Yibiao Liao

Is 4483-003 | digital FOrensic i

CAPSTONE ASSIGNMENT

report of findings

May 9TH ,2021

**Background:**

**Date: April 26th, 2021**

One of the symbols of United States, the Washington Monument was destroyed in a blast. It is a major disaster to the country and its people. Not our national security was threatened, the explosion also took away 72 innocent life. Suspect Ryan Falcony from San Antonio, Texas has been arrested and 3 of his thumb drives were recovered from his residence. All three drives were the same size, 65537 KB, with the names of Ryan\_Falcony\_Thumbdrive\_01, Ryan\_Falcony\_Thumbdrive\_02 and Ryan\_Falcony\_Thumbdrive\_03.

Their MD5 Hash are

6CA3A5FA52D437C96E839A95530232DF,

D3E3616019EE207150822925017D9949,

8BB15E90FB13A9E482F6023E1A2908F0.

Goals:

Find out when and where did Falcony stay at Washington DC.

Find out Falcony’s connection with any known terrorist organizations.

Find out Falcony’s contacts.

Find out what types of explosives he used for this operation, how were the explosives obtained and how was Falcony trained.

Find out Falcony’s plans for the future.

**Items Analyzed**

**Item:** Ryan Falcony’s thumb drive

**File name:** Ryan\_Falcony\_Thumbdrive\_01

**Size:**65537 KB

**MD-5**: 6CA3A5FA52D437C96E839A95530232DF

**Item:** Ryan Falcony’s thumb drive

**File name:** Ryan\_Falcony\_Thumbdrive\_02

**Size:**65537 KB

**MD-5**: D3E3616019EE207150822925017D9949

**Item:** Ryan Falcony’s thumb drive

**File name:** Ryan\_Falcony\_Thumbdrive\_03

**Size:**65537 KB

**MD-5**: 8BB15E90FB13A9E482F6023E1A2908F0

**Discussion of Findings**

**Files Found**

Multiply images of hazard chemicals, travel plans, and encoded message were found in the thumb drives. It is evident that Mr. Falcony planned and create this catastrophe.

1. Exhibit A: \-\(folder)

Airline ticket from San Antonio to Washington DC, breakfast receipt, image of the monument with places circled out and a map direction from his hotel to the monument.

Location: Ryan\_Falcony\_Thumbdrive\_02\-\ walk.jpg

Ryan\_Falcony\_Thumbdrive\_02\-\ ticket.jpg

Ryan\_Falcony\_Thumbdrive\_02\-\ jul.jpg

Ryan\_Falcony\_Thumbdrive\_02\-\ breakfast.jpg

1. Exhibit B: images2.jpg

Multiple communication between suspect and another person called “Mani” was found in the image. A terrorist organization name and suspect’s travel plan were included in the communication.

Location: \Ryan\_Falcony\_Thumbdrive\_01\images2.jpg

1. Exhibit C: images11.jpg

An encoded message was found in this Images including suspect’s contact’s WhatsApp number and directions to creating a bomb.

Location: \Ryan\_Falcony\_Thumbdrive\_03\ images11.jpg

1. Exhibit D: amzn(folder)

Shopping history of suspicious chemicals and potential combining processing images were found in the folder.

Location: \Ryan\_Falcony\_Thumbdrive\_03\amzn

1. Exhibit E: download2.jpg

Multiple communication between suspect and another person called “Mani” was found in the image as well. And some instructions regarding how to make the bomb.

Location: Ryan\_Falcony\_Thumbdrive\_02\download2.jpg

1. Exhibit F: ready

File with no suffix was found in Thumbdrive 1.

Location: \Ryan\_Falcony\_Thumbdrive\_01\)\ready

**Exhibits**

1: Exhibit A: \-\(folder)

图形用户界面, 应用程序

描述已自动生成

Images in this folder showing the southwest airline ticket from San Antonio to Washington DC. 图形用户界面, 文本, 应用程序

描述已自动生成

The hotel suspect stayed in DC. 地图

描述已自动生成

图形用户界面, 地图

中度可信度描述已自动生成

As well as possible bomb placing points.

城市的风景

描述已自动生成

1. Exhibit B: images2.jpg

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

Multiple communication between suspect and Mani was found within the file. As well as a YouTube link to a bomb instruction. Last message also unravels that suspect is a member of terrorist group Al-Shabaab.

3.Exhibit C: images11.jpg

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图片包含 文本

描述已自动生成 图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成 图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

More communication between suspect and Mani was found. 512-239-4880 revealed as Mani’s contact number. And Mani also sent link about explosive making videos to the suspect, and suspect also contacted Mani for futher updates.

1. Exhibit D: amzn(folder)

图形用户界面, 应用程序

描述已自动生成 桌子上放满了不同类型的饮料

低可信度描述已自动生成

Images of suspective chemicals were purchased by suspect on Amazon. Also the pictures of setting up for chemicals were also found in the folder.

1. Exhibit E: download2.jpg

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成 图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成 图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成 图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

文本

描述已自动生成 图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成 地图

描述已自动生成

In suspect discussion with Mani, another video link to explosion making video was found, suspect also told Mani that he will go with Potassium Nitrate for his Washington DC mission. Further, Mani provide suspect another link with details of their future mission plans and well as some suggestions on the chemicals. The message in the link was decoded. And turns out their next target will be Disney Park at Orlando Florida.

1. Exhibit F: ready

人在系鞋带

描述已自动生成

File was viewable after changing to a .jpg file. A photo of a bomb-like device hidden in a gym bag was discovered.