Committee: Legal Committee (GA6)

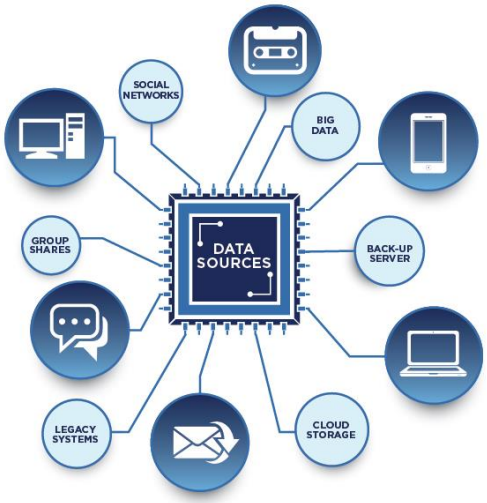
Issue: The question of digital use in criminal investigations

Student Officer: Maira Antonopoulou

Position: Co-Chair

INTRODUCTION

In recent times, due to the development of new technologies and the evolution of ideas and practices, the world has critically changed and is changing day by day. These changes are beneficial not only for current generations, but also for those who are yet to follow, as they change the perspective of all humans and thus their lifestyle habits.
One of the most recent changes is the excessive use of the Internet, not only by teenagers but also by all other social and age groups. According to the UN, in 2016 more than 3.5 million people were using the Internet, a percentage which equates to 47 per cent of the global population. As a result, digitalization of this era is overwhelming the world and leads to the appearance of a multitude of various problems, such as security matters in everyday life.
One of the most up to date and state-of-the-art practices is the use of digital means in criminal investigations. As the world progresses and taking into consideration that we live in a technological era, it is only logical that security and protection need to be enforced with new practices. This issue is very important as it is easier to detect a crime since there is access to a lot of different types of data.
Of course, the job of forensic experts is not an easy one. If there is not educated and well trained staff, appropriate equipment and access, then it is possible that problems will occur. Frequently, criminals use techniques so that they can modify, hide or completely erase a lead, a phenomenon which will make the job of an investigator even more difficult.



DEFINITION OF KEY TERMS

Digital evidence

‘’Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, a personal digital assistant (PDA), a CD, and a flash card in a digital camera, among other places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit

card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime.''*[1]

Digital Forensics

''Digital forensic science is the process of obtaining, analysing and using digital evidence in investigations or criminal proceedings. Digital evidence ranges from images of child sexual exploitation to the location of a mobile phone.'' *[2]

Criminal Investigation

''Criminal investigation is the ensemble of methods by which crimes are studied and criminals apprehended. A criminal investigator seeks to ascertain the methods, motives, and identities of criminals and the identity of victims and may also search for and interrogate witnesses''.*[3]

Internet of things (IoT)

''The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction''.*[4]

Cookies

HTTP Cookies are files which are stored in computers and can be accessed by the web server. Their aim is basically to offer web-Pages that are relevant and tailored to a particular user's hobbies, preferences, etc.

BACKGROUND INFORMATION

Over the last few decades, especially after the introduction of the iPhone, a concern of lots of individuals is that companies have been censoring them and gathering information and this has become remarkably widespread and common. The ''Internet of Things''(IoT) has assumed control of the everyday life of every human been in the 21st century. Smart watches, phones, tablets, computers and basically every electronic device, use systems like cookies, to collect different types of data.

---

*[1] "Digital Evidence and Forensics." *National Institute of Justice*, www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx
*[2] file:///C:/Users/User/Downloads/POST-PN-0520%20(2).pdf
*[3]Britannica, The Editors of Encyclopaedia. "Criminal Investigation." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 2 June 2017, www.britannica.com/topic/criminal-investigation.
*[4] "What Is Internet of Things (IoT)? - Definition from Whatls.com." *IoT Agenda*, internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

Of course, when it comes to important matters, like criminal investigations, the use of data from personal devices is a very sensitive subject. This is why, there has been a lot of debate on whether it is ethical and legally right or not.
For example, in Ohio USA, during a fraud investigation, the police issued a warrant after somehow receiving information from a pacemaker which had been implanted in a suspect's body. That incident stresses two crucial things. First of all, that companies can gather information through any device and secondly, that sometimes, if not in the majority of cases, it is imperative the police have access to personal data for the detection of a crime. On the other hand, even if this kind of data is helpful in solving a crime, is it ethical to expose the ''digital footprint'' of people and make them uncertain of their safety and security from the police or even the government?

