This Project is co-funded by the European Union and the Council of Europe.
Bu proje, Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmektedir.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GUIDELINE FOR PROSECUTORS AND LAW ENFORCEMENT IN CYBERCRIME INVESTIGATIONS IN TÜRKİYE

Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of European Convention on Human Rights Violations in Türkiye

European Union - Council of Europe Joint Project

This Project is co-funded by the European Union and the Council of Europe.
Bu proje, Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmektedir.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GUIDELINE FOR PROSECUTORS AND LAW ENFORCEMENT IN CYBERCRIME INVESTIGATIONS IN TÜRKİYE

Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of European Convention on Human Rights Violations in Türkiye

European Union – Council of Europe Joint Project

Guideline for Prosecutors and Law Enforcement in cybercrime investigations in Türkiye

Prepared by
- Dr. Michael Jameison
- Kemal Kumkumoğlu

This Guide is prepared under the Joint Project on Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of the European Convention on Human Rights Violations in Turkey. The Project is co-funded by the European Union and the Council of Europe and implemented by the Council of Europe. The final beneficiaries of the project are the Ministry of Justice of the Republic of Türkiye, the Directorate General for Criminal Affairs, and the Justice Academy of Türkiye. The Central Finance and Contracts Unit is the Contracting Authority of this Project.

This Guide was produced with the financial support of the European Union and the Council of Europe. The views expressed herein can in no way be taken to reflect the official opinion of either party. The views and opinions in this Report are the sole responsibility of the authors.

Project Stakeholders
- Constitutional Court
- Court of Cassation
- Council of Judges and Prosecutors
- Union of Turkish Bar Associations
- Financial Crimes Investigation Board (MASAK)
- Gendarmerie General Command
- Directorate General of Security
  - Department of Cybercrime
  - Department of Counter Terrorism
  - Department of Anti-Smuggling and Organized Crime
- Information and Communication Technologies Authority
- Council of Forensic Medicine

www.coe.int/tr/web/ankara
Council of Europe Programme Office in Ankara

cas.ankara@coe.int
Ceza Adalet Sisteminin Güçlendirilmesi Projesi
cas_projesi
@project_cas
Ceza Adalet Sisteminin Güçlendirilmesi Projesi

CONTENTS

1 Introduction

In a world that is becoming more and more digitalised, modern technologies have become part of our everyday lives. E-mails, mobile messengers, online banking, online shopping, media streaming services, online gaming, smart homes/cities/cars, cryptocurrencies, and social media are just some examples of the impact that the Internet has on our daily lives.

In the same speed in which people use and adopt new technologies, criminals exploit those same technologies for their own profits. In Türkiye, as elsewhere, cybercriminals do not just defraud, harass, stalk, abuse and threaten innocent citizens online, but they also abuse the Internet for money-laundering, trafficking illegal goods like drugs, guns, and child abuse materials. As if these examples were not exhaustive enough, the Internet and electronic devices are also abused to plan, coordinate, and even facilitate traditional crimes in the physical world including murders, abuses, and terrorist acts.

One of the core missions of criminal justice authorities – police officers and prosecutors – is the protection of citizens by preventing, investigating, and prosecuting crimes. For centuries this only applied to crimes which were committed in the physical world. Now that times have changed, it is obvious that the mission to protect citizens needs to be fulfilled in the digital world alike. To do so, criminal justice authorities need to develop competencies for preventing, investigating and prosecuting cybercrimes and cyber-enabled crimes.

This guideline will seek to provide best practice in the investigation of cybercrime and handling of electronic or digital evidence.[1] In respect to electronic evidence, this Guideline will refer to the following Council of Europe tools for being use which are available to Prosecutors and Law Enforcement officers in Türkiye:

1. the "Electronic Evidence Guide"
2. the "Basic Guide for the Management and Procedures of a Digital Forensics Laboratory"
3. the "Standard Operating Procedures for collection, analysis and presentation of the electronic evidence"
4. the "Guide on Seizing Cryptocurrencies"
5. the "Guide for Developing Training Strategies on Cybercrime and Electronic Evidence for Law Enforcement"

These tools are available via the Council of Europe "Octopus platform"[2].

[1] The terms "electronic" or "digital" evidence are used here synonymously.

[2] Council of Europe "Octopus platform" – Materials section: https://www.coe.int/en/web/octopus/training

2 The purpose of the guideline

The purpose of this guide is to provide support and initial guidance to practitioners in cybercrime investigations who are not necessary cybercrime investigators or part of the specialised cybercrime units, in such ways that they can receive complaints by victims of cybercrimes and that they can conduct primary investigative steps.

The present guide was developed in response to a need expressed by practitioners in Türkiye and serves several purposes:

1. It may serve as a starting point for the development of procedures for practitioners in cybercrime investigations in Türkiye.

2. It may also be applied directly by authorities dealing with cybercrime investigations. However, authorities will need to ensure that such use follows the most recent legal framework in Türkiye.

3. The procedures described in this guide may be used in training activities for police officers or prosecutors to enable a better understanding of technical and tactical procedures to be followed by first responders to cybercrime investigations.

4. It highlights the importance of the practitioners when it comes to cybercrime investigations, particularly because of the criticality of their actions. If the practitioners are not able to collect data in a timely manner, that data may no longer be available. If practitioners cannot demonstrate competence when being confronted with a cybercrime investigation, this will have a direct impact on the visible reputation and trust in law enforcement and the judiciary for their ability of handling such crimes.

5. It is intended that the practical guide not only accords with the most recent legal framework in Türkiye, but also gives accurate information that can avoid violations of fundamental rights outlined in the European Convention on Human Rights (ECHR), by paying particular attention to the right to a fair trial (Article 6), right to respect for private and family life (Article 8) and freedom of expression (Article 10).[3]

–

This guide is not intended to be an instruction manual with step-by-step directions, nor should it be used as Standard Operating Procedures (SOP). Instead, the guide focusses on the specificities of cybercrime offences and provides an outline of the steps required to conduct initial cybercrime investigations. To support further understanding, this guideline provides several useful reference points that could support more complex investigations. In addition to that it provides an overview of the most common cybercrime phenomena.

[3] In parallel, in S. and Marper v. The United Kingdom (GC, 4 December 2008, 30562/04 and 30566/04) the ECtHR states that *"It observed that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. Any State claiming a pioneer role in the development of new technologies bore special responsibility for striking the right balance in this regard."*

3 Cybercrime and cyber enabled crimes

3.1 Cybercrime

There is no agreed international description or definition of what cybercrime is. Some jurisdictions describe it as any offence carried out by means or a computer or digital device and others describe it more specifically as needing a computer to undertake the cyber-attack against a computer or other device being used by a victim or similar.

For the purpose of this document, cybercrime offences are those described in Articles 2 to 9 in the Budapest Convention on Cybercrime and include the following[4].

- Offences against the confidentiality, integrity and availability of computer data and systems;
    - Illegal access – Article 2
    - Illegal interception – Article 3
    - Data interference – Article 4
    - System interference – Article 5
    - Misuse of devices – Article 6
    - Computer-related forgery – Article 7
    - Computer-related fraud - Article 8

- Content related offence
    - Offences related to child pornography – Article 9

Details of specific cybercrime types found in Türkiye are detailed in section 5.

3.2 Cyber enabled crimes

These types of crimes are considered for the purposes of this document as all other criminal offences that are carried out online or using a computer (or other digital device) but could be committed without the use of such technology. Examples include online bullying and social engineering attacks.

4 Description of electronic evidence

There are many descriptions of electronic evidence used when discussing the investigation of cybercrime. For the purposes of this guideline, we will rely upon the description provided in the Council of Europe Electronic Evidence Guide. More information is available from the actual guideline[5].

Electronic evidence is derived from electronic devices such as computers and their peripheral apparatus, computer networks, mobile telephones, digital cameras, and other portable equipment (including data storage devices), as well as from the Internet. The information it contains does not possess an independent physical form.

[4] https://rm.coe.int/1680081561

[5] "Electronic Evidence Guide - A BASIC GUIDE FOR POLICE OFFICERS, PROSECUTORS AND JUDGES", Version 2.1, 03/2020, Council of Europe, https://www.coe.int/en/web/octopus/training

Given its unique characteristics electronic evidence could be defined as any information generated, stored, or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings.

- Characteristics of electronic evidence
- It is invisible to the untrained eye
- It is highly volatile
- It may be altered or destroyed through normal use
- It can be copied without degradation

Criminals are predators and the mass use of digital media, and the Internet has provided new opportunities for them to perpetrate their crimes. They have developed new strategies for traditional offences by exploiting these new channels of communication and novel categories of crime have evolved. Consequently, it is imperative for all those involved in the legal system to be familiar with the different forms of electronic evidence and to know how to deal with them.

Electronic evidence is no different from traditional evidence in that the party introducing it into legal proceedings must be able to demonstrate that it reflects the same set of circumstances and factual information as it did at the time of the offence. In other words, they must be able to show that no changes, deletions, additions, or other alterations have (or might have) taken place. The intangible nature of any data and information stored in electronic form makes it much easier to manipulate and more prone to alteration than traditional forms of evidence. This has created special challenges for the justice system which requires that such data be handled in a special way to ensure the integrity of the evidence it offers.

To that end, preservation of electronic evidence should be handled in accordance with the globally accepted five principles.

1. "Data Integrity" - no action taken should change electronic devices or media, which may subsequently be relied upon in court[6]. When handling electronic devices and data, they must not be changed, either in relation to hardware or software. The person in charge is responsible for the integrity of the material recovered from the scene and thus for commencing a forensic chain of custody. There are circumstances where a decision will be made to access the data on a "live" computer system to avoid the loss of potential evidence. This must be undertaken in a manner, which causes the least impact on the data and by a person qualified to do so.

2. "Audit Trail" - an audit trail or other record of all actions taken when handling electronic evidence should be created and preserved. An independent third party should be able to examine those actions and achieve the same result. It is imperative to accurately record all activities to enable a third party to reconstruct the first responder's actions at the scene in order to ensure probative value in court. All activity relating to the seizure, access, storage, or transfer of electronic evidence must be fully documented, preserved and available for review.

