# Chapter 11
# A Model for Hybrid Evidence Investigation

**Konstantinos Vlachopoulos**
*Department of Informatics, Ionian University, Corfu, Greece*

**Emmanouil Magkos**
*Department of Informatics, Ionian University, Corfu, Greece*

**Vassileios Chrissikopoulos**
*Department of Informatics, Ionian University, Corfu, Greece*

## ABSTRACT

*With the advent of Information and Communication Technologies, the means of committing a crime and the crime itself are constantly evolved. In addition, the boundaries between traditional crime and cybercrime are vague: a crime may not have a defined traditional or digital form since digital and physical evidence may coexist in a crime scene. Furthermore, various items found in a crime scene may worth be examined as both physical and digital evidence, which the authors consider as hybrid evidence. In this paper, a model for investigating such crime scenes with hybrid evidence is proposed. Their model unifies the procedures related to digital and physical evidence collection and examination, taking into consideration the unique characteristics of each form of evidence. The authors' model can also be implemented in cases where only digital or physical evidence exist in a crime scene.*

## INTRODUCTION

Crime is an undisputable part of every society. During the centuries crime has been developed and so did crime investigation techniques. In the 20th century the need for investigating crime in a more accurate way has introduced forensic science, focusing on the collection and examination of evidence connected to a crime. In the 80's-90's the proliferation of computing and Internet technologies has broadened the means of committing a crime. Nowadays, the majority of conventional crime investigations face the need to search for extra evidence that may have been stored in digital form or been produced by digital devices. For example, offenders of the -so called- traditional

DOI: 10.4018/978-1-4666-4006-1.ch011

crimes, like homicides or rapes, may have used the Web, e-mail, or cellular communication services to collect and transfer information related to the crime. Examining this evidence can for example produce valuable information about a crime, the motives of the offenders, the relationship between the offender and the victim, the accomplices of the offender. As a result, digital forensics flourished, becoming the key player in the battle against crime. (Agarwal, Gupta, Gupta, & Gupta, 2011; Beebe, 2009; Garfinkel, 2010; Palmer, 2002; Reith, Car, & Gunsch, 2002; Vlachopoulos, 2007).

In this cyber-physical environment it becomes extremely difficult to collect every single scratch of evidence or to find a specific piece of evidence. In the digital investigation field for example, a number of challenges need to be studied and addressed (Beebe, 2009; Garfield, 2010; Sheldon, 2005), including: The decreasing size of storage devices which makes the creation of a forensic image or the processing of the data they contain, challenging; the expansion of malware stored in RAM that demands the development of specialized RAM forensics tools; the proliferation of smartphones and pervasive computing technologies that extend the need to search for evidence in a variety of new digital devices or physical items with embedded systems-on-chip (SOC), e.g., clothes; the use of cloud computing technologies so that evidence cannot be found in a single computer or network and may be stored and/or processed outside the legal jurisdiction; legal issues related to security and privacy that influence both physical and digital investigation and the admissibility of collected evidence.

Particularly with the advent of smart environments, more and more everyday processes will be supported by pervasive devices (e.g., RFID tags, sensors, actuators etc), networked with each other and with other entities (including human beings) through standard communication protocols and a variety of network technologies (Atzori, Iera, & Morabito, 2010; Lee et al., 2012; Li et al., 2011). Internet of Things (IOT) adds connectivity for anything (ITU Reports, 2005) by embedding short range mobile transceivers into a wide range of gadgets and everyday objects enabling new forms of communication between people and things and between things itselves. Radio-frequency identification (RFID), sensors, miniaturization and nanotechnology are the main technologies in the upcoming environment where objects like food packages, furniture and paper documents become smart having the ability to communicate and interact (Kosmatos, Tselikas, & Boucouvalas, 2011). A smart object can be tracked through space and time throughout its lifetime, can be uniquely identifiable, and characteristics such as its location, temperature and movement can be recorded. This real time monitoring allows the mapping of the real world into the corresponding virtual world (Atzori et al., 2010) where essential information about a person can be recovered by recovering data contained in smart objects around the person. Sterling (2005) coined the term *spime* as an object that can be traced through space and time, from the time before it was made (its virtual representation), through its manufacture, its ownership history, its location until its eventual obsolescence and breaking down back into raw material.

The growing role of digital evidence to support conventional criminal evidence also illustrates the need for law enforcement agencies to adopt new investigation methods. Up to now, most investigation models deal with only physical or only digital evidence, thus imposing a clear separation. For example U.S. National Institute of Justice (2000) manual about the crime scene investigation and Lee, Palmbach, and Miller's (2001) Scientific Crime Scene Investigation Model do not include specifications about digital evidence and their role in the documentation of a case. Even the U.S. National Institute of Justice Special Report for Electronic Crime Scene Investigation (2008), focuses mainly on procedures concerning digital devices and not on the interpretation of the data they contain. On the other hand, state-of-the-art digital forensic models do not sufficiently pay much attention to physical evidence which is also