



GUIDELINES ON CYBERCRIME INVESTIGATION

GUIDELINES ON CYBERCRIME INVESTIGATION

Tirana, 2022

GUIDELINES ON CYBERCRIME INVESTIGATION

Tirana, 2022

Author: Marjan Stoilkovski
International Consultant

© All rights reserved. The contents of this publication may be freely used and copied for educational and other non-commercial purposes, provided that any such reproduction is accompanied by an acknowledgment of the OSCE as the source.

The views expressed in this publication are those of the author and do not necessarily reflect the official position of the OSCE Presence in Albania.

TABLE OF CONTENTS

INTRODUCTION

NATIONAL CAPACITIES FOR INVESTIGATION OF COMPUTER CRIME	8
COMPUTER CRIME LEGISLATION	10
Budapest Convention for cybercrime	10
Criminal code	11
Criminal Procedure Code	13
Other relevant national laws	16
Computer Crimes Legislation in Albania is dealt with in the following laws	17
The legislation in Albania recognize the following safeguards	19
SOURCES OF ELECTRONIC EVIDENCE	21
Types of Electronic evidence from computers and Storage device (Digital forensics)	22
Types of electronic evidence from Mobile telephones (Digital forensics)	25
Electronic evidence hold by Multinational internet service providers (Request for data Preservation, Request for Disclosure of data, MLA)	26
Data retention/data preservation	28
Digital forensics	28
Principles of Electronic evidence	29
Admissibility and presenting an electronic evidence	31
ELECTRONIC/DIGITAL DEVICES: HOW DO THEY RELATE TO CRIMINAL INVESTIGATIONS?	33
Acquisition of Communications Data as Evidence	46
What different types of communications data are available	47
Subscriber Information	47
Service Use Information	48
Traffic Data	48
When we can acquire Communications Data	49

Processes for Acquisition of Communications Data – National Communication Service Provider:	49
Process for Acquisition of Communications Data (Outside Albania)	51
International and National Partners	53
International Police Cooperation Department (IPCD)	53
Europol	54
Eurojust	54
Interpol	54
SELEC – South East Law Enforcement Center	54
Pursuits Unit – (Fugitives)	55
National Partners	55
OPEN SOURCE INTELLIGENCE (OSINT) - OVERVIEW	57
CYBERCRIME AND CYBER ENABLED CRIMES	62
Cybercrime	62
Common examples of cybercrime	64
National Critical Infrastructure	73
Harassment	74
Criminal Services for Hire	74
Child Exploitation Online	75
Appendix A - Visual Guide - How to look up an IP address or domain name registrant	76
Appendix B – Regional Internet Registry data records explained	79
Appendix C - Investigating email	83
Appendix D – Guidelines for conducting initial investigations in computer related crimes and how to deal with digital evidence.	88
Citizen reporting of computer crime or computer related crime	89
Business or Large Organisation complaint of computer crime or computer related crime	94
INVESTIGATING CRIMES INVOLVING DIGITAL MEDIA - COMPUTERS, LAPTOPS	100

INVESTIGATING CRIMES INVOLVING DIGITAL MEDIA – SMARTPHONES, TABLETS AND MOBILE DEVICES.	104
GLOSSARY	116
ACRONYMS	119
ANNEX	123
ANNEX 1	125
ANNEX 2	131
ANNEX 3	134

This document focuses on how the principles set out in legislation apply to the use of the internet, including social media, as an investigative tool.

Each activity should be considered on a case by case basis, in line with Police and Public Prosecutor policies and national legislation on investigation engagement, communications and use of technology.

Some of the guidelines covers areas of Covert investigative techniques likely to interfere with a person's rights and should be used only when necessary and proportionate. Albanian legislation for surveillance and Data Protection provide the framework for ensuring that such action is lawful and in accordance with the European Convention of Human Rights (ECHR).

This document is subject to continuing review and amendment to take account of developments in legislation, technology, the effect of legal judgments and stated cases.

INTRODUCTION

This document is intended to provide an explanation of computer related crimes and provide initial investigation guidance from receiving the initial crime complaint to the point that preparatory plans are made to arrest a suspect and/or seize digital media, and details the approach for initial investigation.

In today's cybercrime cases, dealing with a digital device or a digital investigation is an everyday occurrence as the vast majority of people have an electronic/digital device, the most common we recognise are mobile phones, tablets and laptops, and with the increase in email and social media usage, most crime complaint will involve analysing and understanding these mediums and the potential areas that will assist your investigation.

At first this technology may look complex, but Public prosecution offices and Police officers have adapted to the proliferation of mobile phones and have an understanding of how the devices communicate and that the telecommunication provider will have records of account holders, phone identifiers such as IMEI number, SIM data, the allocated telephone number, records of usage and payment methods.

It is intended to simplify these same elements when it comes to computers, the internet, world wide web and social media, by providing a link to computer crime legislation, an introduction to computer and network terminology and an explanation of its function, and most importantly what information is likely to assist you in when investigating crime complaints, and who can assist you with an investigation.

The specific areas to be covered is the relevant legislation for cybercrime investigation:

- Law No. 7895 from 27.01.1995, Criminal Code of Albania, as amended (by Law No. 43/2021 and 89/2017)
- Law No. 7905 from 21.03.1995, Criminal Procedure Code of Albania, as amended (by Law No. 41/2021)
- Law No. 9918 from 19.05.2008, "On electronic communications", as amended
- Law No. 9887 from 10.03.2008, "On protection of personal data", as amended
- Law No. 9880 from 25.02.2008, "On electronic signatures", as amended

NATIONAL CAPACITIES FOR INVESTIGATION OF COMPUTER CRIME

With the increase in cybercrime and the use of electronic/digital devices by criminals in criminal acts, more intelligence and evidence is found stored in electronic format. To meet this changing environment, the Albanian Police Department have invested in creating specialist units to combat cybercrime and developing officers' skills to undertake and assist in criminal investigations involving electronic/digital media and computer related crimes.

In this moment there are two specialist cybercrime units, their present roles and responsibilities are detailed below, together with details of how they can assist prosecutors with advice concerning initial crime complaints and criminal investigations from securing data on electronic digital media or how to conduct safe research and investigations on the Internet.

Computer Crime Investigations Unit:

The Computer Crime Investigation Unit is based in Tirana and has a National responsibility for cybercrime investigation as follows:

- Unauthorised Computer Access;
- Malware attacks, Hacking;
- Abuse of Networks;
- Protection of Personal Data;
- Indecent Images of Children;
- ATM fraud;
- e-payments fraud;
- Credit/Debit Card Fraud;
- Card Skimming;
- Regional and International Cooperation;
- Cooperation with Banks and Financial Institutions;
- Cooperation with CIRT National Computer Incident Response Team.

In fulfilling its mission and give efficient support to a public prosecutor in the cybercrime investigation and collection of electronic evidence, the Computer Crime Investigation Unit can develop capacities and being aware of number of additional activities, including the following ones:

- Pre-Planning an investigation where it relates to complex computer crime;
- Live Data or Volatile Data will be encountered;
- Information is required on Wireless networks;
- Advice on acquiring communication data from National or International partners (Data Preservation Requests);
- Communication Data investigation – Emails, Social Media, IP addresses, Phone and Internet Service providers;
- Open Source Intelligence (OSINT) advice – Research equipment and operational security when researching Social Media, Chatrooms, IRC, research of suspects or witnesses on-line;
- Covert Open Source Intelligence Research;
- Incidents affecting the National Critical Infrastructure of Albania.

COMPUTER CRIME LEGISLATION

Budapest Convention on cybercrime

The Convention on Cybercrime, is considered the most relevant international agreement on cybercrime and electronic evidence. The Budapest Convention in general provides recommendation in area of:

- the criminalisation of conduct ranging from illegal access, data and systems interference to computer-related fraud and child pornography;
- procedural law tools to investigate cybercrime and secure electronic evidence in relation to any crime;
- efficient international cooperation.

Budapest Convention is a legal document providing for the criminalisation of cybercrime, procedural powers to secure electronic evidence and a legal basis for international cooperation. The implementation of the convention on Cybercrime will provide an impact at the national level on:

- domestic legislation on cybercrime and electronic evidence worldwide;
- domestic investigations based on such legislation;
- international cooperation, including of serious and organised cases of cybercrime;
- public/private cooperation;
- strengthening of criminal justice capacities.

The Convention on cybercrime it reconciles the vision of a free Internet, where information can freely flow and be accessed and shared, with the need for an effective criminal justice response in cases of criminal misuse.

Criminal code

Article 192/b – Illegal computer access

Unauthorized access or access in excess of the authorization to access a computer system or in a part thereof, through violation of the security measures, is punishable by fine or imprisonment up to three years. When this very act is committed in military, national security, public order, civil protection, health computer systems or any other computer system of public importance, it is punishable by imprisonment from three up to ten years.

Article 293/a – Illegal interception of computer data

The illegal interception, with technical devices, of the non-public transmissions of computer data from or within a computer system, including electromagnetic emissions from another computer system carrying such data, is punished with an imprisonment sentence of three to seven years. When this offence is committed from/within the computer systems of the military, public order, civil protection or any other computer system of public importance, it is punished with an imprisonment sentence of seven to fifteen years.

Article 293/b – Data interference

The damaging, deletion, alternation or unauthorized suppression of computer data is punished by an imprisonment sentence of six months to three years. When this offence is committed against the computer data of the military, public order, civil protection, health care or any other computer data of public importance, it is punished with an imprisonment sentence of three to ten years.

Article 293/c – Interference in the computer systems

The serious and unauthorized hindering of the functioning of a computer system by inputting, damaging, deforming, altering, deleting or suppressing of data is punished with an imprisonment sentence of three to seven years. When this offence is committed in the computer systems of the military, national security, public order, civil protection, health care or any other computer system of public importance, it is punished with an imprisonment sentence of five to fifteen years.

Article 293/ç – Misuse of devices

The production, possession, selling, procurement for use, distribution or otherwise making available of a device, including a computer programme, a computer password, access code or other similar data, designed or adjusted to access the whole or part of the computer system, for the purpose of committing the offences established in articles 192/b, 293/a, 293/b e 293/c of this code, are punished with an imprisonment sentence of six months to five years.

Article 186/a – Computer related forgery

Any input, alteration, deletion or suppression of data, without right, with the intent of creating inauthentic data, to be used and presented as authentic, regardless whether or not the data is directly readable or intelligible are sentenced with imprisonment period of 6 months to six years. When this act is committed by the person in charge of retaining and administering computer data, in cooperation, more than one time or when it has led to grave consequences to the public interest, it is sentenced with imprisonment from three to ten years.

Article 143/b – Computer fraud

Entering, modifying, deleting or omitting computer data or interfering in the operation of a computer system, in order to ensure for oneself or for other parties, through fraud, an unfair economic benefit or to cause to a third party asset reduction, are punishable by imprisonment from six months up to six years. This very act, when committed in complicity, or more than once, or when it has brought about serious material consequences, is punished by imprisonment from five to fifteen years.

Article 117 – Pornography Production

Production, distribution, advertisement, export, import, sale, and publication of pornographic materials in environments with children, by any means or form, shall constitute criminal contravention and shall be punishable by imprisonment of up to two years. Production, import, offering, making available, distribution, broadcasting, use, or possession of child pornography, as well as the conscious creation of access in it, by any means or form, shall be punishable by three to ten years of imprisonment. Recruitment, exploitation, compulsion, or the persuasion of a child to participate in pornographic shows, as well as the participation in such shows which involve the participation of children, shall be punishable by five to ten years of imprisonment.

Article 23 Criminal Code – Responsibility for the attempt

The person attempting to commit a crime shall be held responsible. Considering the stage until the realization of the consequence, as well as the causes due to which the offence remained an attempt, the court may mitigate the sentence, and may lower it under the minimum provided for by law, or may decide for a kind of punishment milder than the one provided for by law.

Article 27 Criminal Code - Responsibility of collaborators

Organizers, instigators, and helpers bear the same responsibility as the executors for the criminal act committed. In deciding the sentencing of collaborators, the court should consider the level of participation and the role played by everyone in committing the criminal act.

Criminal Procedure Code

Article 221 Criminal Procedures Code – Limits of permission

- ① The interception of conversations or telephone communication or other forms of telecommunication is permitted only where there is a proceeding for:
- Intentional crimes punishable by imprisonment not less than seven years maximum
 - Criminal offences of insult and threat by phone call.

Article 222 Criminal Procedures Code - The decision authorizing the interception

- ① Upon the request of the prosecutor, in the instances conceded in paragraph 1 of Article 221, the court shall authorise the interception upon a grounded decision, as long as it is indispensable for continuing with the initiated investigation and where a reasonable doubt exists against the person and based on evidence that he has committed a criminal offence.
- ② When there are reasonable grounds to believe that the delay may bring a serious damage to investigations and the conditions of paragraph 1 of this article, are met, the prosecutor shall establish the interception, by a reasoned act, and shall inform the court immediately, but not later than twenty-four hours of the decision taken. When the validation is not done within the due time limit, the interception cannot continue and its outcome cannot be used.
- ③ If any of the two persons to be intercepted is available to carry out and register the relevant action, pursuant to the agreement with the judicial police officer, such action can be carried out upon authorised by the prosecutor.
- ④ In the cases provided for in paragraphs 1, 2 and 3, of this article, the court shall rule by reasoned decision in closed session within 24 hours of the submission of the prosecutor's request. Against the decision for the rejection of the interception's request, a special appeal may be lodged with the court of appeal within 24 hours. The appeal court shall decide within 48 hours of the receipt of acts. Submission of the request for the validation of interception does not result in its suspension.
- ⑤ The interception decision shall indicate the method and time limit for their execution, which cannot exceed fifteen days. Such time limit can be extended by the court for a period of 15 days, upon the reasoned request of the prosecutor, whenever it is necessary, provided that conditions provided for in paragraph 1 of this Article exist and the outcome of the interception dictate the need for extending the time period.

- ⑥ In the court decision on the secret photographic or video interception or on the interception of conversations in private locations, the judicial police officer or the qualified specialist may be authorised to access these locations secretly, acting in accordance with the decision. This authorisation shall be implemented within 15 days.
- ⑦ Any acts ordering, authorising, validating or extending interceptions, as well as the initiation or ending of any interception action shall be indicated in the register kept at the prosecution office.
- ⑧ In the cases referred to in Article 221, paragraph 2, the action is authorised by the prosecutor.

Article 299/a - Expedited preservation and maintenance of the computer data

- ① The prosecutor may order the expeditious preservation of certain computer data, including traffic data, when there are enough reasons to believe that the data may be lost, damaged or altered.
- ② If the computer data is in the possession or control of a person, the prosecutor can order this person to preserve and maintain the integrity of the specified computer data for a period of up to 90 days, in order to search and disclose them. When there are reasonable grounds, this timeframe can be renewed only once.
- ③ The person in charge of preserving and maintaining the computer data is obliged to keep confidential the procedures and actions undertaken under point 2 of this article until the end of investigations.

Article 299/b - Expedited preservation and partial disclosure of computer data

The person in charge of expeditious preservation and maintenance of the traffic data is obliged to undertake all the necessary measures to ensure that the stored data is valid, regardless of whether one or more service providers were involved in the transmission of the communication as well as to provide the prosecutor or the authorized judicial police officer with a sufficient amount of traffic data to enable the identification of the service provider and the path through which the communication was transmitted.

Article 191/a - Obligation to produce computer data

- ① In the cases of proceedings related to criminal offences in the area of information technology, the Court, upon a request from the prosecutor or the plaintiff, orders a person to submit computer data in his possession or control, which is stored in a computer system or other data storage devices.

- ② In these proceedings, the Court orders the service provider to submit all subscriber information relating to the services offered by the service provider.
- ③ When there are grounded reasons to believe that delays would seriously damage the investigations, the prosecutor, by means of a reasoned act, orders the production of computer data specified in points 1 and 2 of this article and notifies the court immediately. The Court reviews the decision of the prosecutor within 48 hours after the notification

Article 208/a - Seizure of computer data

- ① In the cases of proceedings related to criminal offences in the area of information technology, the Court, upon a request from the prosecutor, orders the seizure of the data and the computer systems. The court specifies in the order the right to access, search and obtain data in a computer system, as well as the prohibition of further actions or the securing of the data or computer systems.
- ② When there are reasonable grounds to believe that the computer data sought is stored in another computer system or part of it, and that such data is legally accessible from or available to the initial system sought, the court, upon a request from the prosecutor, immediately orders the search or access to this computer system as well.
- ③ For the purpose of executing the court order, the prosecution or the judicial police officer delegated by the prosecutor takes measures:
 - To stop further activities or to secure a computer system or part of it and other data storage devices;
 - Make and retain copies of the computer data;
 - To render inaccessible or to remove those computer data from the accessible computer systems;
 - Maintain the integrity of the respective stored data.
- ④ In order to have these measures applied, the prosecutor may order an expert, who has knowledge about the functioning of computer systems or measures to be taken to protect the computer data therein. The designated expert cannot refuse the task unless he provides reasonable.

Other relevant national laws

Law no. 9918 dated 19.05.2008 “On electronic communication”

Article 101 “Preservation and administration of data for the purpose of criminal prosecution”

- ① Regardless of other definitions in this law, the operators of networks and public electronic communications are obliged to preserve and administer the data records of their subscribers for a period of two years.
- ② These records should contain data that enable:
 - The identification of subscribers ensuring the registration of their full identity
 - The identification of the end equipment used in the communication
 - The identification of the date, hour, duration of communication and the number called
- ③ These records should be made available, also in an electronic form, to the authorities referred to in the Criminal Procedure Code, based upon their request.

Computer Crimes Legislation in Albania is dealt with in the following laws:

- Law No. 7895 from 27.01.1995, Criminal Code of Albania, as amended (by Law No. 43/2021 and 89/2017)
- Law No. 7905 from 21.03.1995, Criminal Procedure Code of Albania, as amended (by Law No. 41/2021)
- Law No. 9918 from 19.05.2008, “On electronic communications”, as amended
- Law No. 9887 from 10.03.2008, “On protection of personal data”, as amended
- Law No. 9880 from 25.02.2008, “On electronic signatures”, as amended

Criminal Code enlists the following offences:

- Article 74/a Computer-related distribution of pro-genocide or crimes against humanity materials (Added up by law no 10 023, dated 27/11/2008, Article 11)
- Article 84/a Threat under motives of racism and xenophobia through computer-based system (Added up law no 10 023, dated 27/11/2008, Article 12)
- Article 117 /2 Pornography (Paragraph II is added by law no. 9859, dated 21.01.2008, article 1; Amended by law no.144, dated 02.05.2013, article 29)
- Article 119/a Distribution of racist or xenophobic materials through computer-based system (Added by law no. 10 023, dated 27.11.2008, article 13)
- Article 119/b Insult under motives of racism and xenophobia through computer-based system (Added by law no. 10 023, dated 27.11.2008, article 13)
- Article 137/a Theft of electronic communication network (Added by law no.144, dated 02.05.2013, article 34)
- Article 143/b Computer-related fraud (Added by law no. 10 023, dated 27.11.2008, article 15;
- The part that provides fine as main punishment in addition to imprisonment is abrogated by law no.144, dated 02.05.2013, article 48)
- Article 186/a Computer falsification (Added up by Law 10 023, date 27.11.2008, Article 18)

- Article 192/b Unauthorized computer interference (Added up by Law no. 8733, dated 24.01.2001, Article 53; amended by Law no. 10 023, dated 27.11.2008, Article 19)
- Article 293/a Unlawful wiring of computer data (Added by Law no. 10023, dated 27.11.2008, article 23)
- Article 287 Laundering the Proceeds of Criminal Offence or Criminal Activity
- Article 293/b Interference with computer-related data (Added by Law no. 10023, dated 27.11.2008, article 23; Added by the law no. 36/2017)
- Article 293/c Interference in computer systems (Added by Law no. 10023, dated 27.11.2008, article 23; Added by the law no. 36/2017)
- Article 293/ç Misuse of equipment (Added by Law no. 10023, dated 27.11.2008, article 23)

The procedures for investigation and seizing electronic evidence are covered in the Criminal Procedure Code in following Articles:

- Article 299/a of the Criminal Procedure Code (CPC) - expedited preservation and maintenance of computer data (Added by law no. 10054 of 29.12.2008, article 4)
- Article 101 of the Law no. 9918 from 19.05.2008 “On electronic communication” - preservation and administration of data for the purpose of criminal prosecution
- Article 299/b of CPC - expedited preservation and partial disclosure of computer data (Added by law no. 10054 of 29.12.2008, article 4)
- Article 191/a of CPC - obligation to produce computer data (Added by Law No. 10054 of 29.12.2008, article 2)
- Article 208/a of the CPC - Sequestration of computer data (Added by Law No. 10054 of 29.12.2008, article 3; Amended by Law No. 35/2017 of 30.03.2017, article 112)
- Articles 221-223 of the CPC - interception of communications (including provisions on the limits, authorisation and procedure) (Amended by Law No. 9187 of 12.02.2004, article 2, article 3, article 4 and article 5; Amended by Law No. 35/2017 of 30.03.2017, article 117, article 118, article 119, article 120)
- Article 15 (1) of the Law no. 9918 from 19.05.2008 “On electronic communication” states that in the general authorisation the Authority of Electronic and Postal Communications (AKEP) may include conditions related to: “f) permission for interception by competent authorities defined in the legislation in force on interception of telecommunications and implementation of other liabilities arising out of this legislation”.

The legislation in Albania recognize the following safeguards

The Constitution of Albania proclaims that fundamental human rights and freedoms are indivisible, inalienable, and inviolable and stand at the base of the entire juridical order. It also requires that the organs of public power, in fulfilment of their duties, shall respect the fundamental rights and freedoms, as well as contribute to their realization. In addition, Article 17 of the Constitution specifies that any limitation to the rights and freedoms must be established by law, in the public interest or for the protection of the rights of others and should be proportionate. Limitations should not infringe the essence of the rights and freedoms and may not exceed the limitations provided for in the European Convention on Human Rights.

The Constitution guarantees among others:

Article 22 – Freedom of expression

Article 23 - Right to information

Article 36 - Freedom and secrecy of correspondence or any other means of communication

Article 37 - Inviolability of the residence

Additional safeguards are provided by the CPC, Law on Data Protection, Law on Protection of Children Rights. The Code of conduct for safe use and responsive networks and electronic communications services in Albania was signed between Albanian Operators on 07.02.2013 (https://cesk.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/Dokumenti%20i%20Politikave%20per%20Sigurine%20Kibernetike%202015-2017.pdf.)

As a rule, national legislation provides for the requirement of judicial oversight, namely requiring judge's authorization for certain procedural measures if fundamental rights are in danger (for example in cases of interception of communications or for obtaining traffic data).

In addition to Computer Crime Offences, Electronic /Digital devices can also be used in the commission of many other crimes, and in both cases it is important to attribute the device to the suspect and the criminal action.

This document is to inform and facing this type of digital investigation with an introduction to theory and guidelines in relevant areas to include:

- Device identifiers
- Servers

- IP Addresses
- Emails
- Internet
- World Wide Web (www.)
- Data Preservation and Acquisition
- Partnerships
- Open Source Intelligence (OSINT)
- Cybersecurity
- Child Exploitation Online

Each of these subject areas will have a footnote that is intended to provide some keywords that link to the specific section.

SOURCES OF ELECTRONIC EVIDENCE

The use of electronic evidence has increased in the past few years as courts have had to admit and consider electronic evidence in the form of e-mails, digital photographs, ATM transaction logs, word processing documents, instant messages, spreadsheets, Internet browser histories, databases, the contents of computer memory, computer backups, computer printouts and digital video and audio files – all of which constitute digital data.

A digital device involved in crime should be secured just as you would with other forms of physical evidence found at a crime scene, because all such devices remain physical evidence. As with fingerprint and DNA evidence, digital evidence is fragile and easily lost or altered if appropriate precautions are not followed.

It is important to record where the digital device was found and seized, because it can reveal a great deal about the intent of the suspected offender. It is good practice to record the search and seizure by video. This will show the position of digital devices, so that there is no longer an argument, for instance, as to whether the wireless device was found hidden in the loft rather than in an open access area in the sitting room.

