# Recovery of Circumstantial Digital Evidence Leading to an Anton Piller Order: A Case Study

Roland MacKenzie and Matthew Sorell
Convergent Communications Research Group
School of Electrical and Electronic Engineering
University of Adelaide SA 5005 Australia
+61 8 8303 3226
matthew.sorell@adelaide.edu.au

## ABSTRACT
The authors describe the techniques used to gather and analyse evidence of theft of intellectual property, specifically the customer records of their client, by a former employee, for the purpose of obtaining an Anton Piller order to seize records from the former employee's new offices. Importantly, it was not possible to find significant prima facie evidence, but a compelling circumstantial case was built up, based on the recovery and analysis of a large number of access records to the customer database. These records were inadvertently stored on the iMac computer (previously used by the respondent) in the form of intranet web addresses (URLs) in deleted and current files throughout the hard drive, despite obvious efforts to delete a wide range of files and records from the computer.

## Categories and Subject Descriptors
K.4.1 [**Computers and Society**]: Public Policy Issues – *Abuse and crime involving computers*

## General Terms
Security, Legal Aspects

## Keywords
*case study, forensics, data carving, intellectual property theft, Anton Piller order, circumstantial evidence*

## 1. INTRODUCTION
The recovery of digital evidence from a modern computer is becoming increasingly challenging. Investigators are often faced with an overwhelming volume of stored data, impractically short timelines (and budgets) in which to undertake an investigation of that evidence, and security logs which are missing, incomplete, or which have been tampered with. However, if we recognise that it is not the investigator's role necessarily to recover all files on a computer's hard drive, or to retrieve all potential evidence of suspicious activity, but rather to identify sufficient evidence to allow a case to move forward, then it might be possible to achieve the latter goal using incomplete but sufficient investigative techniques.

In this case, the authors were approached by the client, a recruitment firm, in 2006. A former employee had recently resigned and started a competing business in the same business sector, and had succeeded in attracting a small number of former customers of the client. The client expressed concern that their former employee might have in his possession records of their clients – companies seeking potential employees as well as job seekers – and asked us to investigate whether there was evidence of this on the computer which he had previously used.

There are significant difficulties in this type of investigation. The defendent would have had legitimate reason to access the customer database as part of his normal duties, and so finding customer records on his computer would not have been suspicious. We were therefore looking for evidence of customer records being transferred to an external memory device such as flash memory, CD-ROM or external hard drive, but even in that case, there might have been legitimate reasons for such file transfer. We also wished to review his access to the database, but this was complicated by the fact that the database had no access records; and his access to the printer, thwarted again by the fact that no logs were kept. Finally, we wished to discover, if possible, incriminating files such as emails or documents suggesting his active role in his new company while still working for our client.

As matters turned out, we were successful in discovering evidence suggesting abnormal access to the customer database, and our analysis and presentation to the court did result in the issuing of an Anton Piller order [1] (broadly, a civil form of search-and-seize order which does not require the permission of the defendent to be executed). Our evidence, in conjunction with other records held by our client, were sufficient to meet the three-step test required for the issuing of such an order as described in [2]:

1. The plaintiff must have an extremely strong prima facie case.
2. There must be very serious actual or potential damage accruing to the plaintiff.
3. There must be clear evidence that the defendent: (a) has in his possession incriminating documents or things, and (b) might destroy such before an *inter partes* order for discovery can be made.


