CYBERCRIME AND DIGITAL FORENSICS – TECHNOLOGIES AND APPROACHES

CISAR, P.; MARAVIC CISAR, S. & BOSNJAK, S.

Abstract: *This chapter deals with two key terms: cybercrime and digital (computer) forensics. The first part of the chapter introduces the term "cybercrime", defines and explains the categories and the anatomy of different types of attacks as the main form of cybercrime and provides typical examples. In addition, some characteristic cybercrime statistics and trends, such as documented cases of cybercrime are presented. Creating an environment for today's cybercrime prevention is also elaborated on. The second part of this chapter is related to digital forensics – the main procedure of digital crime scene investigation. Finally, this chapter deals with general methodology of computer forensics, forensic framework and process models.*

Key words: *cybercrime, digital forensics, forensics methodology, digital evidence*

Authors´ data: Dipl.-Ing. Dr.inf.sci. **Cisar**, P[etar]*; Dipl.-Ing. Dr. **Maravic Cisar**, S[anja]**; Univ.Prof. Dipl.-math. Dr.inf.sci. **Bosnjak**, S[asa]***, *University of Criminalistic and Police Studies, Cara Dusana 196, 11070, Belgrade-Zemun, Serbia, **Subotica Tech – College of Applied Sciences, Marka Oreskovica 16, 24000, Subotica, Serbia, ***University of Novi Sad Faculty of Economics, Segedinski put 9-11, 24000, Subotica, Serbia, petar.cisar@kpa.edu.rs, sanjam@vts.su.ac.rs, bsale@ef.uns.ac.rs

This Publication has to be referred as: Cisar, P[etar]; Maravic Cisar, S[anja] & Bosnjak, S[asa] (2014). Cybercrime and Digital Forensics – Technologies and Approaches, Chapter 42 in DAAAM International Scientific Book 2014, pp.525-542, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-901509-98-8, ISSN 1726-9687, Vienna, Austria
DOI:10.2507/daaam.scibook.2014.42

1. Introduction

The wide-spread usage of computer technology, in order to further previous possibilities and current requirements, is a sure indication of our digital age (Reith, et al., 2002). Numerous areas of modern life have become more advanced with the implementation of computer. Yet, simultaneously, this advancement of information technologies has also brought along its use as a criminal tool in order to perform, hide, or aid unlawful or unethical activity. This is especially true of the wide-spread use of computers by the general public, yet also enabling the users to seemingly remain anonymous while committing crimes using computer systems. These are classed as "cybercrimes," though they are not so much new types of crimes, but classic crimes, making use of informatics and the easy access to information. These crimes are the result of the combination of computers being all too readily available, and the growing proficiency of computer systems when used with criminal intent. Digital forensic procedures are necessary for investigators to be able apply these to detect, apprehend and take legal action against criminals involved in digital crime (Čisar et al., 2012).

Recently, computer forensics has seen growing focus on digital forensics in terms of stopping and prosecuting computer criminals. Before computer forensics has established solid processes and techniques, there were a number of computer crime cases that were not solved. The reasons for a failure to prosecute are plenty, yet the most prominent one may be that authorities are not suitably equipped to ensure the successful collection of digital evidence in terms of tools and skills (Čisar et al., 2012).

Computer forensics therefore calls for the introduction of cohesion and consistency within this wide-ranging field including the extraction and examination of evidence that was secured from a computer at a crime scene. One needs to make especially sure that evidence from a computer is extracted without compromising the original incriminating evidence (Čisar et al., 2012).

Most of the literature on cybercrime usually begins by defining the terms "computer crime" and "cybercrime". In this context, different approaches have been accepted in recent period to develop as precise as possible definition for both terms. Before evaluating these approaches, it is necessary to determine the relationship between "cybercrime" and "computer-related crimes". Without going into details at this phase, the term "cybercrime" is narrower than computer-related crimes as it has to involve a computer network. Computer-related crimes include even those activities that bear no relation to a network, but only affect independent computer systems.

Within the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions were developed (Gercke, 2013): Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity. Another

broader definition is provided in Article 1.1 of the Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism, which points out that cybercrime refers to acts in respect to cybersystems (Gercke, 2013).

2. Cybercrime

A broad use of the term 'cybercrime' is the description of an activity in which computers or networks are the tool, the target, or the place of criminal activity. This does not mean that the categories are exclusive; some activities can belong to several categories.

How you define cybercrime is highly dependent on the purpose of use. The core of cybercrime consists of a small number of acts directed towards the confidentiality, integrity and availability of computer data or systems. Apart from this, however, it is not easy to define suitable categories for the numerous computer-related acts for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts. These are, in fact, part of the wider meaning of the term 'cybercrime' and difficult to match with a legal collective term. The basic cybercrime acts need a set of definitions. However, a definition of cybercrime is not as relevant for other purposes, such as defining the scope of specialized investigative and international cooperation powers, which have an increased focus on electronic evidence for any crime, instead of a wide, artificial cybercrime' construct (***, 2014a).

