Cybercrime Investigation

How does the criminal justice system respond to cybercrime? The same criminal justice agencies which respond to traditional, terrestrial crime are tasked with responding to cybercrime.

1) Police
    a) Investigage crime scene(s)- often obtaining search warrant;
    b) Interview witnesses, victims, persons of interest, suspects;
    c) Collect, manage, preserve, store evidence;
    d) Arrest suspects.
2) Courts
    a) Prosecutor conducts grand jury or preliminary hearing;
    b) Prosecutor prepares indictment or information charging suspect with crime;
    c) Court arraigns suspect, takes plea, sets bail;
    d) Court tries defendant on criminal charge;
    e) Court sentences defendant (if found guilty).
3) Corrections
    a) Carries out sentence imposed on defendant by court;
    b) Releases convict upon satisfactory completion of sentence.

These same criminal justice agencies must respond to cybercrime to carry out the same duties and responsibilities. However, the task of responding to cybercrime, particularly for police and courts, is considerably more complicated because of certain features of cyber crime we have noted previously.

We have previously noted that certain features of the Internet are conducive to criminal activity. In particular:

1) The Internet has changed the scene or location in which crime occurs- victim and offender no longer have to be in the same place at the same time;
2) Actors on the Internet are (relatively) anonymous- even if offenders use names, there is no guarantee that the names used are authentic;
3) The Internet is decentralized so that no central authority controls the Internet;
4) Everyone on the Internet is connected to everyone else on the Internet;
5) All users of the Internet are equally vulnerable to being victims of some form(s) of cybercrime.

These same features which make cybercrime possible on the Internet also make it more difficult for the criminal justice system, particularly law enforcement, to respond to cybercrime.

Some further complications in investigating cybercrime follow from these features:

•The victims of cybercrime can be dispersed in many different and varied geographical areas around the country and around the world.

• Evidence of the crime may be found at the location of the offender, the location of the victim, or potentially anywhere in cyberspace.

•Digital evidence may be entangled in a maze of other information which may have no bearing on the crime being investigated.

•Figuring out which material is relevant to a criminal investigation can be extremely difficult.

•In the case of encrypted data investigators in the United States face a difficulty posed by the 5th Amendment to the Constitution- because the 5th Amendment protects people from incriminating themselves in an offense, they may remain silent rather than give up the key to encrypted data.

Let's take a closer look at the investigation procedures, particularly search and seizure, employed by police investigating cybercrime.

5th Amendment: No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; **nor shall be compelled in any criminal case to be a witness against himself**, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Although this amendment (and the U.S. Constitution and Bill of Rights) was written to apply to cases of traditional violent and property crimes, it is equally applicable to cybercrime suspects and defendants. It should be clear that it is very difficult and complicated for the criminal justice system and its agencies to investigate, prosecute, try and apply corrections to perpetrators of cybercrime.

Comparing Investigating Traditional Crime and Cybercrime

Traditional Terrestrial Crime	Function	Cybercrime
Victim or witness reports crime to police		User reports "hack" of individual computer or network
Interview witnesses, gather evidence, record events, collect facts at the crime scene, canvass neighborhood, conduct interviews with associates, construct timelines, may use modern technology to collect records.	Investigation	Interview user, system administrator, IT personnel, other knowledgeable parties; gather digital evidence; collect facts-effects of hack on computer or network; conduct interviews to determine if there are other victims; construct timelines; definitely use modern technology…
File for search warrant; may conduct warrantless searches under certain conditions. Searches must be conducted in accordance with 4th Amendment prohibition against unreasonable search and seizure.	Search/Seizure	File for search warrant; usually don't conduct warrantless searches. Searches must be conducted in accordance with 4th Amendment prohibition against unreasonable search and seizure.

4th Amendment: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

United States District Court

(ENTER JUDICIAL DISTRICT)

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

CASE NUMBER:

I being duly sworn depose and say:
I am a(n) Special Agent, Criminal Investigation
Internal Revenue Service, U.S. Treasury
Official Title
and have reason to believe
that ☐ on the person of or ☐ on the property or premises known as (name, description and/or location)

in the Judicial District of (ENTER JUDICIAL DISTRICT)
there is now concealed certain property, namely

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

concerning a violation of Title United States code, Section(s)
The facts to support a finding of Probable Cause are as follows:

Continued on the attached sheet and made a part hereof. ☐ Yes ☐ No

Signature of Affiant

Sworn to before me, and subscribed in my presence

Date at City and State

United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

SEARCH WARRANT

IN THE (DISTRICT) (COUNTY) COURT, TELLER COUNTY, STATE OF COLORADO
CRIMINAL ACTION NUMBER 11SW0604

Whereas **Sergeant R.N. Olmsted** has made an Application and Affidavit to the Court for the issuance of a Search Warrant, and;

Whereas the application is in proper form and probable cause is found for the issuance of a Search Warrant to search the person(s) and or premises specified in the application.