[6] Court of Cassation reiterated data integrity principle while emphasizing the importance of related procedural guarantees being followed: "During seizure process, all data in the system should be backed up (taking image), a copy of the backed-up records should be given to the suspect or his/her advocate if requested, this matter needed to be written to minute and signed. Backup procedure should also be done in the presence of the suspect and/or his/her advocate, and the suspicion that data is is placed in the system before the image is taken and then the image is taken should be annihilated. (Court of Cassation Fn.2016/544 Dn.2020/127 Dt.25.02.2020. / Yargıtay CGK., E. 2016/544 K. 2020/127 T. 25.2.2020)

3. "Specialist support" should be utilized. If it is assumed that electronic evidence may be found during an operation, the person in charge should notify police digital forensics in time. For investigations involving search and seizure of electronic evidence, it may be necessary to consult external specialists. All external specialists should be familiar with the principles laid down in this or similar relevant documents while having the necessary knowledge, expertise, and experience.

According to the Constitutional Court, audit trial and specialist support principles are directly related to the defense rights and right to a fair trial: "It is clear that the technical examination to be made on electronic evidence can be decisive in terms of the evidence of the crimes and on the determination of the suspects' relevance to these crimes. In the face of the applicant's claim that the documents in the electronic evidence were not created and provided by him, an access that would enable him to effectively defend these claims, or a suitable examination by the judiciary should have been made for this purpose." (Yankı Bağcıoğlu and Others, 2014/253, 9 January 2015)

4. "Appropriate training" should be implemented. Personnel and first responders must be appropriately trained to be able to search for and seize electronic evidence if no experts are available at the scene. In exceptional circumstances where it is necessary that a first responder collects electronic evidence and/or access original data held on an electronic device or digital storage media, the first responder must be trained to do it properly and to explain the relevance and implications of his/her actions.

5. "Legality" – the officer and law enforcement agency in charge of the case are responsible for ensuring that the law, the general forensic and procedural principles, and the above listed principles are adhered to. This applies to the possession of and access to electronic evidence.

5 Significant types of cybercrime and cyber enabled crimes

5.1 Cyber-attack – Investigative considerations

Cybercriminals will use one or more computers to launch an attack against a single or multiple computers or a network of computers. A cyber-attack can disrupt or downgrade the functionality of a computer, illegally obtain data and/or use computer(s) as a further launch point to conduct further cyber-attacks.

To that end, there are three main types of cyber-attacks, which are illegal access of a computer system (TCC art. 243), use of malware on a computer system (TCC art. 245/A), and denial of service attacks (TCC art. 244). Other types of attacks are referred to as cyber-enabled crimes because the commission of such criminal acts do not have to rely upon a computer to be **both** the launching point and the subject of the attack.

Cyber-attacks often rely upon a technical infrastructure, which should be considered when receiving the crime report for two main reasons;

- Dismantlement of the infrastructure may prevent or reduce further cyber-attacks,
- The infrastructure may contain evidence that can be used in the investigation to demonstrate how the attack took place and provide some attribution towards a person or entity.

The following paragraphs will provide methods of how well-known cyber-attacks are launched and include descriptions of the potential infrastructure. It is recognised that some of these components also provide anonymity to the attacks.

For example;

- **IP addresses** are allocated when devices connect to networks and the Internet, which may identify the device,
- Proxy IP addresses, virtual private network, and resources such as The Onion Router (TOR) are used to **disguise or conceal IP addresses** from the authorities,
- Domain Name Service (DNS) and domain names[7], which are how users identify Internet Resources, can be used, and abused in the commission of cybercrime
- Attackers often connect attacks to **command-and-control servers** to communicate indirectly with malware installed on victim's computers and control many infected devices simultaneously. Command and control servers may have been hired or be owned or may be illegally controlled by the cybercriminal
- A series of infected computers under the control of a criminal or entity is referred to as a **botnet**. The size of a botnet can range from a few computers up to exponential numbers. Some Botnets are reported to be many millions of infected devices[8]. Botnets are often referred to as 'zombie computers.' As each computer or device has been infected by malware, each should be considered for available evidence and could be considered as an individual crime scene.

5.1.1 Technical investigations in cyber-attacks

Investigations into cyber attacks should consider where the evidence is likely to be stored and seizure of it may be important to help identify attackers and for the occasions when suspects are identified provide valuable evidence for prosecutions. For evidence that is stored outside of Türkiye, prosecutors and law enforcement should use the resources explained in Section 10 of this guideline to obtain the material for use either as intelligence or evidence.

Technical investigations should involve (but not be limited to), analysis of system logs, firewall logs, intrusion protection system logs and other records that would indicate the activities and provide evidence of how the criminals attacked a system or device. These attack methods may also include reconnaissance undertaken before the cyber-attack. Analysis of log files can be undertaken by digital forensic specialists, who will use specialist technical programs to undertake this examination aside from the normal digital forensic processes.

Where a live digital device, that is suspected of holding electronic evidence relating to malware or the unlawful access of a computer system is seized, it is crucial that live digital forensics is considered. Data concerning number of live running processes on computers that will not be saved or recorded when the device is turned off should be obtained in such circumstances. Instructing an expert to collect digital forensic images of live running machines should be considered in such cases.

In the case of malware investigations, it is often extremely useful to have expert describe how the infection took place and what the payload of the malicious programme entails. In many cases these experts will utilise computers and virtual computers, which they infect with the malware in controlled situations, to report to the court what the malware is designed to do. Expertise in malware investigations is a specialist skill and digital forensic examiners may not be able to provide evidence in this specialism. Experts from TK-CERT, academia or elsewhere may be necessary to provide more informed and reliable evidence.

Investigators need to consider that malware is often identified through its hash value and often the creators of malware leave traces in the code that may include nicknames, associated online

[7] https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/

[8] https://www.zdnet.com/article/a-decade-of-malware-top-botnets-of-the-2010s/

resources (such as command and control servers using domain name services), and anonymous email addresses. The identification of these traces and further investigation is crucial in such cases. Reliance upon the experts and conducting open-source intelligence will often support investigative processes to further search and seize evidence connect to the malware, that is located elsewhere (such as command and control servers).

5.1.2 Financial investigation in cyber-attacks

In the case of frauds and financial losses, police and prosecutors should implement a parallel financial investigation as soon as it is practicable to do so. This will support in freezing of stolen funds before and after transfer, as well as enabling 'follow the money' type investigations.

In the first instance, the investigation authorities should take all urgent steps possible to freeze the money if it has been transferred by a victim to a fraudsters account. This step is more likely to be successful within 24 hours after the time of the transfer when traditional banking systems are utilised.

Criminals generally plan for these financial transfers to be followed by additional money laundering processes by transmitting funds onwards through other bank accounts under their control. Other methodology that investigators should consider include the use of 'mule networks' that will cash the money out at ATMs, before sending the funds to the criminals through money transfer services.

Investigations may undertake follow the money processes, which take considerable time and resources, and may end without seizure of funds. But these investigations should be put into place at the earliest possible time to raise any potential for success.

A further investigational tactic is to consider covertly communicating with the suspect to arrange controlled transfers or delivery of money using undercover skills and/or tasking of victims. This tactic has realised some success during investigations, but it will depend on the circumstances of individual investigations. Negotiations to reduce the value of payments in extortion cases, often provides the investigators with more information, and may give more time to consider other investigative options.

Steps that include follow the money investigations are always important so that information that may identify the fraudster and/or the location of any crime proceeds should be undertaken diligently. These investigations may identify opportunities that reveal when money is delivered or collected from financial institutions and enables the suspects or associates can be identified and arrested.

For offences and occasions that utilise virtual payment systems and cryptocurrencies see Section 8 of this guideline.

5.2 Cybercrime and cyber enabled crime types

5.2.1 DDoS

A distributed denial of service (DDoS) attack is a cyber-attack against an online service, server, website, or network, where the Internet traffic is directed overwhelm the resource.

The attacker relies upon a botnet of computers that are controlled by a command-and-control server, which is used to direct the attack. The criminal identifies the attack point, which may be a website or an IP address and instigates data traffic from the botnet towards the resource. Because of the amount of traffic, the targeted system is flooded with data and fails to be available for legitimate users. For online merchants, this can result in serious financial losses.

Motivations for DDoS attacks include extortion demands to stop the attack, revenge, hacktivism, and state-sponsored attacks. Another consideration is that the DDoS attack is a diversion for another cyber-attack.

The investigation should consider the following areas of potential electronic evidence.

- Preservation of logs from the victim's website or server since the beginning of the attack
- Consideration that earlier server logs may show reconnaissance and smaller test attacks undertaken by attackers
- Preservation of any email accounts that may have sent a ransom demand
- Recording of any communication with the perpetrator
- Details of any method of payment.

Mitigation measures relating to DDoS should be sought from the National Computer Emergency Response Team (TK-CERT).

5.2.2 Web application attacks

A web application attack is a cyber-attack against an online service, server, website, or network, where the attackers seek to identify a vulnerability in the computer code and exploit it to obtain unlawful access to the resource.

There are four main types of web application attacks which are:

- SQL Injection;
- Cross-site scripting;
- Remote File Inclusion
- Cross-site Request Forgery

The web applications of many online resources have computer code that allows it to run and receive data from the user, which is input and processed. The data may be a username and password, or it may be a file or something else that can be entered and processed by the server (or computer). In many cases the computer code that has been implemented is running with vulnerabilities that could allow attackers to enter data in a format that the computer will interpret as a process to be followed. But the attacker has crafted the data to undertake the unlawful manipulation of the computer code to grant them access to confidential areas of the server (or computer) and possibly the core infrastructure of a network.

The motivation for these types of attacks is usually financial, such as obtaining financial records and credit card data. But web application attacks can also be used to obtain information, conduct espionage, and implant malware. The global losses to web application attacks are significantly higher than DDoS.

The investigation should consider the following areas of potential electronic evidence:

- Preservation of logs from the victim's website or server since the start of the attack;
- Consideration that earlier server logs may show reconnaissance and earlier attempts to gain access.

