Funded by
the European Union

ONLINE ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS

A GUIDE FOR ENFORCEMENT OFFICERS

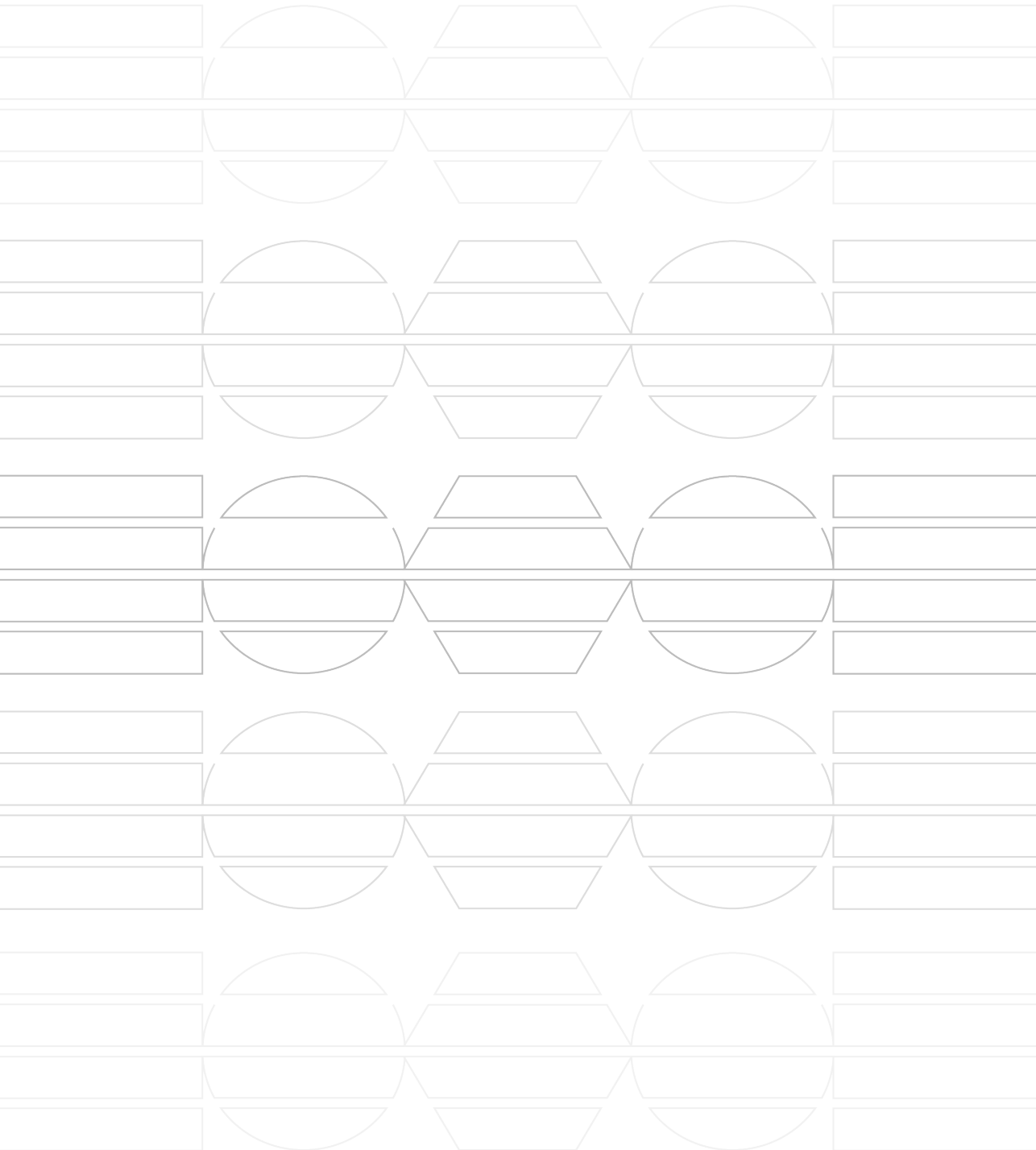
IPRproject
Intellectual Property Rights Project

Prishtinë, 2022

A project implemented by:

ibf INTERNATIONAL CONSULTING

EPLO European Public Law Organization



ABBREVIATIONS

ACPO	Association of Chief Police Officers.
CDN	Content Delivery Network.
DNS	Domain Name System
EUIPO	European Union Intellectual Property Office
GDP	Gross Domestic Product.
IEC	International Electrotechnical Commission.
IIPCIC	International IP Crime Investigators College.
IP	Internet Protocol.
IPA	Industrial Property Agency.
IPR	Intellectual Property Rights.
IPTV	Internet Protocol Television.
ISO	Internet Organisation for Standardisation.
OCRR	Office on Copyright and Related Rights.
OECD	Organisation for Economic Cooperation and Development.
OSINT	Open Source Intelligence.
SEO	Search Engine Optimisation.
TCP	Transmission Control Protocol.
TOR	The Onion Router Project.
TRIPS	Agreement on Trade Related Aspects of Intellectual Property Rights.
UNODC	United Nations Office on Drugs and Crime.
VCP	Voluntary Collaboration Practices.
VM	Virtual Machine.
VPN	Virtual Private Network.
WCO	World Customs Organisation.
WIPO	World Intellectual Property Organisation.
WHO	World Health Organisation.

CONTENTS

5. Online IPR Enforcement Measures

5.1 Introduction
5.2 Obtaining Account Information
5.3 Blocking Access to Websites
5.4 Domain Name Actions
5.5 Actions Targeted at Hosts
5.6 Money Laundering

6. Voluntary Enforcement Measures

6.1 Introduction
6.2 Voluntary Enforcement Measure Example

7. Online Investigations

7.1 Introduction
7.2 “Follow the Stream” Investigation
7.3 “Follow the Money” Investigation
7.4 “Follow the Pixel” Investigation
7.5 Best Practice

8. Open Source Intelligence

8.1 Introduction

9. Digital Evidence

10. Further Learning

1. INTRODUCTION

1.1 Purpose of Guide

The purpose of this Guide is to raise awareness of the Kosovo Police about the importance of intellectual property and the very real threat to society of infringing intellectual property rights (IPR). This Guide will also highlight the national IP system and the national legislation used to protect and enforce IPR online. In addition, the Guide will outline how the Kosovo Police can practically enforce IPR online.

A second Guide titled "*Criminal Enforcement of Intellectual Property Rights - A Guide for Enforcement Officers*" has been developed to assist the Kosovo Police investigate IPR infringements that have **not** been committed in the online environment. Both Guides complement each other and both should be read to obtain a clear picture of IPR enforcement challenges in Kosovo.

1.2 Intellectual Property

According to the United Nations, IPR crime is a transnational criminal activity managed by the same criminal organizations involved in other serious criminality, including narcotics trafficking, arms smuggling, people trafficking, corruption and money laundering[1]- but what is intellectual property?

Intellectual property refers to creations of the mind such as inventions, literary works, artistic works, symbols, names, images and designs used in commerce.[2] Furthermore, intellectual property is traditionally divided into two categories:

- **Industrial Property** which includes trademarks, industrial designs, patents and geographical indications; and
- **Copyright** which includes literary works (e.g., novels, poems and plays), films, music, artistic works (e.g., drawings, paint-

[1]Counterfeiting. A global Spread. A Global Threat. UNICRI.
[2]World Intellectual Property Organisation - What is Intellectual Property? www.wipo.int

ings, photographs and sculptures), software, and architectural design. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings and broadcasters in their radio and television programs.[3]

In order to obtain protection for an **industrial property** in Kosovo, with a few exceptions[4], the creator, or owner, has to register for protection at a government institution called the Industrial Property Agency (IPA). However, **copyright** protection is obtained automatically on the fixation of a work without the need for registration or other formalities.

The owners of intellectual property have certain rights, including the ability to authorise and prohibit others from using their intellectual property. In fact, intellectual property rights are like any other property rights. They allow the creators, or owners, to benefit from their own work or investment in a creation. These rights are outlined in Article 27 of the Universal Declaration of Human Rights, which provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions. In addition, Article 46(5) of the Kosovo Constitution states “Intellectual Property is protected by Law”.

Without IPR to reward creativity and encourage innovation it is doubtful whether inventors or creators would have the financial resources or motivation to discover new medicines, such as life-saving cancer drugs, or develop technologies which improve the quality of our lives, such as smart phones. Consequently, it is essential governments and law enforcement agencies enforce IPR not only to protect the rights of owners but to facilitate the advancement of society.

There are many types of intellectual property objects protected in Kosovo, all of which are listed at Annex I, but the Kosovo Police will most frequently encounter trademarks and copyright:

[3]World Intellectual Property Organisation - What is Intellectual Property? www.wipo.int/about-ip/en/
[4]Well-known trademarks are protected without registration, Article 6bis of the Paris Convention.

- Trademarks are signs, including words and logos, which identify brands and enable consumers to distinguish goods and services in the marketplace. Examples of trademarks are the words “Coca Cola” and “Nike”; and

- Copyright protects creative works such as literary works, films, music, artistic works, software and architectural design.

Trademarks and copyright can work together to offer protection, as an example:

- A registered trademark protects a car’s name and symbol; and

- Copyright protects the car’s software, owner’s manual and even images.

The protection of intellectual property is time limited. However the duration of protection varies for each intellectual property object. For example, copyright for individually authored works is protected for the life of the author plus 70 years. Conversely, trademarks, which are initially protected for 10 years from the time an application is submitted to the IPA, can potentially be protected indefinitely if the owner continues to submit extension applications to the IPA every 10 years.

1.3 IPR Crime - Counterfeiting and Piracy

An entity infringes an IPR when they use an intellectual property without the permission of the owner. The unauthorised use of an intellectual property is potentially a serious crime.

Counterfeiting and **piracy** are IPR infringements which refer to the unauthorised use of **trademarks** and **copyright**, respectively.

Organised criminals often smuggle counterfeit and pirate goods using the same trade routes developed for smuggling narcotics and weapons. Indeed, the profitability of counterfeit and pirate goods often exceeds that of other criminality, including narcotics.

1.4 Impact on Society of IPR Infringements

Economy

A 2019 study by the European Union Intellectual Property Office (EUIPO) and Organisation for Economic Cooperation and Development (OECD) estimated that the international counterfeit and pirate trade was worth up to USD$ 509 billion per year. However, this estimate did not include infringing products made and consumed in the same country or non-tangible digital products. If these types of products were included, the EUIPO and OECD Study opined the value of the international counterfeit and pirate trade would be several hundred billion dollars more than USD $ 509 billion.[5]

The EUIPO and OECD Study highlights the scale of funding governments and legitimate businesses are losing to the counterfeit and pirate trade. Funding which could be used to improve society (e.g. build schools, construct hospitals etc) and create jobs.

Health and Safety

The EUIPO and OECD Study also revealed counterfeiting is not confined to luxury items, such as designer watches and clothing, but has expanded to include pharmaceuticals, food, drink, medical equipment, personal care items, toys, tobacco and automotive parts, threatening consumer health and safety.

Interpol states “Trademark counterfeiting and copyright piracy are serious intellectual property crimes that defraud consumers, threaten health and safety, cost society billions of dollars in lost government revenues, foreign investments or business profits and violate the rights of trademark and copyright owners. Imitation products pose a significant safety threat to consumers worldwide. Unsuspecting customers put their health, and even life in jeopardy each time they use counterfeited products, counterfeited alcoholic beverages and food products or travel in automobiles and aircrafts maintained with substandard counterfeit parts.”[6]

[5] Trends in Trade in Counterfeit and Pirated Goods, EUIPO and OECD, 2019.

[6] International Intellectual Property Crime Investigators College, Interpol, 2016.