Usually the electronic evidence are found in the computer systems. Computer systems can come in many different forms including desktops, laptops, tower computers, rack-mounted systems, minicomputers, and mainframe computers. Other devices commonly connect to these systems including printers, scanners, routers, external hard drives and other storage devices as well have electronic evidence.

The electronic evidence sources that we should consider for searching electronic evidence are:

- ① Storage devices comes in many shapes and sizes and vary in the manner in which they store and keep data. They could be:
 - Hard disk drives and solid state disks
 - Removable media
 - Memory cards
 - USB data storage devices
 - Data storage tape disks
 - Peripheral devices

- ② Tablet devices
- ③ Mobile telephones
- ④ Photo and video recording
- ⑤ Electronic Evidence held by National and Multinational internet service providers

Types of Electronic evidence from computers and Storage device (Digital forensics)

Categories of digital traces: Just as a criminal leaves physical traces behind at a crime scene, the criminal that commits a crime by computer will leave traces at a “digital crime scene”. To get a better idea of the kinds of digital traces that an examiner might discover during forensic analysis, it makes sense to distinguish between two types of digital traces:

Avoidable traces: These are traces that are stored by the operation system and applications by default, but which a system can be configured not to store. Take a web browser as an example. This software will store a suspect’s browsing history as well as details of his or her downloads, form inputs, cookies, etc., but it can either be disabled or deleted by the suspect.

Unavoidable traces: By contrast, unavoidable traces are, of course, those that cannot be disabled or those that require considerable effort to stop temporarily. The probability of finding such traces is correspondingly high even if a suspect has tried to cover his or her tracks.

Every case typically involves some particularly relevant traces. In a fraud case for example documents, spreadsheets and e-mails are typically more relevant while in child-abuse cases pictures, videos and communication traces are more relevant. But even within those categories of cases not every case is the same. That is why the following subchapters included information on procedures based on the type of trace that is relevant rather than the type of case.

E-Mails: To analyse e-mail communication it is not only important to analyse mail clients like Outlook, Thunderbird or Mail but also webmail accounts. In order to analyse an e-mail client it is important to know which artefact that e-mail client produces. Outlook for example stores evidential data in personal folder files such as PST, OST and PAB files while Thunderbird stores messages in mbox files. The forensic software suites can usually parse those files. However, they do not

necessarily extract all messages. Some forensic tools, for example, have problems extracting deleted messages from personal folder files.

Office documents: In cases in which office documents are of importance the digital forensics analyst should conduct a signature analysis and then afterwards filter for the files of interest (e.g. files with a docx signature). When the forensic analyst has found those files it is good practice depending on the policies of the office to extract all of those files and hand it over to the case investigator for a content analysis. When the case officer has identified the relevant documents the forensic analyst can search for further evidence of when those documents have been produced, by which user they have been produced and whether they have been sent or received by other persons.

Pictures/videos: Most forensics software solutions offer support for analysing masses of pictures and videos. After an initial file signature analysis and setting a filter for pictures and video files, the forensics analyst can use a gallery view to inspect the thumbnails of all pictures for case relevant evidence. For a faster analysis of video files certain software offers the feature of extracting still pictures from the videos (e.g. every X seconds/minutes depending on the settings). These extracted images can then be viewed in a gallery view as well.

Internet browser: Internet browsers are of evidential value for a lot of cases. They typically contain the following artefacts which need to be analysed: Website visit history, Local cache / temporary internet files, Bookmarks / favorites, Sessions information, Cookies, Saved usernames and passwords, Entries from form fields, Internet searches Analysing browser artefacts can be important for suggesting purpose or intent (e.g. keywords used in search engines could prove intent). That is why those artefacts should be analysed in most cases.

Software artefacts: Whenever certain software can add evidential value to the case, the artefacts of those programs need to be analysed. Examples of such software include communication software (e.g. Software artefacts Whenever certain software can add evidential value to the case, the artefacts of those programs need to be analysed. Examples of such software include communication software (e.g. Viber, WhatsApp...), file sharing software (e.g. uTorrent), crypto currency software (e.g. Bitcoin wallet), etc).

User activity: The operating system of a computer tracks user activity at many different places. Examples for that include: power on and shutdown times, software settings, most recently used files lists, device usage, user logins, Wi-Fi connections, preferred programs, setup of user environment, and many more. Analysing this user activity helps getting a better understand of the user behavior and can even prove evidential activities. Depending on the operating system that

has been used on the computer those artefacts are stored in various locations. In Microsoft Windows the Registry, Event Logs and several other files need to be analysed by the examiner. On OS X systems the analyst will find most of the evidence in the Library and log folders while on Linux systems most of the data will either be stored in the user home folder, the “/etc” and the “/var” directories.

Log files: Analysing log files is essential particularly in cases of attacks against systems. Digital forensics analyst should extract not only allocated log files but also traces of deleted/unallocated log files. Specialised software is available for log file analysis. The basis of such an analysis is to either search for particular keywords, to search for abnormal pattern or to search the logs that fall within a set time frame.

Unallocated areas: Unallocated areas can contain artefacts of all of the types of evidence mentioned above. Searching and extracting of certain file types in unallocated areas can be automated by carving software. Digital forensics analysts should precisely specify what kind of files they are searching for because data carving is a very time consuming task. Data carving does not work well on fragmented files. Most of the times data found in unallocated areas cannot be associated with a certain user or even a location within a folder structure.

Cloud/remote storage: In situations where the forensic analysts finds traces of cloud services being used on a computer system this might mean that evidential data might not only be stored on that machine but also on a remote storage. In fact the data that is remotely stored might not just be stored on a single physical computer, but on multiple servers in the cloud. Most of the time, even the provider of a cloud service cannot tell on which particular server, in which data-centre, and which country certain parts of the data are stored.

Computer Memory (RAM): When computer memory has been acquired while the seized computer was still running the memory dump can be analysed in the forensics laboratory. Understanding memory structures of different operating systems in order to analyse RAM is a highly technical task. That is why it should only be done by examiners who are qualified for this work. Specialised software is required to analyse RAM dumps. Typical artefacts that can be extracted from RAM dumps include: Running processes including their memory, Process information (e.g. handles), Encryption keys, Opened files, Usernames, passwords, Unsaved documents.

Types of electronic evidence from Mobile telephones (Digital forensics)

Mobile devices contain records and logs of communications, along with times and dates of said communications. In addition to this, mobile devices will also contain media files and location data that can be utilised in an investigation.

Contacts: Contact lists make up the backbone of mobile phone usage. Care should be taken to crossreference other artifacts of data back to contact lists to help identify subjects for investigation. Contacts can include other communication channels, identity information as well as pictures to assist in the identification of individuals. Contacts can also help to identify association between subjects and potentially identify how long such an association has been in place from the created dates of contacts.

Call logs: Call records often carry date/time stamps generated from the handsets internal clock. This can make recovered time/date stamps for call records unreliable. It is often best practice to obtain billing information from a mobile service provider to confirm time and date information for call records. This time stamp is obtained from the mobile service provider's servers and so can be considered accurate (or rather it is more likely to be accurate).

Application artifacts: Due to the amount of different applications and the multitude of application versions that are available, it is often necessary to analyse different artifacts unique to different applications. Many of these applications will, for example, store settings in database files. It may be the case that deleted database files are recovered and these can be used to ascertain the settings of an application at a given point in the past. Due to the closed nature of many applications and the lack of available information, it may often be necessary to obtain a test device and conduct some live research in order to identify the properties of some application artifacts.

E-mail messages: As with computer examinations, e-mail communications on mobile devices can be used within default Mail applications and through web mail accessed through the internet browser. On some devices, such as newer Apple iPhones, the extraction of email messages from the default Mail application is not supported. In these cases the examiner will have to manually record the data or attempt to gather this data from other sources.

Web history: Internet browsers on mobile devices typically store the following information that potentially has evidential value: Web history entries, Web page visit counts, Bookmarks / favorites, Cookies.

Electronic evidence hold by Multinational internet service providers (Request for data Preservation, Request for Disclosure of data, MLA)

Subscriber data:

The term “subscriber information”, stands for any information that can potentially lead to identifying several categories of information related to the subscriber (i.e. user) of the electronic communications. Such categories may include the type and technical data of communication service used (including time), the subscriber’s identity, address and contact data, and any other information on the site of the installation of communication equipment. Those Information are in form of computer data/any other form held by a service provider relating to subscribers of its services (other than content data and traffic data). Those data are:

- Most often sought information in criminal investigations
- Less privacy sensitive than traffic data and content data
- Usually held by private sector service providers, obtained through production orders

Traffic data:

The term “traffic data” stands for any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

Content data:

“Content data refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data). Those data are:

- Content of the communication, i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)
- Includes stored content and future content
- E.g. emails, images, movies, music and other files

Type of Data hold by Multinational ISP:

- Basic subscriber information (name, physical address, email address and telephone number) related to an account, as well as connection logs which are retained up to 30 days
- Basic registration or customer information (name, address, email address and telephone number) related to the registration.
- Subscriber information and connection logs with IP addresses
- Subscriber information (including payment card details) for transactions in Service provider retail stores or online purchases
- Connection logs
- Media Access Control (MAC) addresses of devices
- IP addresses and other device identifiers related to operative system device activation
- Subscriber registration information and Sign-in IP addresses and associated time stamps for accounts;
- Subscriber registration information, Sign-in IP addresses and associated time stamps, telephone connection records and billing information for accounts;
- Blog registration page and blog owner subscriber information for Blogger
- Certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber record
- Stored contents of any account, which may include messages, photos, videos, wall posts, and location information.
- Other data (depends of the Internet Service provider)

**More information could be found on Internet service provider page with information about cooperation with Law enforcement agencies*

Data retention/data preservation

Data retention: A general requirement to retain specific types of communications data for a given period of time (usually no more than 12 months)

Data preservation: Data preservation is a measure which allows the preservation of content and other traffic data which is not preserved through data retention.

Digital forensics

Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analysing, and reporting on data stored electronically. Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations.

The main goal of digital forensics is to extract data from the electronic evidence, process it into actionable intelligence and present the findings for prosecution. All processes utilize sound forensic techniques to ensure the findings are admissible in court.

Live Data Forensics deals with situations where it is necessary to capture data from devices before they are turned off or disconnected from networks or power supplies. It requires a higher level of specialism than the procedure in the search and seizure of dead boxes.

In early years of digital forensics there was rule of “pull the plug” whenever an investigator found a running system during a search and seizure process. In times where the amount of volatile data in memory, remote connections and the usage of encryption, this old rule became outdated. The acquisition and analysis of volatile data is of high importance as it might be of high evidential value. That is one of the reason why Live Data Forensics plays an important part in search and seizure situations nowadays.

The forensic examination of a live system requires specific training, hands-on practical experience, and a set of validated forensic tools. If an examiner with this skillset is not present at the scene, the specialist unit should be asked for support immediately. If nobody can be reached, pulling the plug can make more sense than tampering with the evidence resulting in a possible contamination of the evidence and making it unfeasible for use in court.

Live Data Forensics deals with situations where it is necessary to capture volatile data from devices before they are turned off or disconnected from networks or power supplies.

Volatile Data are data that are digitally stored in a way that the probability is very high for their contents to get deleted, overwritten or altered in a short amount of time by human or automated interaction. (Caches, Unsaved documents, running processes, Passwords and encryption keys, Open network connections, System information, Logged in users, temporarily connected remote storage, Malware binaries only stored in RAM).

Principles of Electronic evidence

The following principles should be considered when we are identifying and collection of electronic evidence. Not all data in electronically form could admissible as an electronic evidence.

Data Integrity: No action taken should materially change any data, electronic device or media which may subsequently be used as evidence in court.

Electronic devices and data must not be changed, either in relation to hardware or software. The person in charge of a crime scene or for collecting the evidence is responsible for maintaining the integrity of the material recovered and for ensuring the forensic chain of custody. Subsequent custodians of the devices and/or data must assume that responsibility. When data is accessed on a running device, this must be done in the manner that causes the least impact on the data and by a person qualified to do so.

Audit Trail, record of all actions taken when handling electronic evidence should be created and preserved so that they can be subsequently audited. An independent third party should not only be able to repeat those actions, but also to achieve the same result.

It is imperative to record accurately all activity at the scene to enable a third party to reconstruct the actions if necessary. All activity relating to the search, seizure, access, storage or transfer of electronic evidence must be fully documented, preserved and available for review.

Any subsequent action related to the processing and examination of electronic evidence should also be amenable to audit in the same way.

Specialist Support: If it is expected that electronic evidence may be found in the course of a planned operation, the person in charge of the operation should notify specialists/external advisers in time and to arrange their presence if possible.

For investigations involving search and seizure of electronic evidence it is always desirable to involve electronic evidence specialists wherever possible. All such specialists, either from within the organisation or as external contractors, should have the appropriate and objectively verifiable knowledge to deal with electronic evidence properly.

Appropriate Training and certification: Any person handling electronic evidence must have the necessary and appropriate training.

In circumstances where no specialist is available, the first responder searching, seizing and/or accessing original data held on an electronic device or digital storage media must be trained to do so according to legally sanctioned procedures and must be able to explain and justify the relevance and implications of his/her actions.

Legality: The person and agency in charge of the case are responsible for ensuring that the law, the evidential safeguards and the general forensic and procedural principles are followed to the letter.

Admissibility and presenting an electronic evidence

Computer Evidence is admissible if it conforms to a series of laws and rules that ensure it is acceptable to the court. The proper procedures must be followed when obtaining evidence. These are articulated in the preceding chapters.

Electronic evidence will be admissible (may differ from jurisdiction to jurisdiction) if during the search and seizing follows the minimum criteria:

- The evidence must establish facts in a way that cannot be disputed and is representative of its original state.
- The analysis of or any opinion based on the evidence must tell the whole story and not be tailored to match a more favorable or desired perspective.
- There must be nothing about the way in which the evidence was collected and subsequently handled that may cast doubt on its authenticity or veracity.
- The evidence must be persuasive as to the facts it represents and the finders of fact in the court process must be able to rely on it as the truth.
- The methods used to gather the evidence must be fair and proportionate to the interests of justice

Electronic evidence is no different to physical evidence, such as a document recorded on a piece of paper. It is necessary to ensure that the evidence is authentic. The difference between electronic evidence and physical evidence is usually the ease with which electronic evidence can be changed and altered, either deliberately or inadvertently.

In the event that there is a doubt about electronic data adduced in evidence, it is for the defence to raise a challenge to its admissibility. Once the issue is raised, the prosecution has to deal with it.

Another important aspect of evidence is how it was obtained and whether the methodology by which that evidence was established is amenable to objective, scientific validation and review. For instance, if the prosecution can produce a telephone bill showing that the defendant connected to his ISP at a certain time of day, then this will be usually accepted. By contrast, if the prosecution claim that 'The defendant deleted all the files on his hard drive, reformatted it, then threw it out of a 10-storey window, but we've been able to reconstruct the files by going to a data recovery firm', then the defence may question the validity of this method of recovering the evidence. It is for the prosecution to demonstrate that the methods used to recover the evidence were valid and convince the court that the evidence should be admitted.

Electronic evidence is dealt with in court in the same way as any other form of evidence. The prosecution will have to prove that the document is authentic, and its contents are admissible. All dealings with electronic evidence must conform to the principles of electronic evidence.

Presentation of electronic evidence to the court is more effective if it is visual, using computer demonstrations, video demonstration, computer graphics, schedules and charts. However, prosecutors should be aware of the bias that using such technology can cause and be prepared to discuss these issues with authority if the defence challenges the use of such technology.

ELECTRONIC/DIGITAL DEVICES: HOW DO THEY RELATE TO CRIMINAL INVESTIGATIONS?

Whether you work in a wired network office or a wireless one, one thing is common for both environments; It takes both network software and hardware (cables, routers, etc.) to transfer data from your electronic digital device (e.g.: computer/ phone) to another device within your home this is done on a private network.

If you want to communicate to the outside world to a device thousands of miles away to yours a similar process takes place but involves routing into a unique public network addressing system to communicate with the specific device.

This can be likened to an office or hotel telephone system where you can dial internal numbers to communicate (private network), but you can also connect to external numbers outside of the confines of the internal network by dialling a specific set of numbers and connecting through the telephone service provider's networks (public network).

With a digital device it has three digital identifiers that act similar to a postal address, to ensure that it is known who it is from and who to reply to:

- The user who made the request (Username/Hostname),
- The device that made the request (MAC Addresses),
- What network the device is located on (IP Address of Local Area Network – LAN), and
- If being sent outside the network will convert to (IP Address of Wider Area network –WAN/Internet).

Username: Some electronic digital devices allow more than one person to use the device (e.g. laptops/desktops). In order to keep each user's details and documents private, each user has an account with a username and often a password, which provides areas for storage of documents relating to that person and enables that person to access the network and/or internet through the electronic/digital device.

Relevancy: Digital investigations regarding attribution.

Host name: This is a name given to the device it is one of the first screens you see when setting up a device up from new.

- In general if it is a personal device, people will give it a name personal to them (e.g.: Kastriot iPhone or Anna's laptop), or;
- In the case of a company it may start with the company named (e.g.: Halkbank-A345) or;

- If the device is on a larger company network, it may have a unique reference in a pre-set format (e.g.: WIN-ABC-123).

Relevancy: Digital investigations regarding attribution.

MAC Address: In order to connect to a network or the Internet the device needs a Network Interface Card (NIC). Every NIC has a unique hardware address that's known as Media Access Control (MAC).

MAC addresses are linked to the hardware of network adapters and are often referred to as a networking hardware address, or the burned-in address (BIA), or the physical address.

Here's an example of a MAC address for an NIC: D0:BF:9C:9B:50:79. The MAC address is a string of usually six sets of two-digits or characters, separated by colons. The MAC address could be found by starting command "getmac" in command prompt.

```
cmd Command Prompt
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Users\marja>getmac

Physical Address      Transport Name
----- = -----
E4-B9-7A-5E-0A-95    Media disconnected
80-2B-F9-81-33-6F    \Device\Tcpip_{62B72B44-A133-490F-94D8-8D3C6C19818D}
80-2B-F9-81-33-70    Media disconnected
```

A MAC address is given to a network adapter when it is manufactured. It is hardwired or hard-coded onto your computer's network interface card (NIC) and is a unique number. For investigations, the MAC address is important to identify the specific device. Additionally the first 6 characters identify who the manufacturer of the device is. This data can be accessed free on the internet www.macvendors.com. By conducting this search I now know that D0:BF:9C:9B:50:79 relates to a Hewlett Packard Device (HP), which can be helpful when conducting searches.

The screenshot shows a web browser window with the URL <https://macvendors.com> in the address bar. The page header includes the logo 'MA:CV:en:ders', navigation links for Home, API, Plans, About, Register, and Login, and a user icon. The main content area features a dark green background with a geometric pattern. At the top, it says 'Find MAC Address Vendors. Now.' Below that is a search input field with the placeholder 'Enter a MAC Address' and the value 'D0:BF:9C:9B:50:79'. Underneath the input field, the text 'Hewlett Packard' is displayed.

A device may have more than one NIC Adapter and therefore more than one MAC address; the following are what you may expect to see:

- NIC Ethernet (is the socket with the Grey or Yellow Cat5 cable connection that will connect from the device to a telephone type socket – internal network);
- NIC Wireless LAN – (this is the Wi-Fi connection - 802.11 bgn Wi-Fi Adapter);
- NIC Ethernet Bluetooth Network Connection – (this enables Bluetooth Device in a Personal Area Network);
- NIC Wireless LAN adapter Local Area Connection – (Wi-Fi Direct Virtual Adapter) this enables the device to become a Wi-Fi hotspot or can be used for virtualisation. Consider seeking advice from Cybercrime Investigation Unit if this is activated.

IP Addresses can be manipulated and falsified for criminal purposes or to hide identities, this is known as MAC spoofing. Considering this issue, not always we could rely on the relevancy of this information.

Relevancy: Digital investigations regarding attribution, communication and networking.

Networks

A computer network is a set of computers connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server.

NODE is a connection point that can receive, create, store or send data along distributed network routes. A networked computer device is also known as a NODE. A server is a computer that we relate to networks and is a NODE.

LAN is Local Area Network; this is the area before the internet router so would include the internal network such as a home, business, school etc.

WLAN is the same as LAN but with Wireless Connectivity.

WAN is a Wider Area Network, these can include large cities, towns but more commonly today will be the Internet Network.

Internet is a massive network of networks, a networking infrastructure. It connects millions of computers (NODES) together globally, forming a network in which any computer can communicate with any other computer (NODE) as long as they are both connected to the Internet.

Peer-to-Peer networks allow users connected to the Internet to link their computers with other computers around the world. These networks are established for the purpose of sharing files.

Relevancy: Digital investigations regarding communication and networking.

Servers a server is a computer program that provides services to other computer programs (and their users) in the same computer or other computers. The computer that a server program runs in is also frequently referred to as a server. That machine may be a dedicated server or used for other purposes as well. Commonly recognised server names that may encountered are:

A file server is a computer responsible for the central storage and management of data files so that other computers on the same network can access them.

A proxy server is software that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service.

A mail server (MX) is an application that receives incoming e-mail from local users (people within the same domain), remote senders and forwards outgoing e-mail for delivery.

A Domain Name Servers (DNS) is the Internet's equivalent of a phone book. They maintain a directory of domain names (www.asp.gov.al) and translate them to Internet Protocol (IP) addresses (185.71.180.3) and devices that connect to the internet or, other private networks rely on the DNS for resolving URLs, email addresses and other human-readable domain names into their corresponding IP addresses.



When we search domain name, the computer is searching the IP address that is related with searched domain name and establish communication with the IP address. DNS has the information what IP is corresponds with which domain name.

A Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users in response to their requests, which are forwarded by their computers' HTTP clients. Dedicated computers and appliances may be referred to as Web servers as well.

Relevancy: Digital investigations regarding attribution, communication and networking, email investigation, website investigations, child exploitation investigations.

IP Address Internet Protocol Address (IP) is a numerical label assigned to each device (e.g., computer, tablet, printer) participating in a computer network that uses the Internet Protocol for communication. There are IP addresses allocated to and used only for a private LAN (connecting your devices in the home or office) and there are public IP addresses for connectivity over the external WAN/Internet network. The IP addresses can be either static or dynamic. There are 2 versions of the IP address IPv4 and IPv6.

Who coordinates the IP Addresses and where does the data come from?

Internet Assigned Numbers Authority (IANA) allocates and maintains unique codes and numbering systems that are used in the technical standards (“protocols”) that drive the Internet; these can be broadly grouped in to three categories:

- Number Resources - Co-ordination of the global pool of IP and autonomous system (AS) numbers, primarily providing them to Regional Internet Registries.
- Domain Names - Management of the DNS Root, the .int and .arpa domains, and an IDN (International domain name) practices resource (technical solution to translate names written in language-native scripts i.e.: Cyrillic, Chinese etc.).
- Protocol Assignments - Internet protocols’ numbering systems are managed in conjunction with standards bodies.

A Regional Internet Registry (RIR) is an organization that manages the allocation and registration of Internet number resources including IP addresses and AS numbers within a particular region of the world, to Internet service providers and end-user organizations.

There are five RIRs:

- African Network Information Centre (AfriNIC) for Africa

- American Registry for Internet Numbers (ARIN) for the United States, Canada, and several parts of the Caribbean region
- Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, and neighbouring countries
- Latin America and Caribbean Network Information Centre (LACNIC) for Latin America and parts of the Caribbean region
- RIPE NCC for Europe, the Middle East, and Central Asia

The RIR allocate blocks of IP addresses to Internet Service Providers (ISP) who in turn allocate them to clients, either on the basis of a static IP address or a Dynamic IP Address. There is a requirement for a register of these allocated IP addresses to be maintained at the RIR.

Appendix B is an example of what information will be provided by the ISP and held by the RIR.

What we need to know about IP addresses?

Static IP addresses never change. They serve as a permanent Internet address and provide a simple and reliable way for remote computers to contact you. Static IP addresses reveal such information as the continent, country, region, and city in which a computer is located; the ISP (Internet Service Provider) that services that particular computer; and such technical information as the precise latitude and longitude of the country, as well as the locale, of the computer.

