International Law Office

May 30 2022

Use of IT forensic evidence in copyright and trade secret litigation in Sweden

Westerberg & Partners Advokatbyrå Ab | **Intellectual Property - Sweden**

HANS ERIKSSON

Introduction

IT forensic reports by third-party IT investigators are commonly used as key evidence in copyright infringement and misappropriation of trade secrets litigation in Sweden. But a recent decision from the Patent and Market Court[(1)] spotlights some inherent limitations of IP forensic evidence and suggests that over-reliance on such evidence can become a significant hurdle for litigants if the findings in the IT forensic evidence cannot be corroborated by other evidence.

Though only a first-instance decision, this case appears to signal something of a shift in the Swedish specialist IP court's scrutiny of IT forensic evidence and may therefore have significant impact on future litigation in Sweden.

Background

IT forensics (also known as "digital" or "computer" forensics) is the field of forensic science that is concerned with analysing data from computers and other data carriers for use in civil litigation or criminal proceedings. In recent years, this kind of evidence has been increasingly used in investigations of suspected IP infringement as well as misappropriation of trade secrets in a modern digital environment.

There are several specialised third-party IT forensic actors that help clients conduct such investigations and prepare materials for submission in Swedish litigation. In a typical case, the IT forensic may be contacted by a company upon a key employee's departure under suspicious circumstances. The IT forensic may be tasked to analyse the former employee's computer and phone and flag any suspicious actions, such as unusual exports of data to private email accounts or unknown USB devices.

In the context of IP litigation, reports produced by IT forensic experts are most often used in copyright and trade secret litigation to establish:

- copyright infringement (ie, that the defendant has copied a file that enjoys copyright protection without the claimant or rights holder's permission); and
- misappropriation of trade secrets (ie, that the defendant has appropriated or spread a document that includes the claimant's trade secret information).

IT forensic reports have certain inherent and likely unavoidable limitations. In the typical case described above, the IT forensic has access only to the former employee's work computer. While the IT forensic may be able to see a large transfer of data to an unknown USB device, if they cannot access the unknown USB device, they can only report their findings with a certain level of likelihood, which amounts to less than legal certainty. Similarly, the modern digital environment – involving various connected devices and networks – is, simply put, complicated, and the former employee can use various kinds of encryptions or other technical tools to hide certain actions. There are also ethical codes for IT forensics to follow. Swedish IT forensics are therefore careful not to overstate the certainty of their findings in written reports and in oral expert witness testimony. In many cases, the somewhat preliminary findings in the IT forensic report must therefore be corroborated by other evidence that the claimant must invoke in the litigation.

One way of securing such corroborative evidence in civil cases of IP infringement (concerning infringement of rights subject to the EU Enforcement Directive) is through the procedural tool of an evidence seizure order. The goal of such a court-ordered action is to secure evidence of the ongoing infringement from the defendant (similar to a dawn raid under competition law). Commonly, Swedish litigants use an IT forensic report to substantiate the facts to the preliminary level needed to be granted the evidence seizure order ex parte – that is, without the defendant's hearing. After the raid is carried out, the preliminary findings in the IT forensic report can be confirmed and corroborated by the digital files seized during the raid, and thus used in the ensuing litigation.

But if the claimant relies on an IT forensic report with some uncertainties and is not granted an evidence seizure order, or cannot otherwise secure corroborative evidence through other procedural tools such as orders to produce information or orders to produce evidence, the IT forensic reports' findings may not be fully accepted by the courts. This was a lesson learned the hard way by the claimant in the recent copyright infringement and trade secret misappropriation case before the Patent and Market Court between two actors in the field of agricultural development (seed priming and vitalisation).

Facts

In 2013, the claimant (company A) entered into an exclusive licence agreement with the defendants (company B and person B) for a patent to prime and vitalise seeds. According to the licence agreement, improvements to the patent belonged to the licensor, company B. At the same time, the parties entered into a consultancy agreement for person B to work for company A in commercialising the invention. Person B also served on the board of company A.

In 2015, company B terminated the exclusive patent licence agreement and subsequently left company A's board. Company A was forced to stop commercialising the invention. Around this time, person B copied a large number of documents, test results and other materials to unknown USB devices and forwarded some sensitive information to a personal email address.

Company A had a leading expert IT forensic firm carry out a detailed investigation. The investigation was presented in several IT forensic reports, detailing different parts of the alleged copyright infringement and misappropriation of trade secrets.

Record number of evidence seizure orders

In what must be a Swedish record, the claimant sought ex parte evidence seizure orders against the defendant no less than four times in this case. The order was denied on various grounds (ie, not sufficient security for costs posed or not sufficient evidence invoked) the first three times, but the court granted a limited order on the fourth try.