Advice about prevention and mitigation steps concerning a web application should be sought from the National Computer Emergency Response Team (TK- CERT).

5.2.3 Malware attacks

A malware attack is a common cyber-attack, where malware (malicious software) executes unauthorised actions on a victim's system. There are many different types of malware, and they undertake a very wide variety of attacks against the system.

It is important to recognise that the descriptions of the malware often relate to how the variants infect the computer system rather than the type of payload that they contain.

For example:

- Computer Virus is a piece of code that can replicate itself and inserting itself in other programs or files, infecting them in the process. Users unknowingly spread virus, by sharing infecting files or sending emails with viruses as attachments in the message
- Computer Worm is a piece of code that can replicate itself and spreads copies of itself from computer to computer without user interaction
- Trojan Horse malware is a type of malware that is disguised as legitimate software and typically gains access to user systems by tricking the user, often through social engineering, to load and execute the malware
- There are many other types of malware, which are not limited to the following;
    - droppers and downloaders (e.g., as part of botnets)
    - info stealers (e.g., keyloggers, spyware)
    - specialised trojans (e.g., banking trojans)
    - backdoors (e.g., rootkits)
    - wipers
    - ransomware.

The motivation for the use of malware is extremely widespread and are used by state actors, cybercriminals, hacktivists, and persons involved in industrial espionage.

5.2.4 Ransomware

Ransomware is a form of malware, where the payload deliberately encrypts the user's files and contents of folders on a computer system or digital device. The attacker accompanies the encryption attack by sending a message or creating a pop up on the computer making a demand for a ransom payment to be made to a dedicated account, which is usually a crypto-currency style transaction. Upon receipt of the payment, the attackers indicate they will decrypt the files and restore access or provide the decryption key. Normally access is restored upon the payment being made, but the ransom payment can range from small amounts up to millions of Turkish Lira.

There are variations of this type of attack including the pretence of being a local, national, or international law enforcement body or some similar kind of agency and indicating the user has breached some legislation and the ransom payment is represented by a fine that must be paid. More recently ransomware has targeted corporate networks, by exploiting various vulnerabilities in the networks or by using social engineering attacks to infect systems.

The infection is identified because the user's computer screen only displays a ransom demand page indicating that the resource is encrypted and can only be decrypted through the payment of the ransom demand. The payment is routinely required in cryptocurrencies and communication with the hackers is often undertaken through anonymous channels. At the time of writing this was undertaken through 'Tox Chat,' which is a peer-to-peer instant messaging protocol.

Since 2021, the market for ransomware is increasingly organised and professional, offering a business model often referred to as ransomware-as-a-service (or RaaS) to commit ransomware offences. This business model has led to cyber criminals involving independent services to negotiate

payments, assist victims with making payments, and some services offering a 24/7 help centre to expedite ransom payments and to assist in the restoration of encrypted systems or data.[9]

To reinforce the demand, attackers have also increased their modus operandi, by copying large swathes of the confidential data from the systems subject of the attack. If the victim refuses to pay the ransom demand, the attackers will post the confidential data in publicly available areas of the Internet to cause reputational damage or often contact the data subjects (for example customers and medical patients) to increase the threat or to make demands of these persons whose personal information is stored on the system subject to the attack.

The investigation should consider that any device that has indications of malware infection should be isolated and preserved for specialised analysis. Examination should consider the recommendations made in Section 5.1.1 of this guideline. Other investigative considerations include whether the victim will pay the demand. Whilst this is an unattractive option, the business (victim) may consider that the payment of the ransom demand will be of a lower cost than the rebuilding of a new system or the continuation of resources without the encrypted data. Any payments made by crypto currency provide an investigative option to 'follow the money' using blockchain technology.

The investigating officers should not forget that the decryption keys may be available through resources such as the No More Ransom site[10]. Other lines of enquiry are to examine the method of infection (usually a phishing email) method and undertake enquiries into the source of the cyber-attack, communication with the attackers, and a full review of systems to identify whether any data has been accesses by the attackers to reinforce demands.

Analysis should be considered either through investigative steps or digital forensic analysis to determine the scope, magnitude, and potential reach of the infection. Identification of the type and number devices is an important step. The type and version of the ransomware malware should be identified as well as how the malware infiltrated devices and networks.

The investigation of ransomware attacks often leads to suspects and evidence in countries where the criminals and evidence remain out of reach (e.g., Russian Federation). The sharing of intelligence with national and international stakeholders (Europol and Interpol) should always be considered even when an investigation and prosecution reaches a stage when it cannot be successfully completed.

Further prevention and support measures can be obtained from the National Computer Emergency Response Team (TK-CERT).

5.3 Data breaches

A data breach is a security violation against a computer system or device, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorised individual. The security violation may be intentional or unintentional, such as a targeted intrusion into resources by persons who are able to pass the security protocols of authentication and authorisation of a data system, or a data leak or data spill caused by poor or careless processes in the handling of sensitive information by an individual, business or government department.

The legal frameworks to consider when dealing with data breaches include the following;

[9] https://rm.coe.int/t-cy-2022-14-guidancenote-ransomware-v4adopted/1680a9355e

[10] https://www.nomoreransom.org

a) Where a criminal attacker obtains illegal access to data on a computer system, without right then legal frameworks will have introduced criminal offences that accord with TCC art. 243

b) Where negligence or carelessness in the handling of data by the person or organisation in control of the personal data results in a data leak or data loss, then the data controller and/or data processor may be fined by Turkish Data Protection Authority according to the Turkish Data Protection Code.

c) In many cases of data breaches, both scenarios are applicable.

When receiving such reports, the investigation may need to seek appropriate advice to identify if those responsible for Data Protection Regulations, such as a Data Protection Authority should also be informed.

5.3.1 Insider-threat (in computer terms)

An insider threat is a person that poses a security risk and is often within a targeted organisation. Typically, such threats involve current or former employees and staff who have access to sensitive information or privileged accounts within an organisation's network or computer system.

The insider threat may use his knowledge or access to undertake a data breach, but the security threat is not limited to such an attack. They may also cause unauthorised changes, deletions or instigate denial of service attacks against an individual or organisation with the intent of financial loss and/or disruption of computer services.

It should be noted that insider threats are often deliberately placed by organised criminal groups to further their enterprise and/or are corrupted by such groups to act in the interest of the criminal venture.

Law enforcement and prosecutors should remember that some of these attacks will involve complex technical skills, such as bespoke malware and the creation of back-door access to online services.

5.3.2 Exploitation of vulnerabilities

A vulnerability is an error, mistake, omission, or bug that regularly exist in computers and technology. Whilst vulnerabilities are not harmful to the system, they may exist when programmers and computer coders create an online service but have not noticed the exposure that exists.

Vulnerabilities exist in operating systems, applications, computer programs, and computer systems hardware. From time to time, vulnerabilities are identified, and patches or updates are created to mitigate the risk. The reality of this patching and update is that those systems that employ the patches and updates, no longer have the vulnerability. But services who do not patch or update quick enough, will have known vulnerabilities that criminals could be aware of through the release of the patch or update.

Security engineers in Information Communication Technology regularly use vulnerability scanners to examine systems to ensure the security. Attackers use identical resources including vulnerability scanners and vulnerability databases to identify potential victims for attack.

Attackers develop exploits, which can be used to expose the vulnerability and gain illegal access to a computer system. Exploits include malware, computer code (sequence of commands) and open-source exploit kits.

Examples of these types of attacks include the following:

- SQL Injection attacks
- Cross-Site Scripting
- Cross-Site Request Forgery attacks
- Security misconfigurations.

5.4 Social Engineering Attacks – by email

There are many descriptions and cybercrime attacks that use social engineering skills to trick a victim into revealing sensitive data or taking an action that compromises the security of a computer system.

Social engineering is recognised as a skill or art that exploits human psychology rather than technical vulnerability, and it enables attackers to gain access to systems and data because the user carries out a seemingly innocent task at the behest of the attacker in which they unwittingly allow access.

Many social engineering attacks are conducted by email, but other examples often result in fraud and cyber-attacks using in social media, in person communication or voice techniques to dupe the user.

5.4.1 Phishing

Phishing is a social engineering attack that uses a disguised email or electronic communication, which is sent to the recipient so that they believe the message is from an individual (such as a friend, colleague or relative) or a genuine service supplier, such as a financial institution, bank, online shopping carts or other web resource and dupes the victim to click on an embedded link or downloads an attachment.

Whilst phishing emails are often professional in their presentation, they are often untargeted and are sent to many recipients, whose email address has been harvested.

Phish is an analogy of an angler throwing several baited hooks out to a large collection of targets and hoping for bites. The bite is where the user is tricked and undertakes the seemingly innocent task.

Embedded links that are clicked upon often redirect the victim to fake or scam websites that ask users to enter their usernames and passwords, which are then harvested by the criminals and used in fraud. Attachments often included embedded malware (or malware downloaders) which compromise the computer system.

Criminals can purchase or construct 'phishing kits,' which can include compromised web servers and websites that the user connects to and enters authentication details. These sites stay live for a short time and are constructed to resist attempts to disrupt their activities by cyber-security professionals.

Domain name services (DNS) and email addresses from the offenders are often obfuscated to enforce the deception, and the appearance of fake websites are often professional replicas of real online services.

When receiving a crime report of a phishing email, the investigation should consider what is permitted by national and international legal frameworks Many jurisdictions do not identify the sending of a phishing email as a criminal offence and any reporting may be reliant upon the victim having been defrauded or subject of a data breach before a cybercrime report is made. When making international requests for information, the Prosecutor must demonstrate reciprocity in Türkiye and the receiving country.

Investigations should consider the use of domain name service and that these services often need to be paid for. Registering a website (even one used for crime) relies upon a server being connected to the Internet with an identifiable domain name. Investigation into the service provider is possible through Whois databases and then requests to service providers, many of which have law enforcement portals.

