Abstract

In physical crime the concepts of crime scene assessment and offender profiling are well-accepted if occasionally controversial. Work by the FBI has put profiling into the mainstream of investigative theories. However, in the digital world no such progress has been made. Further, the notion of offender profiling addresses the psychological continuum whereas we are concerned with the criminological spectrum.

The ongoing research reported in this paper will begin the process of translating physical crime scene assessment techniques into digital practice. The potential benefits of accomplishing this successfully are significant.

Unfortunately, the translation between physical investigation and digital investigation is not straightforward. The addition of particular techniques pioneered by crime assessment experts in physical investigations has turned out to be far more promising than application of psychological profiling.

This research-in-progress paper presents a new approach to cyber crime assessment. It views the computer as the crime scene and it applies a crime typology.

1. Introduction

Crime scene assessment (CSA) has become a key piece of solving the investigative puzzle in the physical world. CSA, in particular, has become well-known, if not well-understood, thanks to television programs such as CSI where it is, presumably, seen through eyes of the crime scene investigator.

Although there has been some work in this area in the digital world (e.g., research by Rogers), there is not yet an overarching crime assessment methodology for cybercrimes in general.

Walter [1] defines Crime Scene Assessment as:

The analysis of probative evidence (physical, direct, circumstantial) by its presence or absence that meets a recognizable pattern of behavior.

He defines an Offender Profile as:

Based upon a reflective crime scene assessment, a profile is a projected cluster of attitudinal, behavioral and identity factors of an offender.

There is the possibility of some implied ambiguity in this definition (“offender profile”) because in the approach discussed in this paper the analyst is concerned first with the crime as assessed through the crime scene, and second with a suspect whose characteristics match those of the crime. We define both of those in terms of the sub-types discussed in Section 2.

Since we project the characteristics of the crime in terms of the sub-types, there is no need for a separate offender profile. The sub-type of the crime will match the sub-type of the offender and the characteristics of the crime will describe the characteristics of the offender since the two are inextricably connected through the crime itself. These characteristics are criminological rather than psychological.

Both of these definitions can exist credibly in the digital world as long as one distinguishes such ambiguous terms as “crime scene”, “profile” and “physical evidence”. However, this paper distinguishes between crime assessment and profiling for an important reason. There are credible techniques – with more being developed – for profiling a digital device. We can create such a profile using digital forensic and other tools such as link analyzers, especially in network assessment.

The application of “profiling” both to offenders – largely psychological - and digital environments – largely technical - then, becomes confusing. Thus, for the purposes of the technique described in this paper,
we will refrain from using the terms “profile/profiling” in the psychological sense applying to offenders and reserve it for describing the unique fingerprint of a digital environment.

As well, there is the important issue of assessing situations where the physical and cyber environments meet. Locard’s Exchange Principal [2] says that when two items come into contact they each leave behind remnants of themselves. When digital items interact with physical items (e.g., a chat room session between a pedophile and a potential victim leading to a physical meeting) evidence of the interaction is present on the endpoint computers, intermediate servers and on network devices such as routers and switches.

This evidence is, often, difficult to isolate and attribute to a specific individual. As storage becomes cheaper and average users tend to have larger and more diverse storage devices, the task of the digital forensic investigator becomes increasingly difficult. It is not uncommon for an average user’s computer to have between 250,000 and 500,000 files. This, as well as improved technology for hiding evidence (called “anti-forensics” [4]) poses a challenge to the forensic analyst.

Understanding a crime scene [3] through an assessment based upon empirically-proven crime assessment techniques and then projecting that assessment upon a field of suspects is of material assistance in identifying, interviewing and convicting the criminal. When the criminal is functioning in the digital environment and the crime scene is the computer, however, the assessment is not always a straightforward translation of its physical counterpart.

Beginning with a credible approach used for decades on several thousands of actual cases, comparisons were made between the physical crime scene and the digital one. The physical approach was modified to remove those assessment factors that are specific to physical crime, especially violent crime where the techniques were developed initially.

Next, a small collection of baseline exemplar crimes that either are direct cyber crimes or consequential cyber crimes were analyzed using the modified assessment criteria. These crimes all had been solved and represented some, though not all, crime types. The result of this assessment was fine-tuned to develop a theoretical cyber crime assessment construct that could be synthesized into a procedure and tested empirically.

