Department of Forensic Computing and Security

**Digital Forensics Fundamentals**

Expert Witness Statement

Conducted by Dawn Fish

1st November 2019

# Table Of Contents

[**Table Of Contents**](#_yeub2j7pp90z) **2**

[1. SIO Brief.](#_36rij4coe81v) 3

[2. Investigation Model Used.](#_6ep1qtz0x13k) 3

[2.1 Identification](#_rb1kwex88jr7) 3

[2.2 Preservation](#_69h5y6vo1o) 3

[2.3 Collection](#_561vi87zzuh) 3

[2.4 Examination & Analysis](#_x3mkg0dfxdhs) 3

[2.5 Presentation](#_2ked0jdofows) 4

[3. Theories, hypotheses, Assumptions, and Objectives.](#_95na0395g1gi) 4

[4. The evidence that points to those crimes, and the strength of that evidence.](#_18803nj3pgmg) 4

[Bibliography](#_n855yryudma4) 7

## 

## 1. SIO Brief.

An individual has been arrested as a result of a lengthy serious crime investigation. A memory stick was among the personal possessions recovered during an authorised search of his home.

The device has been imaged. You have been tasked with a thorough investigation of the image, and with producing a Technical Witness Statement and an Expert Witness Statement.

The statements are to be produced for the SIO and CPS with a view to prosecuting the individual.

## 2. Investigation Model Used.

The investigation method used was DFRWS. This model includes 6 steps: Identification, preservation, collection, examination, analysis, and presentation.

### 2.1 Identification

The individual was profiled and crime was detected, a case was built in order to learn information and arrest the individual.

### 2.2 Preservation

The devices recovered from the crime scene would need to be preserved in order to maintain the integrity of the evidence and the case itself. In this case, the evidence that was recovered was imaged. A chain of custody and analysis was also devised in order to help maintain integrity.

### 2.3 Collection

The relevant data is collected by using approved methods, software, tools and hardware. We performed other recovery techniques and data reduction.

### 2.4 Examination & Analysis

Examination and analysis are the next two steps in the investigation model and they are similar in the way the investigator tackled it. These two steps are where our investigators began to use several different techniques in order to extract hidden and valuable information and data and begin to look for patterns.

### 2.5 Presentation

The last step in the DFRWS model is the presentation. This is where we begin to understand and clarify the information and data and make conclusions. (Infosec Resources, 2019)

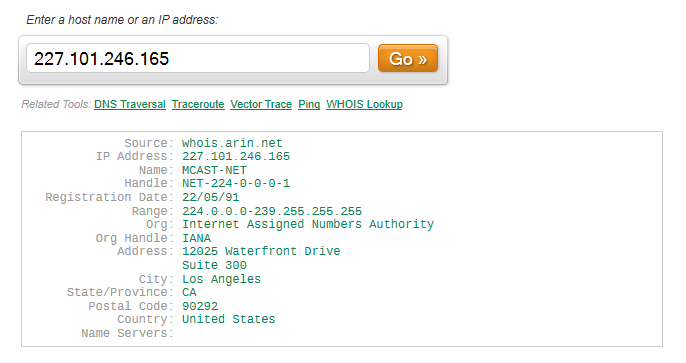
## 3. Theories, hypotheses, Assumptions, and Objectives.

The evidence included drones and one theory is that drones may be another word for a cyber attack considering we found IP addresses associated with the drones. The evidence also included attack ports and protcols, espceially UDP which is known for a UDP flooding attack causing a DDoS attack. Another theory could be that drones are another word for compromised computers in a botnet. A third theory was that Drones may actually be drones and the IP addresses associated are the targets for a drone strike.

## 4. The evidence that points to those crimes, and the strength of that evidence.

I found evidence of 8 drones in play, IP addresses of the targets, attack protocols, attack ports and other concluding evidence; this evidence implies that the planned attacks would be both digital and physical. The IP addresses found with associated Drones when investigated further returned high profile locations such as the Internet Assigned Numbers Authroity that is associated with Drone 1.

|  |  |
| --- | --- |
| Drone 1 | 227.101.246.165 |
| Drone 2 of 8 | 222.228.9.204 |
| Drone 3 of 8 | 185.155.194.207 |
| Drone 4 of 8 | 29.136.122.72 |
| Drone 5 | 30.172.190.59 |
| Drone 6 of 8 | 70.0.175.158 |
| Drone 7 | 55.121.2.25 |
| Drone 8 | 30.4.89.9 |



The evidence found suggests that there will be a total of 4 attacks; 4 attack targets, 4 attacks start dates and 4 attack start times were found. The evidence that suggests that there will only be 4 attacks is extremely strong considering all attack data that was found had 4.

|  |  |
| --- | --- |
| Attack 1 Start Date | 2019-08-02 |
| Attack 2 of 4 Start Date | 2019-08-09 |
| Attack 3 of 4 Start Date | 2019-06-29 |
| Attack 4 of 4 Start Date | 2019-07-21 |

|  |  |
| --- | --- |
| Attack 1 Start Time | 16:45 |
| Attack 2 of 4 Start Time | 19:30 |
| Attack 3 of 4 Start Time | 12:30 |
| Attack 4 Start Time | 21:45 |

The evidence that suggests that it will be a digital infrastructure attack is good; I found no physical addresses such as a house name or number but instead addresses for IPs. However, We reversed search the IP addresses and found that they were tied to physical locations, this could suggest that these locations maybe the target for cyber attack or drone attack.

|  |  |
| --- | --- |
| Address 1 of 3 Xor | 160.200.167.211 |
| Address 2 Xor Part 1 | 207. |
| Address 2 of 3 Xor Part 2 of 3 | 9.22 |
| Address 2 of 3 Xor Part 3 of 3 | 7.217 |
| Address 3 of 3 Xor Part 1 of 2 | 184.129. |
| Address 3 of 3 Xor Part 2 of 2 | 08.122 |

|  |  |
| --- | --- |
| Attack 1 of 4 Port | 25 |
| Attack 2 of 4 Port | 22 |
| Attack 3 Port | 10 |
| Attack 4 Port | 53 |

|  |  |
| --- | --- |
| Attack 1 of 4 Target Part 1 of 2 | 167. |
| Attack 1 of 4 Target Part 2 of 2 | 91.93.5 |
| Attack 2 Target | 159.45.170.145 |
| Attack 3 Target Part 1 | 111 |
| Attack 3 of 4 Target Part 2 of 3 | 90.2 |
| Attack 3 Target Part 3 | 35.86 |
| Attack 4 Target | 167.91.19.255 |

## 

## Bibliography

Infosec Resources. (2019). *Digital Forensics Models*. [online] Available at: https://resources.infosecinstitute.com/digital-forensics-models/#gref [Accessed 14 Nov. 2019].