Different types of data

- Subscriber data

They refer to the information that helps identify an individual/subscriber. This kind of data includes personal information, such as name, date of birth, address, email account (in every electronic platform), telephone number and even payment data/bills.

- Access data

They are the data which do not identify a user, but provide useful elements and leads that are important for a particular person's identification. This category, includes data, relevant to a timeline of the user's access on the web, meaning that the exact time that a user logs in and logs out of a service and the IP address distributed by a service provider is monitored. (In simple terms, an IP address is a unique address which is used by the internet or a local web and helps identify a device)

- Transactional data

This type of data is connected to the type of service. Thus, this category includes information like the format, size date, time of a message, its destination, its protocol, etc.

- Content data

They concern any data which is saved in a digital form. More specifically, they include videos, photographs, voice-messages, etc.

Digital Evidence

''Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for inspection, and possibly results in a suspect being linked with a crime.''*[5]

---

*[5] "Digital Forensic Investigation." *Eurofins Scientific*, www.eurofins.co.uk/digital-forensic-investigation/?gclid=CjwKCAjwuqfoBRAEEiwAZErCshgAIW7TSBvgLBzZqipN53f_kCsCKa0AR0vR6yrRd1vV3QtZ-QveKRoC36EQAvD_BwE.

Types of sources of digital evidence:

1) GPS system and data
2) The Internet of Things (IoT)
3) Pacemakers
4) Software
5) Digital Controllers (which are basically systems which allow a digital computer to act and take the role of a system controller).

Types of electronic devices from a crime scene:

- Storage Devices

This category includes: Removable Media (like Zip Disks, Compact Disks etc.), Hard Drives, External Hard Drives and Thumb Drives. From all these devices it is possible to extract leads such as: email addresses, messages, photographs, videos, financial records, history of browsing in the Net etc.

- Handheld Devices

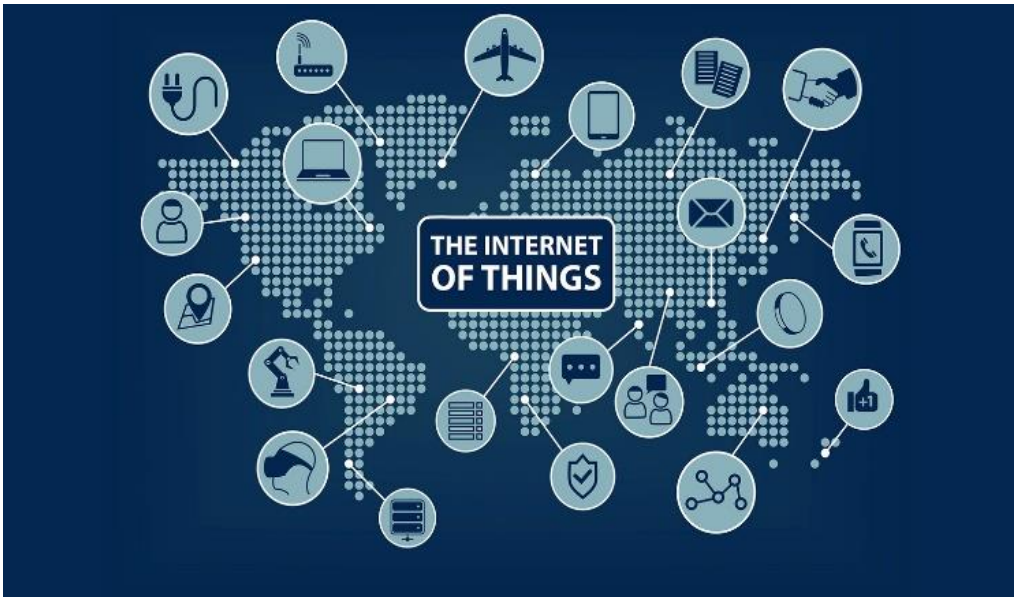
This category includes: Phones, Tablets, Consoles and Computers. All these can provide proof of: Chats on electronic platforms, documents, databases, software applications, etc.

- Peripheral Devices

This category includes: Keyboard and mouse, microphones sticks, Web cameras, memory cards and readers. The potential evidence from all these devices is the information stored in each of them. (For example, incoming and outgoing fax numbers or phones and DNA samples or footprints).

