United Nations
Interregional Crime and Justice
Research Institute

Investigative guidelines on IP Crimes in Italy

A tool to support enforcement activities

- Approach: development of a practical tool for law enforcement agencies supporting investigations and prosecutions
- Inspiration: Handbook developed by EUIPO within EMPACT (Italy co-driver of the initiative)
- Objective: to encourage a ramification of the investigative phase in order to unveil the illicit distribution chain and possibly:
  - People
  - Places
  - Companies
  - Flows of goods
  - Cash flows
  - Related crimes and new trends in the phenomenon
- Focus on the use of technology by criminals and in support of the investigative phase

Launch and implementation of the project

- Project launched by Italian Ministry for Enterprises and Made in Italy (MIMIT)
- Guidelines reserved for enforcement authorities
- Start of activity: July 2024
- Creation of a working group composed by law enforcement representatives and MIMIT
- Step 1: Create the first guideline model
- Topic : social media purchases
- Key elements: operability and applicability
- Finalized in December 2024
- Step 2: Create additional guidelines based on the first model
- Thematic areas: websites, e-commerce platforms, authorized merchants, large-scale distribution
- Finalized in October 2025

Key elements

Creating a streamlined, flexible, and easy-to-use tool

- dedicated to operators in the field
- extension of good practices of specialized departments
- hyperlinks and cross-references
- annex and in-depth sheets

Regulations, procedures and authorizations

Investigative activity of law enforcement:

- Independently
- Subject to judicial authorization
- Investigative technical specifications

!

!

The guidelines

5 investigative guidelines:

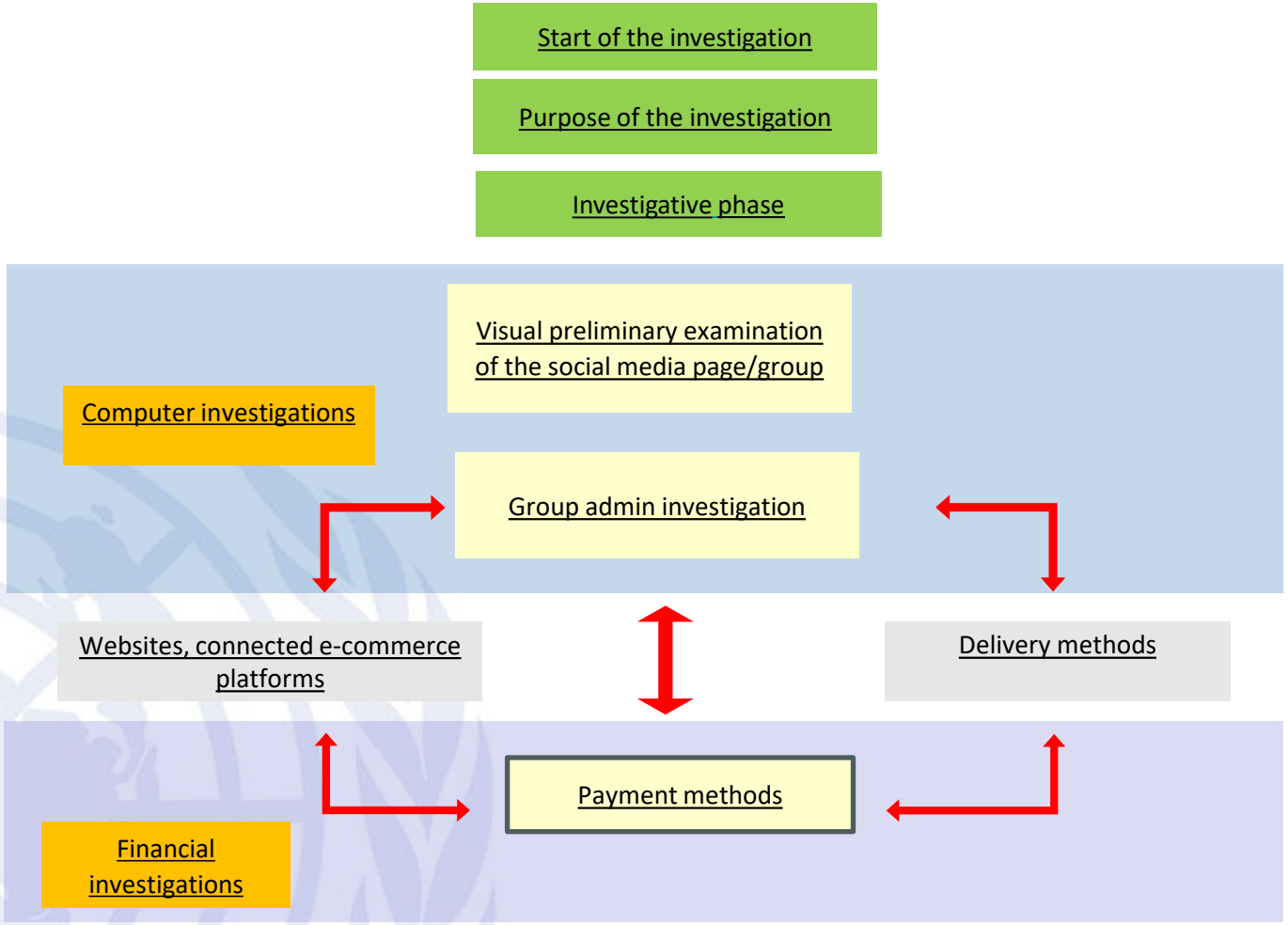
Online sales:

- Social Media
- Website
- e-Commerce platforms

Retail and wholesale

- Sales through authorized merchants
- Storage for later distribution

An integrated approach to investigations



Content: Examples from social media sales

How to use the guidelines

The guidelines contain several hyperlinks within the document to facilitate the identification and reading of the elements of interest. These hyperlinks are activated using the CTRL key + left mouse click. Their use is of course limited to the digital version of the guidelines only and therefore it is not recommended to use a printed version of the same.