This paper describes the theoretical construct and lays the groundwork for further refinement – for example, direct application to digital forensic analyses and searches – and broad-based empirical testing.

2. Background and prior research

The notion of offender profiling in digital crime is not new. However, it tends to be focused on a particular offender group. And, it tends to address psychological analysis, often to the extent of suggesting diagnosis rather than a tool for solving a crime or digital event criminologically. For example, The Honeynet Project has focused on profiling hackers and three key proponents of this process (Chiesa, Ducci and Ciappi) have published their research [13].

Rogers [14] likewise addresses hackers explicitly in his taxonomy. A graduate student of Rogers, Kathryn C. Seigfied-Spellar [15] addresses cyber offender profiling as related to child pornography and pedophilia. It should be noted that the current research does not preclude the additional use of these other approaches as refinement in certain cases.

Parker, et al [16] focus, as well, on hackers with a few improvements over earlier work. For example, the authors deal with a more formalized approach that allows application of metrics and quantitative analysis of attacks. However, the focus in this work really may be thought of as an extension of a direct system attack (in the vernacular of this paper) and, as is usual in earlier work leading up to this research, focuses on an aspect of a specific type of offender, in this case hackers, especially those who might be state sponsored.

Probably the closest work to this research is from Bongardt [17]. An FBI profiler he addresses the psychological profile of a cyber offender in much the same way that the FBI’s Behavioral Analysis Unit (BAU) addresses profiling in physical crime. In the cited paper Bongardt focuses on hackers and network penetrations. This is one area where there is controversy among investigators. Not all investigators agree with the FBI approach to criminal profiling. It is not the province of this research to engage in that debate. The approach reported in this paper is entirely different and proceeds from an entirely different starting point for that of the FBI’s BAU.

The primary difference between these approaches and the current research is that, because it is based upon crime scene assessment, it presents a reliable method for deducing a potential offender from the crime scene left by that offender, an accepted approach in physical investigation. The current research is generalized and criminological in focus (i.e., intended to assist investigators and prosecutors
explicitly) and is foundational across a potentially broad range of criminal activities.

In June of 2011 Stephenson and Walter described the use of crime assessment and four sub-types in solving crimes of cyberstalking [5]. In that paper the authors describe other attempts at developing a methodology for cyber crime assessment [6].

Keppel and Walter describe a typology for classifying and assessing violent crimes that is the basis for this research [7] [8]. These four sub-types - power assertive, power reassurance, anger retaliatory and anger excitation - form a framework for classifying crime scenes and, subsequently, identifying likely suspects.

2.1 Power assertive

The power assertive sub-type is the most common comprising about 38% of all offenders [7]. The core drivers for the power assertive (PA) are power and control. The PA may grow increasingly confident over time and will increase his or her aggression against the target in order to maintain control through intimidation.

The PA needs to brag about his or her accomplishments even though he or she may not have committed the actual offence. This takes the form, occasionally, of taking credit for other people’s acts in order to build power within a group.

The PA uses commanding, assertive language and over-reactions are common. The PA crime scene tends to be organized.

2.2 Power reassurance

There are many similarities between the power assertive and the power reassurance (PR) actors. A major difference, however is that the PR develops his or her approach through fantasy. The actor creates a fantasy, often sexual in nature, and projects that fantasy on the victim, attempting to engage the victim in the fantasy. Stephenson and Walter state in [5]:

"By fantasy we mean the difference between reality and what the actor wants and/or believes to be true via magical thinking. Magical thinking is a volitional associational thought pattern, without boundaries, that creates a desired result without rational thought. Magical thinking requires only belief and want, rather than fact and examination."

The PR exercises power over the target much as the PA does but with a bit gentler ramp-up. The goal of the PR is to encourage the target to engage in the fantasy and eroticize the offensive behavior making it seem acceptable.

It is not uncommon for the PR actor to pretend to be someone – either actual or by creating an image – other than him or herself. Response by the target, regardless of the nature of the response, will be interpreted by the actor as acquiescence. While the actor may present as egocentric and confident, he or she is likely to need reinforcement of his or her lagging self-esteem.