Cybercrime is a rapidly growing area of crime. Because the Internet is a global phenomenon criminals have been enabled to commit almost any illegal activity anywhere in the world. This calls for action on the part of the countries, which have to adjust their domestic offline controls so that they also include crime that took place in cyberspace. An increasing number of criminals abuse the speed, convenience and anonymity offered by modern technologies so that they can commit a wide range of criminal activities. The following are included: attacks against computer data and systems, identity theft, the distribution of child pornography, Internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, botnets, and various email scams such as phishing (Shipley et al., 2013).

One of the vital aspects of cybercrime is the fact that it is nonlocal: the jurisdictions of where criminal actions take place maybe set very far apart. Law enforcement is faced with a serious challenge as crimes that were previously local or even national now call for international cooperation. As a planet-spanning network, the Internet offers criminals numerous places to hide in the physical world as well as in the network itself. Nonetheless, if people walking on the ground leave marks that can be found by skilled trackers, so do cybercriminals by leaving clues who and where they are, despite their best efforts to cover their tracks. If one wishes to trace such clues about identity and location across national boundaries, international cybercrime treaties must be ratified.

While the term cybercrime is often limited to the description of criminal activity in which the computer or network is vital part of the crime, this term further includes traditional crimes where computers or networks are implemented to facilitate the illicit activity. There are a very large number of examples of cybercrime (***, 2014f):

- Examples of cybercrime where computers or networks are used as tools in criminal activity refer to spamming and criminal copyright crimes, particularly those enabled via peer-to-peer networks;
- Examples of cybercrime where the target of criminal activity is the computer or network contain unauthorized access, viruses, malware (malicious code) and denial-of-service attacks;
- Examples of cybercrime where the criminal activity's location is the computer or network include theft of service (telecom fraud) and certain financial frauds;
- Examples of traditional crimes that are enabled by implementing computers or networks (where the primary target is independent of the computer network or device) contain fraud and identity theft, information warfare, phishing scams, child pornography, online gambling, securities fraud, etc. Cyberstalking is an instance of a traditional crime (harassment) in a new form when carried out via computer networks.

Moreover, particular other information crimes, such as trade secret theft and industrial or economic espionage, are often seen as cybercrimes when computers or networks are being used. Cybercrime in the context of national security may take the form of hacktivism (online activity meant to influence policy), classical espionage, or information warfare and related activities.

Most cybercrime is an attack on information regarding individuals, corporations, or governments (***, 2014d). While the attacks do not occur on a physical body, they do occur on the personal or corporate virtual body, which is the set of informational characteristics that classify people and institutions on the Internet. Put it differently, in the digital age one's virtual identities are vital parts of one's daily life: the person is defined as a collection of numbers and identifiers in numerous computer databases which are owned by governments and corporations. Cybercrime underlines the centrality of networked computers in one's lives, as well as the how fragile such apparently solid facts are as individual identity.

Cybercrime includes a wide-range of activities. At one end of the spectrum are crimes that include fundamental breaches of personal or corporate privacy, for example, assaults on the integrity of information held in digital depositories and the use of illegally gathered digital information to blackmail a firm or individual (***, 2014d). Further, this end includes the increasing crime of identity theft. Halfway in the spectrum are the transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting. These crimes have specific victims, but the perpetrator will use the relative anonymity of the Internet as cover. A different aspect of this type of crime includes individuals within corporations or governments who alter data on purpose for profit or political objectives. The spectrum's far end is the crimes that include attempted disruptions in the actual workings of the Internet. Such crimes range from spam, hacking, and denial-of-service attacks against specific sites to acts of cyberterrorism − the using the Internet to cause public disturbances and possibly, death. Cyberterrorism centers on the use of the Internet by nonstate actors to influence a nation's economic and technological infrastructure. Public awareness regarding the threat of cyberterrorism has increased significantly since the September 11 attacks of 2001.

Cybercrime statistics and trends (***, 2014c)

- Yearly cybercrime victim count estimate: Victims per year (556 million), Victims per day (over 1.5 million), Victims per second (18), Identities exposed (more than 232.4 million);
- The estimated annual cost over global cybercrime is $ 100 billion;
- Common types of cyber attacks: Viruses, malware, worms, trojans (50%), Criminal insider (33%), Theft of data-bearing devices (28%), SQL injection (28%), Phishing (22%), Web-based attacks (17%), Social engineering (17%), Other (11%);
- The major motivation behind cyber attacks: Cybercrime (40%), Hacktivism – the use of computers and computer networks to promote political ends, chiefly freespeach, human rights, and information ethics (50%), Cyber Warfare (3%), Cyber Espionage (7%);
- Russia and the U.S. are the largest contributors when it comes to malware attacks making up 39.4% and 19.7% of hosted malware, respectively;
- US Navy sees 110,000 cyber-attacks every hour, or more than 30 every single second;
- More than 600,000 Facebook accounts are compromised every day.

2.1 Examples of authentic cybercrime cases

- Shue giant Zappos experienced a security breach after as many as 24 million customers' credit card numbers, personal information, billing and shipping addresses had been ripped off (***, 2014g);
- EHarmony, the popular online dating site, was the target of a password hacking attack that resulted in 1.5 million stolen passwords, most of which have been cracked. The attack is believed to be by the same hacker who stole 6.5 million passwords from LinkedIn, the career-oriented social network (***, 2014e);
- Wells Fargo website experienced a denial-of-service attacks that delayed or disrupted services on customer websites. The hackers behind the attacks have used sophisticated and diverse tools that point to a carefully coordinated campaign (***, 2014h).