- Network Devices

This category includes: Internet modems, Network hubs, computer network cards, wireless network servers and power supply. The devices themselves, as well as the functions they perform, constitute evidence. IP (Internet Protocol) and LAN (Local Area Network) addresses, also form leads, as they are linked to the computer or/and other devices.



Challenges

The use of digital data in criminal investigation uses a technique called ''Digital forensics'', which identifies digital crimes. Although it may seem easy and beneficial for the progression and development of the whole world, this technique has to face three functional and important challenges.

- Technical Challenges

We live in a world where progress and the discovery of new things never stops. Computer technologies are continually being developed and the Internet has assumed control of our daily life. Of course, everything has both a positive and a negative side. In this particular situation, on the one hand, the usage of new technologies has been extremely beneficial for all mankind, as it facilitates a lot of everyday activities (like transactions, research, acquisition of lots of different things, etc). On the other hand, technology may be used to benefit the targeting of some innocent people and is not invented for the general good.
As a consequence, when a new technology is invented to help investigate and identify crimes and criminals, another one helps the criminals to remain inconspicuous to the police. Unfortunately, digital evidence is easier to modify or completely remove and hide than physical evidence, without living any footprint.

The most common anti-forensic techniques are:

1) Encryption (The process where information is altered and can only be decoded by a decoding key),
2) Steganography (It can be used in conjunction with encryption and cryptography for extra security of the data. It basically conceals the information of a file without changing it outwards),
3) Covert Channel (This technique allows criminals to hide information on the Internet and not be caught by any detection system),
4) Data hidden in storage (Criminals use this technique to hide data in storage areas and at the same time make them invisible).

- Resource Challenges

Another challenge which the investigators have to confront is the fact that the volume of data may be large. In such a case, an investigator has to go through and check all the data information, to gather the ones that are needed in a particular case. Of course, such an action requires time, a limiting factor in criminal investigations.
An investigator is obliged to make sure that all the information gathered has not been modified, altered or damaged, as it cannot be used in an investigation, as it might be regarded as vague leads. Thus, it is of paramount importance that the investigator finds a source that is reliable and secondly, that the collection of data is secured.

- Legal Challenges

Privacy is very important in these kinds of situations. Researchers and experts have to take into consideration that in order to solve a crime and reach the truth, they may have to share private information of a user with others. In that way, they expose the digital footprint of a victim or a criminal. Privacy is a human right, but in such situations this subject is very delicate. Investigators taking a risk by sharing private information with others could end up being prosecuted.

MAJOR COUNTRIES AN ORAGNIZATIONS INVOLVED

The United States of America

The US has taken the lead with the proposal of new technologies, systems and techniques, even in this domain. More specifically, each year there are more cases which are prosecuted in the central offices of the US police than in the whole of the federal judicial system. Digital forensics and digital research are covered by the state and local laws. Digital techniques are used in more than 90% of all criminal investigations, a statistic that makes the US the first country among others that uses extensively digitalization in criminal cases.

China

China has also started taking a stand in the use of digital means in investigations. Although this technique is new, leading firms employing digital forensics have predicted that by 2025, this new idea will be growing at 30 to 50% annually. Presently, more than 30% of all criminal cases are handled with the help of digital means.

The European Commission

The European Commission is also taking a stand in favor of digital forensics. According to the Commission, new laws are necessary in favour of the police and judicial authorities. The initiative includes measures such as:

- Prevention of situations where data are removed, deleted or modified with a European Preservation Order,
- Creation of strong software, in order that data be protected,
- Strong safeguard systems.

UN INVOLVMENT: RELATIVE RESOLUTIONS, TREATIES AND EVENTS

Module 4 from the series relating to cybercrime of the UNODC

The UN has, in its turn, accepted and embraced new techniques for the detection of crimes and tries to impart this idea to all member states. Thus, with the help of the United Nations Office on Drugs and Crimes (UNODC), some useful courses and programs have been run on the subject of digital forensic and relatable issues, during which experts address and fully explain the issues at hand. The main theme of this program is Cybercrime, and Module 4 refers to an ‘’Introduction to digital forensics”.
The key terms of this presentation are: digital evidence, forensics and best practices for digital forensics. This seminar includes also realistic exercises in order for investigators to be familiar with all kinds of techniques.

