Investigation Considerations

Ifeanyi Uzoukwu

CST 640

University of Maryland Global Campus

**Table of Contents**

Introduction……………………………………………………………………………………… 3

Preparing for the Investigation…………………………………………………………………... 3

Forms and Interview Questions…………………………………………………………………. 5

**Introduction**

Investigations are needed for performing fact-finding processes that are impartial and objective for the purpose of establishing patterns in the evidence presented with hopes of leading to a breakthrough that allows for the truth to unfold. This is also true of cyber investigations. When crimes are committed and a trail of evidence is left on devices, networks or on the internet, cyber forensics investigators must find all relevant information and preserve it for analysis. Networks that are thought to be secure are constantly warding off potential attacks from threat actors. Cybercrimes, such as website spoofing, IOT hacking, phishing scams, ransomware, and identity theft are all on the rise as the world moves forward and continues to embrace technological advances. Digital forensics investigators are tasked with finding evidence from devices and making that evidence viewable in a court of law. Targets of cybercriminals range from financial institutions and government organizations to regular citizens and even children. Due to this expanding medium in which criminals are committing heinous crimes, there is an alarming need for cybersecurity professionals to join the ranks of those that protect our well-being online. Cybersecurity Investigators must be trained to find data even when it is being hidden by cyber criminals and create relevant interview questions and determine the specific resources and tools that enables investigators to find out the identity of the cyber threat actors.

**Preparing for the Investigation**

Once the investigator figures out the basic questions of the crime, such as “who are the major players?” and “what kind of evidence are we looking for?”, we can determine the best path to follow to find the evidence. Before initiating the investigation, we need to be sure that we have a search warrant. Once they are authorized by a judge or another figure that is presiding over the specific case, Search Warrants can be used to give the police or the party investigating the crime in question the freedom to examine the whereabouts and belongings of the person of interest. For a search warrant to be obtained, probable cause must be shown, and the warrant itself must specifically list an item or location that the investigators are interested in searching. Laws on search and seizure of property can be found in the fourth amendment of the constitution. Once we can verify that we are authorized to collect the evidence, a chain of custody form must be filled out for each item obtained. The Chain of custody is a form that tracks the lifecycle of evidence, including the names and dates of its initial collection, each time it is moved, where the evidence is being kept, and when the evidence is used or analyzed. Chain of Custody forms must be kept up to date to avoid the investigation being compromised.

Investigators can also serve subpoenas to retrieve the information they are looking to acquire. Subpoenas are writs that are created for the purpose of getting an individual or a member of an organization to appear in court proceedings. Normally, Subpoenas must be followed up with or else the person or party in question can be held in contempt of court. If the requested information is protected by federal and state laws, then the person must sign an authorization form.

The Jurisdiction refers to the territory or sphere of activity over which the legal authority of a court or other institution extends. In terms of a cyber forensics investigation, the jurisdiction is decided by the nature of the crime, the evidence that is found, and the location in which the crime took place. These factors are pivotal to a cyber investigation as they decide if the local, state, or federal office will oversee the case.

The Plain View Doctrine is a rule that states that evidence of a cybercrime that is found in the midst of a search and seizure for another crime, can also be seized. However, a search for additional evidence relating to the new evidence found would require another search warrant. If the plain view doctrine is not adhered to when an investigator finds evidence, then the defense team could argue that because the investigator went outside the original scope of the search warrant, then the evidence that would have found the perpetrator guilty should become inadmissible.

Once the preparation for the investigation is complete, and investigators understand the scope of the investigation to be conducted, we can proceed to the collection of the forms and create a list of the questions to be asked during the interview.

**Forms and Interview Questions**

The figures below represent some of the forms that are commonly involved in cyber investigations.

UNITED STATES DISTRICT COURT

for the

Southern District of New York

 In the Matter of the search of              )  
HP 24 df0076 1IFNEEU39, IP Address:                  )

92.168.14.1,HP Pavilion 52CSHE32T,                                   )         Case No. CR-427832NYC

IP Address 192.168.16.5), and                                     )

SanDisk 64 GB thumb drive                                         )  
                                                                            )  
                                                                            )  
In re Application for a Warrant Under Rule 41

of the Federal Rules of a Criminal Procedure

**SEARCH AND SEIZURE WARRANT**

To: Any Law Enforcement Officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property: **the aforementioned computers and thumb drive** located in the district of **New York.** 

I find that the affidavits provided or any recorded testimony, establish probable cause to search and seize the property described above, and that such search will reveal **evidence of cyberattacks launched against a government organization.**

Figure : Sample Search Warrant

**YOU ARE COMMANDED**  to execute this warrant on or before **July 20th, 2021, at any time in the day or night because good cause has been established.**

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom or from whose premises the property was taken, or leave a copy and a receipt at the place where the property was taken.

The officer executing this warrant, or the officer present during the execution of this warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to **Albert Sambi Lokonga**.

⃞  Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification that may have an adverse result listed in 18 U.S.C. § 1805 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched and seized.

Date and Time Issued: 3:15 July 16th, 2021

Judge’s Signature: Albert S. Lokonga                                                  City and State: New York, New York

Printed Name and Title: Hon. Albert Sambi Lokonga, United States Magistrate Judge

For a search warrant to be obtained, probable cause must be shown.