2.2 Attacks and threats

In order to evaluate the security needs of an organization to efficiently counter cybercrime and to select different security products, policies, procedures and decisions, it is necessary to define requirements and categorization of approaches that satisfy these requirements in a systematic way. One of the approaches is to consider the three aspects of information security:

- Attack – Any action that compromises the security of information. Attack is the basic form of cybercrime;
- Security mechanism – The mechanism that is designed to detect, prevent or recover from a security attack;

- Security service – Service that enhances the security system for the processing and transfer of data. Security service includes the use of one or more security mechanisms.

Essentially, the attacks are actions that are aimed at endangering the security of information, computer systems and networks. There are different types of attacks, but generally they can be classified into four basic categories:

- Interruption – In an interruption, an asset of the system becomes lost, unavailable, or unusable. An example is malicious destruction of a hardware device, erasure of a program or data file, or malfunction of an operating system file manager so that it cannot find a particular disk file (Pfleeger et al., 2006);
- Interception – An interception means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network. Although a loss may be discovered fairly quickly, a silent interceptor may leave no traces by which the interception can be readily detected (Pfleeger et al., 2006);
- Modification – If an unauthorized party not only accesses but tampers with an asset, the threat is a modification. For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted electronically. It is even possible to modify hardware. Some cases of modification can be detected with simple measures, but other, more subtle, changes may be almost impossible to detect (Pfleeger et al., 2006);
- Fabrication – an unauthorized party might create a fabrication of counterfeit objects in a computing system. The intruder may insert spurious transactions to a network communication system or add records to an existing database. Sometimes these additions can be detected as forgeries, but if skillfully done, they are virtually indistinguishable from the original item (Pfleeger et al., 2006).

In the context of information security, the threat can be defined as a set of circumstances that has the potential to cause information loss or harm. Threats can be divided into passive and active:

- Passive threats – Passive threats are those that do not directly affect the system's behaviour and functioning. Example, interception: release of message contents and traffic analysis;
- Active threats – Active threats can affect the behaviour and functioning of the system or the content of data. Example, interruption, modification and fabrication: masquerade, replay, modification, denial-of-service.

2.3 Anatomy of an attack

Once the basic approach is understood, namely that attackers use to "conquer" a system or network, it will be easier to take appropriate defensive actions and to know

what is applied and why exactly that one. The basic steps in attacker methodology are:

- Survey and assess – The first step that is usually taken by the attacker is research of potential targets and the identification and assessment of their characteristics. These characteristics may be supported services, protocols with possible vulnerabilities and entry points. The attacker uses the information collected in this way to make a plan for the initial attack;
- Exploit and penetrate – After having explored a potential target, the attacker tries to exploit the vulnerability, and to penetrate the network or system. If the network or networked computer (usually the server) is fully secured, the application becomes the next potential entry point for the attacker – he will try to enter the system through the same entrance used by the legitimate users. For example, the usage of a login page or a page that does not require authentication. A good authentication method is therefore a method that uses keys that are hard or better yet impossible to copy, keys that cannot be transferred to other users and keys that can be used in any given time (Rakun et al., 2012);
- Escalate privileges – Once the attacker succeeds in endangering the application or the network - for example, by inserting a code into the application or establishing legitimate sessions in the operating system – he will immediately try to increase his rights. In particular, he will try to take administrator privileges, i.e. to join the group of users who have the same rights within the system. Defining the minimum set of rights and services which are necessary to provide the users of application, is the primary defense against attacks increasing privileges;
- Maintain access – When the attacker succeeds for the first time to enter the system, he takes steps to facilitate future attacks and to cover his traces. A common way to facilitate future approaches is the installation of "back door" programs or the usage of existing accounts that are not strictly protected. The concealment of traces often includes deleting log files and hiding the attacker's tools. Taking into account that log files are one of those objects that the attacker wants to modify in order to conceal his tracks, they should be protected and reviewed regularly. By the analysis of log files one can often detect early signs of intrusion attempts, before the damage occurs;
- Deny service – Attackers who cannot access the system or computer network and achieve their goal, often organize an attack that causes denial of service (DoS), in order to prevent others from using the application. For other attackers, the DoS attack is the goal from the very beginning.

3. Digital forensics

Digital forensics is a fairly novel science. It is used synonymously with the term computer forensics; its definition has come to cover the forensics of all digital technology. While computer forensics is understood as "the collection of techniques and tools used to find evidence in a computer" (Caloyannides, 2001), digital forensics has been defined as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation,

documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (Adams, 20012). Certain authors distinguish between computer and digital forensics. However, in this work the distinctions will be disregarded.

There are different, more general forms of definition for digital forensics. As an example: Tools and techniques to recover, preserve, and examine digital evidence on or transmitted by digital devices (Golden, 2006). Another definition can be: extracting evidence from computers or other digital devices (Harrison, 2011).

