



FACULTY OF SCIENCE & TECHNOLOGY
Department of Computing & Informatics
Forensic Computing & Security

Digital Forensics Fundamentals

Paul-David Jarvis
s5115232@bournemouth.ac.uk

Expert Witness Statement

Table of Contents

1.0 SIO Brief	5
2.0 Investigation Model Used	5
2.1 Identification	5
2.2 Preservation	5
2.3 Collection	5
2.4 Examination & Analysis	5
2.5 Presentation	6
3.0 Theories, hypotheses, Assumptions, and Objectives	6
4.0 The evidence that points to those crimes, and the strength of that evidence	6
References	10

List of Figures

Figure 1: IP Lookup. - (Ultratools).....	7
--	---

List of Tables

Table 1: Drone Table.....	
6	
Table 2: Attack Start Dates.....	7
Table 3: Attack Start Times.....	8
Table 4: Addresses.....	8
Table 5: Attack Ports.....	9
Table 6: Attack Targets.....	
9	

1.0 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.

2.0 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)

3.0 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 protocols, especially 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 be drones and the IP addresses associated are the targets for a drone strike.

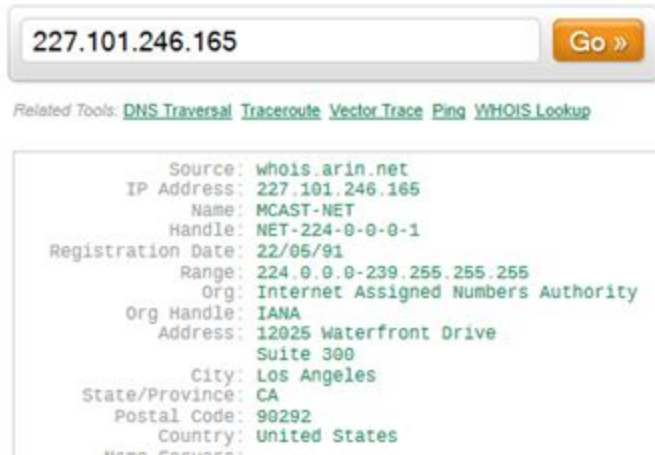
4.0 The evidence that points to those crimes, and the strength of that evidence

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 Authority that is associated with Drone 1.

Drones	
Drone Description	IP Address
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

Table 1: Drone Table



227.101.246.165 Go »

Related Tools: [DNS Traversal](#) [Traceroute](#) [Vector Trace](#) [Ping](#) [WHOIS Lookup](#)

```

Source: whois.arin.net
IP Address: 227.101.246.165
Name: MCAST-NET
Handle: NET-224-0-0-0-1
Registration Date: 22/05/91
Range: 224.0.0.0-239.255.255.255
Org: Internet Assigned Numbers Authority
Org Handle: IANA
Address: 12025 Waterfront Drive
Suite 300
City: Los Angeles
State/Province: CA
Postal Code: 90292
Country: United States

```

Figure 1: IP Lookup. - (Ultratools)

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 Start Dates	
Attacks	Dates
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

Table 2: Attack Start Dates

Attack Starting Time	
Attacks	Times
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

Table 3: Attack Start Times

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 may be the target for cyber-attack or drone attack.

Attack Addresses	
Address	IP Address
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 Xor Part 1 of 2	184.129.
Address 3 Xor Part 2 of 2	08.122

Table 4: Addresses

Attack Ports	
Attack	Port
Attack 1 of 4 Port	25
Attack 2 of 4 Port	22
Attack 3 Port	10
Attack 4 Port	53

Table 5: Attack Ports

Attack Targets	
Attack	IP Address
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

Table 5: Attack Targets

References

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