The PR often selects targets who are either older or younger or who may be viewed by the actor as “damaged goods”, meaning that the target has some deficiency, either physical, mental or emotional, that lets the actor maintain his or her feeling of superiority and power.

The PR crime scene is disorganized and PRs comprise about 34% of offenders [7].

2.3 Anger retaliatory

The anger retaliatory (AR) actor exhibits behaviors that suggest a great deal of rage. That rage may be directed at a person, group or organization that has authority over the actor or it may be directed at one or more persons who represent the real target symbolically.

The actual target usually is one with the ability to condemn or ridicule the actor or one who makes the actor feel injured. The AR often has poor relationships with the opposite sex.

The primary objective of the AR actor is to service his or her cumulative anger and hostility. There may be multiple targets, often all part of the same group. The target often is the same age or older than the actor. Occasionally the target may be a younger person, often a female authority. Targets may represent mothers, wives, girlfriends or female supervisors.

The AR may leave a staged crime scene and in physical cases where the AR action culminates in homicide the victim’s face may be averted from “seeing” the exit of the AR actor. The AR actor does not feel guilt from his or her act and, in fact, has a feeling of well-being having accomplished the crime. ARs comprise about 34% of offenders [7]
2.4 Anger excitation

Anger excitation (AE) actors – sadists - are the smallest sub-type comprising only about 7% of offenders [7]. They are equally rare in cyberspace since sadism is more difficult to accomplish in the on-line world than it is in the physical world.

While the primary motivation for the AE actor is sexual, it is manifested in physical aggression and torture. The AE’s objective is the complete fear and submission of the victim. This feeds the offender’s sexual desires by engendering dependency, dread and degradation on the part of the target.

For the AE offender the joy is in the crime not in its culmination. AE murderers, for example, may find the actual death of the victim anticlimactic and may relive the actions leading to that death for decades, reveling in the emotions he felt performing the acts that ultimately led to the victim’s demise. For the AE the crime is not over until he says it is.

The AE actor will confuse the target with con games, building hope in the target only to dash it and rebuild it. He may select targets from symbolic – to him – categories or targets with particular characteristics. The AE commonly uses cyberspace to locate communicate with and select victims.

2.5 Application of crime assessment in the physical world

Crime scene assessment is the analysis of probative evidence (physical, direct, circumstantial) by its presence or absence that meets a recognizable pattern of behavior.

Walter [3] describes an approach to crime assessment and, subsequently, offender profiling. He also provides the discriminating pair of definitions that are crucial to understanding the relative roles of crime assessment and offender profiling:

Generally investigators should begin the investigation with the crime scene. At this point the crime scene is associated with a particular sub-type as described above. Care is important here because typically the crime scene, as with the perpetrator, may exhibit a balance of more than one sub-type. It is important to view the crime scene holistically applying weighting to the various observed characteristics.

Weighting must also be applied to the value of the evidence observed since not all of it is critical to the case. This is especially true of a cyber crime scene because of the massive amount of potential evidence on a computer disk. As important as what is present in the form of evidence at the crime scene is, of equal importance is what is missing from the scene. Where the crime scene is a computer the missing evidence may be difficult to ascertain due to the sheer volume of data.

Once the crime scene has been analyzed and classified according the sub-types, possible suspects are similarly classified. However, beyond the classification of the suspects as one of the sub-types, pre- and post-crime actions must be considered and mapped onto the short list of suspects.

There always will be pre-crime activities that led up to the crime event. These can be ascertained easily from a crime scene computer using appropriate forensic techniques.

However, a crime committed by a person (as opposed to a digital event that is not related to the actions of an individual) will have post-crime activities as well. The combination of the pre- and post-crime activities with the classification of the crime scene itself usually will yield a very short list – probably only one or two – of credible offenders. When performing a computer forensic analysis this timeline approach becomes especially efficacious due to the metadata present in the device’s file system.

The objective of this approach is to correlate the events and people involved in actions before, during and after the event in the context of the sub-types and the cybercrime scene. The key piece of this puzzle is the correct establishment of the behavior exhibited during the event.

3. Cyber crime assessment construct

Stephenson and Walter in [5] propose that the victim computer be considered the crime scene in a digital event. However, in physical events, there is an implicit assumption that there is, in the particular event being investigated, an actor and a victim.

