With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission - Directorate-General Justice, Freedom and Security

The automation of tasks in forensic analysis on child pornography crimes.

Authors

Alejandro Prieto Castro – INTECO
Juan Prieto Carballal – INTECO
Antonio Sepúlveda Carrero – INTECO

Abstract

The great challenge of the State Security Forces in the forensic analysis of storage devices seized in child pornography cases goes through the automation of tasks in the search for evidence in electronic files.

Content

The latest operations against child pornography in Spain, carried out by the National Police and Civil Guard, shows the large number of storage devices seized in the searches of homes of suspected pedophiles. Without going any further, in the operation called *"Astillas"* developed by the Civil Guard, 116 hard drives and 12 DVDs were collected among other types of storage media, containing around 500,000 allegedly illegal files[i].

In a more recent case, investigators from the National Police seized about 700 discs with over 1000 photographs of a minor in unseemly attitude[ii].

The forensic work carried out by the Security Forces of the State on these storage devices is the key to the success of operations against child pornography. Latest news shows the excellent work of the police agents going through huge volumes of information. Mainly, this work results complex due to two factors. The first one refers to the large number of files that need to be analyzed. The capacity of hardware devices has grown exponentially, allowing the storage of millions of files on a flash drive or an external hard disk. The second one refers to how criminals use concealing techniques of evidences that hinder the forensic investigation of the agents.

Such is the importance of these forensics that in the end they become essential to determine the nature of the charge applied to the suspect. In example, a suspect could be charged on possession of child pornography, but also on distribution if sharing the material through p2p file sharing networks. They are two different charges regulated independently by the penal code. Deciding whether is one crime or the other can be solved after a thorough forensic analysis of seized storage devices. The effectiveness and experience demonstrated when resolving cases of child pornography by the National Police and Civil Guard take anyone committing this type of crime to court. Therefore, the current goal is to minimize the time spent on forensic analysis of seized devices, increasing automation of tasks in the search for evidence.

When a police investigator has a seized device before him, he should consider all possible casuistry. To do this, he takes into account those files that are visible by a normal user, and those that are hidden, for example, when a file is removed, it can be recovered since it is still physically located in the storage device. The operating system and installed applications are also sources of evidence used by the investigator to perform forensic analysis.

Automating tasks under the search criteria used by investigators is a crucial paradigm in future analyze of external devices. This automation should show t at least he device files sorted by priority, where the first are those most likely to be evidence or show valuable clues to solve a case. Undoubtedly, the decision to consider whether a picture, video or document is a evidence lies on the 'human' investigator, more so when dealing with crimes of this nature.

The application of the methodologies used by investigators to automatic processes is proving to be an essential element. As a result it is increasing the police action efficiency against child pornography offenses in particular. The automation in the search for evidence speeds up over the resolution of a case. The delegation of manual tasks to automated processes on searching and file cataloging allows agents to focus on other tasks during the investigation. Accomplishing these tasks manually entails considerable effort that in the long run undermine the efficiency and response capacity of the investigator, causing him to focus more on the process of analysis than on identifying evidence. Once automated, agents finally have a list of files sorted and cataloged according to the criteria that have been established, easing up the task of identification of evidence in a quick fashion.

The execution of automatic processes has the same nature when talking about forensics on storage devices. The different hardware and software architectures found on external devices are known, as well as how to address them. However, the particularity of the search criteria based on the crime committed is what makes the difference in advancing this paradigm. Even within cases of child pornography there are features that makes each one special. This specificity can be fully addressed by modifying or completing the search criteria of the forensic analysis. Customization in this area makes the sorting and cataloging of files more effective. Also, the mechanisms and automated techniques utilize the search criteria set by the investigator, being thus dependent on the type of crime.

The experience of the investigation team and police cooperation between entities or between countries are crucial when shaping specific search criteria for child pornography cases. Deciding what and where to look inside a storage device usually comes from experience, so the union of the experience or knowledge with the potential of automating the analysis of generic storage devices increases the effectiveness and efficiency during investigation, minimizing the time taken to resolve a case.

Today the great work of the Security Forces of the State are getting great results, and many of the people who keep, distribute or produce child pornography content are placed under the judiciary. With the transfer of methodologies and criteria to be consumed by automatic processes the time spent since you get a first evidence until you close a case is being much shorter.

The standardization of methodologies in investigation and registration of child pornography is a crucial feature during forensic analysis and subsequent experience to complement future cases. This normalization minimizes dependence on a specific person, so that the compliance with a fixed methodology ensures effective continuity over time, maintaining quality standards in resolving cases. Records having a fixed structure due to the implementation of these methodologies provides a fair independence of time and human investigators, with all the benefits that this entails.

The adaptation of human experience to the processes and methodologies as well as the automation are being studied and will be studied further to fight child pornography offenses. The large number of devices confirms this thesis, assuming that one should not ignore the consistent implementation of methodologies in the investigation of cases and the incorporation of automatic processes in forensic analysis.

So one of the aims of the European project ASASEC (http://asasec.eu/) against child pornography crimes is to ease up the identification of the evidence seized in a police operation and standardize methodologies in forensic investigation. ASASEC includes a module capable of analyzing large volumes of data recovered from storage devices resulting in a list of the suspicious files sorted by priority. This priority reads the probability of the file being an evidence. Also, due to its nature, it provides a useful and lasting methodology for resolving cases of child pornography for the human agent.

The role of ASASEC as information unifier under predefined protocols would enhance forensics including automation of processes, in the hopes of building an essential tool in the fight against child pornography.

Conclusion

Seizing lots of devices in an operation against child pornography makes necessary to focus on minimizing the time spent analyzing these devices. It is possible to identify the criteria used by investigators for searching evidence and automate them. This will minimize the search time and the agent may focus on determining whether a file is evidence or not. To do this, the investigator works with a list of suspicious files sorted by priority with all the information needed to establish the illegality of their content.

Nothing like the human eye is able to identify files containing child pornography, but those repetitive and pattern-like processes already defined, such as cataloging and searching of files, can be automated. Freeing the human agent from these tasks has obvious advantages in solving this cases.

One purpose of the European Project ASASEC is precisely the aforementioned. Another important element of this software solution is the ability to establish a working methodology and storage that appraise the information obtained during the investigation of a child pornography case.

[i] Civil Guard operation: http://www.europapress.es/catalunya/noticia-detenidas-27-personas-pornografia-infantil-16-provincias-20121015123618.html.

[ii] National Police operation: http://www.abc.es/20121031/espana/abci-detenido-abuso-sexual-menor-201210311102.html.