For unknown reasons, the still-secret order allowing the evidence seizure to be carried out by the enforcement agency was not executed in time. After a few weeks, the Patent and Market Court sent the order to the defendant, likely believing that the evidence seizure had by now been executed, even though this was not the case. Even though the order had been issued ex parte, the defendant thus got the opportunity to file an appeal before the seizure had been conducted. On appeal, the Patent and Market Court of Appeal dismissed the order. Back at the first-instance court for a final decision on the merits, the order was dismissed on the grounds that the defendant had attested as true the file copying that the claimant had alleged and that thus an evidence seizure was not necessary and proportional, something that the claimant turned out to regret.

Following these procedural motions, the claimant sued the defendant for copyright infringement and trade secret misappropriation, seeking permanent injunctions on penalty of a significant fine and about €14 million in damages from the defendants. The claimant relied heavily on the IT forensic evidence to establish the facts of the case.

Decision

The Patent and Market Court dismissed the claimant's action in its entirety and ordered it to pay the defendants' full litigation costs of more than €800,000.

The Court found that the relationship between company A, company B and person B had been governed by the patent licence agreement and the consultancy agreement, and that the parties, which had legal representation, had entered into these contracts freely. The Court interpreted these agreements to mean that both the know-how and results of the parties' joint work commercialising company B's and person B's patent through company A, and the resulting improvements to the patented invention, belonged to company B. The Court also found that person B had an important and broad role within company A as a board member and thus had not only functioned as a hired consultant.

On the merits of the alleged copyright infringement claim, the Court – quite surprisingly – found that even though the defendant had attested as true the file copying alleged by the claimant at the preliminary stage when the evidence seizure orders were being litigated, and even though the timing and contents of this copying was, in the Court's view, suspect and raised several questions about person B's loyalty to company A, the evidence was not enough to establish which files had been copied and thus the copyright infringement claim could not be granted. It seems that the Court was frustrated with the way in which the claimant had prosecuted the litigation, since it had not availed itself of the opportunity to seek the production of evidence needed to corroborate the information in the IT forensic report.

In short, the Court found it factually proven that the defendant had copied several file directories to an unknown USB device, but that it had not been shown which files had been included in said directories. It does not appear from the decision that the defendant disputed the copying or argued that the directories had only been partially copied.

The Court did find it factually proven that the defendant had copied certain schematics and technical drawings that enjoyed copyright protection to an unknown USB device. The claimant was able to show that company A had a company policy against using outside data storage, which this copying would blatantly violate. But the Court – again, quite surprisingly – found that person B had such an important and broad role in company A, as the driving force of the business as well as a board member, that the IT policy would not apply to her work. While the Court recognised the copying as suspect, it held that it had been necessitated by person B's work for company A and thus did not constitute copyright infringement.

On the merits of the alleged misappropriation of trade secrets claim, the Court found that the schematics and technical drawings did include trade secrets belonging to company A. Since the Court had found that the claimant had not substantiated the copying of the other materials in the case in the form of file directories – again, even though person B's copying of these directories had been attested as true by the defendant in the early stages of the proceedings – these directories were not further adjudicated by the Court. The Court reached the same conclusion here as on the merits of the copyright infringement claim – namely, that even though the copying of these schematics and drawings was suspect, it had been necessitated by person B's work for company A and thus did not constitute misappropriation of trade secrets either.

Comment

This case showcases the limits of IT forensic evidence and the risks involved in relying too heavily on such evidence in IP litigation in Sweden. IT forensic evidence is, by its nature, somewhat preliminary, which IT forensic experts themselves are careful to point out. When such evidence is relied on to substantiate important facts of the case, the IT forensic report and expert witness testimony should, to the furthest extent possible, be corroborated by other written or in-person evidence. This is most easily accomplished if an evidence seizure order is sought and granted, but even if this is not the case (and not for lack of trying in this case), a claimant can use several other procedural tools in order to secure the needed additional documents.

All in all, it seems fair to say that the claimant faced a stiff-necked court in this instance. The case involved several interesting questions, such as the relevance of person B's earlier acceptance that the file copying had been carried out as described by the claimant during the early stages of the case and the finding that person B would not be bound by the IT policy forbidding the use of external USB devices because of person B's important role in the company – an argument can be made that the more important the role, the more important following the IT policy becomes. It will be interesting to see whether the case is appealed.

For further information on this topic please contact Hans Eriksson at Westerberg & Partners Advokatbyrå Ab by telephone (+46 8 5784 03 00) or email (hans.eriksson@westerberg.com). The Westerberg & Partners Advokatbyrå Ab website can be accessed at www.westerberg.com.

Endnotes

(1) Patent and Market Court, PMT 8087-20.