Whilst the World Health Organisation (WHO) claims that "Counterfeit" medicines and other health products can have harmful effects on a patient's health, including death."[7]

Organised Crime

The United Nations Office on Drugs and Crime (UNODC) has estimated the global market for illicit narcotics to be over USD$ 320 billion.[8] This is less than the EUIPO and OECD estimate for the value of the international counterfeit and pirate trade, of up to USD$ 509 billion, and highlights the attraction of counterfeiting and piracy to organised crime - especially when you contrast the resources governments and law enforcement agencies allocate to fighting the illicit narcotics trade with the resources allocated to the counterfeit and pirate trade.

According to Interpol, "Transnational organized criminals generate hundreds of billions of dollars annually from the manufacture and distribution of fake (counterfeit and pirate) products, due in part, to the relatively low level of risk and comparatively high level of profit. There is an ever growing need for facilitation and coordination of international efforts in combating this criminality, which operates across international borders and has very serious consequences for the public." [9]

1.5 Disclaimer

This document does not supersede, nor is meant to substitute the requirements of international law, national law or any government regulation or policy.

[7] International Medicinal Products Anti-Counterfeiting Taskforce, 2015
[8] United Nations Office for Crime and Drugs, Annual Report, 2014.
[9] International Intellectual Property Crime Investigators College, Interpol, 2016.

2. THE INTELLECTUAL PROPERTY SYSTEM

2.1 Government Institutions

Introduction

In Kosovo, combating IPR infringements, including counterfeiting and piracy, effectively requires a coordinated effort from multiple institutions, including:

- Industrial Property Agency (IPA);
- Office on Copyright and Related Rights (OCRR);
- Kosovo Customs;
- Market Inspectorate;
- Kosovo Police;
- Prosecutorial Council; and
- Judicial Council.

Industrial Property Agency

The Industrial Property Agency (IPA) is an administrative body within the Ministry of Trade and Industry. It is based in Pristina and has the following responsibilities:

- Developing procedures for issuing patents and supplementary protection certificates;
- Developing procedures for the registration of trademarks, industrial designs, topographies of integrated circuits, designation of origin and geographic indications;
- Compiling and maintaining records prescribed by the basic Law;
- Proposing, designing and publishing the Official Bulletin of IPA, which contains information about the application and the rights granted to industrial property;
- Contributing to, developing and promoting industrial property protection;

- Initiating and proposing the ratification of international agreements in regard to the industrial property area;
- Providing information services in regard to industrial property facilities;
- Organising testing for the authorised representatives of the industrial property right area;
- Preparing proposals for approval of the legal and sub-legal acts in regard to the industrial property area;
- Cooperating with other organisations to implement legal provisions regulating industrial property; and
- Representing Kosovo on international organisation for industrial property.[10]

The IPA can assist police and prosecutors:

- Confirm whether an industrial property (e.g., trademark, industrial design etc.) is protected in Kosovo; and
- Identify the owner of an industrial property right.

Office on Copyright and Related Rights

The Office on Copyright and Related Rights (OCRR) is a department within the Ministry of Culture, Youth and Sports. It is based in Pristina and has the following responsibilities:

- Licensing collective management organizations;
- Supervision of collective management organizations;
- Revoking licenses of collective management organizations;
- Providing information to authors, right holders and the general public about copyright and related rights;
- Monitoring developments in international legislation, with respect to copyright, and subsequently making recommendations to the government.[11]

[10]Ministry of Trade and Industry https://kipa.rks-gov.net/page.aspx?id=2,17
[11] Ministry of Culture, Youth and Sport https://www.mkrs-ks.org/?page=2,102

The OCRR can assist police and prosecutors contact collective management organizations who can:

- Confirm whether a copyright or related right is protected in Kosovo; and
- Identify the owner of a copyright or related right.

Kosovo Customs

Kosovo Customs is part of the Ministry of Economy and Finance. Their Headquarters is based in Pristina but they also have control points at:

Airport.	Merdare.	Qafa Morinë.	Zubin Potok.
Dheu i Bardhë.	Muqibaba.	Quafa e Prushit.	Mitrovica.
Hani i Elezit.	Mutivoda.	Vërmica.	Podujeva.
Interevropa.	Peja.	Leposaviq.	Kula.[12]
HQ Pristina	Glloboqica		

The responsibilities of Kosovo Customs include preventing the import and export of goods, which infringe IPR.

All customs officers are authorised to act ex-officio to intercept goods which they suspect infringe an IPR and, in addition, there is a dedicated IPR Unit within the Operational Investigative Department of the Law Enforcement Directory. The IPR Unit is situated at Headquarters and its responsibilities include:

- Receiving applications for action from IPR owners;
- Distribution of accepted IPR applications for action to control points;
- IPR training for Customs officers; and
- Liaising with IP right holders.

[12] Kosovo Customs www.dogana-ks.org

Kosovo Customs can provide police and prosecutors with the details of shipments they have intercepted containing IPR infringing goods, including the name of the importer and/or exporter. Kosovo Customs can also check the history of shipments to addresses or entities, targeted by police and prosecutors.

Market Inspectorate

The Market Inspectorate is an executive organ within the Ministry of Trade and Industry, which carries out market supervision in the territory of Kosovo. Their Headquarters is based In Pristina but they have offices across Kosovo.

Market inspection authorities have the competence and resources to:

- Inspect locations linked to commerce;
- Check business documentation;
- Inspect goods and services;
- Demand information linked to business;
- Seize evidence of an offence linked to commerce;
- Prevent the release of goods and services into the market; and
- Suspend a business from operating.

The responsibilities of the Market Inspectorate include ensuring that goods and services which are manufactured or used in commerce, in Kosovo, do not infringe IPR.

The Market Inspectorate can assist the police and prosecutors investigate businesses they suspect are manufacturing, importing, exporting or selling goods or services which infringe an IPR.

Kosovo Police

Kosovo Police is part of the Ministry of Internal Affairs. Their Headquarters is situated in Pristina but they also have a presence in every municipality.

All police officers can act ex-officio to prevent IPR infringements. However, complaints concerning IPR infringements that do not involve online protocols, that require investigation, should be brought to the attention of the Unit for Economic Crimes, in the Economic Crimes and Corruption Directory. Conversely, complaints concerning IPR infringements involving online protocols should be brought to the attention of the Cybercrime Unit.

State Prosecutor

The State Prosecutor is an independent institution with the authority and responsibility for the prosecution of persons charged with committing criminal acts or other acts as specified by law. It includes the:

- Basic Prosecution Office;
- Appellate Prosecution Office;
- Special Prosecution Office; and
- Office of the Chief State Prosecutor.[13]

The State Prosecutor does not have a dedicated IPR Unit however, all prosecutors are competent to investigate and prosecute IPR crimes, either ex-officio or on complaint.

The contact details for each of the institutions mentioned above can be located at Annex II.

[13]State Prosecutor https://www.rks-gov.net/EN/f46/judiciary/state-prosecutor

2.2 Cooperation

State Intellectual Property Council

In the majority of countries there are multiple institutions charged with the protection of IPR. Frequently these institutions have overlapping responsibilities. Consequently, it is incumbent on the government and institutions to develop a cooperation model that will ensure the efficient and effective protection of IPR.

In Kosovo, the government has established the State Intellectual Property Council to improve cooperation between institutions involved in the protection and enforcement of IPR.

The Council delivers advice and assistance to the government and other stakeholders involved in the protection and enforcement of IPR.

The Council includes representatives from the institutions discussed under the heading **2.1 government Institutions**, specifically:

- Industrial Property Agency (IPA);
- Office on Copyright and Related Rights (OCRR);
- Kosovo Customs;
- Market Inspectorate;
- Kosovo Police;
- Prosecutorial Council; and
- Judicial Council.

In addition, representatives from the following institutions are also associate members of the Council:

- Drug and Medical Product Agency, for advice on falsified, including counterfeit, medicines and medical devices;
- Veterinary and Food Agency, for advice on counterfeit food and drink;
- Agency for Environment Protection, for advice on environmental issues; and

- Agency for Managing of Sequestrated or Confiscated Assets for advice on confiscation of assets from IPR criminals.

Task Force against Piracy and Counterfeiting

On 4th October 2012, the government adopted a **Strategy Against Piracy and Counterfeiting**, covering the period from 2012 to 2016. The **Strategy** was drafted by the OCRR in cooperation with other institutions responsible for the enforcement of IPR. The **Strategy** aimed to create mechanisms for combating counterfeiting and piracy to improve Kosovo's image and economy.

The Strategy established a Task Force with the following mission:

- Promote effective cooperation between public authorities and social and economic organisations in the field of copyright protection;
- Ensure and coordinate the implementation of the Strategy and the action plan against piracy and forgery;
- Develop and implement public awareness programs and campaigns; and
- Prepare and deliver proposals for drafting legislation related to copyright enforcement

The Task Force includes the following permanent members:

- Director of OCRR;
- Chief Inspector of Market Inspectorate;
- Director of IPA;
- Head of Intellectual Property Sector, Customs;
- Head of Economic Crimes Investigation Sector, Police;
- Head of Cybercrime Investigation Sector, Police;
- Representative of State Prosecutor; and
- Chief of Agency for Managing of Sequestrated or Confiscated Assets, Ministry of Justice.

In addition to the permanent members, the following bodies can be invited to attend meetings:

- Executive Chief of Independent Media Commission;
- Chairman of Directors' Board of Regulatory Authority for Postal and Electronic Communications; and
- Other independent Institutions and organisations.

It is also pertinent to note that the following international organisations have dedicated IP units that may be able to assist with capacity building and cross border investigations:

- Europol;
- Interpol;
- European Commission (Director General Taxation and Customs Union);
- World Customs Organisation (WCO); and
- EUIPO Observatory on Infringements of IPR.

The contact details for each of the above institutions can be located at Annex II.

3. ONLINE IPR INFRINGEMENTS

3.1 Introduction

IPR infringements are increasingly taking place in the online environment. This growing threat to not just the economy but also the health and safety of consumers has led to several recent policy announcements by concerned governments and law enforcement agencies.[14]

Furthermore, IPR infringements in the online environment are diverse, both with regard to the 'content' of the infringement and to the technological means used.[15]

3.2 Types of Online IPR Infringements

Illegal Distribution of Copyright Protected Works.

Copyright infringement, or piracy, arises whenever a protected work is used without the authorisation of the copyright holder and when this activity cannot be regarded as permitted use under one of the applicable exceptions or limitations to copyright.[16]

In the internet era, copyright infringement has become easier, even when committed on an industrial scale. Four popular methods used to infringe copyright online are:

Streaming: This category includes any sites that primarily allow access to unauthorised content via online streaming directly from an end-user's web browser. Sites typically offer a wide range of content, directly searchable from within the site. Some sites host infringing content themselves, but the majority provide links to external hosts (it should be noted that the Court of Justice of the European Union[17] has ruled the transient copies made in the end user's computer while watching the streaming constitute, as a rule, an infringement of the re-

[14]Europol's Serious and Organised Crime Threat Assessment (2017), the EU Customs Action Plan to combat IP infringements (2018-2022), the European Commission's Communication on an Intellectual Property Action Plan (COM 2020 760) and the joint Europol and EUIPO Intellectual Property Crime Threat Assessment (2019).

[15]'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.

[16]Law No. 04/L-065 on Copyright and Related Rights, Chapter IV - Limitations of Author's Rights.

[17] Although not a member of the EU, Kosovo is a potential candidate country for EU membership.

production right and does not benefit from the exception for temporary acts of reproduction).[18]

- **Download**: Includes any sites that primarily allow use of unauthorised content via a direct download in the user's web browser. Sites in this category typically offer a wide range of content, directly searchable from within the site, and downloadable in their entirety. The sites rarely host the content themselves, and link to other sites which host the content;

- **Stream ripping**: Sites in this category allow the ripping, mainly of audio, into downloadable files. This process takes place directly in a user's web browser. Typically, the user simply needs to enter a URL to instantly start the download of the MP3 file. Stream ripping is typically used to rip the audio from music videos, often from legitimate sources. Some sites allow users to rip video content and save it as a video file; and

- **Torrent**: A torrent download portal allows a visitor to search for any content, and then download a small file that initiates the process of downloading the full product. Users of torrent sites must have a separate piece of software, called a torrent client, installed on their device. This is a peer-to-peer (P2P) download process, so the content is not received directly from the site, and instead comes from other torrent users who are sharing the same content. Torrenting can be public, where all torrent download portals are open for anyone to use, or private, where only members of the site can log in and access the site's content. Most private torrent sites operate an invite-only policy on membership.