Support in the investigation of emails and infrastructure can be provided by the 24/7 Single Point of Contact – See Section 6.3 & Section 10

5.4.2 Spear Phishing

Spear phishing emails and communications are more sophisticated phishing attacks. The messages and communications are often professional in their presentation and are targeted towards recipients, so will be sent to a specific individual, organisation, or business. The attackers may have undertaken some additional reconnaissance that will increase the likelihood of the recipient clicking on an embedded link or attachment contained in the communication.

Similar infrastructure used in phishing attacks is employed in spear phishing attacks. Spear phishing attacks are more likely to be successful because of the additional social engineering skills that an attacker puts in messages.

Often attackers involved in Spear Phishing messages will use diverse communication methods (in addition to email) in their communication with the victims. All these communication methods will need further investigation, which can be enhanced through support from the 24/7 Single Point of Contact – See Section 6.3 & Section 10

5.4.3 Whaling

Whaling is a highly targeted phishing attack, which is normally aimed at senior executives in a corporate environment. It is enabled through reconnaissance and social engineering methodology so that the victim initiates a higher level of transfer of funds through.

Initial communication may take place through email and online communication, but often physical and voice interactions are used to support the deception. Whaling emails are often more sophisticated than those seen in phishing and spear phishing, involving some of the following:

- Personal information about the individual or the organisation
- Reinforcement of fraud through a sense of urgency
- Creating a situation of isolation for the victim e.g., the matter needs to be kept confidential for some security reason
- Crafting of messages using business terminology or language.

5.4.4 Business email compromise fraud (BEC)/Chief Executive Officer fraud (CEO Fraud)

BEC/CEO fraud is a highly targeted social engineering attack, which is normally aimed at employees and executives in a corporate environment responsible for financial transactions. However, examples are often seen against individuals who are undertaking large size financial transactions.

BEC/CEO fraud is similar in many ways to phishing attacks such as whaling but occasionally relies upon the attackers having obtained illegal access to an email account so that communications of the supplier and the purchaser can be observed. Attackers are then able to craft an email to the victim that indicates a change of bank account for the transaction is necessary and communications are often accompanied with a message that the payment is urgent. The sender of the message often purports to be a senior manager (CEO level) or similar, to reinforce the instruction to make the payment.

The worldwide financial impact of this type of crime is rated to be one of the most significant types of cyber-attack.

As well as investigation into the source of the email account that sent the message with the criminal bank account details, the time-critical step of this investigation is the urgent freezing of transactions attributable to this attack. Investigators should seek all methods to contact banks or financial institutions in Türkiye and elsewhere to stop onward transmission of the funds. The first 24 hours often result in the successful recovery of these funds and after that time the investigation will rely on a 'follow the money' process, for which success rate is low. Partners such as MASAK and Police Financial Investigators should be considered to support any freezing activity.

5.5 Social engineering attacks - Other

The best actions to take in relation to social engineering attacks is prevention, awareness, and education. These crimes are often complex to solve and invariably include a few international dimensions for investigators to consider.

When a fraud occurs, it is often reliant upon a payment made online or through some other money transferring system (which may include virtual payment systems and cryptocurrencies). It is often difficult to prove a criminal offence under the criminal code until the fraud has been successful, albeit prosecutions could rely on legal frameworks that could include criminal attempt and criminal conspiracy.

Most social engineering attacks will come to the notice of the law enforcement authorities and the prosecutors after a victim has suffered financial losses. See financial steps above in Section 5.4.4.

Aside from the financial investigation, the investigative strategy will rely upon data communication information from the social media platform, emails or other type of system used to undertake the fraud. This may include investigation into email headers or making applications for information from multi-national service providers. Investigations into communication data and international requests for evidence can be enhanced through support from the 24/7 Single Point of Contact. See Section 10 of this guideline for other relevant information.

A lot of these crimes originate from West Africa and the law enforcement authorities in that region have dedicated investigation teams, which are extremely familiar with social engineering frauds such as advance fee and romance frauds. Prosecutors and police in Türkiye should consider early engagement with these resources through appropriate channels of cooperation and collaboration (Interpol, Police-to-police, and Mutual Legal Assistance).

5.5.1 Advance fee fraud.

An advance-fee fraud is one of the most common types of social engineering attacks. The scam typically involves promising the victim a significant share of a large sum of money, in return for a small up-front payment, which the fraudster claims will be used to obtain the large sum. If a victim makes the payment, the fraudster either invents a series of further fees for the victim to pay or simply disappears.

5.5.2 Romance fraud

A romance fraud is a social engineering attack involving feigning romantic intentions towards a victim, gaining the victim's affection, and then using that goodwill to get the victim to send money to the scammer under false pretences or to commit other fraud(s) against the victim. Fraudulent acts may involve access to the victim's money, bank accounts, credit cards, passports, e-mail accounts, or identification documents and/or forcing the victims to commit financial fraud on their behalf.

These crimes are often perpetrated by organized criminal gangs, who work together to take money from multiple victims at a time.

A consideration that should be made in social engineering attacks and especially romance frauds is that often the victims find it difficult to believe that the person that they are having a 'relationship' with is a fraudster. Whilst the investigative strategy may involve negotiation and interaction by law enforcement authorities with the fraudster, care should be taken about how much information is shared with the victim. There are many cited examples where the victim is persuaded by the attacker (through further communication) that they are a genuine person and there is no fraud. Consequently, the suspect(s) are warned of Police investigations by the victim.

5.6 Online fraud

There are many types of Internet fraud, which are often described as cybercrime fraud or deception, where attackers make use of the Internet and through a combination of scams and social engineering methods trick the victim into voluntarily transferring money or property to financial accounts under the control of criminals.

Internet fraud can be partly or wholly based on the use of Internet services, but financial transactions are completely based on the use of technology.

These paragraphs provide some explanation of the most common types of Internet Fraud and their investigation should consider the descriptions of investigative options in Sections 5.4 & 5.5 in this guideline.

5.6.1 Identity theft

Identity fraud occurs when someone uses another person's identifying information, such as name, address, date of birth, financial account information without permission and to commit fraud or other types of crimes.

Often the method used by the offender to obtain the victim's person identifying information is unknown. Common methods of obtaining personal identifying information include phishing, data breaches and malware.

The identities are used a variety of ways to conduct fraud, which include using the victims personal identifying information to make unauthorised purchases, open bank accounts or obtain credit and obtain services such as medical care and drugs.

Investigations will need to consider the legal framework during the reporting of a cybercrime, as identity theft itself is not necessarily a stipulated criminal offence. The criminal framework usually relies upon evidence of a fraud or other criminal act, where the identification is used to commit the offence.

5.6.2 Account takeover

An account takeover is a form of identity theft and is where an attacker successfully gains access to a user's account credentials, such as a username and password or PIN. Once the attacker gains those credentials to access to the account, they can take information for financial gain or undertake unauthorised financial transactions from a bank account or similar.

As financial services security systems have improved to counter the threats of account takeovers, there is now an expectation for customers to provide a supporting method of authentication (two-factor authentication). Such systems include the provision of the customers mobile telephones, social media accounts and/or email accounts which can receive verification messages. Criminals seek to undermine these additional security measures by compromising online accounts or duplicating the victims SIM card from their mobile phone number. Reporting officers should consider these methodologies when reporting these crime types and identify any potential compromises in the crime report.

5.6.3 Technical support scam

A technical support scam is often instigated using a cold calling telephone call, where the attacker claims to be part of a legitimate technical support service. Often offenders purport to be Microsoft or Internet Service Providers technical support departments and seek to use social engineering skills to persuade the victim to provide remote access to their computer or device.

Once remote access is obtained, the attacker can take personal identifying information, such as credit card numbers and alike or to persuade the victim to access online accounts whilst log in information is observed and taken.

A lot of technical support scams are undertaken using a call centre type set up.

5.7 Website defacement

Web defacement is an attack in which malicious parties gain access to website and replace content on the site with other messages. The messages can convey a political or religious content, obscene language or other inappropriate content that could embarrass website owners, or a notice that the website has been accessed by a specific hacker group.

Most websites and web applications store data in environment or configuration files, that affects the content displayed on the website, or specifies where templates and page content is located. Unexpected changes to these files can mean a security compromise and might signal a defacement attack.

Most businesses have an incident response plan to deal with these types of attacks, which would include taking the defaced web-server offline for further investigation. The next step is to identify the vulnerability that was exploited or the method of attack. This will involve research into common exploits such as SQL Injection attacks and cross-site scripting attacks. The places that electronic evidence would normally be found include the server logs and firewall logs, which will show date and times of changes to the data as well as IP addresses that have connected to the server. There are dedicated tools that experts can use for investigation and log analysis.

Other lines of investigation may include open-source intelligence, where the attackers may have displayed some details of the attack on their website or some other resources (e.g., Pastebin).
The prosecutors and police will also need to consider the victim's communication plan, where they will need to advise their customers of the attack and how it is impacting upon access to the resources on the website.

5.8 Online child sexual exploitation and abuse

Online child sexual exploitation includes online sexual grooming, live streaming, consuming sexual abuse material and blackmailing children for sexual purposes. As technology advances new forms of this crime emerge and as the reach of online connectivity grows, further countries and their children are exploited.

With the current technical reach and the tools to protect anonymity, it has never been easier for offenders to contact children, obtain sexually exploitive images and videos of children and share them with other offenders. Often motivations for sharing images are for profit and to inspire others to commit further sexual exploitation against children.

The identification of offenders and victims is often very difficult, as criminals use darknet and other anonymous channels to communicate. Sexual exploitation of children often occurs across many international jurisdictions, with offenders and victims in different countries. Examples include pay-per-view sexual abuse, where a child is abused on a live stream video and the sexual torture and humiliation occurs at the direction of a remote offender. Another complicating factor is the increase self-generated sexually explicit material, which are shared amongst their peers and are obtained by offenders.

The Investigation should consider that these offences include exposure to further sexual abuse, including rape and gross humiliation and to constant threat to the life of child victims. These mean that urgent steps should be undertaken to identify, protect and safeguard the victim. These are the most serious types of offences and all responses by law enforcement should be considered urgent.

