're now applying machine learning to high-volume data analysis by conducting repeatable tasks to cull through an initial pool of data with pre-determined search terms;

* Surfacing — We're putting AI to work on that filtered data set to surface specific evidence by identifying text and images that are responsive to the investigation focus; and

* Judgments — Then we're turning the case over to human investigators who are able to use

subjective analysis of the findings to make reasoned judgments and drive the investigation forward.

In other words, the key is to remember that the investigator remains in control at all times. The AI technology is merely an aid that assists the human being to do their work more efficiently.

Here are five ways that AI is enabling more efficient digital forensics investigations:

1. Investigation

AI makes it possible to quickly document and organize the who/what/where/when fundamentals of the way an investigation is prepared. This allows investigators to proactively use the intelligence gathered in the early phases of the investigation and collection process of quickly identifying focused and relevant information, including crime types, persons of interest, specific date periods and location. Relevant evidence is located quickly, efficiently, and with the clear objective of getting the results they need.

2. Cross-Case Analysis

One of the tremendous efficiency gains that AI delivers to forensic investigations is the power to review numerous case folders simultaneously, to reveal common contacts, geo-locations and images of potential relevance. Investigators frequently work with multi-exhibit cases, but cross-case analysis allows for intelligence and evidence to be gathered across multiple cases. This can include data pertaining to victims, suspects and specific crime information. The strength of cross-case analysis can be seen in large-scale investigations where evidence items are introduced into the evidence set progressively. The strength of AI provides investigators with opportunities to identify relationships between specific subjects without the need to backtrack over previously submitted exhibits.

3. Image Recognition

The newest generation of AI technology applies machine learning technology to images. Essentially, professionals can feed images into the software (e.g., photos of a person of interest) and open-source machine learning technology will train the system to accurately identify what is contained in those images. It goes without saying that investigative work such as victim identification can be heavily supported with the power of AI. Additionally, high-speed identification of specific image objects, such as firearms, drugs, or group affiliations can provide opportunities to get to the heart of the data when time is of the essence.

4. Document Clustering

AI now makes it possible to deploy tools that analyze data contained within a case file and find various links between those pieces of evidence that might have otherwise been overlooked. The software can then organize the data for the forensics professional by conducting smart classification of the evidence into specific document clusters. There are times when investigators, faced with large and unwieldy data sets, need high level information relating the content of documents, emails and communications. Keyword searching is standard in forensic investigations, but this relies on one thing: the knowledge of what to look for. Document clustering provides an investigator with information about document themes, commonly used words and phrases, and the identification of slang terms used to evade detection. This intelligence provides an unparalleled opportunity to review large document sets proactively and can alleviate the need for the review of vast amounts of communication data.

5. Decision Tree

Decision tree investigation, like other AI features, provides the investigator with the ability to drill into the dataset to locate specific data. Investigators can use information gathered during their analysis to mark data samples as "relevant" or "irrelevant". This provides for deep and intelligent filtering of data for information that is relevant and to weed out data that is not. The resulting information is targeted for more developed analysis, saving time, cost and the need for lengthy review of information that may or may not be of evidential interest.

New advanced forensics tools leverage the power of AI to support the digital forensics investigation workflow. These software applications learn from past cases and make it easier to locate, understand and report on key pieces of data. With machine-learning capabilities, the technology reveals new connections in just a matter of hours that can potentially sharpen the focus and direction of a digital investigation.

AI is a tremendous technological breakthrough that is now delivering extraordinary new workflow efficiencies and enabling new investigative discoveries previously not possible.

About the Author

Sarah Hargreaves is Senior Instructor for Digital Investigations, International, at AccessData, a leading provider of integrated digital forensics and e-discovery software. For more information, please go to www.accessdata.com.