Dynamic IP addresses are temporary and are assigned each time a computer accesses the Internet. They are, in effect, borrowed from a pool of IP addresses that are shared among various computers. Since a limited number of static IP addresses are available, many ISPs reserve a portion of their assigned addresses for sharing among their subscribers in this way, and will allocate a limited time for the IP connection. This lowers costs and allows them to service far more subscribers than they otherwise could.

IPv4 – Internet Protocol Version 4 is the most commonly recognised IP address and consists of 4 blocks of digits (each block is known as an Octet) ranging from 0-255, an example is 192.168.1.3 or 77.28.81.50. As with telephone numbers, ranges of numbers have been allocated to be used by service providers, others have been retained for other reasons such as research and development. The same relates to IP addresses.

On a Local Area Network (LAN) which is a private network the following IP address ranges have been allocated for use in configuring internal networks:

- Class A: 10.0.0.0 – 10.255.255.255

- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0 – 192.168.255.255

These ranges of numbers do not function on external networks, they only operate within internal networks such LAN and WLAN as a home network where your router will automatically allocate the private IP addresses, or in a larger network this process will be configured by the network administrator.

Each device connected to the network needs its own address, so in the example IP address above 192.168.1.3 can be identified as a private address and in simple terms is likely to be allocated on a network which ranges from 192.168.1.0 - 192.168.1.255.

There are a few exceptions to this and two examples would be:

- Where a home router only allows 10 devices to be connected then the IP addresses are likely to be within a range of 192.168.1.0 - 192.168.1.12.
- In large networks the system administrators will make the most use of a limited number of IP addresses use a method called sub netting, which will often mean an IP address will look like this 192.168.1.0/24, while this looks complex it is only enabling the network to create smaller networks and increase the number of IP addresses, (it is a variation of a telephone switchboard number having a series extension numbers within a department) - if you encounter sub netting consider contacting the cybercrime unit for further assistance.

IPv4 Public IP addresses are globally routable unicast IP addresses used on a (WAN) and the Internet. Public IP addresses will be issued by an Internet Service Provider and will have number ranges from 1.0.0.0 to 191.255.255.255, with the exception of the private address classes A and B:

(Class A 10.0.0.0 – 10.255.255.255 / Class B 172.16.0.0 – 172.31.255.255)

IPv6 Internet Protocol Version 6 was introduced as it was envisaged with the increase in devices needing to connect with the WAN and Internet that the numbers of IPv4 addresses would run out and IPv6 was developed to prevent this happening.

The primary difference between IPv4 and IPv6 addresses is length. IPv4 addresses are 32 bits long and IPv6 addresses are 128 bits long. This massive length forces IPv6 addresses to be written using a different notation than IPv4 addresses and makes them very easy to distinguish from IPv4 addresses.

IPv6 Notation requires 16 characters and uses for these digits 0-9 and lower case letters a-f referred to as hexadecimal. IPv6 is made up of 16 Octets, visually shown

as 8 segments. Due to the massive length of numbers IPv6 uses zero suppression and zero compression to simplify the appearance.

This may sound complex but it simply means IPv6 will look different and can be displayed in any of the following ways:

- 2001:0db8:0000:0000:0000:0000:0001 (with 8 segment/16 Octets as it would fully appear);
- 2001:db8:0:0:0:0:1 (zero suppression allows the lead 0's to not appear);
- 2001:db8::1 (zero compression is where segments containing consecutive 0's can be removed);
- /64 notation at the end of any of the above examples simply signifies subnetting.

In almost every case you investigate IPv4 will appear and be the main focus of your investigation, but more devices and network servers are including IPv6 in their configuration.

IP Addresses can be manipulated and falsified for criminal purposes or to hide identities, this is known as spoofing. Usually the IP address that is spoofed looks as private IP addresses, but appears that the request is coming from Internet.

Relevancy: All digital investigations regarding attribution, communication, networking and communication data requests.

Protocols

TCP/IP is the protocol on which the Internet is built; it is not a single protocol but rather an entire suite of related protocols.

TCP, which stands for Transmission Control Protocol, is a connection-oriented protocol. TCP allows one-to-one communications enabling a single network device to exchange data with another single network device or on a different network. TCP ensures that each packet is delivered if at all possible. It does this by establishing a connection with the receiving device and then sending the packets. If a packet doesn't arrive, TCP resends the packet. The connection is closed only after the packet has been successfully delivered or an unrecoverable error condition has occurred.

Many well-known Application protocols rely on TCP. For example, when a user running a Web browser requests a page, the browser uses HTTP to send a request via TCP to the Web server. When the Web server receives the request, it uses HTTP to send the requested Web page back to the browser, again via TCP. Other

Application layer protocols that use TCP include Telnet (for terminal emulation), FTP (for file exchange), and SMTP (for e-mail).

Relevancy: All digital investigations regarding communication protocol, networking and can be manipulated for cyber security attacks.

ARP is an Address Resolution Protocol device network systems which is generally the router which maintains an ARP look-up table where information is stored about what IP addresses are associated with what MAC addresses. This enables data to be linked to the correct sender and recipient. The tables are a type of smart logic in that each time it receives a request it will look in its own table to see if the route is known, if not it will make a request across the network and when identified will add the MAC and IP address to the table for future reference. ARP tables can be manipulated for criminal and malicious purposes.

Relevancy: All digital investigations regarding communication protocol, networking and can be manipulated for cyber security attacks.

World Wide Web (www.) is all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP). The hypertext protocol will generally initially appear in the browser as <http://www>. followed by the domain name.

Hypertext Transfer Protocol (HTTP) is a protocol which is standard for websites.

Hypertext is text which contains “links” to other texts, we commonly refer to these as ‘hyperlinks’ and are often denoted in documents by blue underlined text and when clicked on link to another document or website, (i.e.: **Albanian Police** if clicked will hyperlink to <http://www.asp.gov.al> which is also known as a web address.

Domain is a group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the Internet, domains are defined by the IP address. All devices sharing a common part of the IP address are said to be in the same domain.

Domain names are used to identify one or more IP addresses. For example, the domain name microsoft.com represents about a dozen IP addresses. Domain names are used in URLs to identify particular Web pages.

Uniform Resource Locator (URL) and a Web address is the same thing in Internet terminology and is the full address of the website being accessed.

Uniform Resource Locator (URL) dhe një adresë në web është e njëjtë gjë në terminologjinë e Internetit dhe është adresa e plotë e faqes së internetit që po vizitojmë.

A URL consists of several parts: the protocol, the server name, top-level domain and the file path.

How does it function? - The protocol tells the browser how the data should be handled. The most common protocol is HTTP; another is File Transfer Protocol (FTP). The protocol of a URL is always followed by a colon and two forward slashes, e.g., "http://" or "mailto://".

After the protocol comes the server name, e.g. "google.com." This is the main Google homepage directory from which everything in the Google directory originates. The ".com" part is called a top-level domain, and is used for computers in the United States to indicate the type of entity that created the website.

A subdomain is a domain that is part of a larger domain, i.e.: ".gov.al".

The file path is the last part of the URL, this indicates the specific file on the server that should be accessed i.e.: <http://www.asp.gov.al/drejtori-i-pergjithshem-i-policise-se-shtetit/> would look for the profile page/ for the Director.

http://- internet protocol

www.asp.gov.al- domain name

Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network which is widely used on the Internet within a connection encrypted by Transport Layer Security. The main motivation for HTTPS is authentication of the visited website, secure payment sites and protection of the privacy and integrity of the exchanged data.

File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network (ftp:// something). FTP is built on client-server model architecture and uses separate control and data connections between the client and the server.

FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS), those are the secure and encrypted communications.

FTP and FTPS servers are often a feature in investigations into offences against Production and distribution of child pornography. Because those protocols are used by criminals to exchange materials.

Mailto is a Uniform Resource Identifier (URI) scheme for email addresses. It is used to produce hyperlinks on websites that allow users to send an email to a specific address without first having to copy it and enter it into an email client.

The following are examples of each of these six protocols:

Protocols	Domain	Sub-domain of TLD	Top level domain (TLD)	IP Address
http://	asp	.gov	.al	185.71.180.28
http://	google		.com	8.8.8.8
https://	paypal		.com	2.20.33.150
ftp:// & https://	192.168.1.1			192.168.1.1
mailto://	name@email		.com	

DOMAIN is owned by an entity and provided by a registrar

- WIKIPEDIA domain: wikipedia.org

SERVICE is provided by the entity within the domain

- Web site: www. wikipedia.org
- Mail service: smtp. wikipedia.org
- File transfer: ftp. wikipedia.org

Domain Registration

When you register a domain name, the Internet Corporation for Assigned Names and Numbers (ICANN) requires your domain name registrar to submit your personal contact information to the WHOIS database. Once your listing appears in this online domain WHOIS directory, it is publicly available to anyone who chooses to check domain names using the WHOIS search tool.

There are a few exceptions to this:

- Where third party agents (Privacy Companies) are used to register the domain and therefore the true domain owner details will not be present (in those cases we need to use mechanisms of International cooperation).
- Where false information is provided. (International cooperation, MLA request)

Research Tools - On-Line tools and databases for Analysing IP Addresses and Domains:

There are a number of free and paid online services for examining IP addresses with varying levels of accuracy. All will source their data from the RIR, but some do it as a single or periodic download and others link more frequently to the live RIR database. An indicator is the date the entry was last modified; it is worthwhile conducting your check on a second service to confirm you have the most recent information.

Free Services - Types of enquiry:

- Whois Lookup – IP and Domains
- IP Whois Lookup
- Domain Search
- Reverse Whois Lookup
- Reverse IP Lookup
- Reverse NS Lookup
- Reverse MX
- Reverse IP Whois

IP Address Tools for Investigation:

- www.iptracking.com
- www.centralops.net
- www.ipaddress.com
- Many others

See Appendix A - How to look up an IP address.

See Appendix B – Regional Internet Registry data records explained.

Relevancy: Digital investigation, Cyber security investigations, Website attribution, and acquiring telecommunications data.

Email

Email communication features in many criminal investigations not just cybercrime. Analysing email headers can identify senders of threatening, abusive emails, or to identify false email addresses in spam, phishing or fraudulent emails. Checking the email header and IP address against blacklists can often provide confirmation that the email is a part of a criminal act.

Email can be web based or client based and uses three types of Mail Protocol, these factors together with where the mail is stored may need to be considered in the course of an investigation.

Web based email – the email is composed and viewed on a website through an email client implemented as a web application running on a web server, e.g. Gmail, AOL, and Yahoo.

Application based email – is the viewing of email sent and received using an email program that is on your computer/device, (e.g. Microsoft Outlook, Mozilla Thunderbird and Mail for Apple Users).

The three Mail Protocols are:

- Simple Mail Transfer Protocol (SMTP) for sending email
- Post Office Protocol version 3 (POP3) for recovering email from a web server
- Internet Message Access Protocol (IMAP) for recovering email from a web server

Analysing full email headers often means reading the data from the bottom up to establish:

The first occurrences of:	Other Information that may assist with identifying the device used, include:
The sender information	Mail software description
X- originating IP with X- original arrival time	Software language
First received from with an external IP address for ISP	Local device information
First received from with an internal IP address	Local email information

Note: Recent Privacy Issues has led to some companies either removing this data from the email or encrypting the data, so it is not visible in the header.

On-Line tools for Analysing Email Headers:

The following are examples of free Internet tools available for analysing full email headers: include:

- www.iptrackeronline.com – IP Look Up, Email analyser which provides geo-location for Senders IP address, DNS Record Locator and other tools.
- www.mxtoolbox.com – Email analyser, Mail server look-up, Email blacklists for reducing spam, SMTP Diagnostics and other tools.

Appendix C - Investigating email provides additional of how email works, the network protocols for communicating, where data is stored, where to find email header data and what data contained in email headers can assist in criminal investigations.

Relevancy: Email investigation Digital investigation, Communication Data preservation and acquisition, Mutual Legal Assistance Treaty, International Police and Judicial Agencies, Access to International Intelligence databases.

Acquisition of Communications Data as Evidence

Communications data is the information about a communication. It includes the time and duration of a communication, the number or email address of the originator and recipient; it may provide the location of the device from which the communication was made.

Communications data does not include the content of any communication the text of an email or a conversation on a telephone. It is information about a communication, not the communication itself.

Communications data is used in the investigation of all types of crime, including computer crimes and terrorism. It enables to build a picture of the activities, contacts and whereabouts of a person who is under investigation. It can be used as evidence in court.

A Communication Service Providers (CSP) or Internet Service Provider (ISP) are required by law to store certain types of communications data, where they have business reasons to generate or process it. The Public Prosecutor (PP) can

apply to get access to communications data - according the Criminal Procedure Code (CPC) of the Republic of Albania, which sometimes is about special investigative measures. If they can demonstrate that their request is necessary and proportionate. Access is on a case by case basis and the police have no power to get access to communications data where it is not connected to a specific investigation or operation.

An EU Data Retention Directive recommends CSP's and ISP's retain telephony and some internet-related communications data, which is generated or processed in connection with their business, for between 6 and 24 months. The retention period in Republic of Albania is 12 months.

What different types of communications data are available?

There are three categories of data that is available, Subscriber information, Service user information and Traffic Data.

Subscriber Information - is information that private sector CSP's hold about people to whom they provide a service (e.g. names, addresses, telephone numbers, account holder name, payment methods, VAT numbers);

- ‘Subscriber checks’ (also known as ‘reverse look ups’) such as “who is the subscriber of phone number **00 355 69 1234567?**”, “who is the account holder of e-mail account example@example.al? ” or “who is entitled to post to web space www.example.al ? ”;
- information about the subscriber to a PO Box number or a Postage Paid Impression used on bulk mailings;
- information about the provision to a subscriber or account holder of forwarding/redirection services, including delivery and forwarding addresses;
- subscribers’ or account holders’ account information, including names and addresses for installation, and billing including payment method(s), details of payments, VAT numbers;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services, and potentially static IP addresses;

- information about apparatus used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and
- information provided by a subscriber or account holder to a CSP, such as demographic information or sign-up data (to the extent that information, such as a password, giving access to the content of any stored communications is not disclosed save where the requirement for such information is necessary in the interests of national security)

Service Use Information is information about the use a person makes of a service, examples include:

- itemised telephone call records (numbers called);
- itemised records of connections to internet services;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about the use of forwarding/redirection services;
- information about selection of preferential numbers or discount calls; and
- Records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

Traffic Data is information about a communication and the equipment used in transmitting it, including:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the ID number of sender or recipient (including

- copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
 - web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed;
 - anything, such as addresses or markings, written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission and which shows the item's postal routing;
 - records of correspondence checks comprising details of traffic data from postal items in transmission to a specific address; and
 - Online tracking of communications (including postal items and parcels).

When we can acquire Communications Data

- In the interests of national security;
- The Public Prosecutor can apply for an order from the Supreme Court.
- For the purpose of preventing or detecting crime or of preventing disorder;
- According to the CPC, special investigative measures.
- Evidence can be used only for the case that it was asked or ordered for.
- Communication Data can be obtained for some limited period.

Processes for Acquisition of Communications Data – National Communication Service Provider:

Police:

- ① Identify type of data required.
- ② Identify crime and judicial Article it relates to.
- ③ Consider purpose for data request – ‘is it necessary and proportionate’?

④

With IP data be aware of dynamic IP addresses:

- establish the date (if overseas provider name the month to avoid confusion as USA use mm/dd/yyyy and UK/Europe use dd/mm/yyyy),
- time (hh:mm:ss) of activity,
- consider time zone on timestamp (include these in any application together with explanation of calculations or conversion to UTC or PST).

⑤

Any submission must be made to the Public Prosecutor (PP).

Public Prosecutor:

Subscriber User information can be applied for and received through PP:

- ① PP send order to the service provider or obtain court order
- ② If PP finds the evidence is relevant and an acceptable standard.
- ③ PP obtains a court order.
- ④ PP sends a formal request to the Service Provider.
- ⑤ Service Provider sends back to PP.

Service User and Traffic Data information can be applied for and received through PP:

- ① Request/proposal made to PP from Investigator.
- ② If PP finds the evidence is relevant and an acceptable standard.
- ③ PP sends a formal request to the Service Provider.
- ④ Service Provider sends back to PP.
- ⑤ PP sends back to Investigator

Postal Mail Service:

①

Police inform PP,

- ② PP asks court order. The evidences must be real, not only a document about the evidence itself.
- ③ The court can invite a post office representative to the trial.
- ④ If sufficient evidence the Court will provide an order under CPC .

Process for Acquisition of Communications Data (Outside Albania)

International CSP/ISP's are not subject to the same regulations for the retention of communications data as in Albania or Europe, which means that communications data and evidence can be lost.

This coupled with the fact that International requests often need to be supported with a **Mutual Legal Assistance Treaty Request** (MLAT) or Commission Rogatories submitted through judicial and diplomatic channels, often means that the data and evidence can be lost.

To alleviate this problem, a request can be made Police to Police for a **Data Preservation Request**, which generally expires after 90 days whereupon a further 90 day request will need to be made if the data has not been acquired, allowing time to submit a MLAT request.

The preservation requests are generally directed via the International Police Cooperation Department (IPCD) who determines which International Partner is the most effective channel for the Data Preservation Request. This does not mean that the data will be disclosed to the police, this is the channel to facilitate the process of sending the MLA request.

Prosecutor:

Identify type of data required.

- ① Identify crime and judicial Article it relates to.
- ② Identify the name and contact information of the Internet service provider that hold the data
- ③ Identify the country under which jurisdiction is the Internet service provider
- ④ Consider purpose for data request – 'is it necessary and proportionate'?

- ⑤ Send the request for preservation of the data (Template for Data Preservation Request, Annex3)
- ⑥ With IP data be aware of dynamic IP addresses:
 - establish the date (if overseas provider name the month to avoid confusion as USA use mm/dd/yyyy and UK/Europe use dd/mm/yyyy),
 - time (hh:mm:ss) of activity,
 - consider time zone on timestamp (include these in any application together with explanation of calculations or conversion to UTC or PST).
- ⑦ Any submission must be made by the public prosecutor (PP), usually the request for data preservation is made to IPCD.
- ⑧ Send the MLA request (Template for Data Preservation Request, Annex2)
- ⑨ Most data preservation requests last 90 days, can be sent request for extension of the preservation period, before the 90 days expires to ensure the data is not lost, before it is officially acquired through an MLAT.

Relevancy: Email investigation Digital investigation, Communication Data preservation and acquisition, Mutual Legal Assistance Treaty, International Police and Judicial Agencies.

International and National Partners

International Police Cooperation Department (IPCD) JIT - Europol - Eurojust - Interpol - SELEC

The IPCD is based in Tirana and is responsible for the coordination of International Partnerships to tackle International Organised Crime. IPCD consists of:

- National Central Bureau Interpol Unit – NCB Tirana;
- Europol – including liaison with the public prosecutor’s office for operations with Eurojust;
- South East Law Enforcement Centre – SELEC Albania;

IPCD is coordinating with partners focusing on the following crime areas:

- Drug Trafficking;
- Public Safety and Terrorism;
- Trafficking in human beings;
- Illegal Immigration;
- Financial crime;
- Illegal money-laundering activities;
- smuggling and customs fraud;
- Firearms and weapons;
- Stolen motor vehicles;
- Container security;
- Counterfeiting of money and means of payment;
- Crime connected with nuclear and radioactive substances;
- Environmental and nature related crimes;
- Cybercrime.

IPCD is able to assist in Police-to-Police intelligence and information requests, but the information can only be used by Police. Prosecutor could use this instrument for international cooperation, but only the data received by MLA are admissible on court as an evidence.

For any form of evidence including; communication data (with or without a

preservation request), financial information or other private information a MLAT request will need to be made by the Public Prosecutor and submitted through Judicial channels to the Judicial area where the information is held. In cases of extreme urgency IPCD may be able to assist in fast tracking the request through its International partners.

The IPCD has a central point of contact, for coordinating requests for International assistance and identifying the most effective International Partner to assist with an investigation request.

The IPCD can be contacted 24/7.

Joint Investigation Team (JIT)

A **JIT** is an agreement to set up an investigation team for a fixed period and for a specific purpose. The aim of a JIT is to investigate specific cases and enables the fast time process of intelligence and evidence through police and judicial cooperation.

A JIT can be formed for an International investigation involving two or more countries and can include the agencies of Interpol, SELEC, Europol and Eurojust. For the Republic of Albania the Public Prosecutor is the head of the JIT.

Europol

Albania is an operational partner of Europol and has a Liaison Bureau in The Hague who can be contacted through IPCD to assist with operational and strategic co-operation involving Europol members and operational partners.

Eurojust

Eurojust has agreements with the Public Prosecutors Office of Albania and other EU bodies such as the European Judicial Network, Europol, and OLAF. Eurojust provides judicial co-operation in criminal matters to improve handling of serious cross-border and organised crime by stimulating investigative and prosecutorial co-ordination among agencies of the EU Member States and cooperation partners.

Interpol

Interpol (International Criminal Police Organisation) has 190 member countries. The National Central Bureau (NCB Tirana) for Albania has access to INTERPOL's range of criminal and intelligence databases.

SELEC – South East Law Enforcement Center

SELEC provides support for Member States to enhance coordination in preventing and combating crime, including serious and organized crime, where such crime involves or appears to involve an element of trans-border activity.

SELEC operational activities are conducted within the frames of eight Task Forces (TF) addressing issues of the 12 Member states of SELEC are; Republic of Albania, Bosnia and Herzegovina, Republic of Bulgaria, Republic of Croatia, Republic of North Macedonia, Republic of Greece, Hungary, Republic of Moldova, Montenegro, Romania, Republic of Serbia and Republic of Turkey.

Pursuits Unit – (Fugitives)

The Pursuits unit seeks to identify persons wanted at a National or International level. They also have the remit to seek fugitives sought in Target orientated operations.

Relevancy: Cyber investigations

National Partners

AKCESK/NAECCS Computer Incident Response Team

The National Centre for Computer Incident Response has been set up and it is the official national point of contact and coordination in dealing with security incidents on networks and information systems and will identify and respond to cyber security incidents and risks.

The National Centre for Computer Incident Response has the following mission:

-  a Coordinate and help/assist the authorities and public sector institutions in the implementation of proactive services for reducing the risk of computer security incidents, as well as in dealing with incidents when they occur,
-  b Conduct activities for educating and raising awareness among the citizens on the negative effects of cyber threats and cybercrime; and
-  c Providing support for all its constituents which includes the Ministry of Interior.

For further information see www.cesk.gov.al/

Financial Investigation Unit and Financial Intelligence Unit

The Financial Intelligence Unit is a body within the Ministry of Finance of the Republic of Albania, and with financial investigation Unit have specific authorisations pursuant to the Law on Criminal Procedure, these include:

-  Conducting preliminary investigations and evidence gathering into organised financial crime and follows the money trail of significant and

large-volume amounts; to find the perpetrator, to prevent the perpetrator or the accomplice from hiding or fleeing, as well as to gather all information that could be of use for the conducting of the criminal procedures;

- Conducts expert computer analysis of confiscated objects, computer information or data from other electronic and mechanical devices containing information, which can serve as evidence in the course of conducting preliminary investigative procedures;
- Supports other government bodies and institutions, preparing and providing expert findings and opinions within its competence;
- Cooperates with peer bodies from other countries in line with the bilateral agreements and ratified international agreements.

In relation to computer crime they can specifically assist in cyber investigations where an element is to 'follow the money' with online payment services such as PayPal and other complex fraud cases.

Requests for assistance should be directed through the PP.

OPEN SOURCE INTELLIGENCE (OSINT) - OVERVIEW

Hulumtimi dhe hetimi në internet është një mjet i fuqishëm kundër krimit. Ai,

Online research and investigation is a powerful tool against crime. It also presents new challenges to law enforcement as the use of such a tool can still interfere with a person's right to respect for their private and family life which is enshrined in Article 8 of the Human Right Act 1998 and ECHR.

Public authorities must ensure that any interference with this right is:

- necessary for a specific and legitimate objective – such as preventing or detecting crime;
- proportionate to the objective in question;
- in accordance with the law.

Whenever we are using the internet to gather intelligence or evidence we must consider whether we are likely to interfere with a person's right to respect for their private and family life and, if so, whether you should seek authority according to the CPC, where the PP should be informed. The principles in this guidance have been prepared to help you identify if such authorisation is appropriate.