The guidelines show a series of possible investigative choices through which to investigate sales of counterfeit products made through a social media group or a social media page. Sheets 1 to 5, to which the guidelines often refer, provide specific information on survey methods. These sheets are cross-cutting and can also be used for other guidelines developed in relation to different ways of selling counterfeit products. In particular:

Sheet 1 - Investigations on username, IP addresses, geolocation, WHOIS and hosting;

Sheet 2 - surveys conducted via the internet;

Sheet 3 – Survey tools for social media;

Sheet 4 – Cryptocurrency Investigation Tools;

Sheet 5 – Investigative activity starting from images and videos, *EXIF* and metadata of the images;

Sheet 7 – PC anonymization and fictitious digital identities.

In addition, the final section of the guidelines contains the following thematic insights, which can also be accessed using CTRL + Mouse Click on the text below:

- In-depth analysis of the modus operandi;
- Closed social media groups and infiltration;
- Agent provocateur;
- Collaboration with service providers through Eurojust's SIRIUS project;
- Practical examples;
- Hidden links.

Typical modus operandi

The "typical" modus operandi for this illicit activity is described below. The same can of course be subject to changes on a case-by-case basis. Click here for more information on the modus operandi and its variations.

Subject A of the social media SM1 is the administrator of a sales page or group (open or closed) within the social media itself, through which he offers for sale a series of counterfeit products.

An open group refers to the case in which any social media user can access Subject A's page to view the products on offer and make purchases. In the case of a closed group, only users approved by Subject A can access his page, guaranteeing greater anonymity to the same.

Users can make the purchase by interacting with the administrator (Subject A) through various methods, such as:

Start of the investigation

The information available at the beginning of the investigation phase can often vary depending on the way in which the possible illegal activity was received. In principle, the following possibilities can be identified:

Note: By using CTRL + CLICK of the mouse on the type of information, you will be redirected to the section of the guidelines relating to their use for investigative purposes.

1) The suspicious activity was **reported by representatives of the owners of industrial property rights**: in this case, the owners themselves often carried out preliminary research to obtain more information on the illegal activity and the subjects involved. In the complaint, in addition to the indication of the elements certifying the registration of one's trademark/distinctive sign and those on the basis of which it is believed that the product found on social media is counterfeit, useful information could therefore be included, such as:

   - The social media used is the username of the administrator of the social media group or page;
   - Images documenting the alleged illegal activity conducted on the social media;
   - Any email addresses, messaging apps, or phone numbers indicated in the social media to contact the administrator and complete the purchase;
   - Any communication with the administrator (Subject A) through email exchanges, private messages via social media messaging, or messages exchanged via phone numbers or messaging apps.

   This information can be important for investigating the Group Admin.

   - Learn more about other social media groups related to the business, even if they operate on different social media platforms;
   - Information on possible references to web pages or e-commerce platforms to complete the purchase.

   This information may be important for investigating the extent of the illegal activity and connection with other social media, websites or e-commerce platforms.

   The rightsholder may have made a sample purchase and may be in possession of additional information, such as:

   - Payment methods used with reference also to payment instruments. **Useful information** for financial investigations;
   - Method of delivery, including the place where the products are shipped (if it is delivery by shipment) or the place where you pick up the goods in person. **Important information** for the investigation of delivery methods;
   - A physical sample of the product that proves the element of counterfeiting and which can also be used for further investigation.

Content: Examples from social media sales

Investigative activity requiring judicial authorization

If the username/alias of the social media group admin is known

- **Request the collaboration of the social media to obtain useful information for the continuation of the investigation, in particular:**
  - IP addresses related to Subject A's connections to his social media account => below, see working with your internet service provider to use this information. Click here to view a practical example of obtainable information;
  - phone numbers provided to recover the account => subsequently, see working with the telephone provider to use this information;
  - Email addresses associated with your account (including account recovery addresses) => Next, see Working with your email account provider to use that information.

To request the collaboration of the social media, the authorization of the Judicial Authority is required. First, it is necessary to uniquely identify the social profile under investigation. The correct identification of the User ID is an essential element to achieve the unambiguous identification of a profile. See **Factsheet 3: Social Media Survey Tools** for more information on this topic.
Subsequently, a Decree for the acquisition of telematic data so-called "log files" will be requested from the Judicial Authority.

In-depth sheets

10 In-depth sheets

1) Investigating usernames, IP addresses, *whois*
2) Internet investigations
3) Social media investigations
4) Cryptocurrencies investigations
5) Investigations on images and videos
6) Investigating websites
7) PC anonymization online fictitious identities
8) Autonomous police investigative powers
9) Search and seizure actions
10) Phone tapping and video surveillance

Thanks for your attention