Many countries have dedicated units to investigate online offences against children. Any investigation will rely upon significant evidence gathering of communication data, which can be enhanced through support from the 24/7 Single Point of Contact. Many service providers actively support such investigations, and it is likely that a quicker response can be obtained in these types of investigations.

5.8.1 Online sexual grooming

Grooming is when a person builds an online relationship with a young person or child to trick or pressure them into doing something sexual. This may include sending an intimate image of themselves, exposing themselves in front of a webcam and/or meeting for the purpose of sex. At the time of writing, online grooming is not regulated in a specific criminal provision in the legal framework of Türkiye. However, it can be considered in the context of different type of crimes depending on the specifics of a concrete case.

Cases of online sexual grooming demonstrate that adult offenders often provide false details about their identities, such as lying about their age, interests, gender, and reasons for the communication. The offender may send many messages to the victim to find out information and build the relationship. The offenders seek to create a false sense of security and trust in a victim, including the use of secrecy and isolation (especially from parents and carers).

Messages may start innocently, but the offenders will start to indicate sexual conversations which become more intrusive during the communications. Children are usually not able to stop this communication, due to their inexperience, naivety, and politeness. In some cases, children have sent intimate images of themselves to that offender and find they are at the centre of an extortion. In such cases the offender may make demands for more intimate and revealing sexual images and reinforce the demand with a threat of revealing the images already obtained online.

Police and prosecutors, who handle reports of online sexual grooming should consider the impact upon the victim which may include them being frightened, frustrated, angry, ashamed, or depressed. In other examples, victims have low self-esteem and may be inclined to self-harm or commit suicide. Investigators should be aware that victims may react very differently than is normally expected. These reactions must be taken into consideration and the victim's reactions should be noted in reports. investigators should minimize the number of questions addressed to victims, especially avoid asking victims by the causal questions (like why you did or did not do …).

5.8.2 Cyber bullying

Cyberbullying, which is also known as cyber harassment and online bullying is an online form of bullying and/or harassment. Other terms to describe these types of behaviour include Internet trolling and cyber stalking. These types of crimes have become increasingly common and especially amongst younger members of communities such as teenagers or younger.

The evidence for these offences can include posting rumours, making threats, sexual remarks, sexual abuse material without consent, revealing personal information and conducting hate speech. These acts of bullying or harassment are often repeated acts and demonstrate an intent to harm the victim or see the victim come to harm.

In recent years, the ECtHR put an emphasize on cyber violence towards women, and underlined duties of States in relation to the non-discrimination principle:

"*On that occasion the Court lastly pointed out that cyberbullying was currently recognised as an aspect of violence against women and girls, and that it could take on a variety of forms, including cyber breaches of privacy, intrusion into the victim's computer and the capture, sharing and file:///C:/Users/Ay%C5%9Feg%C3%BClAvc%C4%B1/Downloads/evrak_8558590479.udfmanipulation of data and images, including private data*." (Baturaga v. Romania, 11 February 2020, no: 56867/15, §74)

This case concerned the applicant's allegation that the Russian authorities had failed to protect her against repeated acts of cyberharassment. She submitted, in particular, that her former partner had used her name, personal details and intimate photographs to create fake social media profiles, that he had planted a GPS tracker in her handbag, that he had sent her death threats via social media; and that the authorities had failed to effectively investigate these allegations. (Volodina v. Russia (no. 2), 14 September 2021, no: 40419/19)

The method that such bullying and harassment is communicated may not be limited to one method such as messages, but can include text messages, social media postings and comments in online forums, which may include anonymous or semi anonymous channels.

Police and prosecutors, who handle reports of cyber bullying should consider the impact upon the victim which may include them being frightened, frustrated, angry or depression. In other examples, victims have low self-esteem and may be inclined to self-harm or commit suicide.

First responders should be aware that victims may react very differently than is normally expected. These reactions must be taken into consideration and the victim's reactions should be noted in reports. First responders should minimize the number of questions addressed to victims, especially avoid asking victims by the causal questions (like why you did or did not do …).

5.8.3 Online sexual coercion and extortion (Sextortion)

Online sexual coercion and extortion is a new crime phenomenon of the Internet and affects adults and children alike. The widespread availability of the Internet, along with the connectivity of mobile devices with cameras and video recording capabilities are some of the reasons for the growth.

Where children are targeted, the main motivations include a sexual interest in children and/or economic interest, where the offender is seeking to make financial benefit from an extortion. For more information visit the Europol Website report on sexual coercion and extortion.[11]

Further motivations for such sexual coercion and extortion become more complex. For example, many young people, such as teenagers may take self-generated sexually explicit material (SGSEM) and share it with another as a form of flirting and/or experimenting. Other motivations include malice or some type of social gain, which include attention, popularity, and affirmation. Often, when children and young persons are under 18 years old, they are unaware of the legal framework that regularly criminalises such behaviour of making and distributing sexual abuse material of persons under the age of 18.

Teenagers and young persons who are engaged in the creation and sharing of SGSEM, do so with consent, but also because of coercion. These coercions should be noted by the investigation team and the support of specialised units or experts should be sought as a priority. Such examples may include:

- Creation of SGSEM at the request of another
- Sending of an image to a minor who did not ask for it
- Threats and coercion for further material from other children and young persons who may have previously created SGSEM
- Distribution and redistribution to others of such material.

The sharing of SGSEM amongst young persons can present a complex scenario, especially when it is all undertaken by consent amongst a group of friends or peers. The subjects of the images may describe this as normal behaviour and not consider themselves' victims.

Mitigation measures may include education and awareness activities allowing for children and young people to identify and differentiate between acceptable and unacceptable behaviour during online communication.

[11] https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

5.8.4 Child (Sexual) Abuse Material

One of the most reported areas of criminality that face international cybercrime units and forensic investigations involving digital devices involves the possession, display, production, and distribution of child (sexual) abuse material (CSAM).

CSAM relates to a sexual image, including pictures and video materials of a person under the age of 18, that a child who is:

- Nude or partially clothed
- Sexually posing
- SGSEM
- Engaging in penetrative and non-penetrative sexual activity.

The legal framework provides description of the media in which the images are stored, which could include still images, video recordings and pseudo-photographs.

The legal framework specifies the criminal offences to include possession, taking, making and distribution of images of children (TCC 226).

- Possession – means having an CSAM in your possession, whether it is a hard copy or digital copy.
- Distribution – means the sending of an CSAM to another person, which could be done through chat rooms, email, text, phone applications, digital memory storage devices and file sharing websites.
- Production – means making, such as creating an electronic copy of an CSAM and includes the user purposely saving a copy to a device or computer (including automatically downloaded images from file sharing websites).

Many international agencies (such as Interpol and Europol) use surveillance software that tracks offenders who are sharing CSAM online through differing applications, chatrooms, and file sharing networks. Intelligence can be shared with law enforcement agencies in Türkiye, which would identify the IP address, relevant times of online activity and other information that could identify a suspect.

Generally, sufficient intelligence is shared by these agencies that allows for law enforcement authorities and prosecutors to commence a criminal investigation. The normal protocol in such cases is to execute a search warrant and seized digital devices that may contain electronic evidence, including CSAM at the suspects premises. These investigations tend to rely upon the evidence found at the premises and should aim to protect the use of these online surveillance tools so as not to compromise their use in other investigations in Türkiye and elsewhere.

5.8.5 Defamation and insult on the Internet

These offences (TCC 125 (Insult) and TCC 299 (Insulting the President of the Republic)[12]) are detailed in the Criminal Code in Türkiye. One of the normal steps in these types of investigation is to make requests to international partners (law enforcement, judiciary, ISP, social media, and multi-national service providers). Most countries in Europe and North America deal with these matters using Civil Law, which does not involve criminal courts, prosecutors, and police.

[12] On a side note, ECtHR finds that even the very existence of "insulting the President of the Republic" crime is a violation of Article 10 (freedom of expression) for not being proportionate to the legitimate ais pursued and necessary in a democratic society (Vedat Şorli v. Türkiye, 19 October 2021, no: 42048/19)

Therefore, the reliance on making requests for data and communication information in these countries is bound to fail because there is no reciprocity. The legal framework in these countries does not allow for the provision of data and communication information to be shared with law enforcement or the judiciary for matters of defamation and insult on the Internet.

Many European countries do not instigate a legal framework that criminalises defamation and insult on the Internet as they take the view that many of these investigations and subsequent convictions risk violations under Article 10 ECHR – Freedom of expression.

6 Initial actions at time of reporting

6.1 Preliminary steps

This section describes the two core tasks to be undertaken at the initial stages when it comes to investigations in cyber related crimes: the first task being to identify and seize electronic evidence, while the second task is to receive complaints of victims of cybercrimes and initiate the first steps of investigations.

Further information can be found in the Council of Europe Guide for First Responders to Cybercrime Investigations NEW (2021), which details the steps reporting officers must undertake at the time of receiving an allegation of cybercrime

The preliminary steps taken by the first responder or prosecutor that receives the report of cybercrime will normally include the following in relation to the description of complaints

- Assist the victim in filling in a complaint and receive the supportive evidence
- Format of the complaint and qualification of the applicable criminal code(s)
- Acquire the necessary information and description of the facts
- Identify the location of supporting evidence if not in possession of the victim or witness

In relation to identification of digital devices and acquiring electronic evidence, the first responder or prosecutor should evaluate electronic evidence in similar ways to other types of evidence so that the admissibility, integrity, and accuracy are ensured. The chain of custody refers to the handling of electronic evidence and officers should follow organisational procedures so that the fairness for the defendant and the appropriate balance of justice is maintained throughout the investigation and any subsequent court proceedings. These steps include documentation of all movements and transfers of electronic evidence between officers and/or departments. Details that should be recorded include names of persons, locations, dates, times, and full circumstances of the handling of the evidence. For more information, flowcharts, and template forms, please refer to the "Electronic Evidence Guide"[13].

Police officers who receive electronic evidence at the time of the initial report or during the investigation should consider and record if the device is switched on or off. If the device is switched on special consideration is necessary and advice should be sought from a trained officer, the Cybercrime department, or the digital forensic unit. If the device is switched off, it must NOT be switched on. The officer should record the status of the device, such as any damage and document every interaction with the electronic evidence or digital device.