It is also essential to consider the effect of any collateral intrusion on the private and family life of other people not directly connected with the subject of the research or investigation. Case by case judgement is vital when researching or investigating online.

Overview

- Online communication via the internet has, in recent years, become the preferred method of communication with other individuals, within social groups or with anyone in the world with internet access. Such communication may involve web sites, social networks, chat rooms, information networks (e.g. Facebook/Twitter) and/or web based electronic mail.
- Just because other people may also be able to see it, does not necessarily mean that a person has no expectation of privacy in relation to information posted on the internet.
- Using covert techniques to observe, monitor and obtain private information can amount to an interference with a person's right to respect for their private and family life, ensuring an investigator's action is lawful and authorised is essential.

Operational Risk Considerations

- Any online research and investigation leaves a trace or ‘footprint’. An operational decision will therefore need to be made as to whether you wish to ensure that your research is non-attributable i.e. cannot be traced back to law enforcement or to identifiable individuals, or whether you are happy for it to be attributable i.e. capable of being traced back to law enforcement.
- Non-attributable research and investigation must be carried out on equipment that cannot be attributed to law enforcement or identifiable individuals. Using attributable equipment runs the risk of compromising any operational activity which has been conducted on it.
- It is recommended that attributable research and investigation is restricted to publicly accessible search areas e.g. maps, street views, local authority sites, auction sites, etc. and websites which have no requirement to register details in order to gain access.
- It is acknowledged that many officers and staff will have considerable experience of using the internet for their own personal online research. However managers should ensure that staff carrying out online research and investigation for Albanian Police is both competent and appropriately trained.

Security

When undertaking online research and investigation, consideration should be given to:

- The appropriate sourcing of equipment procured for covert use.
- The separation of equipment used for covert and overt activity.
- Ensuring that equipment used for covert activity cannot be attributed to law enforcement.
- How and where to fully capture, record and retain information obtained online.
- How and where to record the actions of the person conducting the research or investigation so that it is subsequently auditable.
- The preferred methods of producing intelligence in an evidential format.

Use of a pseudonym

- The creation of a pseudonym for the purposes of criminal investigation must be authorised by the Public Prosecutor; According to the Special investigative measures in the CPC.
- It is recognised that there will, for covert online research and investigation, be a requirement to create and use a pseudonym account to gather information. The creation of a pseudonym for the purposes of online research may be undertaken but the information received cannot be used as evidence. It may, however, breach the terms and conditions of some sites, particularly social networks.
- Pseudonyms should only be used for covert research and investigations which must be undertaken using a non-attributable computer.
- The Police should maintain a register of all persona profiles created and used. This register should be maintained centrally and periodically reviewed taking into account the necessity and proportionality of maintaining and using each registered pseudonym.
- A log, recording the time, date, user and the policing purpose, should be maintained for each use of a pseudonym.

Open source

- Most of the information available on the internet is available to any person with internet access, either freely or for payment. Such information is widely known as open source information.
- Viewing open source information, either by attributable or non-attributable means, does not amount to obtaining private information because that information is publicly available. If the information is open to public, or publicly available, it's not personal data. For example, if a person makes open for public for the photos from the Facebook account, it's not personal data anymore.
- According to the Special investigative measures articles in the CPC, the PP should be informed from the beginning of the investigation.
- Recording, storing and using open source information in order to build up a profile of a person or a group of people must be both necessary and proportionate and, to ensure that any resultant interference with a person's right to respect for their private and family life is lawful, it must be retained and processed in accordance with the principles of the Data legislation.

Restricted access information

Access to some of the information on the internet is restricted by its “owner”. A common form of such restriction is in social networks where a profile owner may use the privacy settings to restrict access to online “friends”. For viewing restricted access information covertly, the PP will require a Court Order.

Legal considerations

Online research and investigation techniques may impact on all or any of the following:

- Interception of Communications and the Acquisition of Communications Data
- Surveillance and Covert Human Intelligence Sources
- Computer Misuse
- Data Protection
- Human Rights/European Convention on Human Rights - Both of these provide a number of fundamental rights which are central to all actions of law enforcement.

The right most likely to be engaged by officers and staff undertaking online research and investigation is Article 8 which states:

- 8.1 Everyone has the right to respect for his private and family life, his home and his correspondence.
- 8.2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

The following activities may constitute an offence against Computer Crime Legislation:

- to use another person’s username and password without lawful authority or consent to access data or a program;
- to alter, delete, copy or move a program or data;
- to impersonate that other person using e-mail, on line chat or other web based services.

Public Prosecutor

- Special investigation measures of CPC, PP is informed about the investigation.
- Special investigation measures of CPC, obtaining authorization from the PP for the use of a pseudonym.

Practical considerations for OSINT investigations

When conducting any type of investigation, we need to know the parameters under which we operate, but the methodology has a dynamic aspect and as investigators we often “think outside the box” to obtain evidence.

However, when conducting any investigation on the internet, the information available is so vast it is easy to be distracted or diverted from your intended activity, therefore it is imperative that you identify from the outset, the points to prove and have a structured plan for your research; that you keep an audit trail of the actions and decision making, and retain copies of what is found in an electronic or paper format that is relevant to the investigation.

Audit trail of OSINT research methodology must be in sufficient detail to enable Public Prosecutor to reach same conclusion.

Relevancy: Computer Crime Investigation, Criminal Investigation including Fraud, IP & Domain research,

CYBERCRIME AND CYBER ENABLED CRIMES

Cybercrime

Cybercrime is any criminal activity that involves a computer, networked device or a network. The most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them. Others use computers or networks to spread malware illegal information, images or other materials. Some cybercrimes do both -- i.e., target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks.

A primary effect of cybercrime is financial. Cybercrime can include many different types of profit-driven criminal activity, cybercriminals may target an individual's private information or corporate data for theft and resale. Beside classical cybercrime cases we identify other criminal activities that are related with use of computer equipment, and we need to have appropriate mechanism in place in order to investigate and collect the electronic evidences:

Cyber-Enabled Crimes

These are crimes which do not depend on computers or networks but have been transformed in scale or form by the use of the internet and communications technology. They fall into the following categories:

-  Economic related cybercrime, including:
 - Fraud
 - Intellectual property crime – piracy, counterfeiting and forgery
-  Online marketplaces for illegal items
-  Malicious and offensive communications, including:
 - Communications sent via social media
 - Cyber bullying/trolling
 - Virtual mobbing
-  Offences that specifically target individuals, including cyber-enabled violence against women and girls:
 - Disclosing private sexual images without consent
 - Cyber stalking and harassment
 - Coercion and control

-  Child sexual offences and indecent images of children, including:
 - Child sexual abuse
 - Online grooming
 - Prohibited and indecent images of children
-  Extreme pornography, obscene publications and prohibited images

Cyber-Dependent Crimes

Cyber-dependent crimes fall broadly into two main categories:

- Illicit intrusions into computer networks, such as hacking
- The disruption or downgrading of computer functionality and network space, such as malware and Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks.

Cyber-dependent crimes are committed for many different reasons by individuals, groups and even sovereign states. For example:

- Highly skilled individuals or groups who can code and disseminate software to attack computer networks and systems, either to commit crime or facilitate others to do so;
- Individuals or groups with high skill levels but low criminal intent, for example protest hacktivists;
- Individuals or groups with low skill levels but the ability to use cyber tools developed by others;
- Organised criminal groups;
- Cyber-terrorists who intend to cause maximum disruption and impact;
- Other states and state sponsored groups launching cyber-attacks with the aim of collecting information on or compromising government, defence, economic and industrial assets; and
- Insiders or employees with privileged access to computers and networks.

The majority of cyber criminals have relatively low skills levels, but their attacks are increasingly enabled by the growing online criminal marketplace, which provides easy access to sophisticated and bespoke tools and expertise, allowing these less skilled cybercriminals to exploit a wide range of vulnerabilities.

Common examples of cybercrime

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs, data and individuals from online attack, damage or unauthorised access. Cybercrime is the activity that is affecting cybersecurity and usually is focused on illegal access in the computer systems, altering or deleting computer data, computer fraud, computer forgery etc. In practice we identify many different types of cybercrimes. Some of them are listed and explained below:

Malware is short for malicious software, meaning software that can be used to compromise or disrupt computer or mobile operations computer functions, steal data, bypass access controls, or otherwise cause harm to the host computer. Malware is a broad term that refers to a variety of malicious programs. This section will define several of the most common types of malware; including Viruses, Worms, Trojans, Bots, Rootkits, Spyware, Spoofing and Poisoning attacks, Social Engineering through emails, VOIP and physical presence.

Viruses are one of the most well-known types of malware. They can cause mild computer dysfunction, but can also have more severe effects in terms of damaging or deleting hardware, software or files. They are self-replicating programs, which spread within and between computers. They require a host (such as a file, disk or spreadsheet) in a computer to act as a ‘carrier’, but they cannot infect a computer without human action to run or open the infected file.

- Macro virus affects files that are typically created by Microsoft Office applications such as Word or Excel;
- Boot sector virus modifies the boot sector of the hard disk;
- Polymorphic virus changes their appearance after every infection to evade ant-virus; and
- Metamorphic virus recompiles themselves after every infection to evade detection.

Worms are also self-replicating malicious software programs, but they can spread rapidly and autonomously, within and between computers, often using contacts in the Outlook address book or by looking for open ports on other machines without requiring a host or any human action. The impact of worms can therefore be more severe than viruses, causing destruction across whole networks or by using a lot of network resources. Worms can also be used to deploy Trojans onto the network system.

Trojans are a form of malware that appear to be legitimate programs, but facilitate illegal access to a computer. They can perform functions, such as stealing data, without the user's knowledge and may trick users by undertaking a routine task while actually undertaking hidden, unauthorized actions.

A common Trojan is where a client computer is compromised and becomes a bot that can be used for launching attacks against other computers; other Trojans can be used to install remote control agents onto computers. A Trojan would be a visible program running in Task Manager.

Rootkit To install a rootkit, an attacker must first gain access to the root account by using an exploit or obtaining the password by cracking it or social engineering. Rootkit allows viruses and malware to "hide in plain sight" by disguising as necessary files that your antivirus software will overlook.

Rootkits themselves are not harmful; they are simply used to hide malware, bots and worms in the root or kernel of the OS. It cannot be seen using task manager but needs special detection tools. It can be used to capture keystrokes or intercept system calls and divert them to other programs or may allow remote access to a computer. Because rootkits are activated before your operating system even boots up, they are very difficult to detect and are notoriously difficult to remove.

Denial of service (DoS) and Distributed DoS (DDoS) exploit weaknesses in protocols and creates attacks flooding Internet servers with so many requests that they are unable to respond quickly enough. This can overload servers causing them to freeze or crash denying access for legitimate users to a site or service.

- A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have.
- A distributed denial-of-service (DDOS) is an incident where large numbers of compromised systems (sometimes called a botnet) attack a single target.

DoS/DDoS attack can cost the target person or company a great deal of time and money. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services; it can destroy programming and files in affected computer systems and in some cases websites temporarily cease operation.

Common forms of (DOS) attacks are:

Buffer Overflow Attacks are the most common kind of DoS attack; attackers send more traffic to a network address than the programmers who planned its

data buffers anticipated someone might send. The attacker may be aware that the target system has a weakness that can be exploited or the attacker may simply try the attack in case it might work. An example is sending oversized Internet Control Message Protocol (ICMP) packets - Packet Internet or Inter-Network Groper (PING) of death.

SYN Attack when a session is initiated between the Transport Control Program (TCP) client and server in a network, a very small buffer space exists to handle the usually rapid “hand-shaking” exchange of messages that sets up the session. The session-establishing packets include a SYN field that identifies the sequence in the message exchange. An attacker can send a number of connection requests very rapidly and then fail to respond to the reply. This leaves the first packet in the buffer so that other, legitimate connection requests can't be accommodated. Although the packet in the buffer is dropped after a certain period of time without a reply, the effect of multiple bogus connection requests is to make it difficult for legitimate requests for a session to get established.

Teardrop Attack exploits the way that the Internet Protocol (IP) requires a packet that is too large for the next router to handle be divided into fragments. The fragment packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system. In the teardrop attack, the attacker's IP puts a confusing offset value in the second or later fragment, causing the receiving operating system to crash.

Smurf Attack in this attack, the perpetrator sends an IP ping (echo) request to a receiving site. The ping packet specifies that it be broadcast to a number of hosts within the receiving site's local network. The result will be lots of ping replies flooding back to the innocent, spoofed host at a rate that the host will no longer be able to receive or distinguish real traffic.

Fraggle Attack is an attack that involves sending a large amount of spoofed UDP traffic to a router's broadcast address within a network. It is very similar to a Smurf Attack.

(Routers no longer forward packets directed at broadcast addresses, most networks are protected from Fragle and Smurf attacks).

Relevancy: Computer Crime Investigation, Cyber Attacks

Backdoors are services running or ports open that will allow a remote user to connect and bypass standard authentication mechanisms to your computer. Backdoors such as the Netcat utility allow remote connectivity where a malicious

user could do anything he liked on a computer without the logged on user noticing the remote access. Backdoors are used by hackers to allow them to return to a computer after they have gained initial access.

Ransomware attacks are a form of malware where your local files on a computer are locked and access is denied; this is followed with a ransom demand for money to get them unlocked, using some form of untraceable payment method (i.e.: Bitcoin).

Logic bomb is a malicious program timed to cause harm at a certain point in time, but is inactive up until that point. A set trigger, such as a pre-programmed date and time, activates a logic bomb and implements a malicious code that causes harm to a computer or network.

Botnet is a name for a number of Internet computers that, although their owners are unaware of it, been compromised and set up to forward transmissions (including launching denial of service attacks, spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie, a computer “robot” or “bot”. Most computers compromised in this way are home-based and can consist of tens of thousands of infected computers. The computers that form a botnet can be programmed to redirect transmissions to a specific computer, such as a Web site being closed down by having to handle too much traffic; known as a distributed denial-of-service (DDoS) attack.

Keylogger or Keystroke logger is a type of surveillance software that has the capability to record every keystroke you make to a log file, usually encrypted. A keylogger recorder can record instant messages, e-mail, and any information you type at any time using your keyboard. It can be software downloaded onto the device or a physical device placed between the keyboard and computer.

Spyware is software that invades users' privacy by gathering sensitive or personal information from infected systems and monitoring the websites visited, and transmitting to third parties. Spyware can sometimes be hidden within adware, and can capture screenshots of the victim's computer.

Relevancy: Computer Crime Investigation, Criminal Investigations including Fraud,

Social Engineering is where the attack exploits human behaviour and human nature – “hacking the human”. People are encouraged via email, telephone or face-to-face meeting, or impersonation to part with personal information through the process of convincing them that attacker is a genuine person like an administrator,

engineers or technicians who is doing them a service and encourage them to divulge logon, corporate, personal or financial information using plausible stories.

Email - Cyber Threats

The following are specific types of cyber threats conducted via the use of email in either a random or targeted approach.

Spam is unsolicited or ‘junk’ email, typically sent in bulk to countless recipients around the world and is often related to pharmaceutical products or pornography. Spam email is also used to send phishing emails or malware and can help to maximise potential returns for criminals.

Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels. Typically, a victim receives a message that appears to have been sent by a known contact or organization. An attachment or links in the message may install malware on the user’s device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details. Other variations include:

- Spear phishing is a variation that targets specific individuals or groups within an organisation, trying to gain personal information.
- Whaling is the practice of sending phishing mails to specific high-level targets in an organisation, managers and directors etc.
- Vishing is using VoIP networks to send unsolicited phone calls trying to gain information.
- Spim is a variation on Spam where Instant Messaging is used to send unwanted messages.
- Smishing is a variation on phishing but using SMS as the medium.

Email Spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source.

Hoax emails encourage users to carry out some activity on their computer that could be damaging but is totally unnecessary.

Doxing is the practice of researching and broadcasting personally identifiable

information about an individual, searching publicly available databases, social media websites, hacking, and social engineering.

Relevancy: Computer Crime Investigation, Criminal Investigation including Fraud

Physical - Cyber Threats

In addition to social engineering there are other physical threats that create cyber security risks including human presence or electronic capture such as video.

Shoulder Surfing is looking over someone's shoulder when they enter their password on a computer or their PIN number at an ATM. They may look for the pattern being entered into digilocks controlling access to secure areas.

Dumpster diving is the process of sifting through rubbish bins and waste containers looking for useful information, discarded documents and sticky notes etc. Another useful source is the recycling paper bin near the printer.

Identity Theft is a crime in which an imposter obtains key pieces of personal information, such as Email Account, Social Network Account or Banking Account in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials.

Payment card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

Cybersquatting is registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else. The term derives from squatting, the practice of inhabiting someone else's property without their permission. As a crime, it can be related to Software Piracy, Copyright Infringements and Trademark Violations.

Counterfeit Goods and Fake Services most people associate counterfeit goods with clothing, music and film; a wide array of goods in everyday use such as medicines and car parts are reproduced illegally and poorly made in such a way that they can be dangerous to the public.

Access to these goods can sometimes be through on-line legitimate shopping or auction sites, but an increased number are being offered through bogus websites

and emails with a link to a bogus site or advert. These websites and links are often loaded with malware with the intention of disrupting the operational functions a computer or mobile device or to steal the user's personal and financial data.

Payment services associated with the websites are often legitimate but the dataset that personal information is provided to is harvested and later used by or sold to criminal networks for the purpose of fraud.

Relevancy: Computer Crime Investigation, Criminal investigations, Skimming

Spoofing and Poisoning Attacks

A spoofing attack is when a malicious party impersonates another device or user on a network; in order to launch attacks against network hosts, steal data, spread malware or bypass access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this. Some of the most common methods include IP address spoofing attacks, ARP spoofing attacks and DNS server spoofing attacks.

IP Address Spoofing Attacks

IP address spoofing is one of the most frequently used spoofing attack methods. In an IP address spoofing attack, an attacker sends IP packets from a false or "spoofed" source address in order to disguise itself. Denial-of-service (DOS) attacks often use IP spoofing to overload networks and devices with packets that appear to be from legitimate source IP addresses.

There are two ways that IP spoofing attacks can be used to overload targets with traffic. One method is to simply flood a selected target with packets from multiple spoofed addresses. This method works by directly sending a victim more data than it can handle. The other method is to spoof the target's IP address and send packets from that address to many different recipients on the network. When another machine receives a packet, it will automatically transmit a packet to the sender in response. Since the spoofed packets appear to be sent from the target's IP address, all responses to the spoofed packets will be sent to (and flood) the target's IP address.

IP spoofing attacks can also be used to bypass IP address-based authentication. This process can be very difficult and is primarily used when trust relationships are in place between machines on a network and internal systems. Trust relationships use IP addresses (rather than user logins) to verify machines' identities when

attempting to access systems. This enables malicious parties to use spoofing attacks to impersonate machines with access permissions and bypass trust-based network security measures.

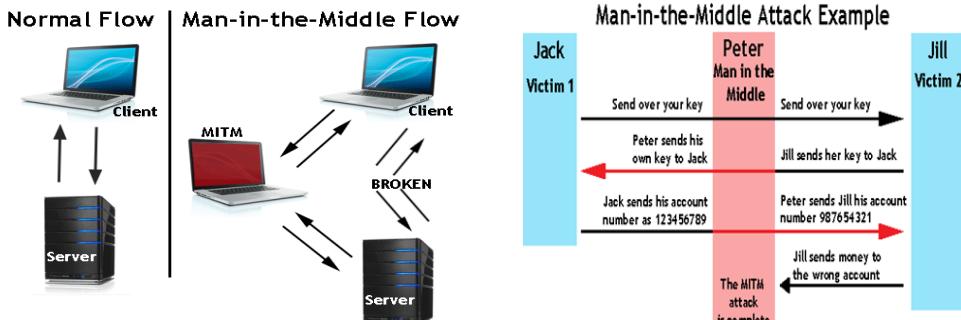
ARP Spoofing Attacks are when a malicious party sends spoofed ARP messages across a local area network in order to link the attacker's MAC address with the IP address of a legitimate member of the network. This type of spoofing attack results in data that is intended for the host's IP address being sent to the attacker instead. Malicious parties commonly use ARP spoofing to steal information, modify data in-transit or stop traffic on a LAN. ARP spoofing attacks can also be used to facilitate other types of attacks, including denial-of-service, session hijacking and man-in-the-middle attacks. ARP spoofing only works on local area networks that use the Address Resolution Protocol.

ARP Poisoning Attacks also known as ARP cache poisoning or ARP poison routing is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised. An effective ARP poisoning attempt is undetectable to the user.

An attacker uses the process of ARP spoofing to "poison" a victim's ARP table, so that it contains incorrect or altered IP-to-MAC address mappings for various attacks, such as a man-in-the-middle attack.

DNS Server Spoofing Attacks are when a malicious party modifies the DNS server in order to reroute a specific domain name to a different IP address. In many cases, the new IP address will be for a server that is actually controlled by the attacker and contains files infected with malware. DNS server spoofing attacks are often used to spread computer worms and viruses.

Man-in-the-Middle Attack is a type of cyberattack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM.



Man-in-the-Middle Attack Examples

In the first example the attacker inserts him/herself in-between the flow of traffic between client and server. Now that the attacker has intruded into the communication between the two endpoints, he/she can inject false information and intercept the data transferred between them. In the second example the hacker is impersonating both sides of the conversation to gain access to funds, the attacker intercepts a public key and with that can transpose his own credentials to trick the people on either end into believing they are talking to one another securely.

DNS Cache Poisoning is changing the local DNS settings (changing the real values of URLs), so you either use a rogue DNS server which directs you to fake copies of web sites or local hosts file is modified to contain false entries. DNS poisoning is also done to inject malware into your computer or network. Once you land on a fake website using a poisoned DNS cache, the criminals can do anything they want. Criminals can also set up fake DNS servers so that when queried, they can give out fake IP addresses. This is high level DNS poisoning and corrupts most of the DNS caches in a particular area thereby affecting many more users.

DNS Hijacking or DNS Redirection is a method used by cybercriminals to hijack your web-browser as it attempts to resolve the IP address of the website you wish to load, through the installation of malware on your computer that changes the trusted default DNS so that whenever your browser tries to resolve a URL, it contacts one of the fake DNS servers instead. This results in your browser loading a malicious website that may compromise your computer or steal your credentials etc.

Pharming is where malicious code is installed on a personal computer or server usually as a result of DNS settings being interfered with, misdirecting users to fraudulent Web sites that is an identical copy of the real one without their knowledge or consent. It is part of the phishing process where the aim is gather personal information from victims.

Privilege escalation is exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorised actions.

Relevancy: Computer Crime Investigation, Criminal Investigation including Fraud

The National Critical Infrastructure (NCI) provides the essential services that underpin the backbone of a nation's economy, security, health, utilities, and transportation and communication systems relied on, on day-to-day basis. The incapacitation or destruction of these vital systems would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Attacks against the NCI can be state sponsored, ideological, criminal or malicious. The following are examples of such attacks.

Infrastructure Hacking is a form of trespass. It is the unauthorised use of, or access into, computers or network resources, which exploits identified security vulnerabilities in networks. Hacking can be used to violate or deface websites (Website Violation and Website Defacement) and to gather personal data or information of use to criminals (Data Breaches).

Equipment Hacking is a growing sector of Cyber Crime, as the rise in the Internet of Things (IoT) has left devices more connected (besides the usual Smartphones and Tablets), yet in many cases more vulnerable, than ever before: this kind of crime ranges from Automotive and Medical hacking to cyber-attacks against the Critical Infrastructures.

Hacktivism is the use of computers and computer networks to promote political ends, i.e. hacking for a cause. Global multinationals such as oil companies are frequently the targets of hacktivists.

Activities usually consist of defacing web sites with political statements or causing denial of service attacks. Groups such as Lizard Squad, Mazafaka, OurMine, Anonymous and Lulzsec have raised the profile of hacktivism attacking social media sites to defacement of government websites.

Relevancy: Computer Crime Investigation, Cyber attacks

Harassment

Cyber Bullying and Cyber Stalking can be against Male or Female Victims and refers to someone or a group engaging in offensive, menacing or harassing behaviour online towards young or adult people. The behaviour may include abusive texts or emails, hurtful messages, images or videos.

Mobbing is the same as Cyber Bullying and Cyber Stalking but is work-related.