In computer incidents that is not always the case. For that reason we break computer events into two general groups: direct and consequential. These two classes are mutually exclusive in that direct events are those that must involve computing devices and cannot be accomplished without them.
Consequential events are those where the computing device plays a peripheral role. While the device could contribute to the event, it is not required to complete the offense.

This distinction is important because direct events, being computer-focused, generally are the primary focus of the investigation. In other words, the investigation is a “computer crime” investigation. That means that the computer itself is either the attacker or the victim or both.

Consequential events, on the other hand, are related to some physical, crime and simply add to the body of forensic data that comprises the investigation. By characterizing events in this manner the investigator can focus digital forensic activity appropriately and develop appropriate interview/interrogation approaches.

Direct events comprise four sub-classes:

- **Personal** – cyber attacks, such as cyber stalking, against persons
- **Theft** – unauthorized appropriation of digital assets
- **System attack** – cyber attacks against one or more computing devices, a network or a network device
- **Terrorism** – cyber attacks in support of terrorist goal

These four types describe the events that must include two or more computers (attacker and victim(s)).

Consequential events likely are more common than direct events. These are events where the computer plays a peripheral role in the event and need not be present for the event to complete. There are three sub-classes of consequential events:

- **Supporting** – use of one or more computing devices in support of the primary physical crime. The computer aids in the commission of the crime but is not required to complete it.
- **Coincidental** – the computing device expands upon the physical crime, perhaps by providing a resource, that is not involved directly with the physical crime, for the criminal
- **Prologue** – the computing device is used in activities that precede the physical event. It is not required to carry out the event, however.

All computer crime scenes are representative of one of the primary classes and one or more of the included sub-classes.

Additionally, cybercrime scenes, as with physical crime scenes, may show signs of MO (modus operandi or method of operating) and signature [12]. MO, if present, is a consistent pattern of behavior that is evident in the actions of a particular offender. In cybercrime scene analysis MO is important because in certain types of crimes there is a clear, repeating MO that can help identify the actor.

The other important aspect – though one not quite so common in cybercrime – is signature. This is something that the actor adds to the crime scene that is not required to complete the crime. For example, a murderer may kill only women (MO) and leave a white rose on the corpse when he leaves (signature). Hackers and malware writers often leave signatures but they are not as common in other cyber events.

### 3.1 Cybercrime assessment process

The first step in assessing a cybercrime is to assess the crime scene. This is not unlike assessing a physical crime scene. The National Institutes of Justice suggests four generalized steps for crime scene investigation [8]:

- Initial response/prioritization of efforts
- Preliminary documentation and evaluation of the scene
- Processing the scene
- Competing and recording the crime scene investigation

Very likely the computer will be collected as part of the evidence in a physical crime. This first step in the traditional processing of a physical crime scene leads directly to the first step in assessing a cybercrime scene. It is important that the circumstances surrounding the involvement of the computer in the crime be ascertained. The first question to answer, of course, is does the investigator consider the computer to have direct or consequential involvement?

If the computer has direct involvement, it is likely that the computer itself is the reason for the investigation. If it has consequential involvement, it will be necessary to understand the circumstances of the physical crime before attempting to assess the
computer’s role.

The second step in the physical investigation is the same as the second step in the cybercrime assessment: document the crime scene. The difference is that if the cybercrime scene is the computer, its heart is the computer’s hard disk. That, however, is not as simple as it sounds.

There may be multiple disks in the computer(s) itself/themselves. There may be external disks and the might be thumb drives, CDs, DVDs, cell phones, tablets, etc. All of these need to be collected under proper chain of custody and transported to the lab. It may be necessary to seize the whole computer, of course, rather than just its disk but once the computer is at the lab it is the disk with which we’re concerned.

We document the cybercrime scene by making forensic images of everything. We then make work copies of our images and store the original (first generation) images in our evidence locker. We work only on the work copies.

When we are assessing the crime itself we are concerned with some specific facts surrounding the case [3].

- When was the crime committed?
- Where was the crime committed (this only is useful at this point in consequential cases)?
- Is the physical crime scene organized or disorganized?
- Is there obvious – “plain sight” – evidence that will help establish the sub-type?
- Is there a signature to the physical scene?