[13] "Electronic Evidence Guide - A BASIC GUIDE FOR POLICE OFFICERS, PROSECUTORS AND JUDGES", Version 2.1, 03/2020, Council of Europe, https://www.coe.int/en/web/octopus/training

When dealing with electronic evidence, there are often time-critical and/or limited opportunities to locate, preserve and acquire online data. This may be due to data changes that occur as part of the normal system processes or the behaviour of a suspect in concealing evidence at the time or at some subsequent time through remote connectivity. It is important that the police officer and/or prosecutor gather all material and does not assume that a cybercrime cannot be solved or that some other investigator will carry out these responsibilities later.

When making requests for evidence and information, investigators should consider that data often contains personal information about persons not involved in the criminal offence or investigation. This is often referred to as collateral intrusion. Collateral intrusion may also include associates and family members of witnesses and suspects. The investigating officers and prosecutor should always consider that the intrusion to privacy of persons not involved in the offence should be minimised as much as possible unless it can be shown to be necessary in the interests of the safeguards described in Article 8 ECHR – Right to respect for private and family life.

In addition, although there is currently no special regulation regarding the processing of personal data in judicial proceedings and law enforcement activities, it is stated in the decisions of the Constitutional Court that judicial authorities should make the necessary assessments within the framework of the constitutional existence of fundamental rights, even if there is no special law (E.Ü., AYM GK, 17 September 2020, No: 2016/13010). Therefore, general principles on processing of personal data stipulated in the article 4 of the Turkish Data Protection Law should be considered in every judicial proceeding:

"ARTICLE 4 – (1) Personal data shall only be processed in compliance with procedures and principles laid down in this Law or other laws.
(2) The following principles shall be complied within the processing of personal data:
a) Lawfulness and fairness
b) Being accurate and kept up to date where necessary.
c) Being processed for specified, explicit and legitimate purposes.
ç) Being relevant, limited and proportionate to the purposes for which they are processed.
d) Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed."

6.2 Assess the urgency, reduce the damages

It is important to recognise that ongoing attacks against individuals, businesses and organisations are often costly or carry significant risk. Whilst it is important for the first responder or prosecutor to preserve the crime scene, it is important to consider the further risks and potential damage to the ICT networks, further financial losses, and the harm to the victim.

Many businesses and organisations have specific procedures in place to deal with cybersecurity incidents, such as malware infection, unauthorised access to ICT systems and denial of service attacks. Often these first steps are not so concerned with the preservation of evidence but concentrate on containment of the infection and mitigation measures to reduce the impact of any attack. These processes are bound to alter the data stored on ICT systems and impact upon the availability of electronic evidence. Alternative responses may include monitoring the incident and concentrate on gathering information about the attacker and their methodology, which can be used as evidence.

6.3 Take the urgent measures to preserve the electronic evidence

There are five steps that are followed in the handling of electronic evidence, which are titled identification, collection, acquisition, analysis, and reporting. Whilst some of these steps are outside the responsibility of the First Responder, the crucial part of collection of data includes evidence preservation, involving the steps of identification and collection. Further information can be found in Section 9.3 & 9.4 in this guideline.

It is important to remember that the existence of electronic evidence stored on servers and often with Multi-National Service Providers outside Türkiye. Examples include, but are not limited to, email servers, social media accounts and cloud storage solutions. Tangible steps must be taken through approved channels and using appropriate legal framework to preserve these types of evidential data and often in collaboration with the entity that is storing it.

The approved channels in Türkiye include a dedicated Single Point of Contact that is available 24 hours a day and seven days a week (24/7 SPOC) within the Turkish National Police.

The 24/7 SPOC and national cybercrime unit remain a constant reference for support and advice for officers on the frontline of policing. The reporting officer and prosecutor should consider, where necessary, requesting guidance in more complex cases of cybercrime and matters involving electronic evidence.

7 IP addresses and other identifiers

7.1 IP addresses – public

When two or more computers (or networked digital devices) are linked by data cables or by wireless connectivity a "network" is established. Such devices in a network can share data and other resources and will often be connected to additional hardware components that extend their scope and the functions available. Computer networks can be limited such as those found in the home (e.g., where members of a family establish a network sharing an Internet modem) or as extensive as those used by major corporations or governments linking hundreds or even thousands of computers together. These are described as Local Area Networks (Private networks or internal networks are other descriptions). Computers and digital devices can also be connected to a Wide Area Network (such as the Internet).

To communicate with other devices on networks, differing types of addressing protocols are used. These include Internet Protocol (IP), Ports, Media Access Control and Transport Control Protocols (TCP). Most investigations rely upon IP addresses for resolving issues and attributing identity of attackers and involved devices. Further research should be undertaken to understand the full details of these and other addressing protocols.

On the Internet, most IP addresses are allocated to routers. The role of a router is to receive, send and forward data packets from one location to another. A data packet sent from a source IP address to the destination IP address, will normally travel through several different routers. For the purpose of an investigation, the case will routinely rely upon the source and destination IP addresses (and not the intermediatory router addresses).

In most of the investigations that law enforcement is likely to conduct, they will be seeking to identify an IP address of a router that is attributable to an offender or identify the physical location of evidence. At the boundary of a private network located at a home, business or other type of enterprise is a router that has a public IP address allocated to it by an Internet Service Provider (ISP). An ISP will keep a record of who it has allocated (leased) its IP addresses to, on a second-by-

second basis. It will be able to provide full customer details in such cases of who has an IP address of interest to the investigation.

IP addresses are not always allocated (leased) on a permanent basis, so the address of a device is likely to change from time-to-time (Dynamic IP address). It is therefore necessary that when attempting to resolve an IP address the full date-time stamp and time zone is identified and included in any requests to resolve the IP address allocation.

7.2 Routers and private IP addresses

A router, which is allocated with a public IP address, is routinely located at the 'boundary of a private network' but this alone does not provide sufficient information to identify the device within the private network that may be responsible for any activities under investigation. As well as a public IP address (issued by the ISP) the router acts as a gateway to the private network, where there are a different set of IP addresses. These IP addresses inside the network are private IP addresses, which are issued by the router.

These gateway routers (by default) keep a record of internal devices that were connected on the private network, which are wired or wireless and the private IP addresses that were allocated.
Investigation into the log files of the router (acting as the default gateway) may identify the device that was connected at the time of the event or offence of interest to the investigation. This is particularly relevant in large private networks, such as businesses or similar and may prevent the analysis of every computer that is connected to the router.

Examination of routers should be undertaken by specialist digital forensic officers or trained first responders.

7.3 IP addresses – allocation to mobile telephones

There is a common misconception that a mobile telephone or mobile device's IP address is always unique and permanent from the perspective of the server it communicates with. This is not the case.

Mobile devices can make requests through a Wi-Fi network and will inherit the IP address of the WIFI router. This means all users on the same Wi-Fi network will be part of the same private network and will have the same public IP address .

This happens on cellular networks in a similar way. When users are in similar geographical locations using the same cellular network, the devices will inherit the IP address of the nearest cellular router.

Because of the number of cellular devices, it is crucial that the investigator or prosecutor can provide the correct IP address, along with the exact date and time, and the port number used in the communications. The port number can be obtained from the server to which the device was connected to at the relevant time.

All this information will need to be submitted to the communication service provider to support applications for subscriber information.

Further information can be obtained from the 24/7 SPOC within the Turkish National Police.

7.4 Virtual Private Network (VPN) and The Onion Router (TOR) - Dark Web

A VPN enables you to connect to the Internet using encryption. Encryption adds security and privacy to communication over networks that may be intercepted (such as wireless networks).

A VPN allows users to create an encrypted tunnel through which data is sent to a remote server operated by a VPN service provider. The VPN server then sends the data to the site that the user wants to connect with, encrypted and safe from the prying eyes of hackers and other cybercriminals. The site will only record the IP address of the VPN service provider and will therefore conceal the IP address of the user from the server.

Whilst more legitimate VPN service providers retain some log data, most do not keep this information. Other VPN service providers will not engage with law enforcement or respond to legal requests.

TOR is a free and open-source software used to enable anonymous communication. It directs Internet traffic through a free, worldwide, volunteer overlay network, consisting of more than seven thousand relays, to conceal a user's location and usage from anyone performing online surveillance and traffic analysis. Using TOR makes it more difficult to trace a user's Internet activity.

TOR's intended use is to protect the personal privacy of its users, as well as their freedom and ability to communicate confidentially through IP address anonymity using TOR exit nodes.

In some ways, TOR, and VPN's work in a similar way. But both provide difficulties for law enforcement to identify the location of suspects and TOR prevents the revelation of the location of hidden services (darknet sites) using the TOR network.

Even though the Dark Web uses the same physical network of the Internet, it uses a different internal network and address space. In addition to knowing the Dark Web uniform resource locator (URL), an investigator will also need to connect via the Dark Web's internal network to see the content of the website.

If an investigation involves VPN and TOR, it is recommended that support and advice is obtained from the Cybercrime Units of TNP or Gendarmerie. The Dark Web is a colloquial description of the criminal websites that exist on TOR. The Dark Web cannot be searched by the standard search engines.

Investigation into the Dark Web is a specialist task that goes beyond the scope of this guideline document. However, the following reading list might point readers into the right direction:

- A beginner's guide to exploring the Dark Net: https://turbofuture.com/internet/A-Beginners-Guide-to-Exploring-the-Darknet
- Deep Web Links: https://deepweblinks.org
- Deep Web Directories and search engines: http://www.thehiddenwiki.net/deep-web-directories-search-engines/
- Guide to TOR Onion services and elements of the TOR network: https://en.wikibooks.org/wiki/Guide_to_Tor_hidden_services_and_elements_of_the_Tor_network
- Investigating the Dark Web – The Challenges of Online Anonymity for Digital Forensics Examiners, https://articles.forensicfocus.com/2014/07/28/investigating-the-dark-web-the-challenges-of-online-anonymity-for-digital-forensics-examiners/

8 Virtual payment systems including cryptocurrencies

8.1 Virtual currencies

A **Virtual currency** can be defined as:

- a digital representation of a medium of exchange
- and/or a unit of account
- and/or a store of value
- it fulfils the above functions by agreement within the community of users of the virtual currency.