Relevancy: Computer Crime Investigation, Criminal Investigation

Criminal Services for Hire!

Criminals adopt conventional approaches that reflect cold business sense from supermarket-style pricing, to outsourcing, to specialists acting as mules, coders, hackers, information vendors, for example. There are many more roles in the criminal underground and it is a complex ecosystem of interdependencies, with some skills being valued above others. The following are examples of services for hire:

Hacker: These are the people who identify the vulnerability in commercial software. Their skills are ever increasing as we see more and more 0day hacks, which the name is given to vulnerabilities the software or anti-virus companies are not aware of.

Coder: Skills to program software to compromise data, for example.

Spammer: Someone with ability to send out bulk numbers of emails for the purposes of infecting machines with malware, directing people to phishing sites or selling them fake goods (for example)

Vendors: operate mainly on the forums – selling credit card / bank login data

Money Mules: people who receive proceeds of fraud from compromised bank accounts and forward the fund to those controlled by the fraudsters for cashing out. Can be professional or duped into carrying out transactions. Keep a cut of the money.

Launderers: Virtual money exchangers knowingly advertising to criminals to transfer ill-gotten virtual gains into the legitimate banking system / cash.

Relevancy: Computer Crime Investigation, Criminal Investigation including Fraud

Child Exploitation Online

The CCIU has specialist teams trained to investigate those transfer and exchange images related to sexual exploitation and sexual abuse of children; criminal groups profiteering from the publication or distribution of child abuse images; support local police with computer forensics and covert investigations and provide authoritative investigative advice and support to maximise the Albanian Police response to crimes of child sexual abuse and exploitation.

The CCIU liaise with the online and technological industries to minimise the possibility of present and future technology increasing the risk of sexual exploitation and sexual abuse to children.

Police Prevention Specialists work together with the CCIU to raise the knowledge, skills and understanding of parents, carers, children and young people.

The Internet is used to transfer and exchange Indecent Images Abuse of Children and to also Live-Stream Child Abuse or Download Child Sex Abuse Material or advocates sexually offensive or extreme adult content (Live Streaming or Downloadable) that is illegal under Article 117/2 child pornography.

Examination of these images and associated information can identify where a child has, or may have been abused or exploited, and can lead to the child being removed to a place of safety by Police.

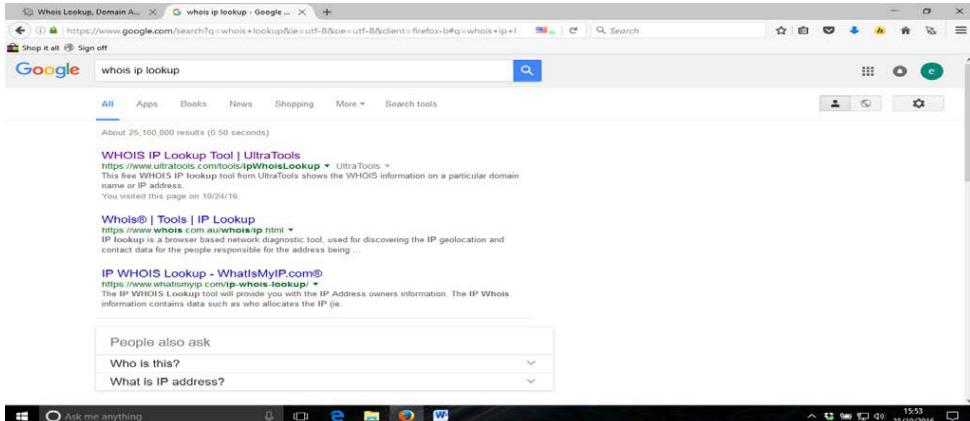
Investigations of these crimes can be complex. Digital evidence is often paramount and with associated risk to the child. It is imperative that **in the event such offences are identified or suspected the CCIU must be contacted for support.**

See Further Guidelines at Appendix 'D'.

Relevancy: Child Exploitation Investigations, Computer Crime Investigation,

Appendix A - Visual Guide - How to look up an IP address or domain name registrant

- 1 Open a website for whois IP lookup OR (Open Google - enter "whois IP lookup" and search);



- 2 Select site – in this case it is <http://whois.domaintools.com/>;



- 3 Input IP address e.g.: 185.71.180.28, (or for domain the website name www.asp.gov.au)

- 4 Press SEARCH;

- 5 The following result will be displayed:

Whois Lookup

Home > Whois Lookup > 185.71.180.28

IP Information for 185.71.180.28

Quick Stats

IP Location	Albania Bajram Curri Albania State Police
ASN	AS201524 ASP, AL (registered Oct 02, 2014)
Whois Server	whois.ripe.net
IP Address	185.71.180.28
Reverse IP	1 website uses this address.

Abuse contact for '185.71.180.0 - 185.71.183.255' is 'leotrim.dani@asp.gov.al'

```

inetnum:          185.71.180.0 - 185.71.183.255
netname:          AL-ASP-20140930
org:              ORG-ASP10-RIPE
country:          AL
admin-c:          ED3744-RIPE
tech-c:           ED3744-RIPE
mnt-by:           RIPE-NCC-HM-MNT
status:           ALLOCATED PA
changed:          2016-04-14T10:22:33Z
last-modified:    2016-04-14T10:22:33Z
source:           RIPE
organization:    ORG-ASP10-RIPE
org-name:         Albania State Police
country:          AL
area-name:        TTB

```

DomainTools Iris
More data. Better context.
Faster response.
[Learn More](#)

Tools

- Monitor Domain Properties
- Reverse IP Address Lookup
- Network Tools



IP Information for 185.71.180.28

Quick Stats

IP Location	 Albania Bajram Curri Albania State Police
ASN	 AS201524 ASP, AL (registered Oct 02, 2014)
Whois Server	whois.ripe.net
IP Address	185.71.180.28
Reverse IP	1 website uses this address.

```
% Abuse contact for '185.71.180.0 - 185.71.183.255' is "emer.mbiemer@asp.gov.al
```

```
inetnum:          185.71.180.0 - 185.71.183.255
netname:          AL-ASP-20140930
org:              ORG-ASP10-RIPE
country:          AL
admin-c:          ED3744-RIPE
tech-c:           ED3744-RIPE
mnt-lower:        MNT-ASPAL
mnt-routes:       MNT-ASPAL
mnt-by:           RIPE-NCC-HM-MNT
status:           ALLOCATED PA
created:          2014-09-30T14:56:24Z
last-modified:    2016-04-14T10:22:33Z
source:           RIPE

organisation:    ORG-ASP10-RIPE
org-name:         Albania State Police
country:          AL
org-type:         LIR
address:          Bulevardi Bajram Curri
address:          1001
address:          Tirane
address:          ALBANIA
phone:            +355694118355
e-mail:           name.surname@asp.gov.al
abuse-c:          AC28059-RIPE
mnt-ref:          RIPE-NCC-HM-MNT
mnt-by:           MNT-ASPAL
mnt-ref:          MNT-ASPAL
mnt-by:           RIPE-NCC-HM-MNT
created:          2014-09-29T14:13:45Z
last-modified:    2021-02-03T09:27:27Z
source:           RIPE

person:           Edrin Dhroso
address:          Bulevardi Bajram Curri 1001 Tirane Albania
phone:            +355 694118663
e-mail:           name.surname@asp.gov.al
nic-hdl:          ED3744-RIPE
mnt-by:           MNT-ASPAL
created:          2014-09-30T08:08:22Z
last-modified:    2014-09-30T08:08:22Z
source:           RIPE

route:            185.71.180.0/24
descr:            Albania State Police
origin:           AS201524
mnt-by:           MNT-ASPAL
created:          2015-09-18T14:05:30Z
last-modified:    2015-09-18T14:05:30Z
```

This is the methodology by which most free tools will return the search query. This search/enquiry process with the online tool is similar for other searches detailed under **Research Tools - On-Line tools and databases for Analysing IP Addresses and Domains: Types of Enquiry**.

Relevancy: Computer Crime Investigation Criminal Investigation, Cyberbullying, IP & Domain Address Research

Appendix B – Regional Internet Registry data records explained

The following table is a translation of the above search result conducted in the email exercise at **Appendix A**, and converts coded data and technical terms into plain language; it also identifies what is relevant to routine and technical criminal investigations through the notations below:

- **ROUTINE:** Relevant to any Internet related Investigation.
- **TECHNICAL:** Relevant to a technical cybercrime investigations - seek support of CCIU.
- **Source Database:** Administrative Information that relates to the database registration requirements.

Data from Who Is Registry	Data held on whois www.domaintools.com	Explanation of Terminology	Investigation
IP Information:	185.71.180.28	Adresa IP	ROUTINE: IP Address subject of enquiry or investigation.
IP Location:	 Albania Bajram Curri Albania State Police	Location of IP address and name of ISP it has been allocated too.	ROUTINE: Where is the IP address? Does the location match the circumstances of your investigation?
ASN	AS201524 ASP, AL (registered Oct 02, 2014)	Within the Internet, an autonomous system Number (ASN) is a collection of connected IP routing prefixes (AS) under the control of one or more network operator that presents a defined routing policy to the Internet. In this case the ASN is AS6821.	TECHNICAL: This is a unique number and the server will contain routing information and protocols.

Whois Server	whois.ripe.net	Indicates this whois search was conducted on the server managed by Regional IP Address Assignment Centre, in this case RIPE.	Source Database
Abuse contact for	Abuse contact for '185.71.180.0 – 185.71.183.255' is 'name.surname@asp.gov.al'	Email contact address for any abuse or infringement of any IP address in this network range.	TECHNICAL CONTACT POINT
inetnum:	'185.71.180.0 – 185.71.183.255'	Denotes the IP address range allocated to this ISP and defined by RIPE as a Local Internet Registry (LIR).	ROUTINE: Is the IP address part of this range.
netname:	AL-ASP-20140930	Network Name Allocated	TECHNICAL: Name of the Network
descr:	Albania State Police	Description of Network – ADSL IP Subnet defines an Internet Access Service	TECHNICAL: Description of the network activity – ADSL IP subnet service.
country:	AL	Country of Operator	ROUTINE: see IP Location above.
admin-c:	ED3744-RIPE	Administrator responsible	TECHNICAL: Information
tech-c:	ED3744-RIPE	Technician responsible	TECHNICAL: Information
status:	ASSIGNED PA	LIR assigned and relates to the technical operation	TECHNICAL: Description of the network activity
mnt-by:	MNT-ASPAL	Administration data	TECHNICAL: Information
Created:	2015-09-18T14:05:30Z	Date registration created	Source Database

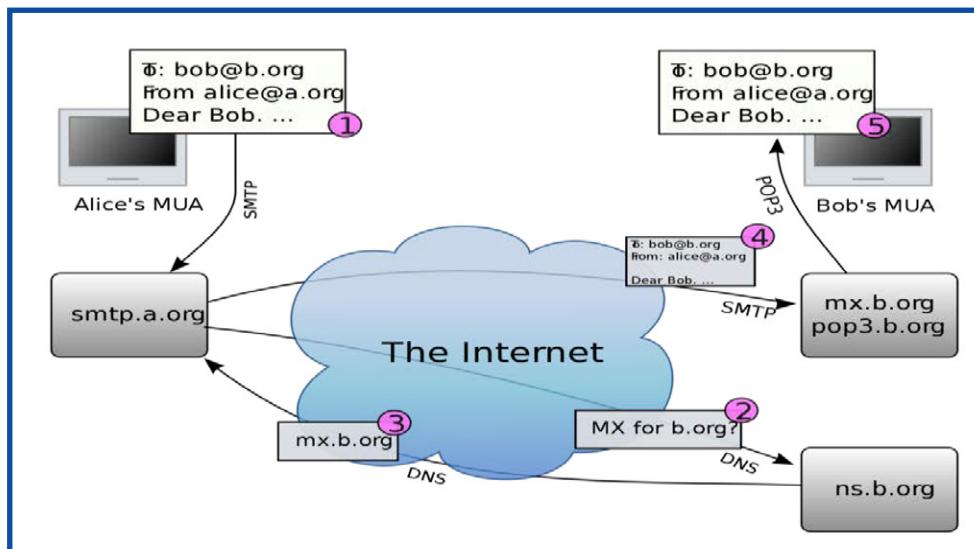
Last-modified:	2015-09-18T14:05:30Z	Date last updated	ROUTINE: Source Database: check date for how recent information is.
source:	RIPE	Database of RIPE	Source Database
role:	ADMIN	Administrator	ROUTINE: Information of role in ISP.
address:	Bulevardi Bajram Curri 1001 Tirane Albania phone: +355 694118663	Location	ROUTINE: Important contact detail for data requests and technical assistance.
e-mail:	name.susrname@asp.gov.al	Contact details normally relates to generic mailbox for Network Administration Team	ROUTINE: may not be populated as it is voluntary and is often same as 'Abuse' above.
admin-c:	ED3744-RIPE	Administrator responsible	TECHNICAL: Information
tech-c:	ED3744-RIPE	Technician responsible	TECHNICAL: Information
nic-hdl:	MA12945-RIPE	A Network Information Centre handle is a unique alphanumeric character sequence that represents an entry in the databases maintained by Network Information Centres. Once a domain name has been registered, its NIC handle can be used to search for that record in the database.	TECHNICAL: Investigation – Device identifier

created:	2015-09-18T14:05:30Z	Date registration created	Source Database
last-modified:	2015-09-18T14:05:30Z	Date last updated	Source Database
source:	RIPE	Database of RIPE	Source Database
route:	185.71.180.0/24	Relates to the routing policy in this case it denotes IP addressing and subnetting protocol.	TECHNICAL: Investigation Networking
descr:	Albania State Police	Hostname attributed to server.	TECHNICAL: Investigation Networking
Origin:	AS201524	Each AS (autonomous network) has a unique number (ASN), which serves as an identifier in the exchange of external routing information.	TECHNICAL: Investigation Networking
mnt-by:	MNT-ASPAL	Administration data for ASN record	TECHNICAL: Investigation Networking
Created:	2015-09-18T14:05:30Z	Date registration created	Source Database
last-modified:	2015-09-18T14:05:30Z	Date last updated	Source Database
source:	RIPE	Database of RIPE	Source Database

Relevancy: Computer Crime Investigation Criminal Investigation, Cyberbullying, IP & Domain Address Research

Appendix C - Investigating email

This appendix provides visual and textual representation of how email works, the network protocols for communicating, where data is stored, and what information is contained in email headers that can assist in criminal investigations. The email process and protocols are explained in stages 1-5 in the below diagram and explanation, for an email being sent from Alice to Bob.



- ① Alice@a.org writes an email to **bob@b.org**, the message is composed on a computer by using an email programme: an email client or mail user agent (MUA). The email program combines the text Alice wrote (the body) with the recipient details bob@b.org, email subject, the programme stamps a date, and time, time zone onto the message (the header).
- ② The email program (the client/MUA) then sends the message off to an email server by using the Simple Message Transfer Protocol, or SMTP. The email server is a program running on another computer located at your Internet service provider (ISP).
- ③ At the server, the message is dissected and the recipients culled from the messages To, Cc, and Bcc fields in the header. The SMTP server then finds the host computer for the recipients, the server looks up b.org and sends the message off to that computer. For a few nanoseconds, the message hops around the Internet as it makes the connection to the destination computer.
- ④ At the destination computer b.org, another SMTP server fetches the message and puts it into a mailbox of bob@b.org. There, it sits and waits until the

bob@b.org logs in to collect mail. The mailbox on the server isn't the same thing as the inbox in your PC's mail program.

- ⑤ Bob logs onto his mail program and collects new messages from his ISP's server. The mail program uses the Post Office Protocol (POP) to fetch the message. POP is used instead of SMTP because the email message is no longer being sent on the Internet; it has arrived. All the POP does is fetch the message waiting on the server and transfer it back to the user's computer and his email program. After the mail messages are on the recipient's computer, they're stored in a database organised by your email program: e.g. Inbox, Deleted Items etc.

The email methods described here does not apply to email systems at large organizations e.g. Microsoft outlook.

In addition to POP is the Internet Message Access Protocol (IMAP) method of reading email. Unlike POP, IMAP doesn't delete messages from the user's mailbox on the server until the user deletes the message. Web-based email programs, such as Gmail and Hotmail, often prefer IMAP. Those information could be disclosed to the Prosecutor base on MLA request.

Full email header both web based and client based emails tend to condense the email header to Time and date received, From, Subject and the email body. The full header is still there but needs to be opened and different web based email operate in different ways to access the full email header; e.g. AOL requires you to hover over the unopened email and right click and this will reveal the header and other source information; Mail.com requires the email to be opened then on the top right is an icon marked 'i', when this is clicked the full email header is shown.

If faced with an email system where you do not know where the extended header will be; a Google search for 'find extended email header in xxx', often provides an answer as shown with the below outlook.com example:

Outlook.com

+ New Reply | v Delete Archive Junk | v Sweep Move to ...

Search email

1 item selected Clear all check boxes

Arrange by v

Folders

Inbox 1

Archive

<input checked="" type="checkbox"/>	Lyris ListManager	Confirmation message from IISD	12:02 PM
<input type="checkbox"/>	Outlook.com Team	Welcome to your new Outlook...	11:53 AM

Right click the message in the message list

What are we looking for?

Analysing headers often means reading the full header from the bottom up to establish. The purpose of analysing the header of the message is to try to identify the IP address of the sender and the exact origin mail from where the message was send. The information from the header are more accurate and relevant and those information could be used as evidence.

First occurrence of any of the following:

- The sender information
- X- originating IP with X- original arrival time
- First received from with an external IP address for ISP
- First received from with an internal IP address
- Extended/Full Headers

Other information that may assist with identifying the device used, include:

- Mail software description
- Software language
- Local device information
- Local email information

Recent Privacy Issues, mean that some companies either remove this data from the email or encrypt the data, so it is not visible.

Relevancy: Computer Crime Investigation Criminal Investigation, Cyberbullying, IP Address Research, Email investigation

Example of a full email header

To: Mum
In-Reply-To: <3392D246-77DF-4EDD-BA99-CC69D1F25770@gmail.com>
X-Received: by 10.28.180.84 with SMTP id d81mr21959784wmf.42.1455646555118; Tue, 16 Feb 2016 10:15:55 -0800 (PST)
X-Received: by 10.28.175.139 with SMTP id y133mr19416441wme.45.1455646554756; Tue, 16 Feb 2016 10:15:54 -0800 (PST)
X-Gm-Message-State:
AG1oYOTgv/RwmBXwVYkFEgRtg3CbY4hM7v29g1OHgdj+2xbeYsS96T3eZ4V1zJfoFe1RTA==
Return-Path: <JulieJulieJulie@outlook.com>
Return-Path: <JulieJulieJulie@outlook.com>
Mime-Version: 1.0
Thread-Index: AQlcBsFXuSeiysZYZt9XplcA3rGn+56Zve3A
Authentication-Results: mx.google.com; spf=neutral (google.com: 2a00:1450:400c:c09::235 is neither permitted nor denied by best guess record for domain of JulieJulieJulie@outlook.com) smtp.mailfrom=JulieJulieJulie@outlook.com; dkim=pass header.i=@gmail.com 20150623.gappssmtplib.com
Message-Id: <011b01d168e6\$29298a10\$7b7c9e30\$@gmail.com>
X-Mailer: Microsoft Outlook 14.0
Dkim-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com 20150623.gappssmtplib.com; s=20150623; h=from:to:references:in-reply-to:subject:date:message-id:mime-version:content-type:thread-index:content-language; bh=QUeNXGaRNPFy6WVKXSh7ZkDY1a1hJ9ebkYz9w1M2mngc=; b=XxRt5Zb+XHtLtnllLxAhyzISGdlcaBwK/ygh4XI+LsO/KXoMLsGAKldHhpJphyBmug1nNcQ2ZjLjSTt+O3g4SuY8CQzvUBz+AMi68yMjMozSK4ggPDNEYURtoxktnYLOehNi9t nMYenfk9gOterqoEmmGU1pYFNCL1SJtkrNaGW4aXHACwVN75/rQgEltwlVCWJZgWlo+2R XYWPzU7FeDIGclj4AUqEkz5aJuCiGjcnPlb6WkUTKwDicPQtgh6CTIB7VkjXAJlenZ/ PBX8uBKaE5htZcZ6qqvG/mUwHgqCgwiNF4qkzLv3mTD6QIV/pedS+vsbkk+hFBAn/a cBWg==
References: <3392D246-77DF-4EDD-BA99-CC69D1F25770@gmail.com>
X-Google-Dkim-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20130820; h=x-gm-message-state:from:to:references:in-reply-to:subject:date :message-id:mime-version:content-type:thread-index:content-language; bh=QUeNXGaRNPFy6WVKXSh7ZkDY1a1hJ9ebkYz9w1M2mngc=; b=bYiTbeneAMFVywIEwmq+XpdXhXIQ07+dnBwRl7bVgjxCodgWmoQcbBdvDGchmuWb hu8aa66GRV4QldsL4DjNX8Wz6+1b5+5Ffv/orVcFW4kXAHMjgRJgy3sC4BQ+hztBXb3e mB7qiaVXYQO8d6u1vE5S8Yrg/XDQmmzIIBCQooPq1eMTirhmyql+odWG0oaTrVs3/Tas MXqOmoUZfpUsdVIOh8s4PXwsVdc9uBWyV+3d6i7FHgLXoFq4BZovkO974h7JFyHx3R 61cp9N7jo/1f/SU82nL5crXToSj3n/m+V2kILKx7aGP9ZVgbQrkq2Sp5AUSnSFevqbu RE9Q==
Content-Type: multipart/mixed; boundary="----=_NextPart_000_011C_01D168EE.8AEF0380"
Received-Spf: neutral (google.com: 2a00:1450:400c:c09::235 is neither permitted nor denied by best guess record for domain of JulieJulieJulie@outlook.com) client-ip=2a00:1450:400c:c09::235;
Delivered-To: mumsmith@gmail.com
Content-Language: sr-me
Received: by 10.27.224.10 with SMTP id x10csp1737087wlg; Tue, 16 Feb 2016 10:15:55 -0800 (PST)
Received: from mail-wmo-x235.google.com (mail-wmo-x235.google.com. [2a00:1450:400c:c09::235]) by mx.google.com with ESMTPS id fa10si50358496wjd.246.2016.02.16.10.15.54 for <mumsmith@gmail.com> (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128); Tue, 16 Feb 2016 10:15:55 -0800 (PST)
Received: by mail-wmo-x235.google.com with SMTP id b205s0122246482wmb.1 for <mumsmith@gmail.com>; Tue, 16 Feb 2016 10:15:54 -0800 (PST)
Received: from Recepција ([95.155.60.218]) by smtp.gmail.com with ESMTPSA id v66sm21581736wmb.18.2016.02.16.10.15.52 (version=TLSv1/SSLv3 cipher=OTHER); Tue, 16 Feb 2016 10:15:53 -0800 (PST)
RE: Where are you?