[18]CJEU Case C-527/15, Filmspeler.

Distribution of IPR Infringing Goods

According to figures from Eurostat, about 71 % of internet users in the EU shopped online in 2019[19] and a large portion of this trade took place through online marketplaces, social media platforms and web shops that operate under a dedicated domain name.

The growth in legitimate online trading is, however, paralleled by a growth in illicit trade. Consequently, online marketplaces, social media platforms and web shops are being used by vendors not only to sell legal goods but also to sell illicit goods such as counterfeit clothes and counterfeit mobile phones[20]. Furthermore, websites, which at first glance appear to be official websites of a particular brand owner, sometimes turn out to be bogus sites selling counterfeit goods. These websites often use domain names that include a third-party trademark and the content and design of the website itself resembles that of the brand owner [21].

Fraud, Extortion and other Traditional Cybercrime Offences

Trademarks are used for acts that are criminal offences from the outset, such as phishing scams. The term phishing is used to describe malicious attempts to acquire money, sensitive information and/or install malware that is initiated through contact with potential victims via emails, postings on social media platforms, blogs or text messaging. The phishing attempt will immediately appear to be sent in good faith and for a legitimate purpose. Furthermore, it will often appear to have been sent by an established company since the sender's address makes use of a domain name, which may be a trademark, that resembles the genuine domain name of that company.

An attacker will often have established a spoofing website, that is, a

[19] As referred to in the Digital Agenda Scoreboard, 2019 https://ec.europa.eu/digital-single-market/en/use-internet and available at http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals

[20]Illustrative examples can be found in Canvas 8 and Canvas 9 in 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.

[21]See 'Research on Online Business Models Infringing Intellectual Property Rights — Phase 2 Suspected trade mark infringing e-shops utilising previously used domain names', EUIPO 2017.

website that is a close imitation of the official website of the impersonated company or person, which is why a visit to the website does not create any suspicion about the malicious circumstances.[22] The phishing communication will usually contain a hyperlink to the said website, but the website can also be visited independently. At the website, the victim will be prompted to reveal information such as 'updated' credit card details, 'confirmation' of passwords and similar sensitive information.

Depending on what the user is lured into doing, such acts may result in one or more criminal offences. It is fraud if the attacker manages to lure the victim into paying a sum for a non-existing obligation or a non-existing product or service. If the attack results in installation of ransomware, it can be characterised as extortion, and installation of malware may amount to vandalism.

Cybersquatting and other IPR Infringing Uses of Domain Names

Cybersquatting is the registration and use of a domain name that is identical or confusingly similar to another's trademark and where the registration and use is in bad faith and with the intention to somehow profit from the registration and use.[23]

A variation of cybersquatting is *typo squatting* where a registrant acquires misspellings of another's domain name with the intention of catching and exploiting the traffic that was intended for the genuine websites.
Both phenomena continue to take place in high numbers,[24] which may be explained not only by the implementation of the many new generic top-level domains such as. xyz and. top, but also by the continuous development of ways to gain revenue from such registrations such as 'pay-per-click' revenues and revenues based on affiliate advertising schemes.[25]

[22]See Canvas 16 in 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016
[23]WIPO Definition of Cybersquatting.
[24]WIPO Cybersquatting Case Filing Surges During COVID-19 at: https://www.wipo.int/amc/en/news/2020/cybersquatting_covid19.html
[25]See the description of such revenue schemes in paragraph 5.3.2 in 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.

4. LEGISLATION

4.1 Introduction

A number of legislative measures have been adopted at the international and national level to strengthen and harmonise the protection and enforcement of IPR, including the online environment. These measures contain provisions which enable right holders and law enforcement agencies, such as the police, to enforce IPR effectively.[26]

4.2 The TRIPS Agreement

The Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) obliges the 164 members of the World Trade Organisation (WTO) to provide harmonised minimum standards related to the protection and enforcement of IPR.[27] In particular, the TRIPS agreement contains the following enforcement related provisions, which are relevant to not just the physical but also the online environment:

- Article 47 - Right to obtain information on the infringement and infringers;
- Article 50 - Provisional measures to prevent an infringement and preserve evidence;
- Article 51 - Suspension of release of infringing goods by customs authorities; and
- Article 61 - Criminal procedures and penalties.

4.3 The Cybercrime Convention

The Cybercrime Convention, which has been signed by both EU member and non-member states, has established a number of instruments that are of relevance to IPR enforcement in the online environment. The Convention explicitly covers offences related to the infringement of copyright and related rights but no other IP objects. However, provisions on computer related forgery and fraud could indirectly encompass the misuse of third-party trademarks in phishing scams.[28]

[26] See the overview of these legislative measures below in Chapter 7.
[27] https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm
[28] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

4.4 National Legislation

Kosovo has adopted a number of legislative instruments that are capable of being used to combat and prevent online IPR infringements.

Substantive IPR legislation

The substantive IPR Laws, enacted by the government in Kosovo, are:

- Law No. 04/L-026 on Trademarks (amended by Law No. 05/L-040);
- Law No. 05/L-058 on Industrial Designs;
- Law No. 04/L-029 on Patents (amended by Law No. 05/L-039);
- Law No. 04/L-065 on Copyright and Related Rights (amended by Law No. 05/L-047 and Law No 06/L-120);
- Law No. 02/L-098 on Protection of Plant Varieties;
- Law No. 05/L-051 on Geographical Indications and Designations of Origin; and
- Law No. 03/L-165 on Determining the Rights and Protection of Topographies of Integrated Circuits.

The substantive IPR legislation outlines how to obtain IPR protection and the scope of the exclusive rights enjoyed by the right holder, including the fact a right holder can prevent third parties from using their IPR without permission.

Most of the provisions in the substantive IPR legislation are 'technology neutral', meaning that the provisions apply regardless of which technological means are used to produce the protected creations or which means are used for an infringing activity e.g. Article 8(2) of Law No. 04/L-026 on Trademarks states the holder of the trademark may prohibit "using the sign on business papers and in advertising." This provision not only relates to physical advertising but also, to the use of an infringing sign as a domain name[29] or Ad Word[30].

[29]CJEU Case C-657/11, BEST v Visys.
[30]CJEU Case C-236/08 et al., Google v Louis Vuitton

The substantive IPR legislation also contains enforcement measures and remedies, similar to the TRIPS Agreement, that are available to right holders and law enforcement agencies, including:

- Right to obtain information on the infringement and infringers; and
- Provisional measures to prevent an infringement and preserve evidence.

The Law on the Information Society Services

Articles 24 to 26 of Law No. 04/L-094 on the Information Society Services is also of major importance in regards to online IPR enforcement. The Law on the Information Society Services outlines the liability of internet intermediaries, which includes their liability in cases where their services are used to infringe IPR. In that context, the Law on the Information Society Services operates with three categories of intermediary services, namely:

- 'mere conduit' - a service that consists of the transmission in a communication network of information from the recipient of the service or the provision of access to a communication network;
- 'caching'- a service that consists of the transmission in a communication network of information for the recipient of the service, including the automatic, intermediate and temporary storage of that information, storage performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request; and
- 'hosting' - the storage of information provided by the recipient of the service.

Article 28 of Law No. 04/L-094 on the Information Society Services is based on the principle that the intermediaries are not obliged to moni-

tor the information, which they send or store, nor do they have a general obligation to actively seek facts or circumstances indicating illegal activity. However, if an intermediary has obtained knowledge or has become aware of such illegal activities the intermediary is required to act expeditiously to remove or to disable access to the information if it is to stay within the 'safe harbour' provisions of the Law.

Criminal Code

The IPR offences listed in the Criminal Code (Law No.06/L-074) are:

- Article 289 "Violating patent rights";
- Article 290 "Violation of copyrights";
- Article 291 "Circumvention of technological measures"; and
- Article 292 "Deceiving consumers".

The actual wording of the offences is reproduced at Annex III.

The Law on Customs Enforcement of IPRs

The Law No. 06/L-015 on Customs Measures for the Protection of IPR provides the procedural rules for customs authorities to enforce IPR in relation to goods that are liable to customs supervision or customs control at the border. If such goods are suspected of infringing an IPR, the release of the goods may be suspended and the goods may be detained by customs authorities at the border if the requirements laid down in the Law have been met.

Law No. 06/L-015 on Customs Measures is applicable to goods that have been acquired and have been shipped from a location outside of Kosovo to a customer within Kosovo, regardless of whether the purchase was completed online or otherwise.

Enforcement in the field of illegal Internet Protocol Television (IPTV), however, presents specific challenges. This is because while fully loaded set top boxes are infringing copyright and fall squarely within the scope of customs action, 'vanilla' devices (i.e. set top boxes that are not yet configured to receive illegal streaming) do not directly infringe any intellectual property. These devices can be sold as such to end users, who will then configure them themselves by following instructions provided by the reseller or found on forums and discussion groups. However, 'vanilla' devices manufactured by dubious businesses may present hazardous features that make them illegal under safety standards.

5. ONLINE IPR ENFORCEMENT MEASURES

5.1 Introduction

Production, marketing, distribution and sale of illicit goods such as pirate software or counterfeit brands are by definition unlawful acts. As discussed above, the applicable IP legislation provides the right holder with the exclusive right to the original products. Traditionally, the right holder can pursue the producer, distributor or vendor of IPR infringing goods through the court or administrative system. However, such actions are complicated when the online environment is used to infringe IPR. Consequently, right holders and law enforcement agencies, including the police, have looked for other ways to pursue IPR infringements in the cross-border online environment. This development has led to a situation where the various online intermediaries have become the 'natural points of control' when it comes to IPR enforcement.

Online intermediaries have acquired an important role in managing online behaviour and enforcing the rights of Internet users. They offer a natural point of control for monitoring, filtering, blocking and disabling access to content, which makes them ideal partners for performing civil, administrative and criminal IPR enforcement.[31]

[31]Quote from p. 9 in Perel Filmar, Maayan and Elkin-Koren, Niva: Accountability in Algorithmic Copyright Enforcement (21 February 2016). Stanford Technology Law Review, Forthcoming. Available at: SSRN: https://ssrn.com/abstract=2607910 or http://dx.doi.org/10.2139/ssrn.2607910

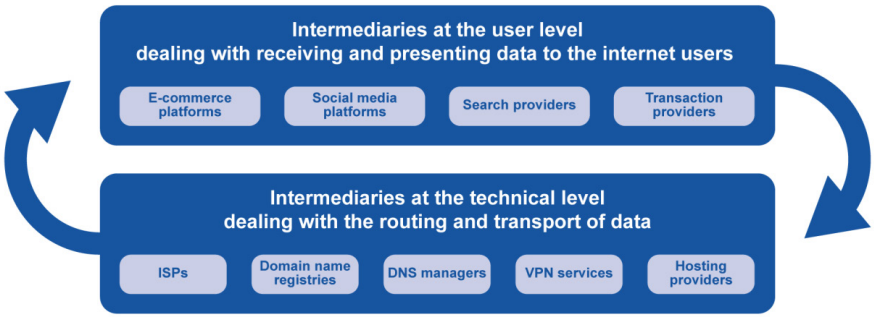


Figure 1 - Examples of Online Intermediaries[32]

As highlighted in Chapter 4, a number of legislative measures have been adopted at both the international and national level to strengthen and harmonise the protection of IPR in the online environment. These measures include remedies, which aim to enable right holders and law enforcement agencies, such as the police, to enforce IPR in an effective manner, including:

- Obtaining account information;
- Blocking access to websites;
- Domain name actions; and
- Actions targeted at hosts.