Digital forensics has become an accepted concept, since law enforcement has come to accept that a number of digital devices are part of modern day life, which can be used and abused for criminal activity, not just computer systems. Computer forensics generally focuses on particular methods for extracting evidence from a specific platform, whereas digital forensics needs to be formed in such a way that it covers all types of digital devices, including future digital technologies. Regrettably, there is no regular or consistent digital forensic methodology; instead, there are a number of procedures and tools based on law enforcement experiences, and those of system administrators and hackers. This is challenging since they must gather evidence by applying approved methods that will reliably extract and analyze evidence without bias or modification.

3.1 Computer forensics methodologies

Computer and network forensics methodologies consist of three basic components that Kruse and Heiser (2002) refer to as three elementary processes of computer forensics investigations: acquiring the evidence while ensuring that the integrity is preserved; authenticating the validity of the extracted data, which involves making sure that it is as valid as the original; analyzing the data while keeping its integrity.

The U.S. Department of Justice published a process model that consists of four phases (***, 2014b):

- Collection – Involves the evidence search, recognition, collection and documentation;
- Examination – This phase is designed to facilitate the visibility of evidence, while explaining its origin and significance. It involves revealing hidden and obscured information and the relevant documentation;
- Analysis – This looks at the product of the examination for its significance and probative value to the case;
- Reporting – This entails writing a report outlining the examination process and pertinent data recovered from the overall investigation.

3.2 The forensic process

By default, electronic evidence means specific challenges in terms of having it admitted in court. In order to counter these challenges one has to adhere proper

forensic procedures. There are four phases among these procedures, although there can be more, as well: collection, examination, analysis, and reporting (U.S. Department of Justice, 2001).

The collection phase means searching for, recognizing, collecting, and documenting electronic evidence. The collection phase may include real-time and stored information which can be lost unless precautions are taken at the scene.

The process of examination will make the evidence visible and elaborate on its origin and importance. This process is set to achieve a number of things. Firstly, the task is to document the content and condition of the evidence in its entirety. Documentation in this way enables all parties to discover the contents of the evidence. A quest for covert or buried information takes place in this phase. As soon as all the information has become visible, the process of data reduction starts, separating the sheep from the goat, i.e. the useful from the not useful. Considering the enormous amount of information which can be stored on computer storage media, this examination is a part of the utmost importance.

Examination is different from analysis in the sense that it considers the examination's product based on how significant and valuable it is in terms of the case. This phase is rather a technical review carried out by the investigative team based on the results of the evidence examination. At this stage, among others, the following activities are performed: identifying relationships between fragments of data, analyzing hidden data, determining the significance of the information obtained from the examination phase, reconstructing the event data, based on the extracted data and arriving at proper conclusions etc. The results of the analysis phase could signal that additional steps are needed in the extraction and analysis processes. One must determine if the chain of evidence is consistent with the timeline. A combination of analyzing tools will ensure better results. The complete and accurate documentation of the results of the analysis is of great importance (Ramabhadran, 2014).

We distinguish between several types of analysis:

- Time analysis – This means determining when the event took place and creating a picture of the crime development step by step. For this analysis the time metadata are inspected (last modification, last access, time of occurrence, change of status) or log files (determine when the user has logged in to the system);
- Analysis of hidden data – This step is helpful when reconstructing hidden data and could point towards ownership, skill or intent. If there are any data with modified extension, this indicates hiding data on purpose. The existence of encrypted, compressed, and password-protected data points to data hiding by malicious users;
- File and applications analysis – This offers suitable conclusions regarding the system and the skill of user. The results of this analysis lead to the following steps to be taken:

- browsing the contents of files;
- identifying the number and type of operating system;
- determining the relationship between files;
- browsing the user settings.

The final step of the analysis is its conclusion. It will 'connect the dots,' form a complete story based on the collected and analysed data.

The examination is completed by a written report summarizing the examination process and the relevant data recovered. It is required that all examination notes be preserved for the purposes of discovery or testimony. It is possible that an examiner might need to testify about both the conduct of the examination as well as the validity of the procedure, and also how they were qualified to conduct the examination.

General forensic and procedural principles should be applied if electronic evidence is involved:

- If one takes actions to secure and collect electronic evidence is not modify that evidence;
- Persons involved in the examination of electronic evidence are to be trained for the purpose;
- It is important to fully document, preserve, and make available for review all activity relating to the seizure, examination, storage, or transfer of electronic evidence.

3.3 Computer forensic framework

The Digital Forensics Research Workshop (DFRW) is another significant participant in developing the forensics process (Reith, Carr & Gunsch, 2002). The unique aspect of DFRW is that it is one of the first large-scale consortiums lead by academia rather than law enforcement. This is an important distinction because it will help define and focus the direction of the scientific community towards the challenges of digital forensics. The DFRW has worked to develop a forensics framework that includes such steps as "identification, preservation, collection, examination, analysis, presentation, and decision". Based on this framework, the scientific community may further development and refinement this model.

A computer forensic framework can be defined as a structure to support a successful forensic investigation. This implies that the conclusion reached by one computer forensic expert should be the same as any other person who has conducted the same investigation (Van Solms & Lourens, 2006). In order to gain wider perception of this matter, it is useful to analyze an overview of methodological frameworks of digital forensics (Čisar & Maravić Čisar, 2011).

