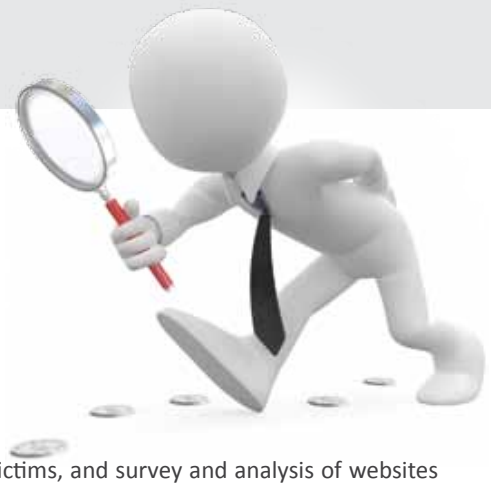
PRACTICE FOR PRIVATE DETECTIVES



by Alexandra Krioni

Since electronic correspondence is often the only connecting link between a victim and an alleged criminal, identifying the owner of the email address remains the most reliable method for quickly achieving the objective of a private investigation. This article lays out recommended practice for private detectives who are regularly required to determine the identity of a lawbreaker from his email address.

Grounds. Private investigations to identify the owner of an email address are conducted in compliance with the Russian Federal Law 'On Private Detective and Security Activity in the Russian Federation'.

This type of investigation is rather difficult, since there are no typical or recommended forms for planning investigations in these cases. Each private detective must independently determine the priorities and areas for gathering evidence, while observing the laws of his country.

At first glance, the almost open nature of electronic correspondence would appear to pose no difficulties in establishing the identity of an email sender. However, this is an incorrect assumption. When committing such crimes as Internet fraud and the sale of counterfeit goods, criminals prepare carefully: they select an anonymous mail hosting service, seek a public point of access, use special hardware to access the Internet, and think of a sophisticated user name or indicate an abbreviated name in their signatures. Members of criminal groups strive to act incognito, camouflaged, with care, and without causing undue disturbance. If a victim starts to act suspicious, they quickly lose interest in him. When advertising their services, criminals use invented names, and pose as bona fide merchants and mid-level managers of known commercial entities and state-owned corporations. The correspondence is well written, and demonstrates knowledge of the business.

Measures for planning identification. An investigation generally begins by obtaining the email address from the victim, or at the initiative of the victim's lawyer, which is typical for cases requiring quick intervention, with very little delay.

In all cases, the investigation plan must presume a state of urgency to determine the identity of the criminal (i.e. to be 'hot on his trail'), and be closely linked to and consistent with the plan for initial private investigative actions. Among the actions planned are questioning of victims, and survey and analysis of websites on which announcements containing the email address under scrutiny have been published.

The operational plan includes actions to investigate websites, and an Internet search for similar business sites where criminals might leave their contact information. However, the investigation must also consider the possibility that the client is hiding information regarding his own unsuccessful attempts to determine the identity of the criminal.

Initial private investigative actions on fraud and illegal use of trademark cases are aimed at identifying the owner of the email address.

The following are determined in the email investigation:

- on what website, when, and under what circumstances the victim found the criminal's email address
- how many people participated in the correspondence, their names, and the organization they represented
- whether the criminals used other methods to communicate with them
- what payment methods the criminals proposed to the victim
- whether the criminals sent any documents as email attachments
- the IP address from which the email was sent. The country and city from which the email was sent, as well as the date and time of correspondence
- the type of domain on which the email address was registered (public or private)
- the login of the email owner
- whether the email address is active or inactive
- the consequences of the illegal acts for the victim

With the raw data, the private detective views the website to detect traces of crime and to compile evidence from the victim with a statement about the event. When investigating cases of counterfeit goods or fraud, by the time the investigation begins, the criminal's website is generally only accessible via the Wayback Machine (www.archive.org/web), and the owner has deleted the email address. Under these circumstances, the private detective must be able to restore traces of the publications removed from the criminal's website. When examining the website and when questioning the victim, the possibility that the victim has carried out his own unsuccessful investigation is checked.

The email investigation should begin with a detailed survey of search engines: Yandex, Google, Hotmail and Yahoo. A criminal may give his email address as a contact when registering a domain name, in signatures to messages on forums, on announcement boards, or in personal comments.

When studying forums, attention must be paid to information which the email owner has left openly accessible. Publicity requires publication of the account owner's personal information in forums, blogs, and other media that are accessible to registered and unregistered users. Data on forum users is open for publication to interested persons, who can find out the user's personal data and statistics on his messages, for example, via site authentication. Special attention should be paid to evidence accessible via the email user's member account area (nickname, name, age, sex, city, interests, number of messages posted, additional email address, telephone, Skype and ICQ number, registration data and date last message posted, as well as a graphic representation of the user – the profile picture). If there is reason to suppose that the criminal did not use the email address anywhere else, then subsequent actions are aimed at a detailed study of the login (everything in front of the "@" symbol). When creating a login, a criminal may use elements of his own first, middle/patronymic or last names, and year of birth (most often the last two digits).

A search of other popular email services (mail.ru, yandex.ru, gmail.com, yahoo.com, hotmail.com), as well as of social networks and online messaging services (Facebook, Twitter, Skype, @Mail.ru, VK, OK Messenger), is performed using a trial registration. The login data in a newly discovered email address or account should correspond to the login of the initial mailbox. If an account or email address with an altered login is discovered, for example, if a dash, digit or dot has been added, further investigation of it should be discarded, and the initial spelling returned to.

If there is reason to assume that the email discovered has precisely the same login, the private detective can use the password recovery service for the new account. The fact is, when attempting to recover the password for the member area of an email service, it is necessary to also answer a question related to the user. Sometimes, a criminal will chose the option of sending messages to an additional email address or mobile phone to recover a password. Despite the fact that the information on the telephone number or email address is not fully shown, this situation can be useful in a number of cases. For example, if a message must be sent to another mailbox owned by the user (generally gmail.com) to recover a password, careful comparison may reveal similarity to the mailbox sought, and it can thus be verified that the criminal is using a minimum of two mailboxes.

Maintaining confidentiality and observing the legal requirements for private investigation procedures is just as important in identification. Thus, investigators should not try to use a password recovery service more than once or twice, in order to avoid notifying an email owner of an attempt at unauthorized access to his account. That is why, when conducting private investigative actions on the Internet, private detectives must make a habit of taking screenshots of every action they undertake.

It must be considered here that the login may be absolutely contrived and not bear any relation to the true name of an email owner. Therefore, in the final stage of the investigation the private detective should try to establish contact with the assumed owner of the electronic mailbox, in order to be sufficiently confident that the evidence gathered does not contain significant errors. Evidence on an email owner discovered by the private detective is divided into that which most likely applies to the case (direct evidence) and that which is less applicable to the case (indirect evidence).

Evidence of direct facts must be considered as follows when the detective writes his final report:

- if the private detective has concluded that the evidence discovered applies directly to the email author, then the private detective should prepare a report containing a substantiation of his conclusion
- if, due to insufficient evidence or insufficient qualifications, the private detective cannot determine the identity of the email owner, he should prepare a report, but he may refrain from drawing conclusions on the investigation

Typical violations discovered during investigations to identify an email owner are:

- failure of the private detective to comply with existing regulatory requirements in some of his actions.
- using forms and methods for gathering information to the detriment of confidentiality.
- absence from the report of any cause and effect relationship in the evidence relating to identification.

W.A.D Member, Alexander Krioni is the founder and CEO of Alexander Krioni Detective Bureau based at Narodnogo Opolchenia 34 123423 Moscow, Russia. www.krioni.com