In addition to the specific legislative measures that have been adopted to strengthen and harmonise the protection of IPR in the online environment, traditional measures, such as money laundering, should not be overlooked or forgotten by the investigating officers.

[32]Study on Legislative Measures Related to Online IPR Infringements, EUIPO, 2018.

5.2 Obtaining Account Information

Establishing the identity of a suspected IPR infringer is complicated when it comes to the online environment, since the identity of the suspected infringer is not immediately available.

When copyright protected material such as live music, sports events and sharing files containing copyrighted works, such as films and music, are streamed it is often possible to determine the IP address that has been used for the infringing activities. However, further investigative actions are required to establish the identity of the entity that used the particular IP address in the execution of an IPR infringement. Additionally, an alleged infringer might conceal their IP address by technical means or use a third party IP address.

If the infringing activity takes place on a dedicated website or an online platform of a third party, such as an online marketplace or a social media platform, it may be possible to identify the 'account' of the alleged infringer. While the specific identification of the holder of the account is not immediately available to third parties such information is privy to the operator of the marketplace or social media platform.

Websites that are used to promote or to distribute products or services that are suspected of infringing the IPR of a third party do seldom - if ever - contain true and reliable information on the party controlling the website, neither in the form of an imprint nor in the form of other contact information. Domain registries will maintain a publicly available WHOIS database of the registrants, but the correctness of the information in these databases does to a large extent depend on the correctness of the information that is provided by the registrants and this is not always true and correct.[33] Additionally, in certain top-level domains, registrants of a domain name can rely on the use of a privacy or proxy service, which conceals the identity of the real registrant in the WHOIS register.

[33]The issue of false contact information is mentioned several times in the WIPO Overview of WIPO Panel Views on Selected UDRP (Uniform Domain Name Dispute Resolution Policy) Questions, Third Edition, available at: <http://www.wipo.int/amc/en/domains/search/overview3.0/>. See as an illustrative example, Section 6B in WIPO Case DNL2017 'Dr. Martens' International Trading GmbH / 'Dr. Maertens Marketing GmbH v Olga Olga' on the domain name <doktermartens.nl>.

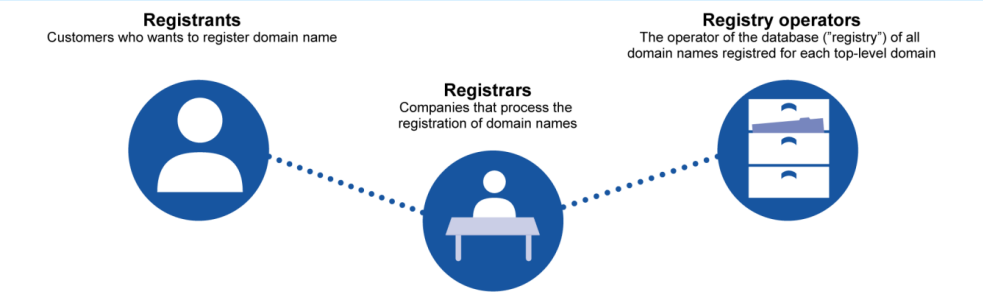


Figure 2 - Registration of Domain Names[34]

It is therefore important - and in most cases essential - to establish whether an online intermediary whose services are being used by one of their customers to carry out IPR infringing activities can be ordered to disclose information on the identity of the customer that they have in their possession.

Disclosure of the Identity of the Holder of a Particular Account

The right to information in IPR infringement cases is stipulated in the substantive IPR legislation e.g. Article 100 of Law No.04/L-026 on Trademarks. As an example, according to this provision the competent judicial authorities may order anyone involved in an IPR infringement to disclose:

- Information on names and addresses of producers, distributors, suppliers and other earlier owners of products and services, wholesale and retail sellers; and
- Information on quantities produced, distributed, received and ordered as well as the prices per product and services.

[34]Study on Legislative Measures Related to Online IPR Infringements, EUIPO, 2018.

In criminal investigations, the police and/or prosecutor, can make an application to the competent judicial authority to order an internet intermediary to disclose such account information, if the request meets the general procedural requirements of being 'justified and proportionate'.

Contact Information on the Holder of a Specific Account

In relation to contact information for the holder of a specific account in the online network or platform, such as a social media network or a digital marketplace, it is possible in civil procedures to get a judicial decision that orders the provider of the online service to disclose this information.

In criminal investigations, the police and/or prosecutor, can make an application to the competent judicial authority to order an internet intermediary to disclose account information on specific costumers.

Contact Information on Entities using an IP Address for IPR Infringing Activities

As regards the contact information on a person or an entity that uses an IP address or makes a server available under an IP address provided by its access provider, the overall picture is the same as for the abovementioned account information: it is possible in Kosovo to use the civil law to get a judicial decision that orders the provider of the online service to disclose this information.

In criminal investigations, the police and/or prosecutor, can make an application to the competent judicial authority to order an internet intermediary to disclose contact information of a person or an entity that uses an IP address or makes a server available under an IP address provided by its access provider.

5.3 Blocking Access to Websites

Introduction

If an IPR infringing activity takes place on or through a dedicated website, an effective way to disrupt the current activities and to prevent them from taking place in the future is to block access to the website. Blocking orders have, therefore, become an import legal remedy that is frequently used by both rights holders and by police / prosecutors.

Another reason for the effectiveness and popularity of this measure is that the target of a blocking order are the various access providers that provide technical access to the internet. These providers are established companies that can be immediately identified and thus be the subject of legal action.

Blocking access to a website is, however, a limited and targeted legal measure. The website as such will thus still exist and may be accessible for those internet users, whose access provider is not covered by the blocking order, including providers in other jurisdictions.

The Kosovo Courts only have jurisdiction over matters that are related to or have an effect on the territory of Kosovo. Blocking orders can, therefore, as a starting point only be issued if the activities on the website at issue infringes or may infringe IPRs that are protected in Kosovo.[35]

Liability of Intermediaries

The general rule on the exemption of the liability of access providers is set out in Article 24(1) of Law 04-L/094 on the Information Society Services and implies that the access provider is not liable for the information that is sent by its customers, if certain, specified conditions are met. This “safe harbour” provision does not, however, affect the possibility for the courts or the administrative authorities to require the access providers terminate or prevent infringements. It follows that

[35]CJEU Case C-324/09, L’Oreal v eBay.

rights holders and law enforcement agencies are in a position to apply for an injunction against intermediaries whose services are used by third parties to infringe IPRs.

Blocking Injunctions

A blocking injunction is a court order to an access provider to block users' access to a certain list of websites. These injunctions have proven to be more effective than orders or requests to hosting service providers to take down offending websites. This is because operators of these websites can easily move to another hosting service, and to move again to hosts based in remote jurisdictions which do not respond to notice and takedown requests. By contrast, blocking injunctions to internet access providers make the website unavailable to users in the country where the order is made regardless of the host where the website is located.[36]

Dynamic Blocking Injunctions

Blocking injunctions can specify not only the domain name and IP address of the website(s) to block access but also any further domain names under which infringements relating to the same rights are committed. Such 'dynamic' orders extend the efficacy of blocking access to a website and allow preventing future infringements.

Live Blocking Injunctions

Blocking Injunctions can work by requiring internet access providers to block users' access to servers hosting infringing streams of live sporting events. The so-called 'live' blocking orders are particularly effective in tackling illegal IPTV, as they target specifically the servers that stream illegal content during live events broadcast.

[36] The CJEU in UPC Telekabel (Case C-314/12) has found this type of injunction compatible with EU law, providing that they do not deprive internet users from the possibility of lawfully accessing the information available and they have the effect of preventing (or of making more difficult) the access to infringing content.

De-Indexing Injunctions

These injunctions request search engines to de-index infringing websites, so that the links to those websites do not appear in the list of search results.

5.4 Domain Name Actions

Introduction

As mentioned in Chapter 3, domain names play a key role in various types of IPR infringements in the online environment, including cybersquatting and phishing scams.

Domain names are also used as internet addresses for websites that contain infringing content, including websites with links to illegal digital content, websites that contribute to video streaming and torrent websites.[37] In these situations it is not the domain name per se that is infringing but the content of the website.

If a domain name is used for IPR infringing activities, a court may order the infringer to cease the infringing activities under the domain name, just as the court may impose damages, fines and other sanctions, whether civil, administrative or criminal.

Within the last few years, law enforcement agencies in a number of countries have obtained court orders in which a large number of domain names have been seized. The most notable is "Operation In Our Sites" that is coordinated by Europol[38] and has seized 10,000s of domain names that were used as internet addresses for IPR infringing websites.

The legal basis that is applied to seize domain names is typically the general provisions on forfeiture. However, since a domain name is not a physical commodity that can be detained, the seizure entails an order to ensure the domain names are not transferred, deleted or otherwise released.

[37]See the business models described in Canvasses 21, 22, 23 and 25 in 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.
[38]https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-in-our-sites-ios

5.5 Actions Targeted at Hosts

Introduction

As mentioned above in Section 5.1, the various online intermediaries have become the 'natural point of control' when it comes to enforcement. This is particularly so for those intermediaries that act as hosts - companies that operate online platforms from or on which IPR infringing activities take place. Examples of hosts are digital marketplaces[39] and social media platforms.[40]

Liability of Intermediaries

The general rule on exemption of liability for hosting providers is set out in Article 26(1) of Law 04-L/094 on the Information Society Services and the provision implies that the provider is not liable for the information that is stored by their customers, if specified conditions are met. This so-called "safe harbour" provision does not, however, affect the possibility for the courts to require hosting providers to terminate or prevent IPR infringements.

Consequently, there are several procedures that can potentially be taken against intermediaries that act as hosts, including:

- Taking down sales or advertisements for IPR infringing goods; and
- Blocking accounts used to distribute IPR infringing goods and services.

[39]See Canvas 8 Marketing Goods or Digital Content on Third Party Online Wholesale Marketplace (B2B) in 'Research on Online Business Models Infringing Intellectual Property Rights. Phase 1 Establishing an overview of online business models infringing intellectual property rights', EUIPO, July 2016.

[40]See Canvas 9, Sale of Non-Genuine Goods through Social Media Networks, in 'Research on Online Business Models Infringing Intellectual Property Rights. Phase 1 Establishing an overview of online business models infringing intellectual property rights', EUIPO, July 2016.

Taking Down Sales or Advertisements for IPR Infringing Goods

A 'takedown' is at the outset a procedure whereby a third party can file a complaint ('a notice') to an operator of an online marketplace, a social media platform or a similar platform and request the operator of the platform to remove ('take down') a product that is offered for sale or advertised on the marketplace by a third party. It is then the individual operator of the platform concerned that decides whether to accept or to reject the complaint, that is, whether to take down the infringing listing or not.

Such 'Notice and Takedown' procedures are implemented and applied by most digital marketplaces as well as by most social media platforms and they form an integrated part of the platform's terms and conditions. In many countries, 'Notice and Takedown' procedures are used in huge numbers daily and are generally perceived as efficient tools when it comes to enforcement if IPRs in the digital environment.[41]

However, if the operator refuses to act, not only do they become liable for the IPR infringement, but it is also possible to apply for a court order to force the operator to act.

Blocking Accounts Used to Distribute Infringing Goods and Services

In addition to the possible takedown of actual sales offers or advertisements, a third party can file a complaint to an operator of an online marketplace, a social media platform or a similar platform and request the operator of the platform to block or suspend the account used to distribute IPR infringing goods and services. It is then the individual operator of the platform concerned that decides whether to accept or to reject the complaint.

However, if the operator refuses to act, not only do they become liable for the IPR infringement, but it is also possible to apply for a court order to force the operator to act.

[41] 'A Digital Single Market Strategy for Europe', Communication from the European Commission, 6 May 2015, COM(2015) 192 final, Section 3.3.2., p. 12; 'Communication on Online Platforms and the Digital Single Market' {COM(2016) 288}, Section 5.II), p. 7 ff.