Starting from the previous forensic protocols, there exist common steps that can be abstractly defined to produce a model that is not dependent on a particular technology or electronic crime. The basis of this model is to determine the key aspects of the aforementioned protocols as well as ideas from traditional forensics. This proposed model can be thought of as an enhancement of the DFRW model since it is inspired from it. The abstract digital forensics model proposes a standardized

digital forensics process that consists of the following components (Reith, Carr & Gunsch, 2002):

- *Identification*: which recognizes an incident from indicators and determines its type;
- *Preparation*: which entails the preparation of tools, techniques, search warrants, and monitoring authorizations and management support;
- *Approach strategy*: that develops a procedure to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim;
- *Preservation*: which involves the isolation, securing and preservation of the state of physical and digital evidence;
- *Collection*: that entails the recording of the physical scene and duplicate digital evidence using standardized and accepted procedures;
- *Examination*: which involves an in-depth systematic search of evidence relating to the suspected crime;
- *Analysis*: which involves determination of the significance, reconstructing fragments of data and drawing conclusions based on evidence found;
- *Presentation*: that involves the summary and explanation of conclusions;
- *Returning evidence*: that ensures physical and digital property is returned to proper owner.

In accordance with digital forensic analysis methodology (***, 2014i), three processes are essential: preparation/extraction (1), identification (2) and analysis (3). A more detailed explanation of certain processes is given by the following algorithmic scheme presented in Fig. 1.

Carrier and Spafford (2003) proposed the Integrated Digital Investigation Model (IDIP) that organizes the process into five groups:

Readiness phases – the goal of this phase is to ensure that the operations and infrastructure are able to fully support an investigation. It includes two phases: operations and infrastructure readiness;

Deployment phases – the purpose is to provide a mechanism for an incident to be detected and confirmed. It includes two phases:

- Detection and Notification phase; where the incident is detected and then appropriate people notified;
- Confirmation and Authorization phase; which confirms the incident and obtains authorization for legal approval to carry out a search warrant.

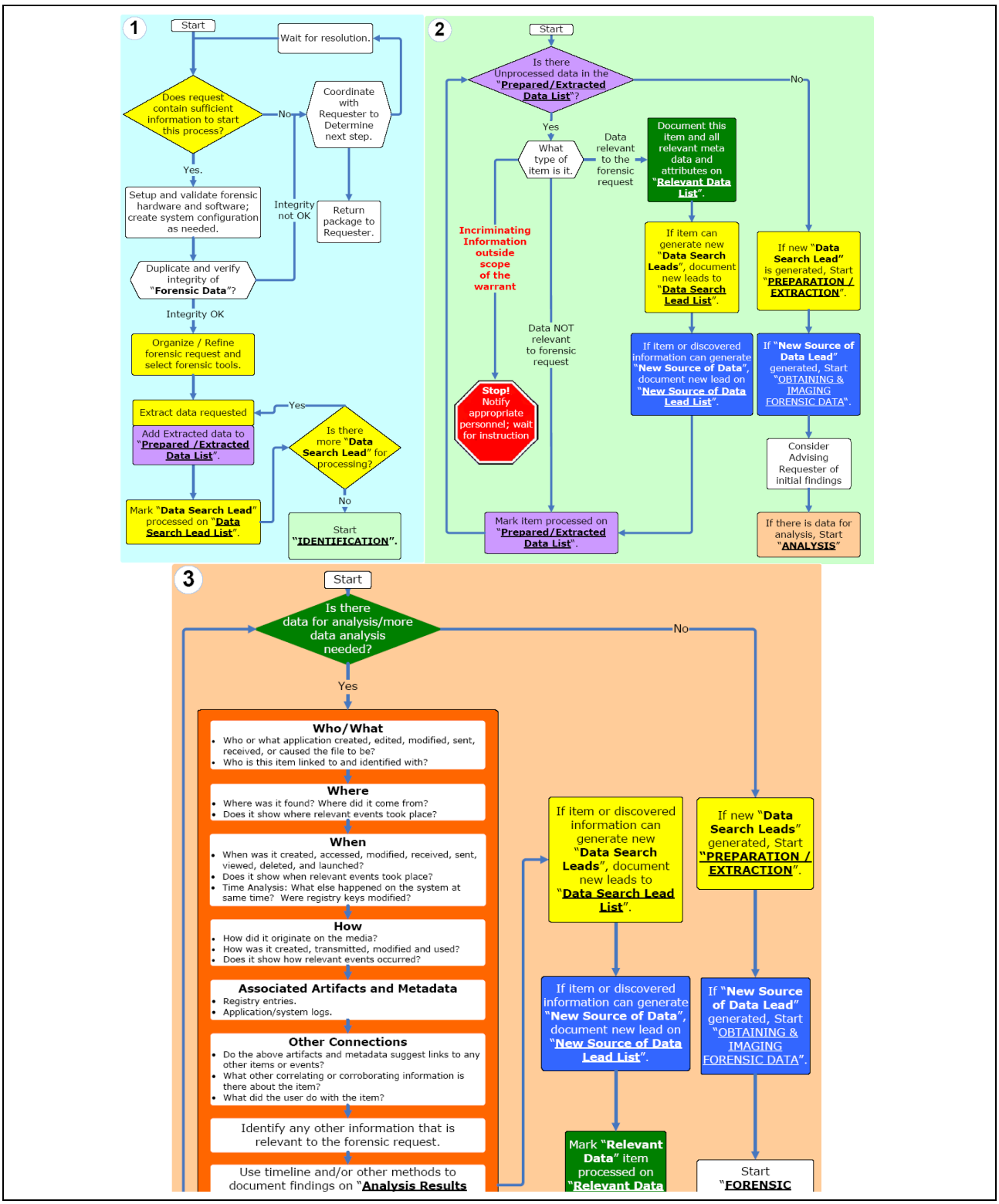

Fig. 1. Digital Forensics Analysis Methodology (**, 2014)