Translating to the cyber world and adding unique requirements:

- Is the crime direct or consequential?
- What type(s) are represented within the grouping?
- Once a preliminary view of the computer is established (this can be accomplished during the process of making forensic images with most good imagers) is the digital crime scene organized or disorganized?
- Is there obvious – “plain sight” – evidence that will help establish the sub-type?
- What is the likely relationship between the computer(s) and the event? Can opening assumptions be made regarding sub-types?
- Next the digital crime scene must be processed appropriately and the analysis begins. Is there further evidence that suggests a sub-type? This is an iterative process. As new information is gleaned from the computer suggesting one or more sub-types, those suggested sub-types in turn suggest where to look within the computer’s file system.
- Is there anything in the analysis of the digital crime scene that leads to a cybertrail leaving the computer/network? What pieces of digital evidence are implicit in the cybertrail?

Once the sub-type of the crime/crime scene is established, are there credible suspects who match the sub-type? That is an important question to answer and it is answered in different ways for direct and consequential events. In a direct event establishing the suspect(s) may be a tedious task. When a consequential event is being investigated one generally knows the suspect in advance (e.g., searching for evidence that an employee used company resources to run a personal business in violation of policy).

In the case of a consequential event this approach provides a deeper understanding of the actual activities of the suspect. If the consequential event is tied to a physical crime the assessment of the crime scene and the suspect must interact with the profile of the computer. In other words, the assessments must match so that the suspect(s) match(es) as well. Also, the investigator must consider pre- and post-events.

The final step in physical crime scene investigation is extended on the computer. It includes continuing the digital scene assessment, setting bookmarks in the computer forensic analysis, tracing the cybertrail and collecting/preserving logs, etc.

### 3.2 Using the digital crime scene assessment results

There are several ways to apply the cybercrime scene assessment and they all have to do with establishing attribution unambiguously. Beginning with direct events, establishing unambiguous attribution can be challenging. There is a chance that the attacker is quite remote from the target.

Nonetheless, the scene still can be assessed and a sub-type assigned. Once that is done, the attacker can be hypothesized initially. The purpose at this point is leading the investigator to a cybertrail. Once a cybertrail has been identified, preliminarily at least, hypothetical suspects may be identified and assessed.
for inclusion in the sub-type in question.

This will help move the investigation towards one or more suspects. If the attacker is a group, the group may end up filling the appropriate sub-type or the evidence may suggest one or two actors within the group. Once the suspect is arrested and his/her computer seized, it can be assessed in the same manner. It should be consistent with the victim computer and crime sub-types.

Finally, the pre- and post-crime activities must be assessed and the suspect matched using the sub-types. The result is that there likely will be very few credible suspects who match the assessment and whose pre- and post-crime activities fit with the crime itself.

Understanding the suspect’s sub-type also helps in the interview/interrogation process since the interviewer will understand how the subject is likely to behave. There is an important aspect of this that reflects throughout the crime assessment process: this process functions within the criminological, not the psychological, continuum.

There is no application of this approach to diagnosis and treatment of mental aberrations. Those aberrations may be useful in understanding the assessment but it does not work in the other direction. All we are interested in is identifying and convicting the perpetrator.

If the event suggests a consequential crime, the assessment is considerably simpler in most cases because the suspect is known. The objective now becomes associating the suspect with activities on the devices(s) and correlating that evidence with any physical evidence involved with the physical crime.

In the case where there is a strong connection to a physical crime, a physical crime scene assessment can be associated closely with the digital crime scene assessment to provide supporting evidence to the physical investigation.

More important, however, is the degree of granularity in the analysis of the computer that this approach facilitates. On modern devices – especially servers – there can be well over 100,000 files on a hard disk. On many servers this grows to over 1,000,000. This huge file system makes searching for evidence challenging. Although current digital forensic tools certainly can accommodate very large images, there are practical issues as well.

For example, conducting file/keyword searches is a common practice but often is a hit-or-miss proposition. Paging through thousands of graphic images for needed evidence is tedious and error-prone. Performing a raw data search when there are hundreds of thousands of files is very slow and often fraught with false positives. Understanding the profile of the computer under examination (crime scene) is useful for directing and refining these searches.