13th UN Congress on Crime prevention and Criminal Justice

During this congress, which was held in 2015, some discussions were held concerning cybercrime and how digital means can enhance the solving of a criminal case.
After the congress, resolution 72/192, which focuses on techniques used to prevent crimes, was published. In the resolution, references were made to digital forensics and digital evidence, as ways to solve a digital crime, and ways to achieve this goal.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

The Euromed Manual on Digital Evidence for counter-terrorism cases

The Euromed Police is a program funded by the European Union which aims to secure and protect all citizens across the Euro-Mediterranean area and, therefore, deals with a variety of different issues that may be hazardous for humanity. As a result, on the 26th September 2018, Euromed Police, in accordance with the Euromed Justice, launched the ''Euromed Manual on Digital Evidence for counter-terrorism cases''. The goal is to create a set of guidelines in order to help law enforcement and judicial authorities, not only in cases of cyber-crimes, but also for any other criminal case or investigation. This manual provides judges and investigators with the appropriate tools to engage with the digital society (for example Google, Facebook etc.) and thus, if there is an adequate handling of electronic evidence, this can lead to criminals being brought to justice.

Digital Forensics in Maritime Investigations

Within the framework of a rise in maritime crimes, INTERPOL (the International Criminal Police Organization), recently held a forum called ''Digital Forensics on Shipborne Equipment'' at the INTERPOL Global Complex for Innovation, in Singapore.
The aim of this program is to make clear the importance of the existence of police/investigate forces, which are equipped with the appropriate tools and means, but also trained, so that they can identify and extract any leading evidence in digital form, in a criminal case.

The aim of this seminar was to explain that if electronic equipment is used correctly, it can provide the police with critical evidence, such as information related to organized criminal networks.

POSSIBLE SOLUTIONS

In order to tackle this crucial issue, all possible solutions or acts that can be implemented should be taken into account.

First of all, the introduction and acceptance of a unified criminal detection system by a number of countries will cooperate, exchange information, create databases, etc.

Secondly, the use of all techniques in the detection of digital crime would be very beneficial. The creation of a training system, which will prepare and train specifically only those who will be involved in such kinds of investigations, is also of paramount importance.

Moreover, it is imperative that public awareness is raised to enhance and support this unified system in order to become more effective in the global confrontation of crime.

Safeguards need to be introduced to secure private information in order for citizens to be certain that their personal data will not be exposed in public, except in exceptional cases.

Another measure that can be taken in order for digital forensics to be promoted is the publication of results achieved and best practices enforced against International Crime.

Constant exploitation of new techniques and scientific parameters used in the detection of criminal cases would also be very beneficial.

In order for crimes to be detected earlier, access to federal sources databases, as well as the cooperation of all government agencies, would be essential.

Lastly, the judicial systems of each member state and the applicability of the laws of each state should be inter-connected in order that findings of criminal investigations be always legally binding and enforceable in the courts of justice.

BIBLIOGRAPHY

- "Digital Evidence and Forensics." *National Institute of Justice*, www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx.
- file:///C:/Users/User/Downloads/POST-PN-0520.pdf
- "Security Union: Commission Facilitates Access to Electronic Evidence." *European Commission - PRESS RELEASES - Press Release - Security Union: Commission Facilitates Access to Electronic Evidence*, europa.eu/rapid/press-release_IP-18-3343_en.htm.
- https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1513005472.pdf
- file:///C:/Users/User/Downloads/6520-Article%20Text-20609-1-10-20180315.pdf
- *A/RES/72/192 - E - A/RES/72/192*, undocs.org/en/A/RES/72/192.
- Kkienerm. "Cybercrime Module 4." *Cybercrime Module 4*, www.unodc.org/e4j/en/cybercrime/module-4/index.html.
- http://www.aitd.net.in/pdf/13/12.%20Digital%20%20Evidence-%20Technical%20Issues.pdf
- "Top Challenges and Changes in the Use of Digital Forensics Evidence." *Cellebrite*, 16 Dec. 2018, www.cellebrite.com/en/topics/investigative-techniques/webinar-top-challenges-and-changes-in-the-use-of-digital-forensics-evidence/.
- Jackson, and Brian A. "Using Digital Data in Criminal Investigations." *RAND Corporation*, 15 May 2017, www.rand.org/blog/2017/05/using-digital-data-in-criminal-investigations-where.html.
- "What Is Internet of Things (IoT)? - Definition from WhatIs.com." *IoT Agenda*, internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.
- "INTERPOL Spotlights Role of Digital Forensics in Maritime Investigations." *INTERPOL*, www.interpol.int/News-and-Events/News/2018/INTERPOL-spotlights-role-of-digital-forensics-in-maritime-investigations.
- Bricheux, Benjamin. "A Practical Guide for Requesting Electronic Evidence." *Euromed Police*, 10 Sept. 2018, www.euromed-police.eu/launch-of-euromed-digital-evidence-manual/.
- Britannica, The Editors of Encyclopaedia. "Criminal Investigation." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 2 June 2017, www.britannica.com/topic/criminal-investigation.