Information contained in the email relevant to an investigation:

To: Mum
 In-Reply-To: <3392D246-77DF-4EDD-BA99-CC69D1F25770@gmail.com>
 X-Received: by 10.28.180.84 with SMTP id 1y133m19410441wme45-1455040554/50; Tue, 16 Feb 2016 10:15:55 -0800 (PST)
 X-Received: by 10.28.175.139 with SMTP id 1y133m19410441wme45-1455040554/50; Tue, 16 Feb 2016 10:15:54 -0800 (PST)
 X-Gm-Message-State:
 AG1oYOTgv/RwmBXwVYkFEgRtg3CbY4hM7v29g1OHgdj+2xbeYsS96T3eZ4V1zfoFe1RTA==
 Return-Path: <JulieJulieJulie@outlook.com>
 Return-Path: <JulieJulieJulie@outlook.com>
 Mime-Version: 1.0
 Thread-Index: AQIcBSFXuSeiysZYZtgXplcA3rGn+56Zve3A
 Authentication-Results: mx.google.com; spf=neutral (google.com: 2a00:1450:400c:cog::235 is neither permitted nor denied by best guess record for domain of JulieJulieJulie@outlook.com) smtp.mailfrom=JulieJulieJulie@outlook.com; dkim=pass header.i=@gmail.com 20150623.gappssmtp.com
 Message-ID: <011b01d168e6\$29298a10@outlook.com>
 X-Mailer: Microsoft Outlook 14.0 Identifies the mail client is Microsoft Outlook 14.0 which is the version Microsoft Office 2010
 Dkim-Signature: v=1; a=rsa-sha256; c=rh; d=outlook.com; h=from:references:in-reply-to:subject:date:message-id:mime-version:content-type:thread-index:content-language; bh=QUEuNXGaRNPFy6WKXSh7ZkDY1ahJgebkYzgwM2mngc=; b=XxRt5Zb+XHTLtnlLxAhyzISGdIcaBwK/ygh4Xl+LsO/KXoMLSgAKIdHhpJphyBmug1nNQz2JzJSTr+O394SuY8CQzvUBz+AMi068yMUMozsK4ggPDNEYURtoxktnYLOeHnigt nMYenfk9OteroqEmmgU1pYFNCL1SjtkrNaGW4aXHACwVN75/rQgEltwlVCWJZgWlo+2R XYWPzUjFEdIGclqAUqEkzgajuCiGjcnPlbWkUTKwDipQtgh6CTIIByVklXAJlenZ/PBX8uBKAEStlZcZ6qgvG/mUlwhGwqCgwNF4qkzLvg3mTD6QIV/pedS+vsbbk+hFBAn/a cBWg==
 References: <3392D246-77DF-4EDD-BA99-CC69D1F25770@gmail.com>
 X-Google-Dkim-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=2013o820; h=x-gm-message-state:from:to:references:in-reply-to:subject:date:message-id:mime-version:content-type:thread-index:content-language; bh=QUEuNXGaRNPFy6WKXSh7ZkDY1ahJgebkYzgwM2mngc=; b=yITbenefAMFVywiEwmq+XpdXhXIQ07+dnBwRiL7bVgjxCodgWmoQcbBdvDGclhmuWbhu8af66RV4Qldsl4DjNX8WZ6+1b5+5Fv/orVcfW4KXAHMjgRJgygsC4BQ+htBXBje mB7qjaVXYQ08d6uVeM58Yrg/xdQnmzIeBCQoPqeMTirhmyql+odWGooaTrVs3/Tas MXqOmoUZPpUsdVIOh8s4PXwsVdlcgubWYv3d6i7FHgLXoFq4BZovkO974h7JFyHx3R 61cp9Njjo/1f/SU8znL5crXoSeJ3n/m+V2kLLKxyaGPgZvGbOrKq2SpsAU5nSFevqbuREgQ== Content-Type: multipart/mixed; boundary="----=_NextPart_000_011C_01D168EE 8AEF0380"
 Received-Spf: neutral (google.com: 2a00:1450:400c:cog::235 is neither permitted nor denied by best guess record for domain of JulieJulieJulie@outlook.com) client-ip=2a00:1450:400c:cog::235;
 Delivered-To: mumsmith@gmail.com
 Content-Language: sr-me Java Locale Serbian (Montenegro) (sr-ME)

Received: by 10.27.224.10 with SMTP id k10csp1737087wlg; Tue, 16 Feb 2016 10:15:55 -0800 (PST)
 Received: from mail-wmo-x235.google.com (mail-wmo-x235.google.com [2a00:1450:400c:cog::235]) by mx.google.com with ESMTPS id fa10si50358496wjd.246.2016.02.16.10.15.54 for <mumsmith@gmail.com> (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128); Tue, 16 Feb 2016 10:15:55 -0800 (PST)

Received: by mail-wmo-x235.google.com with SMTP id b205s0122246482wmb.1 for <mumsmith@gmail.com>; Tue, 16 Feb 2016 10:15:54 -0800 (PST)
 Received: from Recepjija ([95.155.60.218]) by smtp.gmail.com with ESMTPSA id v66sm21581736wmb.18.2016.02.16.10.15.52 (version=TLSv1/SSLv3 cipher=OTHER); Tue, 16 Feb 2016 10:15:53 -0800 (PST)

Domain tools who is look up identifies IP address as registered to ISP telekom.me

Indicates sender Google mail server (SMTP)

Date and Time email sent 10:15:53 Timezone is -0800 PST

Appendix D – Guidelines for conducting initial investigations in computer related crimes and how to deal with digital evidence.

Appendix D is intended to form the basis of a handbook for investigation of cybercrime cases when receiving initial reports of computer crimes or computer related crime and at the initial crime scene attendance.

It is also intended to enable investigators to be able to make preliminary investigations into email addresses, IP addresses and website hosting locations and registration, as digital evidence crosses over with all forms of crime.

Each of the guidelines deals with a specific area:

-  Citizen complaint of computer crime or computer related crime;
-  Obtaining Evidence from a Business affected by computer crime - Digital Media Networks, Computers, Laptops, Data/Media Storage and Mobile Devices;
-  Investigating Crimes Involving Digital Media - Computers, Laptops and Data/Media Storage Devices;
-  Investigating Crimes Involving Digital Media - Smartphones and other mobile devices;
-  Managing and seizing evidence related to Child Abuse Images (Child Pornography) Investigation held on Digital Media;
-  Obtaining data from National and Multinational Internet service providers

Guideline, Citizen Complaint of computer crime or computer related crime

Citizen reporting of computer crime or computer related crime

This guide is to support a Public Prosecutor and Police Officer receiving an initial crime complaint, a citizen or small business that involves digital evidence and how to securely and lawfully preserve and obtain evidence from a Victims Digital Device such as a Phone, Computer or Data/Media Storage. (For additional information on organisations and businesses that have large networks and servers see Business or Large Organisation complaint of computer crime).

Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device. Text messages, SMS, Contacts, calls to and from a device, emails, pictures, videos, files and internet searches are some of the most common types of digital evidence.

A suspect's interaction with another electronic device while performing computer crimes or computer enabled crimes will leave a digital forensic trace.

Digital Evidence/Prosecutor actions	Investigation process
<p><i>The case is reported to the Prosecutor:</i></p> <p><i>Prosecutor:</i> At this moment Prosecutor is informed for the case and Prosecutor issuing an order to the judicial police to collect information about the reported case.</p>	<ul style="list-style-type: none"> • Criminal Intent; • Location and time of crime; • Relationship with victim(s); • Relationship with other suspect(s); • Evidence of crime
<p><i>The Report with information about the case is submitted to the Prosecutor. Prosecutor:</i></p> <ul style="list-style-type: none"> - <i>Identifying the criminal act that should be investigated.</i> - <i>Identifying if the evidence could be obtained in electronic or paper form</i> - <i>Identifying the legal authority who hold the evidence, Prepare Order for preservation and disclosing of evidence</i> - <i>If some of the evidence are stored on the computer, Issuing Order to seizing the device and Order for forensics examination of the devices.</i> <p><i>Additional:</i></p> <p><i>Prosecutor could request collection and recording the data from Open source (OSINT)</i></p>	<ol style="list-style-type: none"> 1. Identify the offence and points to prove; 2. Identify the evidence required to prove the offence; 3. Identify legal authority to seize the evidence; 4. Identify whether the victims evidence can be provided electronically or in paper print-outs; 5. Evidence seizure of documents or electronic evidence ; OR 6. Does the device need to be imaged and examined? 7. Obtain written authorisation from the victim to examine the device. 8. To deal with seizing and preserving evidence on a digital device? - Go To Status of Device:

<p>Important:</p> <p>The correct preservation and collection of evidence including digital evidence is important.</p> <p>Is the crime happening now or has it already happened? Is there an element here that is time critical, e.g. data being remotely deleted, threat to life?</p>	
<p>Status of Device: <i>Is the Electronic/Digital Device On or Off?</i></p>	<p>Device Powered On – Go to 10. Device Powered Off – Go to 18.</p>
<p>Device Powered On:</p> <p>Prosecutor:</p> <p><i>Prosecutor need to advice, if the computer is power off, do not turn it on.</i></p> <p><i>Prosecutor could request seizing computer data if computer is power on and there is risk data to be lost after power off.</i></p> <p><i>Prosecutor need to advise the investigative team to document every action on the scene during the search and seizing</i></p> <p><u>DO NOT TAKE ANY ACTION THAT MAY CHANGE DATA</u></p> <p><i>The correct preservation and collection of evidence including digital evidence is important.</i></p> <p><i>Is evidence displayed on the device?</i></p> <p><i>If the crime involves someone communicating with another i.e. Fraud, Threats, Ransomware, the judicial police should make sure that they are not further communicating without first consulting the matter with the Public Prosecutor.</i></p> <p><i>What will be lost if the network is disconnected?</i></p> <p><i>What effect will using the device to obtain evidence have on your investigation?</i></p> <p><i>Is Malware deleting or corrupting data?</i></p>	<p><u>DO NOT POWER OFF DEVICE</u> - It will change evidence.</p> <p>9. In the event any changes are made, accidentally or intentionally, record time, date and the action with detail of the change that occurred;</p> <p>10. If there is a visible display on the screen of the evidence, take photographs and notes of any material on the computer screen and software programmes displayed in the task bar;</p> <p style="text-align: center;">Visual inspection only</p> <p><u>Do Not be tempted to navigate the computer using the mouse or keyboard.</u></p> <p>11. Request any charger or manuals for the device;</p> <p>12. Ask Victim for password and/or PIN number of device and other security features such as biometrics or in the case of encryption ask victim for password/passphrase and retain record of the details.</p> <p>13. To Prevent Remote Data Changes – consider isolating the device from Ethernet, Wi-Fi or communication network. With a mobile device or laptop, if competent, consider changing setting to airplane mode and record actions;</p> <p>14. Not sure whether to close down the device or disconnect the power? <u>If not confident or competent to conduct actions at 12 or 13, seek assistance from an experienced technician – CCIU/DFU..</u></p>

	<p>15.If there is an indication that the computer has malware installed that is wiping or corrupting data from the hard drive, <u>disconnect the device immediately from its power source</u>, in the case of a laptop or mobile device also remove the battery. Record the reason and actions you have taken.</p> <p>16.Go To Seize Device.</p>
<p>Device Powered Off?</p> <p>Prosecutor need to advice, if the computer is power off, do not turn it on.</p> <p>Prosecutor need to advice the investigative team to document every action on the scene during the search and seizing</p> <p>Give advice to the investigator to obtain all the credential for the seized equipment</p>	<p><u>DO NOT TURN IT ON</u> it will change evidence.</p> <p>17.Ask victim for passwords, establish if device is encrypted ask victim for password/passphrase;</p> <p>18.Obtain the device charger and manuals.</p> <p><u>DO NOT TAKE ANY ACTION THAT MAY CHANGE DATA</u></p> <p>19.In the event any changes are made, accidentally or intentionally, record time, date and the action with detail of the change that occurred.</p> <p>20.Go to Seize Device.</p>
<p>Data and Media Storage Devices:</p> <p>Examples of these devices include, Hard Drives (USB/Wireless) USB Memory sticks, DVD, SD cards etc.</p> <p>Prosecutor need to advice the investigative team to document every action on the scene during the search and seizing</p>	<p>21.If the device is 'powered on' or connected to a live computer that is 'powered on' then any removal may make changes to the data and/or cause the data to be lost. Deal with the device as at Action 12-14.</p> <p>22. If the device is isolated and/or powered off Action as at 16-18.</p> <p>23.Go to Seize Device.</p>
<p>Smartphone or Mobile Devices Communication Data:</p> <p>(IMEI - International Mobile Equipment Identity) IMSI - International Mobile Subscriber Identity)</p> <p>Prosecutor is issuing an Order for disclosing telephone communication from the National telephone operator for the identified telephone number and some more information for the IMEI number</p>	<p>24.Obtain from victim device identifiers:</p> <ul style="list-style-type: none"> • Telephone number • IMEI number • IMSI number; <p>25.Written consent from victim to obtain communication data from CSP Communication Service Provider and/or Internet Service Provider.</p>

<p>Social Network/Auction/ Shopping/ Email Providers:</p> <p>Email and Social Media evidence with consent from the victim can be acquired from the victim's mailbox or account.</p> <p>Traffic Data and Logs relating to email etc. held by the CSP or Social Network Site (SNW) can only be obtained by PP/Court.</p> <p>Most CSP and SNW have law enforcement guidance pages on their websites of what data they retain and for how long.</p> <p>Prosecutor need to issue order for preservation data if the data are hold by multinational internet service provider.</p> <p>Prosecutor need to issue an order for disclosing of data if the data are hold by national internet service provider</p>	<p>26.Does the victims' account already hold digital evidence of the crime?</p> <p>27.Yes – establish how it can be downloaded as evidence with the victims' consent. Consider best method for capturing evidence files/video?</p> <p>28.Establish whether victim can obtain the data for evidence as part of terms and conditions.</p> <p>29.Social Network Sites/Auction/Shopping sites - Obtain from victim their Username, Account name and Account unique identification number;</p> <p>30.Email Accounts - Obtain from victim account name and email addresses;</p> <p>31.Identify dates relating to the criminal offences;</p> <p>32.Obtain from the victim written consent to obtain data from these service providers;</p>
<p>Seize Device:</p> <p>WARNING – It may be necessary to collect other forensic evidence including fingerprints, biological samples, DNA, etc. from devices. Consult with scene of crime forensic officers to preserve evidence and the integrity of the data on the device.</p> <p>Prosecutor need to issues an order for forensic examination of the seized equipment.</p>	<p>33.Inform victim why the device is being seized and for how long;</p> <p>34.Obtain written consent from victim for forensic examination of device;</p> <p>35.Seize and Package device in accordance with SOP/Law;</p> <p>36.Consider requesting other computers or storage devices that may contain device backups;</p> <p>37.Package the device so it will not be physically damaged or deformed;</p> <p>38.Package the device in evidence bags or boxes;</p> <p>39.Hazardous material on the device must be detailed on the packaging and the DFU informed.</p>
<p>Prosecutor need to issues an order for forensic examination of the seized equipment.</p> <p>This process should be fast in order not some evidence to be lost</p>	<p>40.Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as possible;</p>

	<p>41.Protect from extreme temperatures, static electricity, magnetic fields or moisture.</p> <p>42.Retain Audit record for continuity of evidence.</p>
<p><i>Prosecutor need to issues an order for forensic examination of the seized equipment.</i></p> <p><i>The order from prosecutor should be concrete what evidence should be searched.</i></p> <p><i>The order should have exact description and serial number of each exhibits</i></p>	<p>43.Inform of the PP of Criminal offences identified and Procedures Undertaken.</p> <p>44.Obtain Authorisation/Order from PP for further investigation.</p>
<p>Prosecutor could follow the process of digital forensics and extracting of digital evidence</p>	<p>If devices have been seized for Digital Forensic Imaging or Examination; inform DFU of the seized material and investigation decisions of the Public Prosecutor.</p>

Obtaining Evidence from a Business affected by computer crime - Digital Media Networks, Computers, Laptops, Data/Media Storage and Mobile Devices

Business or Large Organisation complaint of computer crime or computer related crime Digital Media Networks, Computers, Data, Mobile Devices and Malware Attacks

Businesses and large Public or Private Organisations are likely to face computer crimes the same as a citizen, but will also be vulnerable to hacking and malware attacks. Some of these attacks will be to businesses and organisations that form part of the National Critical Infrastructure of Albania; others will face financial impact from the attack and may be reluctant to report the crime. In these cases it is important for the Public Prosecutor, CCIU to be informed of the crime at the earliest opportunity.

Businesses and large organisations often need to be dealt with differently when they are victims of computer crime or computer related crime, it can be harmful to their business to remove devices from the workplace, it will also be commercially harmful to remove the business from networks or the Internet for the purpose of acquiring evidence.

In most cases it will be necessary to identify key individuals responsible for the business (CEO) and the digital networks and infrastructure responsible for dealing with a 'cyber incident' (contracted or in-house network manager/engineer/administrator) and consult with them at an early stage along with the CCIU/DFU and the Public Prosecutor.

During a cyber-incident, a victim organisation should immediately make an assessment of the nature and scope of the incident to determine whether the incident is a malicious act or a technological glitch.

Digital Media Smartphones, Computers, Servers and Data Storage Devices will contain Digital Evidence. Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device.

A suspect's interaction with another electronic device while performing computer crimes or computer enabled crimes will leave a digital forensic trace.

Digital Evidence/Prosecutor actions	Investigation process
<p>The case is reported to the Prosecutor:</p> <p>Prosecutor:</p> <p>At this moment Prosecutor is informed for the case and Prosecutor issuing an order to the judicial police to collect information about the reported case.</p> <p>Companies devices and networks may contain critical information to prove a criminal act.</p>	<ul style="list-style-type: none">• Identify - Criminal Intent;• Location and time of crime;• Relationship with victim(s);• Relationship with other suspect(s);• Evidence of crime.

<ul style="list-style-type: none"> - <i>Identifying the criminal act that should be investigated.</i> - <i>Identifying if the evidence could be obtained in electronic or paper form</i> - <i>Identifying the legal authority who hold the evidence, Prepare Order for preservation and disclosing of evidence</i> - <i>If some of the evidence are stored on the computer, Issuing Order to seizing the device and Order for forensics examination of the devices.</i> - <i>Identifying what expert profile to involve in the process of identifying and seize electronic evidence</i> - <i>Prosecutor should give order to seize the computer data, doing live forensics or seizing entire equipment that have electronic evidence</i> <p><i>Identify key persons from Organisation;</i></p> <p><i>Ensuring the Preservation and Collection of evidence including digital evidence is important</i></p>	<ol style="list-style-type: none"> 1. Identify the offence; 2. Identify person responsible/decision makers, accountable for any actions that may directly impact on the business : <ul style="list-style-type: none"> • Business (CEO/Manager/Owner) • Network and Infrastructure (Network Manager, Network Engineer network Administrator); • Managing a Cyber Incident. • Third party service providers engaged by the company to provide elements of the network and business infrastructure that is being attacked (ISP's, CSP's, Remote or Cloud software or data storage etc.); 3. Identify where the evidence is; 4. Identify legal authority to seize/examine the evidence; 5. Secure the scene; 6. Identify whether the victims evidence needs to be provided by; <ul style="list-style-type: none"> • Electronically; • Print-outs; 7. Does the device need to be seized, imaged and/or examined on-site or can it be taken off site? <ul style="list-style-type: none"> • Forensic Image (DFU); • Live Forensic Imaging (DFU); • Live Forensics (DFU). 8. Evidence - seizure of documents or electronic evidence to follow SOP; OR 9. Obtain written authorisation from the victim to seize and examine the device. 10. To deal with seizing and preserving evidence on a digital device? - Go To Status of Device:
<p><i>Prosecutor/investigator is following the actions taken by the Network Manager/Engineer/Administrator</i></p> <p><i>NO action should destroy any electronic evidence</i></p> <p><i>If needed Prosecutor is issuing an order to seize some computer data for analysis (usually server logs)</i></p>	<ol style="list-style-type: none"> 11. Establish whether the business has a cyber-incident response plan. 12. Request they keep an ongoing, written record of all steps undertaken, where practicable. 13. Do they have appropriate network logging capabilities enabled as these can be critical to identifying the cause of the cyber incident? 14. In case of a sustained attack, request that consideration be given to increasing the default size of log files on its servers to prevent losing data. 15. Request preservation of relevant existing logs.

The preservation and collection of evidence including digital evidence is important

The isolation of any cyber-attack is a business priority!

Prosecutor need to advise the investigative team to document every action on the scene during the search and seizing

16. Using log information, a system administrator should attempt to identify:
 - The affected computer systems;
 - The apparent origin of the incident, intrusion, or attack;
 - Any malware used in connection with the incident;
 - Any remote servers to which unauthorized data was/is being sent; and
 - The identity of any other victim organizations, if such data is apparent in logged data.
17. Establish and document:
 - Which users are currently logged on;
 - What the current connections to the computer systems are;
 - Which processes are running; and
 - All open ports, their associated services and applications.
18. Any communications (in particular, threats or extortion demands) received by the organization that might relate to the incident should be provided to Police and also be preserved;
19. Suspicious calls, emails, or other requests for information should be treated as part of the incident and preserved as evidence;
20. Document and preserve evidence that an intrusion or other criminal incident has occurred, this will typically be:-
 - Logging or file creation data indicating that someone improperly accessed,
 - created,
 - modified,
 - deleted or copied files or logs;
 - changed system settings; or
 - Added or altered user accounts or permissions.
21. The victim organisation should be requested to ensure that its actions do not unintentionally or unnecessarily:

	<ul style="list-style-type: none"> • Modify stored data in a way that could hinder incident response or subsequent criminal investigation; • relevant files should not be deleted, if at all possible; • avoid modifying data or if absolutely necessary to modify data keep an audit record of how and when information was modified. <p><i>The company may make a “forensic image” of the affected computers, which will preserve a record of the system at the time of the incident for later analysis and potentially for use as evidence at trial – PP/CCIU/DFU should be informed of this action.</i></p>
<p>Prosecutor:</p> <p>Prosecutor need to advice, if the computer is power off, do not turn it on.</p>	<p>In most cases involving businesses the CCIU/DFU will take over the investigation at this stage guided by the Prosecutor, however if this support is not available you may need to consider the following stages of action:</p> <p>Device(s) Powered On – Go to 22.</p> <p>Device(s) Powered Off – Go to 30.</p>
<p>Prosecutor:</p> <p>Prosecutor need to advice, if the computer is power off, do not turn it on.</p> <p><u>DO NOT TAKE ANY ACTION THAT MAY CHANGE DATA</u></p> <p><u>Important:</u></p> <p><u>The preservation and collection of evidence including digital evidence is important</u></p>	<p style="text-align: center;">DO NOT POWER OFF DEVICE</p> <p style="color: red; text-decoration: underline;"><i>It will change evidence it may also damage the victims business.</i></p> <p class="list-item-l1">22. In the event any changes are made, accidentally or intentionally, record time, date and the action with detail of the change that occurred;</p> <p class="list-item-l1">23. If there is a visible display on the screen of the evidence, take photographs and notes of any material on the computer screen and software programmes displayed in the task bar; Visual inspection only <i>Do Not be tempted to navigate the computer using the mouse or keyboard.</i></p> <p class="list-item-l1">24. Request any charger or manuals for the device;</p> <p class="list-item-l1">25. Ask Victim for password and/or PIN number of device and other security features such as biometrics or in the case of encryption ask victim for password/ passphrase and retain record of the details.</p> <p class="list-item-l1">26. To Prevent Remote Data Changes – consider isolating the device from Ethernet, Wi-Fi or communication network. With a mobile device or laptop, if competent, consider changing setting to airplane mode and record actions;</p>

<p>Remote Access or Remote Data – could make Changes</p> <p>Malware Attack – Data could be wiped or corrupted.</p> <p><u>Qasja në Largësi ose Të Dhënata në Largësi mund të shkaktojnë ndryshime</u></p> <p><u>Sulm nga Programe Keqdashëse – Mund të fshihen apo korruptohen të dhëna.</u></p>	<p>27. Not sure whether to close down the device or disconnect the power?</p> <p>Firstly and urgently consult with business owner & Network Manager before disconnecting devices or networks immediately from its power source,</p> <p>If not confident or competent to conduct actions at 13 or 14, seek assistance from an experienced technician – contact the CCIU/DFU.</p> <p>28. If there is an indication that the computer has malware installed that is wiping or corrupting data from the hard drive, urgently consult with business owner & Network Manager before disconnecting devices or networks immediately from its power source, in the case of a laptop or mobile device also remove the battery. Record the reason and actions you have taken.</p> <p>29. Go To Seize Device</p>
<p>Device Powered Off?</p> <p>Prosecutor need to advice, if the computer is power off, do not turn it on.</p> <p>Giving instructions equipment to be properly seized, packed and labelled.</p>	<p>DO NOT TURN IT ON it will change evidence.</p> <p>30. Ask victim for passwords, establish if device is encrypted ask victim for password/passphrase;</p> <p>31. Obtain the device charger and manuals.</p> <p>DO NOT TAKE ANY ACTION THAT MAY CHANGE DATA</p> <p>32. In the event any changes are made, accidentally or intentionally, record time, date and the action with detail of the change that occurred.</p> <p>33. Go to Seize Device.</p>
<p>Data and Media Storage Devices:</p> <p>Examples of these devices include, Hard Drives (USB/Wireless) USB Memory sticks, DVD, SD cards etc.</p>	<p>34. If the device is powered on or connected to a live computer ‘powered on’ then any removal may make changes to the data and/or cause the data to be lost. Deal with the device as at Action 23-29.</p> <p>35. If the device is isolated and/or powered off; deal with the device as at 30-33.</p> <p>36. Go to Seize Device.</p>
<p>Smartphone or Mobile Devices Communication Data:</p> <p>(IMEI - International Mobile Equipment Identity)</p>	<p>37. Obtain from victim device identifiers:</p> <ul style="list-style-type: none"> • Telephone number

<p>IMSI - International Mobile Subscriber Identity)</p> <p>Prosecutor is issuing an Order for disclosing telephone communication from the National telephone operator for the identified telephone number and some more information for the IMEI number</p>	<ul style="list-style-type: none"> • IMEI number • IMSI number; <p>38. Written consent to obtain communication data from CSP Communication Service Provider and/or Internet Service Provider.</p> <p>39. If phone seizure is necessary - Go to Seize Device.</p>
<p>Seize Device:</p> <p>WARNING – You may need to collect other forensic evidence including fingerprints, biological samples, DNA, etc. from devices. Consult with scene of crime forensic officers to preserve evidence and the integrity of the data on the device.</p>	<p>40. Inform victim why the device is being seized and why;</p> <p>41. Obtain written consent from victim for forensic examination of device;</p> <p>42. Seize and Package device in accordance with SOP/Law;</p> <p>43. Consider requesting other computers or storage devices that may contain device backups;</p> <p>44. Package the device so it will not be physically damaged or deformed;</p> <p>45. Package the device in evidence bags or boxes;</p> <p>46. Hazardous material on the device must be detailed on the packaging and DFU informed.</p>
<p>Prosecutor need to issues an order for forensic examination of the seized equipment.</p> <p>This process should be fast in order not some evidence to be lost</p>	<p>47. Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as possible;</p> <p>48. Protect from extreme temperatures, static electricity, magnetic fields or moisture.</p> <p>49. Retain Audit record for continuity of evidence.</p>
<p>Prosecutor need to issues an order for forensic examination of the seized equipment.</p> <p>The order from prosecutor should be concrete what evidence should be searched.</p> <p>The order should have exact description and serial number of each exhibits</p>	<p>50. Inform of Criminal offences and Procedures Undertaken.</p> <p>51. Obtain authorisation/Order for further investigation.</p>
<p>Prosecutor could follow the process of digital forensics and extracting of digital evidence</p>	<p>52. If devices have been seized for Digital Forensic Imaging or Examination; inform DFU of the seized material and investigation decisions of Public Prosecutor.</p>

Investigating Crimes Involving Digital Media - Computers, Laptops and Data/Media Storage Devices

INVESTIGATING CRIMES INVOLVING DIGITAL MEDIA - COMPUTERS, LAPTOPS

Digital Media Computers and Data Storage Devices will contain Digital Evidence.

Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device. Instant messaging, emails, files, pictures and videos, and internet searches are some of the most common types of digital evidence.

Suspects in computer crimes or computer enabled crimes will leave a digital forensic trace on their device and the victim's device.

Digital Evidence/ Prosecutor actions	Investigation process
<p><i>The case is reported to the Prosecutor:</i></p> <p><i>Prosecutor:</i></p> <p><i>At this moment Prosecutor is informed for the case and Prosecutor issuing an order to the judicial police to collect information about the reported case.</i></p>	<p>Conduct Criminal Investigation to identify:</p> <ul style="list-style-type: none"> • Criminal Intent; • Location and time of crime; • Relationship with victim(s); • Relationship with other suspect(s); • Evidence of crime.
<p><i>The Report with information about the case is submitted to the Prosecutor.</i></p> <p><i>Prosecutor:</i></p> <ul style="list-style-type: none"> - <i>Identifying the criminal act that should be investigated.</i> - <i>If some of the evidence are stored on the computer, Issuing Order to seizing the device and Order for forensics examination of the devices.</i> 	<ol style="list-style-type: none"> 1. Secure the scene; 2. Do not allow the suspect near any devices or power sources; 3. Identify legal authority to seize the evidence; 4. Seize devices in accordance with evidence seizure SOP; 5. Ensure seized devices are not exposed to extreme temperatures, static electricity, magnetic fields or moisture; 6. Record details of the device and location and condition in which found; 7. Photograph or Video the device where found; 8. Make notes of where found and from whom seized;

<p>Important: The correct preservation and collection of evidence including digital evidence is important.</p> <p><i>Is the crime happening now or has it already happened? Is there an element here that is time critical, e.g. data being remotely deleted, threat to life?</i></p>	<p>9. Maintain a chain of custody;</p> <p>10. Consider informing the Public Prosecutor, CCIU and DFU if there are significant impact and risks to this crime.</p>
<p>Status of Device: <i>Is the Electronic/Digital Device On or Off?</i></p>	<p>Device Powered On – Go to 11. Device Powered Off – Go to 20.</p>
<p>Device Powered On:</p> <p>NOTE – Many computer devices save power by turning off screens or reverting to sleep mode after a specified amount of time. Despite the screen status, the device is likely still active; actions such as opening the lid of a laptop can re-initiate the device.</p> <p><u>DO NOT TAKE ANY ACTION THAT MAY CHANGE DATA</u></p>	<p>11. Determine if the device is on or off;</p> <ul style="list-style-type: none"> • Look for lights; • Listen for sounds; • Feel for vibrations or heat; • Ask if the device is powered on; • DO NOT POWER OFF DEVICE it will change evidence. <p>12. In the event any changes are made, accidentally or intentionally, record time, date and the action with detail of the change that occurred.</p> <p>13. If there is a visible display on the screen, take photographs and notes of any material on the computer screen and software programmes displayed in the task bar;</p> <p style="text-align: center;">Visual inspection only</p> <p style="color: red;"><u>Do Not be tempted to navigate the computer using the mouse or keyboard.</u></p> <p>14. Seize charger and manuals for device;</p> <p>15. Ask suspect for password of computer; identify biometrics or encryption security features; request and record the password/passphrase;</p>

<p>Prosecutor need to advice, if the computer is power off, do not turn it on.</p> <p>Giving instructions the equipment to be properly seized, packed and labelled.</p>	<ol style="list-style-type: none"> 16. <u>Prevent Data</u> change; if competent, consider isolating the device from Ethernet and Wi-Fi networks. With a laptop consider changing setting to airplane mode -record actions; 17. Not sure whether to close down the device or disconnect the power? <p>If not sufficiently competent to conduct any of the actions at 15 or 16, contact an experienced technician at the CCIU/ DFU.</p> <ol style="list-style-type: none"> 18. If there is an indication that the computer has anti-forensic software installed and it has been activated and is wiping data from the hard drive, <u>disconnect the device immediately from its power source</u>, in the case of a laptop also remove the battery. Record the reason and actions you have taken; 19. Go To Seize Device.
<p>Device Powered Off?</p> <p>NOTE – Many computer devices save power by turning off screens or reverting to sleep mode after a specified amount of time. Despite the screen status, the device is likely still active; actions such as opening the lid of a laptop can re-initiate the device.</p>	<p><u>DO NOT TURN IT ON</u> it will change evidence.</p> <ol style="list-style-type: none"> 20. Ask suspect for password; 21. Seize any charger or manuals for the device; 22. Establish if device is encrypted if it is ask the suspect for password/passphrase; <p><u>DO NOT TAKE ANY ACTION THAT MAY CHANGE DATA</u></p> <p>In the event any changes are made, accidentally or intentionally, record time, date and the action with detail of the change that occurred.</p>
<p>Data and Media Storage Devices:</p> <p>Examples of these devices include, Hard Drives (USB/Wireless) USB Memory sticks, DVD, SD cards etc.</p>	<ol style="list-style-type: none"> 23. If the device is powered on or connected to a live computer ‘powered on’ then any removal of an attached device may make changes to the data and/or cause the data to be lost. Deal with the device as at Action 11-19; 24. If the device is isolated and/or ‘powered off’. Deal with the device as at Action 20-22.
<p>Seize Device:</p> <p>WARNING – You may need to collect other forensic evidence including fingerprints, biological</p>	<ol style="list-style-type: none"> 25. Inform suspect that device is being seized and why; 26. Obtain written consent from suspect for forensic examination of device. 27. Seize and Package device in accordance with SOP/Law;

<p><i>samples, DNA, etc. from computer devices. Consult with scene of crime forensic officers to assist with 27-31 to preserve evidence without disturbing the integrity of the data on the device.</i></p>	<ul style="list-style-type: none"> 28. Consider seizing other computers or storage devices that may contain device backups; 29. Package the device so it will not be physically damaged or deformed; 30. Package the device in evidence bags or boxes; 31. Hazardous material on the device – Detail on the packaging and inform DFU.
<p><i>Prosecutor need to issues an order for forensic examination of the seized equipment.</i></p> <p><i>This process should be fast in order not some evidence to be lost</i></p>	<ul style="list-style-type: none"> 32. Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as possible; Storage of devices will be at the DFU; 33. Protect from extreme temperatures, static electricity, magnetic fields or moisture; 34. Retain Audit record for continuity of evidence.
<p><i>Prosecutor need to issues an order for forensic examination of the seized equipment.</i></p> <p><i>The order from prosecutor should be concrete what evidence should be searched.</i></p> <p><i>The order should have exact description and serial number of each exhibits</i></p>	<ul style="list-style-type: none"> 35. Inform of Criminal offences and Procedures Undertaken; 36. Property seized; 37. Obtain authorisation/Order for further investigation.
<p><i>Prosecutor could follow the process of digital forensics and extracting of digital evidence</i></p>	<ul style="list-style-type: none"> 38. Inform of seized material and decisions of Public Prosecutor.

Investigating Crimes Involving Digital Media - Smartphones and other mobile devices

INVESTIGATING CRIMES INVOLVING DIGITAL MEDIA – SMARTPHONES, TABLETS AND MOBILE DEVICES.

Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device. Text messages, SMS, Contacts, calls to and from a device, emails, pictures and videos, and internet searches are some of the most common types of digital evidence found in Smartphones, Tablets and other mobile devices.

Suspect's devices connecting with a victim's device will leave a forensic trace at a number of stages of communication.

Digital Evidence/Prosecutor actions	Investigation process
<p>The case is reported to the Prosecutor:</p> <p>Prosecutor:</p> <p>At this moment Prosecutor is informed for the case and Prosecutor issuing an order to the judicial police to collect information about the reported case.</p> <p>Criminals now leave a digital trail:</p> <p>A suspect's phone or mobile device will contain files that provide critical information as points to prove in a criminal investigation: -</p>	<ul style="list-style-type: none"> • Criminal Intent; • Location and time of crime; • Relationship with victim(s); • Relationship with other suspect(s); • Evidence of crime.
<p>The Report with information about the case is submitted to the Prosecutor. Prosecutor:</p> <p>- Identifying the criminal act that should be investigated.</p>	<ol style="list-style-type: none"> 1. Secure the scene; 2. Do not allow the suspect near any devices or power sources; 3. Identify legal authority to seize the evidence; 4. Seize devices in accordance with normal evidence seizure procedures;

<p>- If some of the evidence are stored on the computer, Issuing Order to seizing the device and Order for forensics examination of the devices.</p>	<ol style="list-style-type: none"> 5. Ensure seized devices are not exposed to extreme temperatures, magnetic fields or moisture; 6. Record details of the device and location and condition in which found; 7. Photograph or Video the device where found. 8. Make notes of where found and from whom seized; 9. Maintain a chain of custody. 10. Consider informing the Public Prosecutor, CCIU and DFU if there are significant impact and risks to this crime.
<p>Status of Device:</p> <p><i>Is the Electronic/Digital Device On or Off?</i></p>	<p>Device Powered On – Go to 11.</p> <p>Device Powered Off – Go to 19.</p>
<p>Device Powered On:</p> <p><i>NOTE – Many mobile devices save power by turning off screens after a specified amount of time. Despite the screen status, the device is likely to still be active.</i></p> <p><u>DO NOT TAKE ANY ACTION THAT MAY CHANGE DATA</u></p> <p><i>Prosecutor need to advice, if the computer is power off, do not turn it on.</i></p> <p><i>Giving instructions the equipment to be properly seized, packed and labelled.</i></p>	<ol style="list-style-type: none"> 1. Determine if the device is on or off; <ul style="list-style-type: none"> • Look for lights; • Listen for sounds; • Feel for vibrations or heat; • Ask if the device is powered on; • DO NOT POWER OFF DEVICE it will change evidence. 2. In the event any changes are made, accidentally or intentionally, record time, date and the action with detail of the change that occurred. 3. Seize any charger or manuals for the device; 4. Ask suspect for password and/or PIN number and other security features of phone, retain record of details; 5. Prevent Data Emanation - Isolate the device from cellular and Wi-Fi networks using Faraday Bags or wrapping in foil; SCFU to assist here; 6. If competent consider and it is essential to prevent phone from connecting to a network, consider changing phone setting to airplane mode and record actions; 7. If not competent seek assistance from an experienced technician from CCIU/DFU. 8. Go To Seize Device.

<p>Prosecutor need to advice, if the computer is power off, do not turn it on.</p> <p>Giving instructions the equipment to be properly seized, packed and labelled.</p>	<p>NOTE: Many mobile devices save power by turning off screens after a specified amount of time. Despite the screen status, the device is likely still active.</p> <p>DO NOT TURN IT ON it will change evidence.</p> <ol style="list-style-type: none"> 9. Ask suspect for password and/or PIN number; 10. Seize any charger or manuals for the device.
<p>Seize Device:</p> <p>WARNING – You may need to collect other forensic evidence including fingerprints, biological samples, DNA, etc. from smartphones and mobile devices. Consult with crime forensic officers to assist with 22-26 to preserve evidence without disturbing the integrity of the data on the device.</p>	<ol style="list-style-type: none"> 11. Inform suspect that device is being seized and why; 12. Obtain written consent from suspect for forensic examination of device; 13. Seize and Package device in accordance with SOP/Law; 14. Consider seizing computers or devices that may contain device backups; 15. Package the device so it will not be physically damaged or deformed; 16. Package the device in evidence bags or boxes; 17. Hazardous material on the device? – Detail on the packaging and inform the DFU.
<p>Prosecutor need to issues an order for forensic examination of the seized equipment.</p> <p>This process should be fast in order not some evidence to be lost.</p>	<ol style="list-style-type: none"> 18. Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as possible; Storage of devices will be at the DFU; 19. Protect from extreme temperatures, static electricity, magnetic fields or moisture; 20. Retain Audit record for continuity of evidence.
<p>Prosecutor need to issues an order for forensic examination of the seized equipment.</p> <p>The order from prosecutor should be concrete what evidence should be searched.</p> <p>The order should have exact description and serial number of each exhibits</p>	<ol style="list-style-type: none"> 21. Inform of Criminal offences and Procedures Undertaken; 22. Obtain authorisation/Order for further investigation.

Prosecutor could follow the process of digital forensics and extracting of digital evidence

23. Inform of seized material and action any decisions of Public Prosecutor.

Managing and seizing evidence related to Child Abuse Images (Child Pornography) Investigation held on Digital Media

Seizing Digital Media - Child Abuse Images (Child Pornography) Investigation.

Digital Media will contain Digital Evidence. Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device. Text messages, emails, pictures and videos, files, documents and internet searches are some of the most common types of digital evidence.

Suspects in Child Exploitation investigations often use private communication, private file sharing (P2P), file storage techniques and encryption to disguise and hide their actions with accomplices.

The Public Prosecutor should be contacted at the earliest opportunity and provided with an outline of the crime, crime, the impact, any vulnerable persons and any risks.

Digital Evidence/Prosecutor actions	Investigation process
<p><i>The case is reported to the Prosecutor:</i></p> <p><i>Prosecutor:</i></p> <p><i>At this moment Prosecutor is informed for the case and Prosecutor issuing an order to the judicial police to collect information about the reported case.</i></p>	<p>Criminal Investigation to identify:</p> <ul style="list-style-type: none"> • Criminal Intent; • Location and time of crime; • Relationship with victim(s); • Relationship with other suspect(s); • Evidence of crime.
<p><i>The Report with information about the case is submitted to the Prosecutor. Prosecutor:</i></p> <ul style="list-style-type: none"> - <i>Identifying the criminal act that should be investigated.</i> - <i>Identifying if the evidence could be obtained in electronic or paper form</i> - <i>Identifying the legal authority who hold the evidence, Prepare Order for preservation and disclosing of evidence</i> 	<ol style="list-style-type: none"> 1. Secure the scene; 2. Do not allow the suspect near any devices or power sources; 3. Seize evidence - Identify legal authority; 4. Seize devices in accordance with normal evidence seizure SOP's; 5. Ensure seized devices are not exposed to extreme temperatures, static electricity, magnetic fields or moisture; 6. Record details of the device and location and condition in which found; 7. Photograph or Video the device where found;

<ul style="list-style-type: none"> - If some of the evidence are stored on the computer, Issuing Order to seizing the device and Order for forensics examination of the devices. <p>Additional: <i>Prosecutor could request collection and recording the data from Open source (OSINT)</i></p> <p>Important: <i>The correct preservation and collection of evidence including digital evidence is important.</i></p> <p><i>Is the crime happening now or has it already happened? Is there an element here that is time critical, e.g. data being remotely deleted, threat to life?</i></p>	<ol style="list-style-type: none"> 8. Make notes of where found and from whom seized; 9. Maintain a chain of custody.
<p>Status of Device:</p> <p>Is the Electronic/Digital Device On or Off?</p>	<p>Refer to:</p> <p>Seizing Digital Media - Smartphones and other mobile devices.</p> <p>Seizing Digital Media - Computers, Laptops & Data/Media Storage Devices.</p>
<p><i>Prosecutor could issue an order for seizing computer data or perform Live data forensics</i></p> <p>Important:</p> <p>Peer-to-Peer (P2P) Application Software:</p> <p><i>P2P is commonly used by suspects to share child Exploitation Images; individuals in these networks maintain "libraries" of images for others to share.</i></p> <p><i>Popular P2P software is Gnutella, Fast-Track, BitTorrent, eDonkey, Limewire and Freenet.</i></p>	<ol style="list-style-type: none"> 10. Look for P2P software displayed on the device screen or device toolbar; 11. Ask suspect for IP addresses, account ID's/ passwords and any other security features of the P2P network such as encryption and retain record of details. <p style="text-align: center;">Visual inspection only</p> <p style="text-align: center;"><u>Do Not be tempted to navigate the computer using the mouse or keyboard.</u></p>

Encryption:

Suspects involved in the collection and distribution of Child Abuse Images (Child Pornography) often use encryption.

Prosecutor could issue an order for Live data forensics

Identifying what expert profile to involve in the process of identifying and seize electronic evidence

Prosecutor:

- *Identifying if the evidence could be obtained in electronic or paper form*
- *Identifying the legal authority who hold the evidence, Prepare Order for preservation and disclosing of evidence*
- *If some of the evidence are stored on the computer, Issuing Order to seizing the device and Order for forensics examination of the devices.*
- *Prosecutor should give order to seize the computer data, doing live forensics or seizing entire equipment that have electronic evidence*

Communication Method:

Social Media sites such as Facebook, Twitter etc. are communication methods for grooming in Child Pornography.

IRC (Internet Relay Chat) is still used as private communication between Child Exploitation Suspects. Popular IRC software is Freenode, IRCNet, QuakeNet, EFNet, Undernet & Rizon.

If device ON - DO NOT TURN IT OFF
Evidence may be lost - contact CCIU/DFU.

12. Ask suspect for password/passphrase;
13. If there is a visible display on the screen, take photographs and notes of any material on the computer screen and software programmes displayed in the task bar;

Visual inspection only

Do Not be tempted to navigate the computer using the mouse or keyboard.

14. Only a competent person or accredited Digital Forensic Examiner should undertake a 'Live' Digital Examination. Contact CCIU and DFU.
15. Look for Social Media/IRC software on the device display screen or displayed in the device toolbar;
16. Ask suspect for account ID's/passwords and any other security features of the communication method such as encryption and retain record of details.

Visual inspection only

Do Not be tempted to navigate the computer using the mouse or keyboard.

Data & Media Storage Devices:	Refer to: Seizing Digital Media - Computers, Laptops & Data/Media Storage Devices.
Seize Device(s): <i>WARNING – You may need to collect other forensic evidence including fingerprints, biological samples, DNA, etc. from computer devices. Consult with scene of crime forensic officers to preserve evidence without disturbing the integrity of the data on the device.</i>	<p>17. Inform suspect that device is being seized and why.</p> <p>18. Obtain written consent from suspect for forensic examination of device.</p> <p>19. Seize and Package device in accordance with SOP/Law;</p> <p>20. Consider seizing other computers or storage devices that may contain device backups;</p> <p>21. Package the device so it will not be physically damaged or deformed;</p> <p>22. Package the device in evidence bags or boxes;</p> <p>23. Hazardous material on the device – Detail on the packaging and inform DFU.</p>
<i>Prosecutor need to issues an order for forensic examination of the seized equipment.</i> <i>This process should be fast in order not some evidence to be lost</i>	<p>24. Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as possible;</p> <p>25. Protect from extreme temperatures, static electricity, magnetic fields or moisture;</p> <p>26. Retain Audit record for continuity of evidence.</p>
<i>Prosecutor need to issues an order for forensic examination of the seized equipment.</i> <i>The order from prosecutor should be concrete what evidence should be searched.</i> <i>The order should have exact description and serial number of each exhibits.</i>	<p>27. Inform of Criminal offences and Procedures Undertaken;</p> <p>28. Obtain authorisation/Order for further investigation.</p>
<i>Prosecutor could follow the process of digital forensics and extracting of digital evidence</i>	<p>29. Inform of crime for specialist investigation advice and support.</p> <p>30. Inform of seized material and decisions of Public Prosecutor.</p>

Obtaining data from National and Multinational Internet service providers

Obtaining data from National and Multinational Internet service providers

As the investigation of cybercrime by law enforcement is often not effective without the cooperation of Internet service providers, it is essential that both cooperate with each other in an efficient manner.

The roles of both are different: law enforcement must uphold the law, while service providers are to provide users with the ability to communicate.

The question that many countries are faced with is how both can best cooperate with each other to make the Internet safer while at the same time respect their different roles and the fundamental rights of users. And very important how Internet service providers could support criminal investigation of cybercrime and cyber enable crimes.