Additionally, savvy computer users can use such subterfuges as virtual machines, steganography [9][10], anti-forensics [4] and encryption to hide evidence. Encryption as an obfuscation technique by system crackers has been used at least as far back as 1986 [11]. Understanding the cybercrime scene and the credible suspect(s) can help uncover possible obfuscation on the cybercrime scene computer.

Finally, when dealing with mobile devices there are two general approaches: treating the device as unique and viewing it forensically in the context of other forensic data. Obviously, the most useful investigative analysis is to associate all involved devices where possible. There is an extension of this: the development of a cyber trail.

Focusing the forensic effort as an investigation rather than a digital forensic exercise allows the analyst to draw conclusions that are useful to other, non-forensic, investigators. The result is that the iterative investigative/analysis process that exists between these two groups becomes more productive.

4. Exemplar cases

The following cases have been solved, not always using the methodology described in this paper. However, the authors have applied these techniques to the cases with the results that we report below. These four cases are a subset of the total actual exemplar cases analyzed.

4.1 Cyberstalking

Case: cyberstalking - this case is reported in [5]
Class: Direct
Sub-Class: Personal
Victim: middle-age female human resources supervisor
Stalker: middle-age female human resources employee
Cyber connection: email
Actor sub-type: PA
Cybercrime scene sub-type: PA
Synopsis: The victim experienced a physical stalking some years prior to this event. Because her employer at the time refused to take action, she left that job and took the one that she held at the time of this incident. The victim began receiving emails from an anonymous source that sounded as if they came from the original physical stalker. Email traces successfully traced them to the actual stalker, one of the victim’s. The stalker did not have the computer skills to anonymize the emails but had convinced her husband who did have some computer skills to do it for her.
Analysis: There was no opportunity to apply cybercrime assessment techniques since this incident occurred over 15 years ago. However, today we would see that the event/cybercrime scene was clearly PA based upon analysis of the emails. We also would see that the employee – who confessed in writing to the act – was a strong PA with some, though not sufficient, computing skills. We could have cleared the former physical stalker based upon describing him as AR (anger and resentment against a female supervisor) and we would have, as we did, followed the cybertrail of the email.
Demonstrates: use in clearing an apparently obvious suspect.

4.2 Misuse of a company computer (pornography)

Case: Misuse of company computer (pornography)
Class: Consequential
Sub-Class: Supporting (enabled easy access to pornographic images)
Actor: Employee of the organization taking administrative action for violation of organizational policy
Cyber connection: Surfing pornographic web sites using a computer supplied by his organization
Actor sub-type: PA
Cybercrime scene sub-type: PA
Synopsis: the employee was accused of misusing his business-supplied computer to surf pornographic web sites and was interviewed by investigators. He defied the investigators (“catch-me-if-you-can”) and even provided the name of a single pornographic site claiming that he visited only one once and that for the purpose of testing the organization’s filters. Forensic searches of his computer failed to reveal pornographic images until a virtual machine was discovered and exported to a test computer. Within that virtual machine the forensic investigator found over 100 pornographic images from over seven distinct pornography sites. When confronted with the evidence the actor feigned confusion until the forensic investigator implied that he had visited a child pornography site (he had not) at which time the actor exploded in rage admitting that he had visited all of the other sites but he had never visited a child pornography site as he was no pervert.
Analysis: The actor was a classic PA. He talked down to investigators who he viewed as inferior to him, especially in technical skills. He took a catch-me-if-you-can attitude towards them, being so bold as to provide a tantalizing hint of his activities with the clear expectation that his hidden images would not be found. During the interview with the forensic investigator he became submissive, another PA characteristic: when a PA is confronted by a more powerful PA he or she becomes submissive. The computer (cybercrime scene) was a model of PA organization, including the methodical hiding of the fruits of his crime. Realizing that the actor was a true PA, the forensic investigator confronted him with an image of a young-looking girl from the actor’s collection of pornographic images. A true PA will attack when confronted with accusations of weakness and perversion is viewed as a major weakness. The confrontation with the young female image provoked an uncontrolled rage that culminated in an admission.
Demonstrates: use in interview/interrogation and uncovering obfuscation on the computer.