8.2 Cryptocurrencies

The Financial Action Task Force has defined a **Cryptocurrency** as

- as a math-based currency
- decentralised convertible virtual currency
- that is protected by cryptography
- relies on public and private keys to transfer value from one person (individual or entity) to another
- and must be cryptographically signed each time it is transferred.

The Council of Europe has published a "Guide on Seizing Cryptocurrencies" which offers in-depth knowledge about cryptocurrencies, their concepts and how to seize them[14]. The level of detail and information about matters such as cryptocurrency mining, the blockchain and analysis tools are beyond the scope of this document.

There are two main ways for people (including suspects) to possess cryptocurrency. One is to download software to their computer or possess a device that holds the private key of a cryptocurrency address or wallet (a virtual wallet). The other way is to outsource this task to a Virtual Asset Service Provider (Coinbase, Binance, Kracken, etc.,) and have an account with that organisation.

During search and seizure operations, it is important to know that cryptocurrencies can be seized by law enforcement. This should be seen like seizing money and other assets which are proceeds of crimes. However, access to the virtual wallets which store the cryptocurrencies is typically protected. Besides potential credentials that are stored on a computer system, other passwords, seed phrases or two-factor authentication devices may be needed. For this reason, investigators should look to devices and traces at the search scene.

It is imperative that any action to seize and confiscate cryptocurrencies are undertaken urgently. This is because virtual wallets can be duplicated, and this capability allows for criminals to move the assets beyond the reach of the confiscation process very quickly. Seized funds should be placed into a Government Wallet and access to it should be strictly controlled. Further operating processes and/or decisions are necessary to manage the conversion of the funds to fiat currencies at the appropriate time. Further guidance is available in the published guide detailed above.

For funds held by VASPs, a law enforcement officer or prosecutor should liaise directly and urgently with them through their dedicated contact point. A request to hold the funds should be accompanied by the necessary legal documentation to support the seizure and confiscation processes in Türkiye.

9 Search and seizure – electronic evidence

[14] https://www.coe.int/en/web/octopus/home?desktop=true#{%2264860390%22:[1]}

The search and seizure of electronic evidence is a crucial step in many investigations. In this guideline, it has been described that electronic evidence is easy to delete, change or overwrite deliberately or unintentionally.

When the location of electronic evidence has been ascertained by the investigation, all steps to preserve it in its original state should be undertaken by the police and/or prosecutor. On many occasions an informal request made using the 24/7 SPOC will suffice. They will make an approach to the service provider through trusted communication methods and request that the data is preserved. Legal frameworks, such as search warrants and production orders should then be made requesting that this preserved data be provided in evidential condition to the Prosecutor. Examples may include email accounts, social media accounts, communication data and stored data on the cloud resources.

Failure to complete preservation requests is likely to result in loss of meaningful evidence. This process is an essential component of modern-day investigations aiming to seize electronic evidence.

All activities in the search and seizure of electronic evidence must be assessed concerning the interference with the fundamental rights such as the right to a fair trial (Article 6), the right to respect for private and family life (Article 8)[15][16] and the freedom of expression (Article 10)[17]. Regarding the admissibility of electronic evidence, such assessments should also include balancing test of rights and the impact of the evidence on the conviction18. In addition to these, necessary procedural safeguards are needed to be implemented and respected.

9.1 Production orders.

[15] The ECtHR held that there had been a violation of Article 8 (right to respect for private life and correspondence) of the Convention, finding that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such as in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications. (Roman Zakharov v. Russia, 4 December 2015)

[16] The ECtHR held that there had been a violation of Article 8 (right to respect for correspondence) of the Convention. It observed in particular that, although the applicant had benefited from a number of procedural safeguards, the review chamber to which he had referred the case had given only brief and rather general reasons when authorising the search of all the electronic data from the applicant's law office, rather than data relating solely to the relationship between the applicant and the victims of his alleged offences. In view of the specific circumstances prevailing in a law office, particular reasons should have been given to allow such an all-encompassing search. In the absence of such reasons, the seizure and examination of all the data had gone beyond what was necessary to achieve the legitimate aim. (Robathin v. Austria 3 July 2012, 30457/06)

[17] The ECtHR held that there had been a violation of Article 10 (freedom of expression) of the Convention. It emphasised that the right of journalist's not to disclose their sources could not be considered a privilege, dependent on the lawfulness or unlawfulness of their sources, but rather as an intrinsic part of the right to information that should be treated with the utmost caution. In this case the investigating authorities had failed to properly balance the interest of the investigation in securing evidence against the public interest in protecting the journalist's freedom of expression. (Nagla v. Latvia, 16 July 2013, 73469/10)

[18] "*The lack of an assessment - which has to be conducted thoroughly, in an adversarial manner, of all the circumstances of the case with a view to allaying any doubts as to the authenticity of evidence to that effect, is in itself being prima facie conflicting with the requirements of fairness guaranteed by Art. 6 § 1 ECHR*" (Mehmet Zeki Çelebi v. Turkey, 28 January 2020, No: 27582/07, § 51). See also Guide on Admissibility of Evidence in Criminal Matters – Focus on Türkiye

Production orders also offer valuable resources for collecting electronic evidence in combatting cybercrime. Since almost all types of technologies are being used in cybercrimes, three types of data which may be relevant for the purposes of a criminal investigation, namely, subscriber information, traffic data, and content data can be requested from different type of service providers (telecom operators, internet service providers, websites, hardware manufacturer, software developers etc.) retaining them. Usually, conditions to access for subscriber information tend to be lower than for traffic data and the strictest regime applies to content data.

In Turkish legal system, there is a legal basis to make technology and service providers to retain subscriber and traffic data and to share them with legal authorities if requested with a production order. To name the most important one, the Law on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts ("Internet Law") regulates the legal, criminal, and administrative liability of Internet actors, such as content providers, hosting providers, ISPs (or so-called access providers), public use providers, and social network providers. There is also special type of production order regulated in the Additional Article 7 of the Law on Police Duties and Entitlements on the intelligence duties of the police and the fight against cybercrime.

In that regard, ECtHR highlighted the risks of regimes for obtaining communication data from service providers concerning fundamental rights[19] in its case-law and also emphasized the necessity of the requirement of "end-to-end safeguards" especially for bulk interception regimes[20]

However, since most of the social network providers are multinational private actors, cross-border production orders and international cooperation methods are becoming more and more important.

9.2 Search warrants.

[19] The Grand Chamber held: unanimously, that there had been a violation of Article 8 (right to respect for private and family life/communications) of the Convention in respect of the bulk intercept regime; unanimously, that there had been a violation of Article 8 in respect of the regime for obtaining communications data from communication service providers; by twelve votes to five, that there had been no violation of Article 8 in respect of the United Kingdom's regime for requesting intercepted material from foreign Governments and intelligence agencies; unanimously, that there had been a violation of Article 10 (freedom of expression) of the Convention, concerning both the bulk interception regime and the regime for obtaining communications data from communication service providers; Big Brother Watch and Others v. the United Kingdom (GC, 25 May 2021, 58170/13, 62322/14 and 24969/15)

[20] This case concerned the alleged risk that the applicant foundation's communications had been or would be intercepted and examined by way of signals intelligence, as it communicated on a daily basis with individuals, organisations and companies in Sweden and abroad by email, telephone and fax, often on sensitive matters. The Grand Chamber held, by fifteen votes to two, that there had been a violation of Article 8 (right to respect for private and family life, the home and correspondence) of the Convention. It found, in particular, that although the main features of the Swedish bulk interception regime met the Convention requirements on quality of the law, the regime nevertheless suffered from three defects: the absence of a clear rule on destroying intercepted material which did not contain personal data; the absence of a requirement in the Signals Intelligence Act or other relevant legislation that, when making a decision to transmit intelligence material to foreign partners, consideration was given to the privacy interests of individuals; and the absence of an effective ex post facto review. As a result of these deficiencies, the system did not meet the requirement of "end-to-end" safeguards, it overstepped the margin of appreciation left to the respondent State in that regard, and overall did not guard against the risk of arbitrariness and abuse. (Centrum För Rättvisa v. Sweden, GC, 25 May 2021, 35252/08)

To seize electronic evidence and to be able to search and confiscate computers, computer logs and programs, first a general search warrant in accordance with art. 116 of the Criminal Procedure Code ("CCP") and its continuation articles is needed to detect and obtain the devices used by the suspect. If the link between the suspect and the device is clear, the judge or, where there is a peril in delay, the Public Prosecutor should issue a decision to examine the materials to be obtained within the scope of art. 134 of the CCP and the art. 17 of the Regulation on the Judicial and Preventive Search ("RJPS"). According to these provisions, other prerequisites of the warrant decision are that there should be i) an investigation, ii) strong grounds for suspicion based on concrete evidence, iii) no opportunity to obtain evidence in any other way.

As can be understood from the title of the article, the place or thing where search and seizure can be made on computer and computer programs and computer logs. It has been a matter of debate whether especially network connections can be evaluated in this context in the face of developing technologies. The controversy arising from this deficiency in the regulation has been tried to be resolved with the expression added in Article 17 of the RJPS, "*This process also applies to computer networks and other remote computer files and removable hardware*."

The article 134/2-5 of the CCP provides some procedural safeguards. The article requires law enforcement authorities to create a backup of all data included within the system confiscated and giving a copy of that backup to the suspect or his attorneys with a signed form[21].