Physical Crime Scene Investigation phases – The goal of these phases is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident (Agarwal et al., 2011). It includes six phases:

- Preservation phase; which seeks to preserve the crime scene so that evidence can be later identified and collected by personnel trained in digital evidence identification;
- Survey phase; that requires an investigator to walk through the physical crime scene and identify pieces of physical evidence;
- Documentation phase; which involves taking photographs, sketches, and videos of the crime scene and the physical evidence. The goal is to capture as much information as possible so that the layout and important details of the crime scene are preserved and recorded;
- Search and collection phase; that entails an in-depth search and collection of the scene is performed so that additional physical evidence is identified and hence paving way for a digital crime investigation to begin;
- Reconstruction phase; which involves organizing the results from the analysis done and using them to develop a theory for the incident;
- Presentation phase; that presents the physical and digital evidence to a court or corporate management.

Digital Crime Scene Investigation phases – The goal is to collect and analyze the digital evidence that was obtained from the physical investigation phase and through any other future means. It includes similar phases as the Physical Investigation phases, although the primary focus is on the digital evidence. The six phases are (Agarwal, 2011):

- Preservation phase; which preserves the digital crime scene so that evidence can later be synchronized and analyzed for further evidence;
- Survey phase; whereby the investigator transfers the relevant data from a venue out of physical or administrative control of the investigator to a controlled location;
- Documentation phase; which involves properly documenting the digital evidence when it is found. This information is helpful in the presentation phase;
- Search and collection phase; whereby an in-depth analysis of the digital evidence is performed. Software tools are used to reveal hidden, deleted, swapped and corrupted files that were used including the dates, duration, log file etc. Low-level time lining is performed to trace a user's activities and identity;
- Reconstruction phase; which includes putting the pieces of a digital puzzle together, and developing investigative hypotheses;
- Presentation phase; that involves presenting the digital evidence that was found to the physical investigative team.

Review phase – Reviewing the investigation to identify areas of improvement.

The crime scenes and digital forensic framework is the subject of detailed analysis in many papers (Bulbul et al., 2013; Chang et al., 2013; Kang et al., 2013; Hildebrandt et al., 2013).

3.4 Process models

Numerous attempts have been made to design a process model but to date there are no universally accepted ones. This may partly be ascribed to the fact that a number of the process models were especially designed for a given environment, e.g. law enforcement. Thus they were not readily applicable in other environments, such as incident response. The main models dating from 2001 are listed below in chronological order (Adams, 2012):

- The Abstract Digital Forensic Model (Reith, et al., 2002) – Built upon the initial framework of the DFRW and claimed to have abstractly defined common steps from previous forensic protocols. These steps reflect the traditional forensics approach applied to a digital context;
- The Integrated Digital Investigative Process (Carrier & Spafford, 2003) – Adopts physical crime scene processes for digital crime scene with the computer being treated only as one of the transition phase;
- An Extended Model of Cybercrime Investigations (Ciardhuain, 2004) – In order to model the entire information flow associated with a digital forensic investigation the author identifies thirteen activities of which only the first eight are relevant to evidence acquisition: awareness, authorisation, planning, notification, search and identification of evidence, collection of evidence, transport of evidence and storage of evidence;
- The Enhanced Digital Investigation Process Model (Baryamureeba & Tushabe, 2004) – Follows the same basic form and takes the same fundamental standpoint as original version of the IDIP in that the digital evidence is treated in the same way as physical evidence.
- The Digital Crime Scene Analysis Model (Rogers, 2004) – The idea of building on the similarities between digital and physical investigations at a conceptual level was progressed by Rogers, despite the fact that this introduces new challenges, as this enables a common approach to be defined with the benefit of bringing digital forensics into the recognized field of forensic science;
- Hierarchical, Objectives-Based Framework for the Digital Investigations Process (Beebe&Clark, 2004) – An alternative to the abstract approach for producing a digital forensic model is proposed by Beebe and Clark on the basis that the focus on the abstract is at the expense of the fundamental investigative principles. The authors of this concept concluded that although previous models are useful in explaining overarching concepts, they lack the detail required to be of practical use;
- Framework for a Digital Investigation (Kohn, et al., 2006) – Kohn et al. conclude that the important factors in a digital forensic model are knowledge of the legal environment and that the model should contain three stages, namely preparation, investigation and presentation;