Multimedia Sources

- "Https://Www.google.com/Url?Sa=i&Source=Images&Cd=&Ved=2ahUKEwjDy7Wq-IfjAhVHa1AKHaUwDwgQjRx6BAgBEAU&Url=Https://Www.transperfectlegal.com/Solutions/Forensic&Psig=AOvVaw1zwJAhUT7a0KovsMDvh9Gy&Ust=1561665722972420." *Https://Www.google.com/Url?Sa=i&Source=Images&Cd=&Ved=2ahUKEwjDy7Wq-IfjAhVHa1AKHaUwDwgQjRx6BAgBEAU&Url=Https://Www.transperfectlegal.com/Solutions/Forensic&Psig=AOvVaw1zwJAhUT7a0KovsMDvh9Gy&Ust=1561665722972420*.

- “Https://Www.coindesk.com/Uk-Government-Pilots-Blockchain-in-Bid-to-Secure-Digital-Evidence.” *Https://Www.coindesk.com/Uk-Government-Pilots-Blockchain-in-Bid-to-Secure-Digital-Evidence*.
- “Https://Www.google.com/Url?Sa=i&Source=Images&Cd=&Cad=Rja&Uact=8&Ved=2ahUKEwiNqPSm-ofjAhVDblAKHeDqAyYQjRx6BAgBEAU&Url=/Url?Sa=i&Source=Images&Cd=&Ved=&Url=Https://blog.Eccouncil.org/6-Skills-Required-for-a-Career-in-Digital-Forensics/&Psig=AOvVaw1lcZ6zOEaw8MDR4AsOm--g&Ust=1561666176652231&Psig=AOvVaw1lcZ6zOEaw8MDR4AsOm--g&Ust=1561666176652231.” *Https://Www.google.com/Url?Sa=i&Source=Images&Cd=&Cad=Rja&Uact=8&Ved=2ahUKEwiNqPSm-ofjAhVDblAKHeDqAyYQjRx6BAgBEAU&Url=/Url?Sa=i&Source=Images&Cd=&Ved=&Url=Https://blog.Eccouncil.org/6-Skills-Required-for-a-Career-in-Digital-Forensics/&Psig=AOvVaw1lcZ6zOEaw8MDR4AsOm--g&Ust=1561666176652231&Psig=AOvVaw1lcZ6zOEaw8MDR4AsOm--g&Ust=1561666176652231*.
- “Https://Www.google.com/Url?Sa=i&Source=Images&Cd=&Ved=2ahUKEwiS2ZGY-4fjAhWMIlAKHTg1ChIQjRx6BAgBEAU&Url=Https://Www.fbi.gov/Investigate/Cyber&Psig=AOvVaw0jFlS1MM3o2u4eNTAe04PR&Ust=1561666485683873.” *Https://Www.google.com/Url?Sa=i&Source=Images&Cd=&Ved=2ahUKEwiS2ZGY-4fjAhWMIlAKHTg1ChIQjRx6BAgBEAU&Url=Https://Www.fbi.gov/Investigate/Cyber&Psig=AOvVaw0jFlS1MM3o2u4eNTAe04PR&Ust=1561666485683873*.
- “Https://Www.google.com/Url?Sa=i&Source=Images&Cd=&Ved=2ahUKEwjr_4Cy_YfjAhXCL1AKHeFLDUgQjRx6BAgBEAU&Url=Https://Www.itpro.co.uk/Internet-of-Things-Iot/30715/Iot-Security-Measures-Need-Teeth-to-Counter-the-Spread-of-Hackable&Psig=AOvVaw3GS1zOKkRgvlQ_VnVTdsdB&Ust=1561667069088770.” *Https://Www.google.com/Url?Sa=i&Source=Images&Cd=&Ved=2ahUKEwjr_4Cy_YfjAhXCL1AKHeFLDUgQjRx6BAgBEAU&Url=Https://Www.itpro.co.uk/Internet-of-Things-Iot/30715/Iot-Security-Measures-Need-Teeth-to-Counter-the-Spread-of-Hackable&Psig=AOvVaw3GS1zOKkRgvlQ_VnVTdsdB&Ust=1561667069088770*.