5.6 Money Laundering

Commercial scale IPR infringements are by definition all about earning money and, as stated in Section 1.4, the money involved in IPR infringing activities is huge.[42]

The 'follow the money' approach is regarded as an important means to prevent and combat illicit activities, including IPR infringements. This approach does not only enable the authorities to identify, seize and confiscate the money but it also enables or at least facilitates the identification of the perpetrators.

The Swedish case SweFilmer[43] illustrates how the 'follow the money' investigative approach, and anti-money laundering enforcement measures, can be used to investigate IPR infringements. In the SweFilmer case, the streaming of unlicensed audio visual works and underlying money laundering activities were central to the investigation. The main defendant was subsequently charged with both copyright infringement and money laundering. The case ended at first instance with a finding of guilt resulting in a custodial penalty and payment of damages to the rights holders.

Article 302 of the Kosovo Criminal Code and the Law on the Prevention of Money Laundering and Terrorist Financing establishes money laundering as a crime in Kosovo.

[42]Trends in Trade in Counterfeit and Pirated Goods, EUIPO and OECD, 2019.

[43]Varberg Regional Court Case No T-1463-15 and Göta Appeal Court, Case No B 1565-17, 22 February 2018.

6. VOLUNTARY ENFORCEMENT MEASURES

6.1 Introduction

As right holders and law enforcement agencies cannot be expected to investigate and initiate legal action against every online IPR infringement, they have sought other solutions to disrupt the activities of IPR infringers, such as Voluntary Collaboration Practices (VCPs).

VCPs are intended to respect both the law and the fundamental rights of citizens, while combating IPR infringements, including online IPR infringements. VCPs typically consist of codes of conducts and practices aimed at taking down IPR infringing sites, removing advertising from IPR infringing sites or denying IPR infringing sites access to online payment systems.

VCPs usually share certain commonalities, specifically:

- They are voluntary and therefore do not impose compulsory sanctions for not complying with the duties and procedures envisaged by them;
- They establish preventive and/or proactive measures in order to prohibit or to detect infringements of intellectual property; and
- The majority of VCPs do not involve any costs or fees to stakeholders.

6.2 Voluntary Enforcement Measure Example

As an example, in Austria, after consultation with right holders, the Austrian Advertising Industry (Werberat) developed a VCP as part of their self-regulatory Ethics Code for the Austrian Advertising Industry.

According to this Austrian VCP, it is contrary to advertising principles to place an advertisement in an unlawful environment, such as an infringing website.

In practice, on receipt of a right holder complaint about an advertisement, the Werberat carries out a preliminary examination. If the Werberat considers the complaint justified, it issues a request to the responsible advertising agency or advertiser to review the advertisement within three working days. The requests of the Werberat are not legally binding and the Werberat cannot sanction copyright infringements.

If the advertiser agrees to remove the advertisement, no further action is taken. However, if the advertiser considers the right holder complaint unfounded, the complaint and the grounds for the advertiser's disagreement are referred to the (advertising) Small Senate for a decision.

The vast majority of advertisers remove the highlighted advertisement without reference to the Small Senate, thus depriving the infringer of income.[44]

In Kosovo, right holders and law enforcement agencies, including the police, should work with intermediaries to develop VCPs to prevent online IPR infringements.

[44]Study on Voluntary Collaboration Practices in Addressing Online Infringements, EUIPO, 2016.

7. ONLINE INVESTIGATIONS

7.1 Introduction

Investigations are usually initiated by right holders who, sometimes, provide the authorities with a full private investigation file, including statements, photographs and surveillance.

The importance of comprehensive contributions from right holders must be stressed as this helps to deliver high-performance policing through the efficient and effective deployment of resources. For example, if right holders agree *a priori* on the structure, approach and format of an investigation file this will result in a coordinated and homogenised approach, allowing law enforcement agencies to perform a more effective and streamlined investigation.

In addition, as discussed previously, to overcome legislative boundaries relating to intellectual property laws, investigators should keep in mind that other offences may also be committed which frequently present opportunities to prosecute without involving the complex difficulties in obtaining rights statements etc. For example, IPR infringements could also involve offences of:

- Money laundering;
- Tax evasion;
- Criminal conspiracy;
- Racketeering;
- Fraud (and conspiracy to defraud); and
- Custom offences.

Regardless, the critical **first step** in an online IPR infringement investigation - as in any other criminal investigation - is to obtain knowledge of the relevant legislation and consider what is required to bring any subsequent prosecution through to a successful conclusion.

Furthermore, in respect of online IPR infringements, there are three main methodologies that investigators can employ separately or in combination:

- “Follow the Stream”;
- “Follow the Money”; and
- “Follow the Pixel”.

7.2 “Follow the Stream” Investigation

“Follow the Stream” refers to identifying the actual pirate content from the consumer right down to its source. It is an arduous task to investigate and map each particular criminal network end to end (the full stream) as it can involve not only mapping the entire labyrinth pirate ecosystem, which interconnects the plethora of actors - both legal and illegal, but also circumventing anonymisation technologies employed by many offenders to hide the traces of their illegal activities to deliver the pirate content. Even so, not all IPR infringers are computer savvy or careful enough to eliminate traces and efficiently hide their digital footprints. Consequently, investigators should endeavour to carefully gather different clues and indicators (either in digital or in physical form) from many sources and be alert to parallel investigations that may emerge.

7.3 “Follow the Money” Investigation

Financial gain is the dominating motive in many cybercriminal activities and IPR infringements are no exception. As a result, when the involved actors are elusive, another potential clue is the money trail. By following the money trail, the entire IPR infringement operation can be outlined. While criminals try to hide their identities and their digital footprints, the money they exchange is often hard to hide and hard to give up. Although electronic, digital, virtual and crypto currencies (such as Bitcoin and Monero) can potentially offer a higher level of secrecy and anonymity, the transactions performed can still be traceable, in principle.

Furthermore, when payment providers, such as a credit cards or PayPal are used, the details of link accounts can be disclosed to the authorities, in accordance with national legislation. In addition, a banking authority can be ordered to freeze an account. From that point on, any access or attempt to access money could reveal valuable traces and evidence, such as the IP address used to log on to the website, payment provider or other services.

At the centre of any financial investigation lies the transaction identification and analysis of the payments for the illegal services. Seized digital devices from a law enforcement operation may reveal evidence of subscriptions leading to customer information, including how and when the illegal actors paid for their services and the final cost of the services provided. The analysis of email records and other digital artefacts may lead to the identification of bank accounts, payments for services, money movements and provide evidence towards obtaining the business turnover figures.

The basic principle to keep in mind is that while the money is the motive, investigators should try to examine the money transfer mechanism used and try to disrupt it. By disrupting the money flow, the involved actors, at times can be forced to make a desperate move, which may potentially increase the chances of making mistakes. Hence, “Follow the Money” is a beneficial investigation thread and could lead to identifying suspects or persons of interest.

In short, there are two questions that, if answered, have the potential to reveal a large part of the IPR infringement network:

The “Who paid for?” question:

- Who paid for the domain name? (This information is available at the top-level domain organisation);
- Who paid for the hosting service? (This information is available at the hosting provider); and
- Who paid for the Domain Name System (DNS) server? (This information is available at the DNS service provider).

The “Where does the money go?” question:

- If there are payment processors installed on the pirate’s website (PayPal, Visa, etc.) this information is available at the company appointed to handle credit card transactions; and
- If there is a mobile payment installed on the infringer’s App, this information is available from the mobile telecoms provider.

1.4 “Follow the Pixel” Investigation

The term “Follow the Pixel” is used to encompass all online advertising related technologies, which are now an integral part of web-based services. The term ‘pixel’ in the social media and online marketing world is refers to the enabling technologies used for implementing online marketing campaigns, including capabilities for reporting their effectiveness, as well as for distribution of the generated income among the involved parties. Since such activities require the identification of the beneficiaries, this investigation thread is highly supportive and complementary of the “Follow the Stream” and “Follow the Money” methodologies.

IPR infringing sites and mobile apps are largely ad-supported, although some have adopted a subscription model while others accept donations from users. Consequently, illegal income may come not only from subscriptions and donations, but in the form of advertising revenue, generated by per-click payments, pay per download payments and payments related to banners displayed on websites.

This process is facilitated by advertising intermediaries and the adverts may be visible on the actual webpages, pop up in separate tabs when a user clicks on certain sections of a web page or through ‘pixel stuffing’ - which is accomplished by the inclusion of tiny Ad Spaces (1x1 or 5x5 pixels wide) within the top or bottom of a webpage.

Another fraudulent practice is so-called ‘ad stacking’, where multiple adverts are layered on top of each other in a single advert placement. Through this aggressive practice, pirates gain enhanced profits, even in the case of “free” IPR infringing services.

7.5 Best Practice

Introduction

The proliferation of social networks and open source information coupled with their need to advertise and reach as many end-users as possible, force IPR infringers to expose their data online. Gathering information about IPR infringers in an online investigation cannot be considered a straightforward task. Conducting online investigations requires preparation and a degree of sophisticated pre-planning to ensure that the task is undertaken in an efficient and focused manner, while always being conscious of the traces an investigator leaves behind.

Although there is no “one size fits all’ checklist, due to the high complexity and variety of every case, there are some key considerations the investigator should observe at the pre-planning stage of an online investigation:

- Protect one’s anonymity;
- Search widely, keep tracks and backup copies to reinforce your findings;
- Document ALL evidence discovered online with the appropriate timestamps;
    - Screen shoot all evidence with clear time identification on every single item;
    - Take copies of websites;
- Record every trace (nickname, email, user ID) the investigator “offers” to the infringing website with clear timestamps;
- Have a good knowledge of the environment under investigation, familiarise yourself well with the terminology the IPR infringers are using, the options the websites offer, etc; and
- In cross-border cases, seek international assistance.

Anonymity

As social networks and online information sources either allow targets to see who has been researching them or provide some obvious clues as to who is looking at their information, investigators should keep their identity hidden while performing online research. These are some of the actions that can be performed by investigators in order to conduct an anonymous online investigation:

• **Create a** new **email account** to be used for the investigations when needed. While anonymity is important, investigators should start creating an appropriate persona that has nothing to do with their identity. This email account should not refer by any means to the investigator's identity. Some piece of advice in achieving this is are as follows:

  - Do not give any information that could potentially identify the investigator's real identity. No real nicknames, birthdates, badge numbers, geographic indicators, sports teams or children's names in the User ID section;
  - Do not answer the security questions truthfully;
  - Do not link this email account to other legitimate email addresses;
  - Keep records of what has been submitted and don't forget the password.

- **Create new social media accounts** associated with the newly created email account. When it comes to social media undercover profiles, investigators should know (a) who can see whom through these platforms; and (b) what they can find browsing the targeted accounts.
- **Consider using VPN solutions**. Using VPN solutions and services while conducting an online investigation allows investigators to connect to their network through a VPN tunnel and at the same time to exit from a different location around the world. For instance, nordvpn.com's VPN offers exit nodes in over 60 countries across the planet. Unfortunately, most VPN services and solutions are not free. At the same time, it **is not recommended** that investigators use free proxy/VPN solutions. Investigators should always have in

mind that even if their traffic is encrypted as is crosses through the VPN nodes, unless there is end-to-end encryption, they are putting a certain level of trust in the exit node that decrypts their traffic as it appears in plain text.