- The Four Step Forensic Process (Kent, et al., 2006) – Kent et al. developed a guide whose aim is to provide information that would allow an organization to develop their own digital forensic capability, using IT professionals, for security incident response. They identify several basic stages (collection, examination, analysis and reporting) in other models with the main differentiator being the degree of granularity adopted in describing the detail for each stage of the process;
- FORZA (Ieong, 2006) – Digital forensics investigation framework – Ieong adopted a different focus for his information flow model, by seeking to accommodate the involvement of legal practitioners in the process of a digital forensic investigation by assigning them specific roles within the framework and using high - level business model descriptions for the various stages rather than technical terms;
- Process Flows for Cyber Forensics Training and Operations (Venter, 2006) – Suggesting that the benefit of the process flow approach is that it will potentially reduce errors whilst enhancing the standard of documentation, Venter describes four design principles for the development of a process flow model: 1. Ease of use for non-IT professionals 2. Applicable in most cases 3. Assist with expert testimony or at least not interfere with it 4. Can be utilized during operations and not only during training;
- The Common Process Model (Freiling & Schwittay, 2007) – Freiling and Schwittay clearly identify the distinction between incident response and digital forensics. This model consists of three main phases: pre-analysis, analysis and post-analysis;
- The Two-Dimensional Evidence Reliability Amplification Process Model (Khatir, et al., 2008) – Khatir et al. conclude that the issue of the reliability of evidence has still not been addressed and thus present the model which consists of five major phases (of which only the first two are relevant to data acquisition: initialization and evidence collection), sixteen sub-phases (of which only the first five are relevant: confirmation, case assessment, authorization, physical evidence collection and digital evidence collection) and four 'umbrella activities' which apply to all phases (documentation, preservation and authenticity, case management and team setup and computer tools utilization);
- The Digital Forensic Investigations Framework (Selamat, et al., 2008) – Selamat et al. identify common phases in previous models and relate them to a more concise framework to produce a map of the Digital Forensic Investigations Framework. Their framework identified five phases to which the reviewed models could be mapped. Of these phases only Phase 1 (preparation) and Phase 2 (collection and preservation) are relevant to data acquisition. They note that their review showed that whilst all the models contain Phases 2, 3 and 4 (collection and preservation, examination and analysis, presentation and reporting) only a few contain Phases 1 (preparation) and 5 (disseminating the case) which they consider to be important;

- The Systematic Digital Forensic Investigation Model (SDFIM) (Agarwal, et al., 2011) – SDFIM is proposed to assist forensic practitioners and organizations to establish their policies and procedures. This model has eleven phases covering all aspects of a forensic practitioner's work but in contrast to many previous models the analysis phase is not the main focus of the activities described.

4. Conclusion

It is not only law enforcement and the police force that are playing close attention to cybercrime, but also ordinary home users, system administrators and even the governments. Cybercrime has reached a stage where enormous amounts of money are involved and used for driving crime rather than professional challenges and experimentations. Given the lack of efficient prevention and recovery from having one's computer being controlled, it is becoming ever more difficult for users enjoy the benefits of the Internet. Luckily, the burgeoning field of cyberforensics is proof that perpetrators who commit digital crimes are not outside the reach of the law. Taking into consideration that much work has been done in terms of standardizing the processes and procedures, it is apparent that most criminals cannot stay anonymous forever. Based on successful forensic investigations, it is up to the law and government to take punitive measures. It has and will continue to pose a challenge for law and policy makers who are traditionally slow in their reactions. Besides, international cooperation is vital in terms of solving digital crimes successfully, requiring comprehensive agreements between states.

Finally, there can be no discussion of cybercrime without the analysis of the directions this field is headed towards, since all preparatory steps must be taken. It seems certain that criminals will increasingly use the Internet to commit malicious acts. The actual challenge is for researchers, industry, law enforcement and the government to synchronize their activities so as to gain control over the ability to commit crimes and keep it down at a manageable level. Cybercrime in its various forms is not likely to disappear; instead, it is increasing in volume and strength. If one studies incidents of the past, one can draw conclusions from and use that information to prevent future crime. Cyberlaw will need to modify and develop as fast as hackers do in order for it to keep up with controlling digital crime. Law must also find a balance between protecting citizens from crime, and infringing on their rights. The advantage of the Internet is its vastness and freedom. The question is whether or not it will be able to remain this way while simultaneously taking tougher actions against criminals? This remains to be seen over time. So far, the results offer cause for optimism.

5. References

Adams, R.B. (2012). The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice, PhD thesis, *Available from:* http://researchrepository.murdoch.edu.au/14422/2/02Whole.pdf *Accessed on*: 2014-08-25

Agarwal, A.; Gupta, M.; Gupta, S. & Gupta, S. (2011). Systematic Refined Digital Forensic Investigation Model, *International Journal of Computer Science and Security* (IJCSS), Volume 5, Issue 1, pp. 118-132

Bulbul, H.I.; Yavuzcan, H.G. & Ozel, M. (2013). Digital forensics: An analytical crime scene procedure model (ACSPM), *Forensic Science International*, Volume 233, Issue 1-3, pp. 244-256

Caloyannides, M. A. (2001). Computer Forensics and Privacy, Artech House, Inc

Carrier, B. & Spafford, E.H. (2003). Getting Physical with the Investigative Process, *International Journal of Digital Evidence*, Volume 2, Issue 2

