Operation Stop Hack

Carlos Llerena

Strayer University

SEC 340 Computer Forensic

Professor Darcel Ford

October 21, 2022

**Operation Stop Hack**

The Law in the United States has spelled the bare minimum for the officers when collecting digital evidence (Bill, 1). Ideally, technology has been incredibly advanced, and law enforcement officers deal with new challenges every time. In the case of an operation stop hack, following the confirmation of the IP addressed, a warrant is issued to investigate and collect evidence related to a potential underground hacking ring. In that connection, law enforcement officers must follow legal procedures when collecting evidence.

**Legal consideration**

The legal statutes require that an officer be guided by probable cause before obtaining a search warrant (Bill, 1). The officer should be convinced beyond reasonable doubt that there is evidence in the place or person the officer wishes to search. The guiding principle is the preponderance of the evidence. After getting a warrant and arriving at the crime scene, the law enforcement officer should secure the crime scene to avoid evidence contamination (Phillips, 4). The lead officers should reduce the number of officers entering the crime scene; once in the room, the officer should take a photo of the crime scene.

The next step would be to identify the number of digital devices in plain view. Document the devices against their serial numbers or models, identify the Operating System (OS) and estimate the possible storage capacity of the devices. Using appropriate tools, the police should collect fingerprints from the crime scene. It is an important step because it will help identify the suspects. Legally, law enforcement officers should seize all digital devices. The other step would be to try and establish those in charge of the facility. Save for the investigator if the suspect is found in the facility; if not investigator should determine whether there is any document (in plain view), that can identify the suspect (Maras, 3). Once all the documents have been seized, they should be taken to the lab for processing of the data.

**Processing of Digital Evidence**

Ideally, when processing digital evidence, the basic rule is to only allow investigators only at the crime scene (Maras, 3). Eliminate onlookers and officers who have no role in the investigation. The first step would to take a video of the whole view of the room, the ceiling, the floor, and the connection of the computers. Secondly, sketch the arrangement of the devices and their connection. Keeping a record of the proceedings would help immensely. However, officers should only record evidence that is related to the case. The officer should check the state of each digital device. For instance, if the computer is off should be left off. For the case of the desktop, if the desktop is on, the experts should use Virtual Machines to recover all data that may be lost when the device goes off. Virtual Machines will help run OS on the existing physical computer to access any hidden information (Phillips, 4). The officer should use that opportunity to identify computer-stored and computer-generated records.

Since the warrant identified the IP of the computers, the law enforcement officer can determine the computer-stored records. Using that approach, the officer can determine the sites that the device has accessed. The device will show who the suspect communicates with. Besides, the officer can access the computer-generated records in the computer. The information stored in the word processor should make part of evidence documentation. Once the officer is through with extracting data and saving it in an external device, he or she should shut down the device.

The lead officer should assign one police officer to log the collected evidence. The evidence should contain the date, time, and name of the officer in charge; the lead officer should verify the evidence to avoid contamination. Lastly, the officer should remember to create a backup for the evidence. The officers should seize all the devices to repeat the same process in the lab.

**Analysis of Crime Scene Diagram**

The crime scene had a brown four-legged wooden table. All the digital devices were on the table; there was nothing else except six electronic devices. The officer collected all six digital devices that were linked to the crime. The first device to be collected was a wireless access point. Officers can use a wireless access point to determine the devices that access it. Since it is a window to access the internet, any information that the suspect accessed through it can be identified (EC-Council, 2). The second device to be confiscated was an external media drive. Ideally, it was an external hard drive that the suspect used to save documents. Using a digital forensic tool, the officer can extract the content from the hard disk. The printer can also be used for forensic evidence. The scanned documents can be left on the computer, which can be used to corroborate the collected evidence (EC-Council, 2). More so, the printed documents held hints about the printer used. The law enforcement officer can also use the collected router by issuing a "show command" to determine the logs and networks used. Besides, the officer can also use a PC to determine the images, emails, and computer documents that the suspect used. Lastly, the officer will also rely on the smartphone to corroborate the evidence collected on the other devices. Through the smartphone, the officer can isolate transactions, texts, and emails sent to different individuals. With all that information, the officer will have gathered enough evidence to exonerate or incriminate the suspect.

Sources

1. Bill Nelson. 2019. Guide to Computer Forensics and Investigations (6th ed.). MindTap/Cengage.

2. EC-Council. No date. [Computer Hacking Forensic Investigator Certification](https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/). <https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/>

3. Maras, M. H.2015. Computer forensics. Jones and Bartlett Learning.

4. Nelson, B. Phillips, .2014. Guide to computer forensics and investigations. Cengage Learning.