Digital Evidence/Prosecutor actions	Process
<p><i>The case is reported to the Prosecutor:</i></p> <p><i>Prosecutor:</i></p> <p><i>At this moment Prosecutor is informed for the case and Prosecutor issuing an order to the judicial police to collect information about the reported case.</i></p> <p><i>Identifying the internet service provider that hold data/evidence for the case</i></p>	<ul style="list-style-type: none"> • Criminal Intent; • Location and time of crime; • Relationship with victim(s); • Relationship with other suspect(s); • Evidence of crime.
	<p>National Internet Service provider</p> <p>Internet service provider under other country jurisdiction</p> <p>Multinational Internet service provider (usually ISP under US jurisdiction)</p>
<p><i>Data hold by National internet service provider</i></p>	<ol style="list-style-type: none"> 1. Identify the national internet service provider; 2. Identify the address and responsible person for disclosing the needed data

<p>Prosecutor:</p> <ul style="list-style-type: none"> - <i>Identifying the criminal act that should be investigated.</i> - <i>Issuing request for preservation of data</i> - <i>Issuing request for disclosing of data (MLA)</i> 	<ol style="list-style-type: none"> 3. Check if the Internet service provider hold the needed type of data (according the company policy, regulation for protection of personal data, retention policy) 4. Create and send the request for preservation and disclosing of data 5. Analyse the received data 6. Decision if those data could be accepted as a admissible
<p>Data hold by internet service provider under other country jurisdiction</p> <p>Prosecutor:</p> <ul style="list-style-type: none"> - <i>Identifying the criminal act that should be investigated.</i> - <i>Issuing request for preservation of data</i> - <i>Issuing request for disclosing of data (MLA)</i> 	<ol style="list-style-type: none"> 1. Identify the internet service provider; 2. Identify the country/jurisdiction 3. Obtain the information if we have bilateral agreement for cooperation and exchange of evidence 4. Check if the Internet service provider hold the needed type of data (according the company policy, regulation for protection of personal data, retention policy) 5. Prepare request for preservation of data 6. Send the request for preservation of data by official channel 7. Use the police channel (24/7 Contact point) for sending the request 8. Start the process of MLA in order data to be disclosed and be admissible. 9. Analyse the received data
<p>Data hold by Multinational internet service provider</p> <p>Prosecutor:</p> <ul style="list-style-type: none"> - <i>Identifying the criminal act that should be investigated.</i> - <i>Issuing request for preservation of data</i> - <i>Issuing request for disclosing of data (MLA)</i> 	<ol style="list-style-type: none"> 1. Identify the Multinational internet service provider; 2. Identify the address and responsible person for disclosing the needed data 3. Check if the Internet service provider hold the needed type of data (according the company policy, regulation for protection of personal data, retention policy) 4. Check the Provider policy for cooperation with Law enforcement agency 5. Create and send a request for preservation of data 6. Create and send a request for disclosing of data 7. Analyse the received data 8. Decision if those data could be accepted as a admissible

	<p>Preservation request</p> <p>Request for disclosing of data (MLA request)</p>
<p>Request for preservation of data</p> <p>Annex2</p>	<ol style="list-style-type: none"> 1. Identify the Multinational internet service provider; 2. Identify the address and responsible person for disclosing the needed data 3. Check if the Internet service provider hold the needed type of data (according the company policy, regulation for protection of personal data, retention policy) 4. Check the Provider policy for cooperation with Law enforcement agency (which data could be preserved) 5. Prepare the request for preservation of data
<p>Request for disclosing of data (MLA request)</p> <p>Annex3</p>	<ol style="list-style-type: none"> 1. Identify the Multinational internet service provider; 2. Identify the country/jurisdiction 3. Obtain the information if we have bilateral agreement for cooperation and exchange of evidence 4. Check if the Internet service provider hold the needed type of data (according the company policy, regulation for protection of personal data, retention policy) 5. Prepare request for preservation of data 6. Start the process of MLA in order data to be disclosed and be admissible. Use the police channel (24/7 Contact point) for sending the request (only to speed up the process of sending the request) 7. Send MLA request by official channel (Ministry of justice, Ministry of foreign affairs)
	<p>Subscriber data</p> <p>Traffic data</p> <p>Content data</p>

<p>Subscriber data</p> <p>Prosecutor issuing order/request for disclosing Subscriber data</p>	<ol style="list-style-type: none"> 1. Identify the internet service provider; 2. Identify the address and responsible person for disclosing the needed data 3. Check if the Internet service provider hold the needed type of data (according the company policy, regulation for protection of personal data, retention policy) 4. Check the Provider policy (law if it is national internet service provider) for disclosing data to Law enforcement agency 5. Prepare the request
<p>Traffic data</p> <p>Content data</p> <p>Prosecutor/judge is issuing order/request for disclosing Traffic and Content data</p>	<ol style="list-style-type: none"> 1. Identify the internet service provider; 2. Identify the address and responsible person for disclosing the needed data 3. Check if the Internet service provider hold the needed type of data (according the company policy, regulation for protection of personal data, retention policy) 4. Check the Provider policy (law if it is national internet service provider) for disclosing data to Law enforcement agency 5. Prepare the request

GLOSSARY

Asymmetric encryption	A public key is used for encryption, a private key for decryption.
Backdoor	Widespread malicious code that is usually introduced and installed by viruses, worms or Trojan horses.
Bot	Term for a hacked computer which has been integrated into a botnet.
Botnet	Robot Network initially compromised by worms or Trojan horses that then wait for instructions.
C&C Server	Command and Control server to control the bots.
Computer virus	Manipulates system areas, programmes or their environment out of the user's control.
Container	Term for encrypted files.
Cyber Bullying	See Online Harassment
Cyber Stalking	See Online Harassment
DNS	Domain Name System translates the computer name or the URL of a website into an IP address.
Drive-by download	Inadvertent/unnoticed download of malware when visiting a website.
Drop	Someone taking parcel deliveries, exchanging labels and forwarding parcels.
Drop Leader	Organise Drop(s) and assign their tasks.
Encryption	A process that converts plaintext into encrypted text with an encryption algorithm and usually a secret key.
eTAN	Small electronic device replacing the (TAN) input creating new codes in real time. During data input of the online transactions, the bank's website generates a control number that is entered by the clients into their eTAN devices. The eTAN device then generates a reply number enabling the client to complete the transaction.
Exploit	Software or a sequence of commands exploiting specific weaknesses and/or malfunctions of another computer programme.

Exploit or zero-day exploit	Exploiting a security hole on the same day or before the vulnerability is publicly known is called zero-day exploit.
IMEI	International Mobile Equipment Identity - a 15-digit serial number that can be used to uniquely identify mobile devices.
IMSI	International Mobile Subscriber Identity uniquely identifies network subscribers. The IMSI is stored on a SIM (Subscriber Identity Module). IMSI is a unique 15 digit number assigned exclusively to every single worldwide SIM card by network operators.
Internet applications	Software as a Service (SaaS) delivery models and words and phrases about web sites, e-commerce
IP Address	Internet Protocol address - Unique number specifying the address of computers and other devices within an IP network.
iTAN	Indexed TAN, clients are asked by the bank to enter one particular TAN from their lists indexed with position numbers.
Letschka List	A list of personal data of individuals who reacted to spam, to act unwittingly for criminal group E.g.: Money Mules/ Drops.
Malware	Malicious software - Computer programmes performing harmful activities not wanted by the user.
Man In The Middle	The attacker is located between the two communication partners either physically or logically without them knowing having control over data traffic between two or more network participants and can read and/or manipulate information as desired.
Mobbing	Similar to Online Harassment but focused in the workplace.
Money Mule	Money mules withdraw illegally obtained funds in cash as soon as the money arrives in their account and send them abroad via money transfer services.
mTAN	Mobile TAN's involve the SMS channel.
Network security –	Terms related to network security, including intrusion prevention, VPNs and firewalls.

Online Harassment	Online harassment is sometimes referred to as cyber bullying, cyber stalking or trolling. Because of greater access to the internet this crime is becoming more prevalent and can range from simple name calling to a sustained campaign of harassment including threats to kill and utilising numerous online fake profiles.
P2P	Peer to Peer
Parcel Mule	Parcel mules dispatch parcels.
Peer to Peer	In a peer-to-peer network (P2P), all computers are equal and can provide services as well as utilise services.
Phishing	E-mail used to try and trick recipients into revealing access data and passwords to online banking and other payment systems.
Private key (secret key)	An encryption key whose value should never be made public. The term may refer to the private key of an asymmetric key pair or a key shared by parties who are using symmetric key pairs.
Proxy	Agent that accepts requests from clients and then establishes connections to other clients from his own IP address.
Server	Software within the client-server concept or computer on which this software programme is running.
Spyware	Mainly Trojan programmes that collect information about the user's activities and forward them to third parties.
Symmetric encryption	A single key is used for both encryption and decryption.
TAN	Relates to mTAN, eTAN, iTAN -Transaction authentication number -a one-time password used in online banking.
Trojan	(Trojan horse) Combination of a host programme with a concealed malicious part, often spyware or a backdoor. A Trojan horse does not spread by itself but encourages the user to install it by advertising the usefulness of the host programme.
Trolling	See Online Harassment
VOIP	Voice over Internet Protocol - Telephony over the Internet - Speech data are digitalised and sent over the Internet in small data packets.
VPN	A virtual private network extends a private network securely across a public network, such as the Internet.

Acronyms

AfriNIC	African Network Information Centre
API	A programming interface
APNIC	Asia-Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
ASN	Autonomous System Number
ASN.1	Abstract Syntax Notation One
AV Partners	Anti-Virus partners
BIA	Burned-in Address (relates to MAC)
C&C	Command and Control
CCIU	Computer Crime Investigations Unit
CHIS	Covert Human Intelligence Source
CPC	Criminal Procedure Code of the Republic of Albania
CSP	Communication Service Provider
DDoS	Distributed Denial of Service
DFU	Digital Forensic Unit
DNS	Domain Name Server
DNS	Domain Name System translates the computer name or the URL of a website into an IP address.
DoS	Denial of Service
DPR	Data Preservation Request
Drop	Drop/drop leader

ECHR	The European Convention on Human Rights
Eurojust	European Judicial Network
Europol	European Union law Enforcement Agency
FCU	Financial Crime Unit
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICPO	International Criminal Police Organisation (Interpol)
IDN	Internationalized Domain Name
IDNA	Internationalizing Domain Names in Applications
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP	Internet Protocol Address
IP Address	Internet Protocol address
IPCD	International Police Cooperation Department, Tirana
IPv4	Internet Protocol Address Version 4
IPv6	Internet Protocol Address Version 6
ISP	Internet Service Provider
JIT	Joint Investigation Team
LACNIC	Latin America and Caribbean Network Information Centre

LAN	Local Area Network
LEGAT	FBI legal attachés based in U.S. embassies
MAC	Media Access Control
MiM	Man-in-the-Middle Attack
MIM	Man-in-the-Middle Attack
MITM	Man-in-the-Middle Attack
MitM	Man-in-the-Middle Attack
MLAT	Mutual Legal Assistance Treaty
MX	Mail Server
NCB	National Central Bureau Interpol Unit
NIC	Network Interface Card
ns	Network simulator (specifically ns-1, ns-2 and ns-3).
OLAF	Office européen de lutte antifraude (European Anti-Fraud Office)
OSINT	Open Source Intelligence
P2P	Peer-to-Peer
P2P	Peer-to-Peer
POP3	Post Office Protocol 3
PP	Public Prosecutor
RIPE	Réseaux IP Européens (European IP Networks)
RIR	Regional Internet Registry
SaaS	Software as a Service
SELEC	South East Law Enforcement Centre
SIM	SIM (Subscriber Identity Module)

SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TAN	Transaction Authentication Number
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	Application Layer Protocol
TLS	Transport Layer Security
VOIP	Voice over Internet Protocol
VOIP	Voice over IP
VPN	Virtual Private Network
VPN	Virtual Private network
WAN	Wider Area Network
Wi-Fi	Wireless networking
WLAN	Wireless Local Area Network
WWW	World Wide Web www.

ANNEX

Open Source Investigation Guide (annex 1)

Mutual Legal Assistance Request for subscriber information (annex 2)

Data Preservation Request (annex 3)

ANNEX 1

Open Source Investigation Guide

WARNING: *Any online research and investigation leaves a trace or 'footprint'. An operational decision will therefore need to be made as to whether the research will be non-attributable i.e. cannot be traced back to law enforcement or to identifiable individuals; or whether it is ok for it to be attributable i.e. capable of being traced back to law enforcement.*

- 1. Determine and establish 'points to prove' of investigation and intelligence already held.**
- 2. Compile a communications profile and set parameters of investigation.**
- 3. Choose the most appropriate equipment and tools for the investigation.**
- 4. Agree a methodology and naming convention to store material into folders for easy reference, examination and/or dissemination**
- 5. When searching names and numbers consider every possible configuration including nickname, usernames, account names, dialling codes, format etc.**
- 6. Secure material of interest immediately using capture tools or browser add-ons.**
- 7. Consider using screen capturing software to capture entire online investigation.**
- 8. Utilise advanced search techniques and consider regional indexes and domains.**
- 9. Search databases including electoral register, telephone directories, business databases, maps and genealogy sites.**

10. Search social networking sites and online communities such as Facebook, Twitter, and Instagram for name, emails, and telephone numbers.

11. Search marketplaces, groups and repositories.

12. Search for secondary targets such as friends, associates, family members, ex-partners, children, etc. (Digital Shadow).

13. Search for peripheral information such as vehicles, previous addresses, images or information in the press referring to similar or past offences.

14. Search visual media sites such as Google Images, Flickr, YouTube, Tin eye etc.

15. Establish current and historical registrant and host of any IP addresses or domain names.

16. Use translation tools to search for information in other languages.

17. Examined digital images for background information and explore EXIF data for date, time, equipment specification and physical location.

18. Trace email headers to point of origin and capture network / device information.

19. Maintain an audit trail of your data collection methodology and findings as at this stage it will be research intelligence and the Public Prosecutor (PP) will need to replicate the methodology to obtain the same results and produce as evidence to a court.

20. Consider Special Investigative measures Article of CPC - authorisations required from PP.

ANNEX 2

Adopted by the T-CY at its 19th Plenary

Strasbourg, 9 July 2018

T-CY(2018)10

[Add logo or use letter head of requesting organization if necessary]

**Mutual Legal Assistance Request
for subscriber information**

under Article 31 Budapest Convention on Cybercrime¹

Date
DD/MM/YYYY

Reference / Case number

Request status

- Follow up to previous MLA request (details added below)
- Follow up to previous preservation request (details added below)

REQUESTED AUTHORITY

REQUESTING Authority	
Organisation	
Person in charge of the request	
Address	
Telephone number	
Cell phone number	

¹ This template was adopted by the Cybercrime Convention Committee (T-CY) at its 19th Plenary (9-10 July 2018) to facilitate the preparation and acceptance of requests by Parties. Use of this template by Parties to the Budapest Convention is optional.

E-mail address	
Fax number	
Office Hours	
Time Zone	
<input type="checkbox"/>	Response by email or other expedited means preferred
<input type="checkbox"/>	Response preferred by means of:

SHOULD ADDITIONAL confirmation FROM THE requesting authority be needed, PLEASE CONTACT:

Name:	
Job Title:	
Function:	
Telephone number	
Cell phone number	
E-mail address	

Investigative/Operational AUTHORITY in charge of the case

(if different from Requesting Authority)

Organisation	
Person in charge of the case	
Address	
Telephone number	
Cell phone number	
E-mail address	
Fax number	

Prosecution office or Court in charge if applicable

Prosecution office in charge and case number	
--	--

Court in charge and case number	
Prosecution or Court decisions related to the MLA request	

Information on previous MLA request If applicable

Date	
Ticket/reference number	
Contact details of authority having requested previous MLA	
Contact details of authority having responded to (or executed) previous MLA	
Communication method used to submit previous request (email address, fax number, etc)	

Information on previous preservation request If applicable

Date	
Ticket/reference number	
Contact details of authority having requested preservation	
Contact details of authority having responded to (or executed) the preservation request	
Channel for communication	

Domestic legal basis for request IF APPLICABLE

Relevant decision by Court, Prosecution or other authorised body; or other legal basis for request	
Please attach order or statutory authority	

1 SUMMARY OF THE CASE

Including:

- brief description of the facts
- how the data sought is related to the investigation/offences
- purpose and necessity of request for disclosure of subscriber information
 - charges pressed/list of offences (with reference to domestic legal provisions and applicable penalties)

CASE STATUS

On trial n trial /list o

Other details:

SUBSCRIBER INFORMATION to be Disclosed²

Subscriber information related to the following IP addresses requested:			
Subscriber information related to following accounts requested:			
Period of interest	Start date: DD/MM/YYYY Start time (and time zone):	End date: DD/MM/YYYY End time (and time zone):	

² Use ANNEX for details.

Information identifying the service provider AND – if available – the location of the computer system

Please provide as much information as possible to help identify the service provider (including aliases, telephone numbers and other contact details or associated email addresses)

URGENCY

URGENT

Response expected by: DD/MM/YYYY

REASONS FOR URGENCY (check more than one if applicable)

- Threat to life or limb
- Suspect/offender in custody
- Suspect/offender to be released from custody
- Crime in progress
- Volatility of data
- Imminent threat of a serious nature to public security
- Statute of limitation due to expire
- Trial is imminent or in progress
- Other:

Brief details for urgency

CONFIDENTIALITY

CONFIDENTIALITYfor urgency gressspire custody plicable)identify the service provider (including aliases, telephone numbers and other contact details or associated email addresses) tall it by advertising the usefulness of the host programme.ssment including

Confirmation/notification requested

Confirmation/notification requested

Additional NOTES, IF ANY

Signature and / or stamp of REQUESTING Authority if applicable

Name	
Position	

Date / place	
Signature and/or stamp	

21 Annex: Details of information requested³

Subscriber information needed for IP addresses		
Subscriber information related to the following IP address/es requested (to the extent permitted by your law):		
Period of interest:	Start date and time:	End date and time:
Time zone:		
Details requested:		

<input type="checkbox"/>	Subscriber names	
<input type="checkbox"/>	User names	
<input type="checkbox"/>	Screen names, or other identities	
<input type="checkbox"/>	Email, social media and other accounts related to the IP address/es	
<input type="checkbox"/>	Mailing addresses	
<input type="checkbox"/>	Residential addresses	
<input type="checkbox"/>	Business addresses	

³ Please note that the law of the requested state may not necessarily consider all of the following data to be subscriber information.

<input type="checkbox"/>	Telephone numbers, other contact information	
<input type="checkbox"/>	Billing records	
<input type="checkbox"/>	Billing address	
<input type="checkbox"/>	Payment method	
<input type="checkbox"/>	Payment History	
<input type="checkbox"/>	Billing period	
<input type="checkbox"/>	Information about length of service and the types of services the subscriber(s) or customer(s) used	
<input type="checkbox"/>	Any other identifying information, whether such records are in electronic or other form	

Subscriber information needed for accounts

Information on the following accounts /s requested, to the extent permitted by your law:		
Period of interest:	Start Date and Time:	End Date and Time:
Time zone:		
Details requested:		

<input type="checkbox"/>	Subscriber names	
<input type="checkbox"/>	User names	
<input type="checkbox"/>	Screen names, or other identities	
<input type="checkbox"/>	Mailing addresses	
<input type="checkbox"/>	Residential addresses	
<input type="checkbox"/>	Business addresses	
<input type="checkbox"/>	Email addresses	
<input type="checkbox"/>	Telephone numbers, other contact information	
<input type="checkbox"/>	Billing records	

<input type="checkbox"/>	Billing address	
<input type="checkbox"/>	Payment method	
<input type="checkbox"/>	Payment History	
<input type="checkbox"/>	Billing period	
<input type="checkbox"/>	Registration date	
<input type="checkbox"/>	IP address used for the initial registration of the accounts	
<input type="checkbox"/>	Last registered date of access	
<input type="checkbox"/>	IP address used for the last registered access to the accounts	
<input type="checkbox"/>	IP address used for access to the account in the period: Start date: DD/MM/YYYY Time: End date: DD/MM/YYYY Time: Time zone:	
<input type="checkbox"/>	Other Email, social media and other accounts related to the person or account	
<input type="checkbox"/>	Information about length of service and the types of services the subscriber(s) or customer(s) used	
<input type="checkbox"/>	Any other identifying information, whether such records are in electronic or other form	

ANNEX 3

Adopted by the T-CY at its 19th Plenary

T-CY(2018)11

Strasbourg, 9 July 2018

[Add logo or use letter head of requesting organization if necessary]

Data Preservation Request under Articles 29 and 30 Budapest Convention on Cybercrime⁴

DATE
DD/MM/VVVV
Reference / Case number
REQUEST STATUS
<input type="checkbox"/> New request
<input type="checkbox"/> Extension of previous request
<input type="checkbox"/> Ticket/reference number of previous request:
AUTHORITY TO WHOM THE REQUEST IS ADDRESSED
REQUESTED AUTHORITY *
Organisation
Person in charge of the request
Address

⁴ This template was adopted by the Cybercrime Convention Committee (T-CY) at its 19th Plenary (9-10 July 2018) to facilitate the preparation and acceptance of requests by Parties. Use of this template by Parties to the Budapest Convention is optional. Please note that items marked with asterisk (*) are required information pursuant to Article 29, paragraph 2 of the Convention on Cybercrime.

Telephone number	
Cell phone number	
E-mail address	
Fax number	
Office Hours	
Time Zone	
	Response by email or other expedited means preferred
	Response preferred by means of:

SHOULD ADDITIONAL confirmation FROM THE requesting authority be needed, PLEASE CONTACT:

Name:	
Job Title:	
Function:	
Telephone number	
Cell phone number	
E-mail address	

Investigative/Operational AUTHORITY in charge of the case

(if different from Requesting Authority)

Organisation	
Person in charge at the authority	
Address	
Telephone number	
Cell phone number	
E-mail address	
Fax number	

Prosecution office or Court in charge if applicable	
Prosecution office in charge and case number	
Court in charge and case number	
Prosecution or Court decisions related to the request	

FOLLOW UP THROUGH MUTUAL LEGAL ASSISTANCE	
<input type="checkbox"/>	Please be informed that we intend to submit a request for mutual legal assistance to request the production of data.*
<input type="checkbox"/>	Please find enclosed a mutual legal assistance request for the production of data.

OFFENCES SUBJECT TO CRIMINAL INVESTIGATION OR PROCEEDINGS*	
<input type="checkbox"/> Offence/s corresponding to Articles 2 through 11 Budapest Convention	Please specify offence under the law of the requesting State:
<input type="checkbox"/> Other offence/s	Please specify under the law of the requesting State:

Summary of the case*	
Including:	
- brief description of the facts	
- how the data sought is related to the investigation/offences	
- purpose and necessity of request for preservation and/or partial disclosure of traffic data	
- charges pressed/list of offences in the case	

Data to be preserved*		
<input type="checkbox"/> Subscriber information	Please specify:	
Period of interest	Start date: DD/MM/YYYY YYYY	End date: DD/MM/ YYYY
	Time (and time zone): Time (and time zone):	Time (and time zone):
<input type="checkbox"/> If the system is a shared system, please preserve all basic subscriber information for all virtual systems on the IP.		
<input type="checkbox"/> Traffic data	Please specify:	
Period of interest	Start date: DD/MM/YYYY YYYY	End date: DD/MM/ YYYY
	Time (and time zone): Time (and time zone):	Time (and time zone):
<input type="checkbox"/> Content data	Please specify:	
Period of interest	Start date: DD/MM/YYYY YYYY	End date: DD/MM/ YYYY
	Time (and time zone): Time (and time zone):	Time (and time zone):

Information identifying the person or organisation (e.g. Service provider) in possession or control of the stored computer data AND The location of the computer system, IF AVAILABLE*

EXPEDITED DISCLOSURE OF PRESERVED TRAFFIC DATA UNDER ARTICLE 30 OF THE CONVENTION ON CYBERCRIME

Details/description of data to be disclosed⁵

This request seeks to preserve traffic data concerning a specific communication. If, in the context of this request, the server reveals that a service provider in another jurisdiction was involved in the transmission of this communication, please immediately disclose to us the identity of that service provider and the path of the communication in line with Article 30 of the Convention on Cybercrime.

⁵ If necessary, please fill in the Annex (data specification form).

CASE STATUS

- Pre-trial phase
- On trial
- Crime in progress

Other details if necessary:

Urgency

- URGENT

Response expected by: DD/MM/YYYY

REASONS FOR URGENCY

- Threat to life and limb
- Imminent threat of a serious nature to public security
- Crime in progress
- Suspect/offender in custody
- Suspect/offender about to be released from custody
- Volatility of data
- Statute of limitation due to expire
- Trial is imminent or in progress
- Other:

Brief details for urgency, if any

CONFIDENTIALITY

- We request that this preservation request is kept confidential and that customers are not notified.

Please inform us if your domestic law requires us to explain the reason for confidentiality; or – before taking any action – whether your domestic law requires customer notification or if you suspect that the provider may not comply with the request for confidentiality.

Confirmation/notification requested, if available:

- Confirmation of receiving the request
- Confirmation of preservation of the data
- Information on the preservation period
- Information on whether data is beyond the jurisdiction of the requested country
- Information on whether the data preserved will be destroyed after the preservation period
- Other:

Additional NOTES, IF ANY**Signature and/or stamp of REQUESTING Authority if applicable**

Name	
Position	
Date / place	
Signature and/or stamp	

Annex: Data specification form

Please complete a separate form for each person or organisation believed to be in possession or control of data. Please complete as much as is possible or applicable.

Details of person or organisation believed to be in possession or control of data

Business Name	
Legal Name	
Contact name	

Guidelines on Cybercrime Investigation

Address		
Country		
Phone		
Email		
Address		
IPv4	1-255	1-255
URL		
Date		
Time		
Time Zone		
Proxy		
Anonymization		
Port number		
IPv6	Subnet – 64 bit	Host – 64 bit
URL:		
Date		
Time		
Time Zone		
Proxy		
Anonymization		
Other data		
E-mail address		
Social Networking ID		
Date		
Time		

Time Zone	
Proxy	
Anonymization	