- **Consider using TOR for anonymity.** TOR (The Onion Router project), is a network of nodes designed by the United States Naval Research Laboratory for the US Navy. This network of nodes is used to pass users' traffic to a destination host using encryption and routing through random paths. TOR only works with Transmission Control Protocol (TCP) traffic and only the destination host is able to see the exit nodes IP address while the source IP address of the host that initiated the communication remains unrevealed. So far so good, but since a list of TOR exit nodes is publicly available if the target of the investigation blocks the access from IP addresses that come for TOR nodes, investigators will not be able to reach their target. Another key to consider while investigating online via TOR, is that even though the investigators source IP address remains hidden, their user agent string will still be passed on to the IPR infringing website. So, if for example investigators pretend to be Russian speakers yet their user agent string reveals that their language is 'EN-US' this could trigger suspicions. Furthermore, if investigators pretend to be located in the US, but are regularly online at times consistent with someone located in an Eastern Time Zone, this might tip off the target as well; and
- **Consider using a Virtual Machine for all online investigations.** Virtual Machines (or VM's) are cross-platform virtualisation applications that imitate the behaviour of another (secondary) computer within the investigator's machine. Apart from allowing users to run multiple different operating systems on the same computer - with great flexibility in settings configuration and personalisation of the installed third-party software or tools - VMs also offer security benefits, especially when investigating risky applications, files and websites. Once inside the VM environment, investigators also benefit from the ability to create system-level snapshots to recover or restore VM images and services on demand.

8. OPEN-SOURCE INTELLIGENCE

8.1 Introduction

Open Source Intelligence (OSINT) refers to the practice of collecting information from publicly available sources that do not require covert or clandestine methods of collection. Although OSINT is a relatively new activity for law enforcement agencies, major organisations and agencies (such as Interpol and Europol) are systematically promoting and investing in OSINT through workshops, seminars and other activities, due to its importance for criminal investigations.

In online IPR infringement investigations in particular, OSINT is a crucial and integral activity rather than a bolt on to the investigation process. This is evident from the IPR infringement ecosystem, where the essence of the infringement requires that the majority of actors either interacted using the internet or make use of the core internet infrastructural services to deliver the infringing content. The latter poses a particular challenge as an actor may not be necessarily proactively involved in an infringing activity, similar to a postal service delivering illegal narcotics for example. Nevertheless, the OSINT exercise will need to capture all relevant information and validate it in order to allow the follow-up technical or legal actions.

The United Kingdom's Association of Chief Police Officers (ACPO) Principles should be observed when conducting OSINT based investigation[45]. Although OSINT does not necessarily involve accessing the suspect's systems directly, the investigator will need to possess a good understanding of the core internet enabling technologies such as DNS, autonomous systems, protocols, stream encoding standards, content delivery networks, to name a few. The identification of the location of services, domains and IP addresses is particularly stressed, as these can be hidden, obfuscated and anonymised - not necessarily to avoid detection, but to deliver the required level of service, as described in the case of Cloudflare and other privacy shield services for example.

[45]www.digital-detective.net/digital-forensics documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

A detailed logging of the actions and time (ACPO Principle 3) is of paramount importance in OSINT. By requesting and capturing information from external and potentially untrusted sources, the investigator should appreciate that the underlying systems are both complex and dynamic and as such their state may change considerably throughout an investigation. For example, in a “Follow the Stream” approach, as the infringing content can be delivered by a Content Delivery Network (CDN), it is likely that a domain or an IP address will present more than one effective location. On the other hand, the ‘” Follow the money” examination may return findings (again IP addresses and domains) that are less volatile, since such an investigation focuses on billing portals, payment accounts (such as PayPal and bitcoin wallets) and other structures that have a greater ‘time to live’. This caveat is also true for many external OSINT sources since they may capture the information in different past times and therefore present conflicting or incompatible information. As such, some forensic-based OSINT tools try to compensate by also maintaining a timeline of the data.

The IPR infringement ecosystem presents both opportunities and challenges for an investigator performing OSINT. The IPR infringement business models success is heavily based on the premise that the infringing products and services are easily discoverable, visible and accessible to the end-user/customer. To this end, OSINT can be very effective and does not require particular skills to discover the customer facing tier of information.

Therefore, not only are the sites visible, but the owners perform search engine optimisation (SEO) activities to improve their ranking.

It is a well-known and good practice for an investigator to build a portfolio of assorted tools to perform a particular task in order to validate and confirm their findings. With OSINT, in particular, it is critical to employ more than one tool in performing a particular action. Due to the nature of the OSINT data, different tools are expected to produce different information, as they are bound by their respective local caching and storage strategies, the way they query live systems and the timings of the queries. It is the investigator’s task to interpret and prioritise the information produced by an OSINT exercise.

The outputs produced from OSINT tools and particularly those that are open source or free should be used as a guide and the investigator should proceed with caution when interpreting the results. The support and reliability of freeware OSINT software can be limited as it may not be consistently maintained.

9. DIGITAL EVIDENCE

9.1 Introduction

In order to meet the challenges of harmonising the investigation processes across borders when dealing with online IPR infringements, this section is designed to aid investigators in all phases of handling potential digital evidence. According to ISO/IEC 27037 standard, these phases are **identification**, **collection**, **acquisition** and **preservation** of digital evidence. Although many agencies have their own national guidelines, standard operating procedures and protocols, it is crucial for the first responders and the investigators to appreciate the complexity the crime scenes may have and the fragility of digital evidence which can be easily damaged or altered due to improper handling, whether by accident or on purpose. Therefore, only properly trained personnel should attempt to seize the underlying equipment, by keeping a chain of custody of all digital evidence with structured processes that are accepted by the courts.

One consideration for investigators to bear in mind is that many IPR infringement cases may necessitate the presence of subsequent responders (i.e. forensic examiners) at the scene to complete more extensive triage procedures - that is, prioritisation and approach of the acquisition strategy of the digital artefacts discovered on the scene - or onsite imaging and response. For example, when seizing and acquiring live transponder devices, careful handling of those will need to be performed in order to capture and log volatile information (such as open network connections, ingress content streams, etc.).

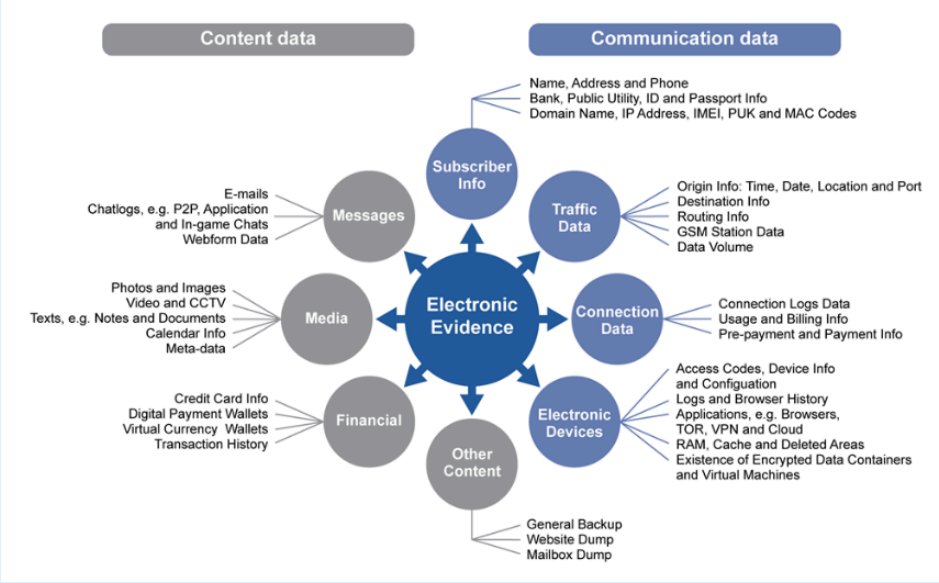


Figure 3 - Types of Digital Evidence

9.2 Crime Scene

Upon arrival at the crime scene, an investigator needs to be assured or have access to the following:

- **A secured crime scene.** This might be one of the key roles of a first responder, to keep a boundary on an area around the scene and keep everyone back and out for the better preservation of the evidence and better chances for valuable forensic results. It should also be highlighted that under no circumstances should a suspect be allowed to touch any electronic equipment that is present nor to communicate with anyone. Systems can be shut down remotely via the internet or mobile or even via smart swatches and important evidence may be lost or destroyed;

- **Visual material** (i.e., photographs) of the crime scene along with the suspect system (front and rear view and network connectivity of all devices), in order to officially seal the state of the scene and the devices upon the arrival of the first responders. This material will also be useful to the forensic examiners team if there is a need to replicate the device(s) and networked environment in the laboratory;

- **Detailed documentation** of all actions taken;

- Documentation of the **professional level and area of expertise of suspects**; and

- **Evidence preservation**. Failure to preserve the evidence is congruent to failure to prosecute.

9.3 Equipment Considerations and Investigation Toolkit

A 'digital evidence collection toolkit' refers to the equipment and supplies that should be taken to handle and manage a crime scene. In most cases, devices containing digital evidence can be collected with the use of standard seizure tools. Nonetheless, all crime scenes can be considered to be unique, so this the use of tools should be adapted to any given situation. The multitude and diversity of the devices that may be encountered during an IPR infringement investigation would dictate a flexible toolkit accompanied also with a variety of procedures. It is also recommended for the investigators to maintain a directory of resources to refer to, if the situation would demand knowledge and skills beyond their capabilities.

This investigation toolkit should be prepared in advance, taking into account either the possible conditions to be met on the crime scene or the actions investigators will be called upon to perform. As for the actions taken onsite, investigators should consider:

    - Conducting a network scan if possible;

- Capturing the network traffic for certain, specific time frames that all have to be documented;
- Accessing the computers to look for administration tools which display user information and email accounts;
- Running checks on log files;
- Identifying IP addresses of other users;
- Looking for customer data (either in digital or hardcopy format);
- Looking for financial information (either in digital or hardcopy format);
- Retrieving login details - both usernames and passwords (either through the use of specific forensics software or by interviewing the suspects); and
- Documenting in detail, all the actions taken.

Moreover, a specific equipment list should be created and routinely updated in order to assist the investigators while onsite for both collecting and processing the evidence. This list should include items such as:

- Notepad and pens (if documentation is taken by hand);
- Standardised forms for documentation (if available);
- Gloves;
- Digital camera / voice recorder (fully charged);
- Screwdriver case with every type of head imaginable;
- Brown paper evidence bags;
- Anti-static or faraday storage bags;
- Evidence tags;
- Flashlights;
- Evidence tape and packaging tape;
- Sharpie marking pens;

- Labels;
- Rubber bands (or twist ties);
- Write-blockers;
- Adequate sanitised storage (Different types of Sterile media);
- Adapters;
- Cables;
- Laptop: forensic processing platform; and
- Mobile device forensic platform.

9.4 Types of Data

There are various types of data that will need to be handled while conducting a computer forensic investigation. These are typically classified by their degree of volatility:

- Volatile data - data that disappears when the device is switched off. Consequently, an immediate onsite imaging is suggested (i.e., from a device still running, in 'live' state);

- Non-volatile data - data that remains on devices and may be transported to a location where proper forensic imaging and analysis may be completed.

According to the ISO/IEC 27037 standard, ''digital evidence can be fragile in nature, it may be altered, tampered with or destroyed through improper handling or examination''. Handlers of digital evidence should be competent to identify and manage the risks and consequences of potential courses of action when dealing with digital evidence. Failure to handle digital devices in an appropriate manner may render the potential digital evidence contained on those digital devices to be unusable.

In order to avoid damage and loss of potentially crucial data, manipulation of the system can be done according to the following four ACPO general principles:

- No action taken should change data held on a computer or storage media that may subsequently be relied upon in court;

- In circumstances where a person finds it necessary to access original data held on a computer or on a storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions;

- An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result; and

- The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Identification Process of Evidence

The identification phase is a three-step process which involves the **search** for, the **recognition** and the **documentation** of the potential evidence which are relevant to the online infringement incident. It is extremely important for investigators to prioritise the collection of evidence based on their volatility (see Types of Data section). With regards to **live** systems, the right order of acquisition is the one that preserves the most volatile data first. Failing to identify correctly all the relevant volatile data that must be collected may severely impact the investigation effectiveness and outcome, but may also be challenged in court.