THEREFORE, the applicant, and any other peace officer into whose hands this Search Warrant shall come, is hereby ordered, with the necessary and proper assistance, to enter and search within the next ten (10) days the person, premises, location and any appurtenances thereto, description of which is: **Any and all motor vehicles located on the property which may contain evidence to include a 2001 green Dodge Stratus VIN# 1B3EJ46XZ1N518288 with a Colorado Temporary plate of 479597.1 located in the rear window. All of which is located in the unincorporated area of the County of Teller, State of Colorado.**

The following person(s), property or thing(s) will be searched for, and if found seized:

See Attachment "B"

The "Attachment B" attached hereto is herby incorporated by reference.

as probable cause has been found to believe that it:

( ) Is stolen or embezzled, or
( ) Is designed or intended for use in committing a criminal offense, or
(X) Is or has been used as a means of committing a criminal offense, or
( ) Is illegal to possess, or
(X) Would be material evidence in a subsequent criminal prosecution, or required, authorized or permitted by a statute of the State of Colorado, or
(X) Is a person, property or thing the seizure of which is expressly required, authorized or permitted by a statute of the State of Colorado, or
( ) Is kept, stored, transported, sold, dispensed, or possessed in violation of a statute of the State of Colorado under circumstances involving a serious threat to the public safety, or order, or to the public health.

(Mark "X" according to fact)

Furthermore, a copy of this warrant is to be left with the person whose premises or person is searched along with a list of any and all items seized at the time of its execution. If said person cannot be located or identified, a copy of the search Warrant and the list of property seized shall be left at the place from which the property was taken.

Further, a return shall be promptly made to this Court upon the execution of this Search Warrant along with an inventory of any property taken. The property seized shall be held in some safe place until the Court shall further order.

Done by the Court this 25 day of February, 2011

Judge: Gold DG

Legal requirements for issuance of a search warrant(s) specific to New Jersey can be found at: https://www.njcourts.gov/attorneys/assets/rules/r3-5.pdf

Police may conduct warrantless searches in connection with traditional crime(s) under certain conditions. However, police must have probable cause* to believe that the person(s), place(s), or vehicle(s) to be searched have committed or are involved in the commission of a (particular) crime(s). The following table presents circumstances in which police may conduct a warrantless search.

Search incident to a lawful arrest	Police may search the area within the immediate control of the person.
Search in plain view	Police may search an area in which (potential) evidence is clearly visible- in "plain view"; police may not move objects to reveal any objects under the moved object.
Consent search	Police may search an area if a person gives the officer permission to conduct a search.

Police may conduct a warrantless search of an automobile if they have probable cause to believe a crime has been committed and waiting for a warrant would result in loss of evidence.
Police may conduct a pat-down search of an individual if they have reasonable suspicion that the person may be carrying a concealed weapon and/or is a threat to the officer(s) or others in the vicinity.

* Probable cause: likelihood that there is a direct link between a suspect and a crime.

However, searches in incidents of cybercrime generally require a valid search warrant. The following table summarizes reasons why it is usually not possible to conduct a warrantless search in cases of cybercrime.

Basis for Warrantless Search	Warrantless Search in Cybercrime?
Search incident to a lawful arrest	Criteria for arrest in cases of cybercrime can be complex- hence, it can be difficult to determine what constitutes a "lawful" arrest. [This will be discussed further below.]
Search in plain view	The evidence in cybercrime cases is generally not in plain view- investigating it requires the law enforcement agent to examine the files on the (victim's or suspect's) computer, some of which may be personal and private; this is regarded as an intrusion into the suspect's personal "space". [The issue of intrusion will be discussed further below.]
Consent search	The victim of a cybercrime may give consent to search his/her computer, but it is highly unlikely a cybercrime suspect will give such consent; if either the suspect's computer contains encrypted data which might be used as evidence, the suspect cannot be compelled to provide the encryption key (see earlier remark about 5th Amendment).

The next slide presents a consideration of the intrusiveness of a search on an individual's privacy.

The issue of personal privacy and threats to it in cyberspace has come up before. Here we want to present a more detailed look at intrusion on privacy. We can identify 6 levels of intrusiveness, ranging from 1) least intrusive to 6) most intrusive.

Level of Intrusiveness	Description
1) Least	Order is issued to Internet Service Provider (ISP) to preserve data [of potential suspect(s)]
2)	Order is issued to ISP or other service provider to surrender data on individual(s) or traffic on service
3)	Order is issued to provider to surrender stored data [of suspect(s)]
4)	[Suspect(s)] Stored data are collected in real time
5)	[Suspect(s)] Data are collected as they are being transmitted in real time
6) Most	Search and seizure of suspect's files, software, and/or hardware

Note that these levels of intrusion move from simply preserving or saving data an ISP might have from a [potential] suspect through dealing with or collecting a suspect's data as it is being stored or transmitted to taking possession of a suspect's data and equipment. These 6 levels represent increasing penetration of an individual's privacy by law enforcement agents as they investigate cybercrime. In the United States, there has long been a necessity for law enforcement to ***balance*** the need to investigate criminal activity with the rights to privacy which American citizens have traditionally enjoyed. It is not always easy to achieve this balance in the investigation of traditional crime; it is even more difficult when investigation turns to cybercrime.