Chang, Y.T.; Chung, M.J.; Lee, C.F.; Huang, C.T. & Wang, S.J. (2013). Memory forensics for key evidence investigations in case illustrations, *Information Security* (Asia JCIS), Article number 6621658, pp. 96-101

Čisar, P., & Maravić Čisar, S. (2011). Methodological Frameworks of Digital Forensics, IEEE 9th International Symposium on Intelligent Systems and Informatics SISY 2011, Subotica, Serbia, Proceedings CD ROM, pp. 343-347

Čisar, P. & Čisar, S. M. (2012). General Directions of Development in Digital Forensics. *Acta Technica Corvininesis-Bulletin of Engineering*, 5(2)

Digital Forensics Research Workshop, "A Road Map for Digital Forensics Research" 2001., *Available from:* www.dfrws.org

Gercke, M. (2013). Training on Cybercrime and Discussion of the Draft Bill, Special Training on Cybercrime, 2nd Workshop on Transposition of SADC Cybersecurity Model Laws In National Laws For Namibia Windhoek, Namibia. *Available from*: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/Special% 20Training % 20on%20Cybercrime%20%281%29.pdf *Accessed on:* 2014-07-29

Golden, R. (2006). Research in Next-Generation Digital Forensics, University of New Orleans, *Available from*: http://cs.uno.edu/~golden/Lectures/faculty-lecture-forensics-nov2006.ppt *Accessed on:* 2014-07-29

Harrison, W. (2011). Developing an Undergraduate Course in Digital Forensics, PSU Center for Information Assurance, Portland State University, *Available from:* http://www.ccsc.org/northwest/2006/ppt/forensicstutorialHARRISON.pdf *Accessed on:* 2014-07-14

Hildebrandt, M.; Kiltz, S. & Dittmann, J. (2013). Digitized forensics: Retaining a link between physical and digital crime scene traces using QR-codes, Proc. SPIE 8667, Article number 86670S

Kang, J.; Lee, S. & Lee, H. (2013). A digital forensic framework for automated user activity reconstruction, *Lecture Notes in Computer Science*, Volume 7863, pp. 263-277

Kruse, W. & Heiser, J.G. (2002). Computer Forensics: Incident Response Essentials, Addison-Wesley

Osterburg, J.W. & Ward, R.H. (2014). Criminal Investigation: A Method for Reconstructing the Past, 7th Edition, Anderson Publishing, page 279

Pfleeger, C.P. & Pfleeger, S.L. (2006). Is There a Security Problem in Computing?, *Book Security in Computing*, 4th Edition, ISBN-10: 0-13-239077-9, Published by Prentice Hall

Rakun, Jurij; Berk; Peter; Stajnko, Denis; Ocepek, Marko & Lakota, Miran (2012), Digital Image Processing Approach to Fingerprint Authentication, *Chapter 43 in DAAAM International Scientific Book 2012*, pp. 517-526, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-901509-86-5, ISSN 1726-9687, Vienna, Austria DOI: 10.2507/daaam.scibook.2012.43

Ramabhadran, A. (2014). Forensic Investigation Process Model for Windows Mobile Devices, *Available from:* http://www.forensicfocus.com/downloads/windows-mobile-forensic-process-model.pdf *Accessed on:* 2014-08-25

Reith, M.; Carr, C. & Gunsch, G. (2002). An Examination of Digital Forensic Models, *International Journal of Digital Evidence*, Volume 1, Issue 3

Shipley, T. & Bowker, A. (2013). Investigating Internet Crimes, An Introduction to Solving Crimes in Cyberspace, ISBN: 978-0-12-407817-8

Van Solms, S.H. & Lourens, C.P. (2006). A Control Framework for Digital Forensics, IFIP 11.9

*** (2014a) United Nations (2013) Comprehensive Study on CyberCrime, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf

*** (2014b) U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, Electronic Crime Scene Investigation. A Guide for First Responders, 2001, *Available from:* http://purl.access.gpo.gov/GPO/LPS14094 *Accessed on:* 2014-07-07

*** (2014c) http://www.go-gulf.com/blog/cyber-crime/ – GO-Gulf, Cybercrime Statistics and Trends *Accessed on:* 2014-07-16

*** (2014d) http://www.britannica.com/Ebchecked/topic/130595/cybercrime – Encyclopaedia Britannica, *Accessed on:* 2014-08-25

*** (2014e) http://articles.latimes.com/2012/jun/06/business/la–fi–tn–eharmony-hacked-linkedin - 20120606 – Los Angeles Times, 2012/06/06, *Acceseed on:* 2014-08-25

*** (2014f) http://www.newworldencyclopedia.org/entry/cybercrime – New World Encyclopedia, *Accessed on:* 2014-07-07

*** (2014g) http://www.nypost.com/p/news/national/zappos_cyber_attack_pWsrU60crm8SGHJWYGuP7K–New York Post, 2012/01/17 *Accessed on:* 2014-07-29

*** (2014h) http://www.reuters.com/article/2012/10/12/net-us-wellsfargo-cyberattacks-idUSBRE89B1C620121012 – Reuters, 2012/10/12 *Accessed on:* 2014-07-29

*** (2014i) Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Cybercrime Lab (2007). *Available from:* http://www.justice.gov/criminal/cybercrime/docs/ forensics_chart.pdf *Accessed on:* 2014-07-29