In an operation of any size, investigators will have to be prepared to face and seize several types of devices that may contain information describing the access to the IPR infringement ecosystem. These devices are, but not limited to:

- Servers (including transcoder devices);
- Computers and/or laptops;

- Set Top Boxes / portable devices / smart televisions;
- Tablets and smartphones;
- Game consoles;
- Routers;
- External disk drives;
- USB thumb drives; and
- Card readers and smart cards.

The information stored on these devices may provide details about the two “Follow the Stream” or “Follow the Money” types of investigation. It is worth noting that the devices are expected to contain crucial information in the form of email accounts and correspondence, describing how individuals paid for services, details of connections to IP addresses, as well as information about the amount of data transmitted and received.

An essential consideration of the seizure process is to collect along with the aforementioned devices, all the peripherals (i.e., input or control devices), associated chargers and power supplies, cables and even manuals found on the crime scene.

Another consideration at this stage is to ensure that necessary actions have been taken to protect transient or volatile data that may be quickly lost or be corrupted. To this end, software-based or hardware-based techniques for capturing the memory must be obtained. Furthermore, as network activity is volatile and dynamic, a network forensics investigation must be performed on the historical and current network activity, capturing network events and activity as they occur in real-time. Consequently, it is highly recommended investigators perform a full packet network capture, in order to capture and record the suspect’s network connections and activity by documenting the exact time of those events.

9.5 Traps and Bombs

Investigators should always keep in mind that malicious software acting like a trap or a logic bomb might be covertly resident on the system being investigated. It is not unknown for a device to be booby-trapped to destroy potential evidence or the device itself. These types of sophisticated, pre-loaded software (or set of commands) are designed to destroy critical data residing on devices to be seized when a predefined condition is met. For instance, the suspect might activate them using a remote control or even they might be triggered by themselves when they detect a certain software, command or query is running such as ‘nmap’, ‘netstat’, ‘whois’ etc.

Finally, investigators may encounter any of these three types of pre-loaded malicious software:

- A ‘Hot Key Bomb’: refers to any keystroke combination assigned that can execute a command or series of commands;
- A ‘Booby Trap’: pre-installed software that appears to perform a certain function but is actually doing something different; and
- A ‘Terminate and Stay Resident Programme’: software that stays resident in the computer’s memory so it can be (re)activated by a system interrupt.

Although rare, these types of scenarios can occur. Consequently, while onsite, investigators should be aware of potential technologies (such as infrared devices) that could give the suspect remote access to the system, or even the existence of destructive booby trap programmes on devices that could damage crucial evidence needed to identify and prosecute the culprit.

Ensuring that no one touches the keyboard (which is the most common rule that applies in warrant execution regarding digital evidence) will prevent the purposeful or inadvertent initiation of any sequence of events that could damage the fragile data on the devices.

9.6 Storage and Preservation of Digital Evidence

All collection procedures for bagging and tagging physical evidence need to be applied to electronic devices in order to safeguard their integrity and preserve them in their original condition. Therefore, investigators have to follow a strict chain-of-custody protocol, to handle digital devices with precision and care in order to protect them from physical damage and damage from electromagnetic sources. Exposure to factors such as extreme temperatures, high altitude, static electricity, moisture or to electromagnetic sources like radio frequencies and magnets are considered as potential sources of damage to digital evidence. According to ISO/IEC 27037, the baseline activities investigators shall address are:

- Wear lint-free gloves;
- Label all potential digital evidence and devices according to the national jurisdiction's
  specific requirements regarding the labelling format of the evidential material;
- Seal with tamper-evident labels the digital devices which have openings and/or movable parts;
- Digital devices with attached batteries should be checked on a regular basis so as to have adequate power supply;
- Use suitable containers to shield the device against potential threats. Consider using
  antistatic bags; paper bags or cardboard boxes are still acceptable, but never store them in plastic bags;
- Package digital devices in a way that prevents damages from shock, vibration, highaltitude, extreme temperatures and radio frequencies during transportation;
- Pay special attention to magnetic storage devices that have to be stored in packages that are magnetically inert, antistatic and free of particles; and
- Be vigilant in circumstances where digital devices contain latent, trace or biological evidence, because the collection of such evidence has to be conducted before the digital evidence imaging.

10. FURTHER LEARNING

10.1 IP Crime Investigators College

If the Kosovo Police wish to increase their knowledge on how to investigate IPR infringements in the online environment, it is recommended they visit the International IP Crime Investigators College (IIPCIC).

IIPCIC is operated by Interpol and is a fully interactive on-line IP crime training facility providing courses in English, Spanish, French, Arabic, Mandarin and Portuguese.

Over 150 countries have visited the IIPCIC site since its launch and over 600 law enforcement agencies have enrolled in the training. IIPCIC is mandated to develop, coordinate and administer training programs to support international efforts to prevent, detect, investigate and prosecute transnational organized IP crime.

The course is free for law enforcement officers but users first need to obtain log in details at

www.iipcic.org

ANNEX I - INTELLECTUAL PROPERTY OBJECTS

Introduction

Intellectual property (IP) refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.

IP is divided into two categories:

- Industrial property, which includes inventions (patents), trademarks, industrial designs and geographic indications of source; and

- Copyrights, which include literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcasters in their radio and television programs.[46]

Industrial Property

The purpose of the system of industrial property rights is to encourage and to motivate inventors and creators, to protect their rights and to instill confidence in the maintenance of business activities. Industrial property rights include:

- Patents;
- Trademarks;
- Industrial designs;
- Geographical indications and designations of origin, and
- Topographies of Integrated Circuits.

[46]World Intellectual Property Organisation www.wipo.int/about-ip/en/

Right holders should register their industrial property with IPA to obtain protection in Kosovo. Right holders, including foreign entities, who do not register their industrial property with IPA may still have certain rights but their status should always be clarified with IPA before initiating an investigation.

Patents

A patent is an exclusive legal right granted for an invention. An invention is a product or a process that provides a new way of doing something, or offers a new technical solution to a problem.

Trademarks

A trademark is a distinctive sign which distinguishes certain goods or services as those provided by a specific person or enterprise from the same goods or services of other enterprises. Its origin dates back to ancient times, when craftsmen reproduced their signatures, or “marks” on their artistic or utilitarian products. Over the years these marks evolved into today’s system of registration and protection. The system helps consumers to identify and purchase a product or service because its nature and quality, indicated by its unique trademark, meets their needs.

Industrial Designs

An industrial design is the ornamental or aesthetic aspect of an article. The design may consist of three-dimensional features, such as the shape or surface of an article, or of two-dimensional features, such as patterns, lines or colors. Industrial designs are applied to a wide variety of products of industry and handicraft: From technical and medical instruments to watches, jewellery, and other luxury items; From courseware and electrical appliances to vehicles and architectural structures; From textile designs to leisure goods. An industrial design must appeal to the eye. This means that an industrial design is primarily of an aesthetic nature, and does not protect any technical features of the article to which it is applied.

Geographical Indications and Designations of Origin

A Geographical Indication (GI) is a name of a region, a specific place or in special cases the name of a state, which is used to describe a product originating from that region, specific place or state, possesses a quality, reputation or other specific characteristics which come as a result of geographical origin, production and / or processing and / or preparation of which takes place entirely in the defined geographical area name used to indicate that a product originates in a country or a region or a specific place whose given quality, reputation or other characteristic is essentially attributable to its geographical origin; and at least one of the production steps of which take place in the defined geographical area.

A designation of origin (DO) is the name of a region, a specific place or in special cases, the name of a state, which is used to describe a product originating from that region, specific place or state, qualities or characteristics of which are essentially or exclusively as a result of a particular geographical environment with natural and human factors inherited from this environment, and as a result of the production, processing and preparation of the product which is entirely developed in the defined geographical area.

Topographies of Integrated Circuits

A topography of an integrated circuit is the three-dimensional arrangement of the elements, at least one of which is an active element, and of some or all of the interconnections of an integrated circuit, or such three-dimensional arrangement prepared for an integrated circuit intended for manufacture.

An integrated circuit means a product, in its final form or an intermediate form, in which the elements, at least one of which is an active element, and some or all of the interconnections are integrally formed in and/or on a piece of material and which is intended to perform an electronic function.

A topography is protected if it is original, i.e. if it is the result of its creators' own intellectual effort and is not commonplace among creators of layout designs and manufacturers of integrated circuits at the time of its creation.

Copyright

Copyright and Rights Related to Copyright

Copyright as it exists under the Continental European system to which Kosovo adheres is called "author's rights" and deals with the legal protection of authors in their works. As a rule, authors are protected for works in the literary, artistic, musical, scientific and similar domains, such as for their novels, poems, musical compositions, sculptures, paintings, drawings, cinematographic works, architecture, choreography, photography, and the like; Such works must be intellectual creations and fulfil a certain level of creativity. For such works, authors are regularly protected by non-economic and economic rights. Non-economic rights protect the personal and artistic interests of the author in his work and are called moral rights; they include in particular the right of paternity (the right to be named as the author of the work, to stay anonymous, or to choose a pseudonym), the right of divulgation (first act of making the work available to the public in whatever form), the right of integrity of the work (in particular the right to object to any mutilation or other unwanted modification), and the right of withdrawal (the right to revoke the assignment of his property rights if there are serious moral reasons for that, on condition that the assignee is compensated for the damage caused by such revocation). In addition, the economic rights regularly recognise the exclusive control of the author over the exploitation of his works, so as to prohibit or authorise a broad range of uses. In a few cases, the law recognises only a statutory right of remuneration instead of an exclusive right. The exclusive rights are subject to explicitly regulated limitations and exceptions in favour of the general public. The duration of protection is usually limited to 70 years after the author's death. The right of divulgation and the right of

withdrawal according to Kosovo Copyright Law run for the life of the author. Such protection aims at recognising the importance of creation for culture by enabling the author to gain rewards from the exploitation of his works.

Since authors' rights do not protect any non-creative achievements, but such other achievements have been internationally recognised to be of great value to the availability of culture in a society, countries of the Continental European system have also introduced so-called rights related to copyright. Their main feature is that they do not protect "works" in the meaning of author's rights but similar achievements which in part promote or assist in making available works to the public. The main related rights recognised worldwide are the rights of performing artists (singers, other musicians, dancers, actors and others who perform works); producers of phonograms; producers of films; and broadcasting organisations. Additional kinds of related rights have been introduced in other countries. Also, the duration of protection is shorter than that of author's rights. While performers are protected for their artistic achievement, e.g., the performance of works, the other holders of related rights are protected for their technical, organisational and financial investment in the production of recordings, in the broadcasting activity, etc.

Copyright protection is granted without any formalities. Thus, no registration of rights is required by the Law in Kosovo. It arises as soon as the work is created.