A ground-breaking decision by the Court of Cassation (16. CD., E. 2019/2637 K. 2019/5904 T. 10.10.2019) stressed out the special character of the 134 of the CCP and the impact of relevant procedural steps on the admissibility of the digital evidence in a criminal judgement: *According to Article 134 of the Criminal Procedure Law, searching and seizing computers, computer programs, and logs are subject to stricter conditions than general searches and seizures due to the involving more interference with the privacy of personal life. When searching and seizing without a judicial order by persons who perform the search, ignoring the fact that this action is a special form of search and seizure, the data in the system is seized without making a backup copy of the data (image-copy) and without giving a copy to the suspect or their advocate, in cases where it is objectively necessary to acknowledge the lack of the possibility of backup and copying on-site for the reasons mentioned above, the digital evidence must be properly recorded by the law enforcement unit conducting the search and seizure, without tampering with it, by writing the serial numbers in a report and sealing it. The suspect or their lawyer must be given the opportunity to accompany and supervise the examination process before the seal is opened and the digital media's image is taken. The copy of the image and the original media must be delivered to the suspect or their lawyer as soon as possible without delay. If the suspect or their lawyer cannot be present during the unsealing process, the seal must be opened in the presence of the judge who ordered the search and seizure, and the image-taking process must be carried out during this time. If the search and seizure is conducted without following these procedures, it will be deemed unlawful, and the evidence obtained through this process will be inadmissible in court."*

[21] However, this requirement creates problems especially for crimes such as child pornography where giving a copy of criminal evidence obtained back to suspect is detrimental to the very essence of the crime. Therefore, there is a need for a change of provisions in that regard.

9.3 Considerations during search and seizure.

The instructions of the prosecutor conducting the investigation regarding the execution of the search and seizure order should be detailed and clear. The further success rate in collecting evidence in cybercrimes is a crucial indicator of the fight against cybercrimes. Reliable complete detection and harmless collection of electronic evidence is possible with proper first crime scene response. In parallel, collecting evidence requires special expertise. For this reason, law enforcement personnel to be assigned in search and seizure processes related to cybercrimes should be equipped with necessary knowledge and technical capacity.

When searching home/office premises, to eliminate the risk of discarding/destroying important evidence or of suspects leaving the scene where computer systems, computer data and digital devices are to be seized, all location access routes need to be secured prior to the search.

Digital data is highly volatile and thus consideration must be taken about the speed of entry to the scene. It is prudent to prevent the suspect from deleting/wiping/destroying data at the time of entry and steps should be taken to isolate the suspect from any device which may contain digital evidence.

The following activities are recommended to be carried out immediately after entering a location where computer systems, computer data and digital devices are to be seized from:

- Identify and determine the number of computer systems available on site, their type, whether they are connected to a network and can access the Internet.
- Forbid access to computer systems/data and digital devices or other electronic equipment as well as to power supply sources, of persons identified at the location where the activity/search is to be conducted.
- Document the scene, all sources of digital evidence that might be target of seizure and their status and connections.
- Use protection gloves when handling computer systems, computer data and digital devices in order to avoid damaging latent prints and ensure successful collection of fingerprint/DNA evidence, as applicable.
- Check the operational status of each of the identified computer systems:
  - if the computer system is shut down, do not turn it on; If circumstances require an on-site analysis of the system, it is recommended to start the system by using either a forensic clone of the original disk or a write-protection / write-caching mechanism to maintain the integrity of the original disk.
  - if the computer system is running check if live data acquisition is to be conducted or not. After that the computer system may be shut down depending on the operating system.

Practice has shown that the location searched can provide other data and information to support the subsequent analysis of computer systems, computer data and digital devices. Non-electronic, but related evidence, such as: written passwords and other handwritten notes, blank pads of paper with indented writing (but do not shade with graphite pencil), paper wallets for virtual currencies, hardware and software manuals, text or graphical computer printouts, photographs or information about personal interests that may be useful during the investigations.

9.4 Digital Forensics - Overview of processes

Forensic science is the study of any field as it pertains to legal matters. Forensic evidence refers more specifically to evidence which meets stringent standards of reliability and scientific integrity for admissibility in court. Digital Forensics is a branch of forensic science related to the acquisition,

processing, analysis, and reporting of evidence that is stored on computer systems, digital devices, and other storage media with the aim of admissibility in court.

In a case that involves Digital Forensics the standard procedure normally consists of five steps (Identification, collection, acquisition, analysis, and reporting.

Identification and collection of devices is described in search and seizure above.

"Acquisition" is where the digital evidence needs to be obtained, normally using specialist software to obtain a digital forensic image of the data stored on a digital device. This can happen by acquiring volatile data in a search & seizure scenario, by imaging a suspect's hard drive from a seized computer or in any other process during a case where the investigator needs to forensically acquire data from other sources.

The acquisition step is very crucial as a lot of irreversible errors can be made at this early step. It is important to keep the chain of custody intact, to document all steps and to verify everything that was acquired.

Digital forensic examiners will also consider processing the data. Processing electronic evidence is very important whenever time, effectiveness or large data volumes are an issue. In this step forensic examiners can prioritise certain devices or data, they can apply smart, case-specific filters (Data Mining) or they can just process the image in a way that a normal investigator can do the analysis (e.g., by recovering deleted files, mounting containers, breaking encryption, parsing application data like internet history, chat logs, etc).

"Analysis" is where a competent digital forensic examiner searches for electronic evidence on the digital forensic image(s). This step can be very time consuming and can require a lot of expert knowledge to interpret traces and artefacts. Digital forensic examiners tend to use certified digital forensic software to complete these steps. This software allows them to search for identified words, files, images, or other data that is deemed relevant to the case. Whilst this activity is undertaken by the digital forensic examiner, the investigator and Prosecutor have an important role to play which is described below in Section 9.5.

"Reporting". After all the evidence has been identified through the analysis, it should be copied so that it can be used in the court case. To fulfil this step the digital forensic examiner needs to create a report for the trial. His role is to illustrate and to translate complicated technical contexts to judges and prosecutors in a way that you can easily understand what evidence was found, where it was found, how it was found and how/when it could have gotten there.

9.5 Requests for Digital Forensic Investigation by prosecutors and judges

The part of digital forensics regarding electronic evidence collection and storage processes has been provided in the previous sections.

The provision for the digital forensic examination of digital devices and the acquisition of data from them will normally be undertaken at digital forensic laboratories. Once a digital forensic image has been obtained the analysis and reporting stages follow. As indicated above, the prosecutor and investigators have a significant role in providing the digital forensic examiner with clear instructions. Many digital forensic laboratories have templates that should be completed when the prosecutor or investigator submits the devices for examination. The accurate completion of these templates (or written requests) is crucial for the accurate analysis of the forensic image.

Where a prosecutor or investigator does not provide specific instructions, the digital forensic examiner may undertake unnecessary analysis of the evidence and not search for the significant material. These failings in communication of the instructions often result in additional costs, delays, and inaccurate reports.

The templates (or written requests) should include an accurate summary of the investigation. Details such as victims, suspects, relevant events, dates, times, and other salient information should be included in the summary. The template (or written request) should identify what is sought and this may be records of activity, types of images, details of a fraud etc., and this should be outlined. The digital forensic software used in the analysis allows for the examiner to conduct word searches. For example, if the case relates to credit card fraud, the examiner can look for numerical strings of 16 characters and if the case relates to a particular email account, the examiner can find all the records of such occurrences using word searches. The investigator and/or prosecutor should identify relevant search terms that the examiner can employ in his investigations.

ECtHR addressed the need for procedural guarantees including specific instructions for search and seizure and digital forensics of electronic evidence in Kırdök and Others v. Türkiye (3 December 2019, No:14704/12), Trabjo Rueda v. Spain (30 Mays 2017, no: 32600/12) and Särgava v. Estonia (16 November 2021, 698/19) decisions.

Reporting is determining which findings can be used for that investigation and presenting them to the judicial authorities in this direction. However, precisely for this reason, judges, and prosecutors, who are judicial authorities, should draw up a clear framework for the forensic expert who will make the technical report, including the precise scope of the analysis to be made regarding the factual background of the crime, electronic and other evidence, and the clear instructions and questions to reach to a final technical opinion. Art. 62-68 of the CPP stipulates the procedural framework for public experts. Legal authorities can also ask law enforcement and gendarmerie criminal laboratories and Forensic Institute for an expert opinion according to their special provisions.

In the report presented as a result, the technical aspect of how digital evidence is obtained, and which methods of forensic information are used should also be stated in an understandable language. The report should also include information about the incident, the time period of the research, the electronic evidence examined, information about the software and hardware used during the examination, the methods used during the examination, and the findings obtained at the end of the research. All in all, digital forensic expert reports should be lawful and auditable.

10 Requests for international cooperation in a cybercrime investigation

Cooperation between competent authorities and multinational service providers is essential to secure electronic evidence. International cooperation for Türkiye could be based on multilateral agreements (i.e.Budapest Convention, Warsaw Convention) or bilateral agreements, and in the absence of these, are to be executed within the framework of the rules of customary international law or the principle of reciprocity.

24/7 Network of the Budapest Convention (created under article 35) plays a critical role for direct exchange of information and assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. General objectives of these contact points are facilitating international co-operation, giving technical advisory to other contact points, activating the proper mechanism to

expedited preservation of data, urgently collecting evidence (stored and traffic data), and identifying and discovering suspects. The delivery of article 35 is only undertaken through the dedicated 24/7 SPOC within the Turkish National Police.

For all that, only a preservation measure, for urgent reasons and does not automatically imply disclosure of the preserved data. For example, considering of reciprocity rules, it should be remembered that most countries will not meet the production orders of Turkish authorities for criminal defamation cases for not having the criminal liability basis and standards.

Other methods to obtain international cooperation include, but are not limited to, Interpol, Europol, EuroJust, bilateral police relationships, Global Prosecutors eCrime Network (within the International Association of Prosecutors)[22] and others

[22] https://www.iap-association.org/GPEN/Home

This Project is co-funded by the European Union and the Council of Europe.
Bu proje, Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmektedir.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

This Report was prepared under the scope of the European Union and the Council of Europe Joint Project on "Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of the European Convention on Human Rights Violations in Türkiye".

This Project is co-funded by the European Union and the Council of Europe and implemented by the Council of Europe. The beneficiary institutions of the Project are the Ministry of Justice of the Republic of Türkiye and the Justice Academy of Türkiye. The contracting authority for this Project is Central Finance and Contracts Unit.

The Council of Europe is the continent's leading human right organisation. It includes 46 member states. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.