4.3 Misuse of a company computer/cell phone

Case: Sexting
Class: Consequential
Sub-Class: Supporting (allowed transmission of erotic images over the Internet/mobile phone system)
Actor: Young-middle-age female
Cyber connection: Transmitting suggestive and erotic images of the actor presumably for the purpose of encouraging men to date her.
Actor sub-type: PR
Cybercrime scene sub-type: PR
Synopsis: the actor, a young middle-age female employee of an organization used the cell phone and computer supplied to her by the organization to send suggestive photos of herself to her personal correspondents. She also had her own cell phone which she had, against organizational policy, connected to her organization-supplied computer for the purpose of transferring images between her personal cell phone and her organizational computer. When confronted about the unauthorized installation of a personal program on her organizational computer...
and her sexting activities she lied to investigators until the forensic investigator established that she had, in fact, made the connections.

**Analysis:** The cybercrime scene – the actor’s cell phones and computer – showed characteristics of the power subtypes however two aspects suggested a PR. First, there was a strong aspect of fantasy (engaging recipients of the actor’s pictures in her vision of herself) and the cybercrime scene was disorganized. There was little evidence of planning and most images seemed to be created and sent in a sporadic manner. When the actor was interviewed by the investigators she feigned ignorance of how to install and use the program that connected her Blackberry to her organization-provided computer. Forensic examination proved that she was lying since there was evidence that she had installed and then uninstalled the program. Her vision of herself was an example of magical thinking and she attempted to project that image – a sexy young woman who could have any man she wished – in her face-to-face actions. This image matched the one found on her computing/cell phone devices. Logs on the computer showed that the program had been installed and removed from the computer after attempting unsuccessfully to install on a network drive.

**Demonstrates:** use in uncovering lies by directing forensic analysis to evidence and obfuscation on the computer.

### 4.4 Unauthorized access to multiple computing systems

**Case:** Infomaster - this case is reported in [12]

**Class:** Direct

**Sub-Class:** System attack (hacking)

**Victim:** Multiple

**Attacker:** Young male

**Cyber connection:** Multiple system intrusions across universities, National Laboratories and other organizations

**Actor sub-type:** PA

**Cybercrime scene sub-type:** PA

**Synopsis:** A young teenage male spent all of his time hacking into university computer systems and using those systems to enter other systems. Some of the secondary systems were other universities, some were National Laboratories and some were other organizations such as defense contractors. The actor was extraordinarily patient and persistent. His computer skills were somewhat better than average, improving significantly over the course of his activities. He defied system administrators, law enforcement and even his own brother. In true PA fashion he was arrogant and assertive in his interactions with other people. He was obsessed with hacking and computers and rarely left his room or his computer.

**Analysis:** This event took place well over twenty years ago, long before the techniques described in this paper became available. Law enforcement agencies did not take hacking. Hackers as a group tend to be PA but those who spend all of their time with computers and little with other people tend to develop strong PA characteristics. This actor, in particular, would attack a computing system until he succeeded in cracking it, thus showing his power over it. He was given to extensive bragging, in some cases taking credit for hacks he did not do. Additionally, when the actor’s computer could be seized it would show characteristics of a PA computer user. Following the cybertrail would reveal patterns of attack that could establish an MO.

**Demonstrates:** use in analyzing a complex cybertrail.

### 5. Summary

The evolution of crime scene assessment from physical crimes to cyber crimes is not a straightforward translation. Thus far, the authors have begun exploring a process for interpreting the physical crime scene assessment techniques begun by Keppel and Walter, for analyzing violent crimes, in cyber crimes.

### 6. Future research

The next step in this ongoing research is twofold. These techniques need to be applied directly to the assessment of the cybercrime scene. That means taking the generalized processes proposed in this paper and applying them directly to a computer.

Second, in order to analyze the efficacy of the approach an empirical study must be undertaken. The authors currently are collecting cases that can be used to perform assessments in all of the areas of cybercrime discussed in this paper using the synthesized procedure.

Ultimately, there are some important refinements necessary to complete this research. For example, the granularity through which this technique can identify a suspect needs developing. The authors expect this refinement, along with other related ones, such as perpetrator skill level, victimology, and, deeper correlation using social media in the cybertrail, to come out of the empirical study.
7. References