ANNEX II - CONTACT POINTS

Kosovo - Contact Points

Industrial Property Agency

Address: Ministry of Trade and Industry
Rr. “Muharrem Feiza”, p.n. Lagja e Spitalit,10000 Pristina
Tel: +381 (0) 38 200 36 544
Fax: N/A
Web: www.kipa-ks.org
Email: nezir.gashi@rks-gov.net

Office on Copyright and Related Rights

Address: Ministry of Culture, Youth and Sport
Sheshi Nëna Terezë pa nr. Prishtinë
Tel: +381 (0) 38 200 563
Fax: N/A
Web: http://www.autori-ks.com/
Email: valon.kashtanjeva@rks-gov.net

Kosovo Police, Unit for Economic Crimes

Address: “Luan Haradinaj”str . 10000 Pristine-Kosovo
Tel:
Fax:
Web: www.kosovopolice.com
Email: info@kosovopolice.com

Kosovo Police, Cybercrime Unit

Address: “Luan Haradinaj”str . 10000 Pristine-Kosovo
Tel:
Fax:
Web: www.kosovopolice.com
Email: info@kosovopolice.com

Kosovo Customs

Address: Veterniku 1, Zona Industriale - Pristina
Tel: +381 (38) 540 350
Fax: +381(38)542065
Web: www.dogana-ks.org
Email: info@dogana-ks.org
Info: http://dogana.rks-gov.net/en/Contact

Market Inspectorate

Address: Ministry of Trade and Industry
Rr. “Muharrem Feiza”, p.n. Lagja e Spitalit,10000 Pristina
Tel: +381 (38) 512407,
Fax: tel:038512798
Web: www.mti-ks.org
Email:

State Prosecutor

Address:
Tel:
Fax:
Web:
Email:

Prosecutorial Council

Address:
Tel:
Fax:
Web:
Email:

Judicial Council

Address:
Tel:
Fax:
Web:
Email:

Drug and Medical Product Agency

Address:
Tel:
Fax:
Web:
Email:

Veterinary and Food Agency

Address:
Tel:
Fax:
Web:
Email:

Agency for Environment Protection

Address:
Tel:
Fax:
Web:
Email:

Agency for Managing of Sequestrated or Confiscated Assets

Address:
Tel:
Fax:
Web:
Email:

Independent Media Commission

Address:
Tel:
Fax:
Web:
Email:

Regulatory Authority for Postal and Electronic Communications

Address:
Tel:
Fax:
Web:
Email:

International - Contact Points

EUIPO Observatory

Address: Avenida de Europa, 4, E-03008 Alicante, Spain
Tel: +34 96 513 9100
Email: observatory@euipo.europa.eu
Web: https://euipo.europa.eu/ohimportal/en/web/observatory/home

Interpol (Trafficking in Illicit Goods and Counterfeiting)
Address: General Secretariat 200, quai Charles de Gaulle
69006 Lyon France
Tel: +33 (0)4 72 44 71 63
Email: **info@iipcic.org**
Web: http://www.iipcic.org

Europol (IP Crime)

Address: Eisenhowerlaan 73, 2517 KK The Hague, The Netherlands
Tel: +31 7 03 531575
Email: **o3@europol.europa.eu**
Web: http://www.europol.europa.eu

World Customs Organisation (Counterfeiting and Piracy Group)

Address: Rue du Marché, 30, B-1210 Brussels, Belgium.
Tel: +32 2 209 92 11
Web: http://www.wcoomd.org/
Email:

World Intellectual Property Organization (WIPO)
Address: 34, chemin des Colombettes, CH-1211 Geneva 20, Switzerland
Tel: +41 22 338 9111
Web: www.wipo.int
Email:

ANNEX III - LEGISLATION

Criminal Code

Article 289 - Violating patent rights

1. Whoever, in the course of engaging in an economic activity, uses without authorization, a patent registered or protected by law or a registered topography of a circuit of a semi-conductor shall be punished by a fine or by imprisonment of up to three (3) years.

2. The objects provided for in paragraph 1. of this Article which were manufactured for unauthorized use shall be confiscated.

Article 290 - Violation of copyrights

1. Whoever, under his own name, or somebody else's name discloses or otherwise communicates to the public a copyrighted work or a performance of another, in whole or in part, shall be punished by a fine and imprisonment of three (3) months to up to three (3) years.

2. Whoever during use of copyrighted work or a performance of another intentionally fails to state the name, pseudonym or mark of the author or performer, when this is required by law, shall be punished by fine and imprisonment for up to one (1) year.

3. Whoever distorts, mutilates or otherwise harms a copyrighted work or a performance of another, and discloses it in such form or otherwise communicates it in such form to the public shall be punished for by fine or imprisonment for up to one (1) year.

4. Whoever performs or otherwise communicates to the public a copyrighted work or a performance of another in an indecent manner, which is prejudicial to the honour and reputation of the author or performer, shall be punished by a fine or imprisonment for up to one (1) year.

5. Whoever without authorization uses a copyrighted work or subject matter of related rights, shall be punished by imprisonment up to three (3) years.

6. If, during the commission of the offense described in paragraph 5. of this Article, the perpetrator obtained for himself or for another person at least ten thousand (10,000) EUR but less than fifty thousand (50,000) EUR, he or she shall be punished by a fine and imprisonment of not less than three (3) months to five (5) years.

7. When the perpetrator of the offense in paragraph 5 of this Article obtains for himself, herself, or for another person more than fifty thousand (50,000) EUR, he or she shall be punished by a fine and imprisonment of not less than six (6) months to eight (8) years.

8. The objects and the equipment for their manufacturing provided for in this Article shall be confiscated.

Article 291 - Circumvention of technological measures

1. Whoever commits any act of circumvention of any effective technological protection measure or any act of removal or alteration of electronic rights management information, as provided for by the provisions of the Law on Copyright and Related Rights shall be punished by imprisonment for up to three (3) years.

2. The objects and the equipment for their manufacturing provided for in paragraph 1. of this Article shall be confiscated.

Article 292 - Deceiving consumers

1. Whoever, in the course of engaging in an economic activity and with the intent to deceive purchasers or consumers, uses or possesses with intent to use another’s trade name or trademark, another’s goods trademark or services trademark or another’s trademark related to geographical origin or any other special trademark of goods or components thereof in his or her own trade name, trademark, or special

trademark of goods shall be punished by imprisonment of up to three (3) years.

2. Whoever, with the intent to deceive purchasers or consumers, uses in production another's sample or another's model without authorization or distributes articles manufactured in this way shall be punished as provided for in paragraph 1. of this Article.

3. The objects and the equipment for their manufacturing provided for in this Article shall be confiscated.

ANNEX IV - DEFINITIONS[47]

Online infringements: Infringements that take place on the open part of the internet[48] and the primary focus is on infringements of a commercial scale, meaning that the infringing acts are 'carried out for direct or indirect economic or commercial advantage'.[49] The use of terms online and online environment in this Guide include any activity on the open internet, including websites, lower level pages, user profiles on social networking websites, online auction and trading platforms, email and internet connected applications on mobile devices.

Intermediaries: Internet intermediaries are entities - usually companies - that bring together or facilitate transactions between third parties on the internet. They give access to, host, send or index content, products and services originated by third parties on the internet or provide internet-based services to such third parties.[50]

Domain name: The domain name system (DNS) serves the essential and central function of facilitating the internet users' ability to navigate the internet[51]. A domain name is the user-friendly address of a specific

47Study on Legislative Measures Related to Online IPR Infringements, EUIPO, 2018.

[48]The Guide will, therefore, not cover activities on the un-indexed parts of the internet, often referred to as the darknet. See the definition of 'darknet' on p. 14 in 'Research on Online Business Models Infringing Intellectual Property Rights. Phase 1. Establishing an overview of online business models infringing intellectual property rights', EUIPO, July 2016.

[49]As defined in Recital 14 of Directive 2004/48 on the enforcement of intellectual property rights. The study will thus not focus on infringements of copyrights and related rights that are committed by private persons as such.

[50]https://www.oecd.org/internet/ieconomy/44949023.pdf

[51]It is the internet Corporation for Assigned Names and Numbers (ICANN) that coordinates the key technical functions of the DNS and defines policies for how the 'names and numbers' of the internet should run.

computer's underlying numeric IP address (see definition below). The domain name 'euipo.europa.eu' for example is tied to the computer with the numeric IP address 109.232.208.177, which means that instead of remembering and typing in '109.232.208.177' in the internet browser an internet user can type in 'euipo.europa.eu' to be connected to the EUIPO website.

Technically, the DNS works through a network of distributed databases that are operated by the designated domain name registries. These databases contain the lists of domain names and their corresponding IP-numeric addresses and perform the function of mapping the domain names to their numeric IP addresses for directing requests to connect computers on the internet.

Domain names must be registered with the registry[52] that is responsible for the specific top-level domain, and registrations have to be filed through an accredited domain name registrar. By way of an example, if a company wants to register an .eu domain name the company must contact an accredited .eu registrar and request the registrar to file an application to register the domain name on the company's behalf. If the domain name is vacant and all other formalities are fulfilled the domain name will be registered and entered into the .eu DNS database.

All domain names will be connected to one or more domain name servers, which is a 'computer server that contains a database of public IP addresses and their associated hostnames, and in most cases, serves to resolve, or translate, those common names to IP addresses as requested'.[53] The DNS servers are operated by entities who are authorised to do so by the registries - often referred to as 'name server managers' (DNS managers). Many of the accredited registrars are also authorised to operate as DNS managers.

The registries do not examine the applications for a new domain name against prior rights of third parties such as trademarks, company names or personal names. Third party rights holders are therefore compelled

[52]Many TLDs apply a shared registry model, in which case the registrars have access to register domain names directly in the registry database. The registry database is then administered by a dedicated registry administrator.
[53]As defined by LIFEWIRE, https://www.lifewire.com/what-is-a-dns-server-2625854

to enforce their rights after the domain name has been registered, if they find that a registered domain name infringes their rights.[54]

IP address: The term is an abbreviation of internet protocol address, which is an identifier that is assigned to each computer or other device (e.g., a mobile device) that is connected to the internet or to another network using the TCP/IP protocol. The IP address is used to locate and identify the device in communications with other devices on the network.

An IP address may be static which means that the address will be the same each time the user uses its account with the provider to connect to the internet. A dynamic IP address means that the access provider will assign one of the IP addresses that it has available in its 'address pool' to the user when he or she logs on, but the said IP address will only be assigned for a limited amount of time, namely for the particular session. The IP address may subsequently be assigned to a new user.[55] It is determined in the agreement between the user and its access provider, which type of IP address that will be applied for the devices that are covered by a service agreement. However, mobile devices such as laptops, tablets and mobile phones can be and are very often connected to the internet via an access provider whose services are available at the place where the user is currently located. Such services will typically use dynamic IP addresses.

Digital evidence: Domain names and IP addresses are just two types of digital evidence. As the figure below illustrates there are many other types of digital evidence that may be relevant to collect in the particular cases that involve online infringements of IPRs.

[54]Definition from the abovementioned 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016

[55] Additional information on IP addresses can, inter alia, be found in the article 'What is a static IP-address?' https://www.lifewire.com/what-is-a-static-ip-address-2626012. The term 'address pool' originates from here.

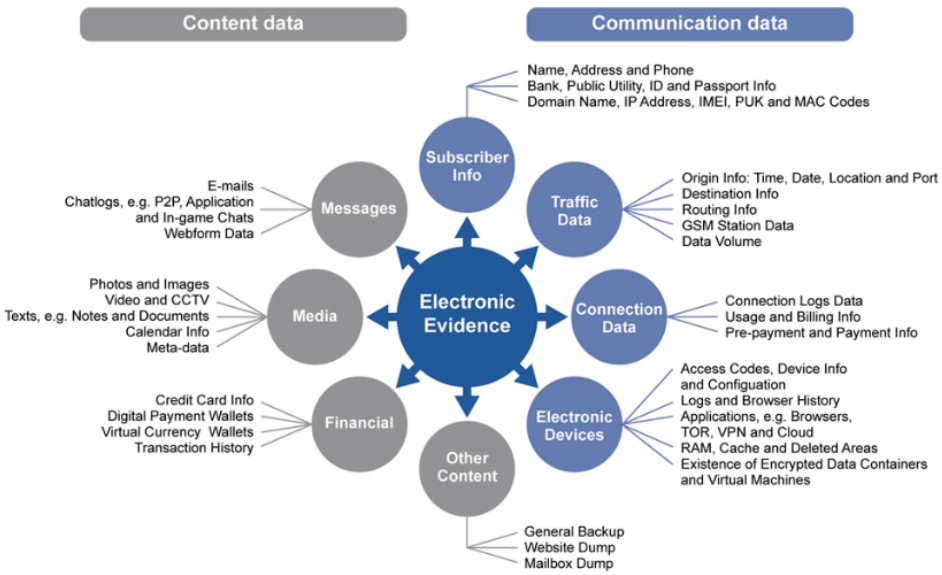


Figure 4 - Different Types of Digital Evidence[56]

[56] Study on Legislative Measures Related to Online IPR Infringements, EUIPO, 2018.

IPRproject
Intellectual Property Rights Project

Rr. ”Johan V. Hahn”,
10000 Pristina, Kosovo
Tel: 038 726 688
IPRKosovo