E-FORENSICS 2008, January 21-23, Adelaide, Australia

DOI 10.4108/e-forensics.2008.2765

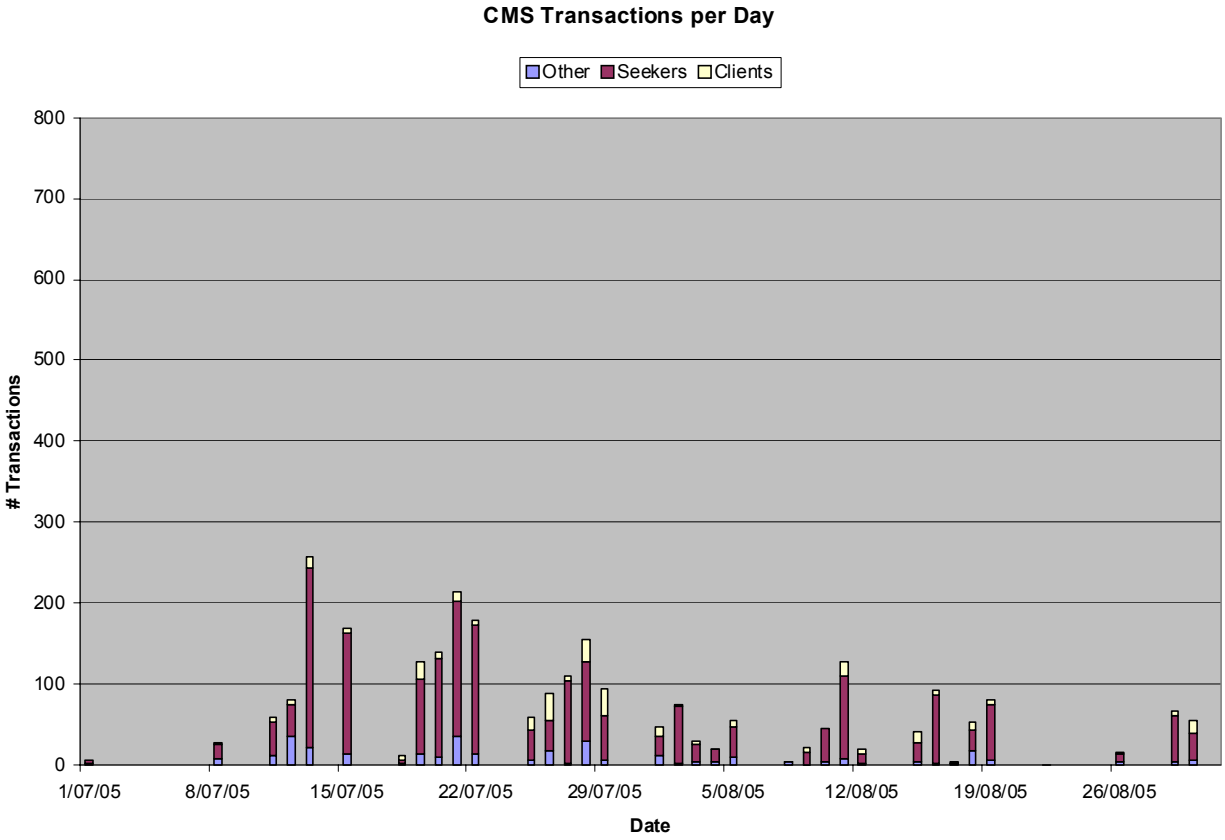


**Figure 1: Showing typical CMS access behaviour**

Our role as investigators was in establishing points 1 and 3(a). Importantly, we identified compelling circumstantial, not prima facie, evidence, which was considered sufficient by the Court.

## 2. PROCEDURE

We began by making a bit-exact copy (clone) of the hard drive of the iMac computer and using our copy to perform analysis. The size of this hard drive – 60 Gigabytes, is small by today's standards but even so is an overwhelming volume of data. There was some evidence of suspicious behaviour, namely that many of the log files had been deleted for periods in 2006, as well as all emails before May 2006. This is not compelling evidence, however, as it is plausible that the respondent was merely behaving belligerently towards his former employer.

There was some evidence that external storage devices had been attached to the computer, but log records were incomplete and we were unable to demonstrate clearly that this had been done in order to download customer records.

It is particularly difficult to recover deleted files on an iMac computer because of the way in which files are indexed using the file system, known as HFS+ [3]. When a file is deleted, the computer loses track of where the file was stored on the disc. Although a copy remains on the disc until it, or part of it, is overwritten, there are no details of where each segment is stored. This makes it difficult, although not impossible, to recover a file. While it is possible to extract such file segments and reassemble them, solving this jigsaw puzzle is time consuming, and in our case was well beyond the time and resources we had available. Had we been working in PC environment, in contrast, our task would have been much easier. This is because a file is "deleted" by overwriting one byte in the name of the file, but the file itself remains intact and each segment points to the next in turn.

Our next step was to filter the hard drive contents for text. In doing this, we acknowledge that evidence which might have been encrypted, and particularly evidence such as log files which might have been compressed, would not have been discovered. However, given our very short timeline, we had little choice but to try the easy options first. Text filtering reduced the volume of data by around 70%.

Our client supplied us with a list of keywords of interest, notably the names their clients who had begun dealings with the respondent. We were unable to find these names in an incriminating context (such as within the contents of an email), but we did note at this point that client names often came up within an intranet web address or Universal Resource Locator (URL), which turned out to be transactions between this computer and our client's Customer Management System (CMS) database.

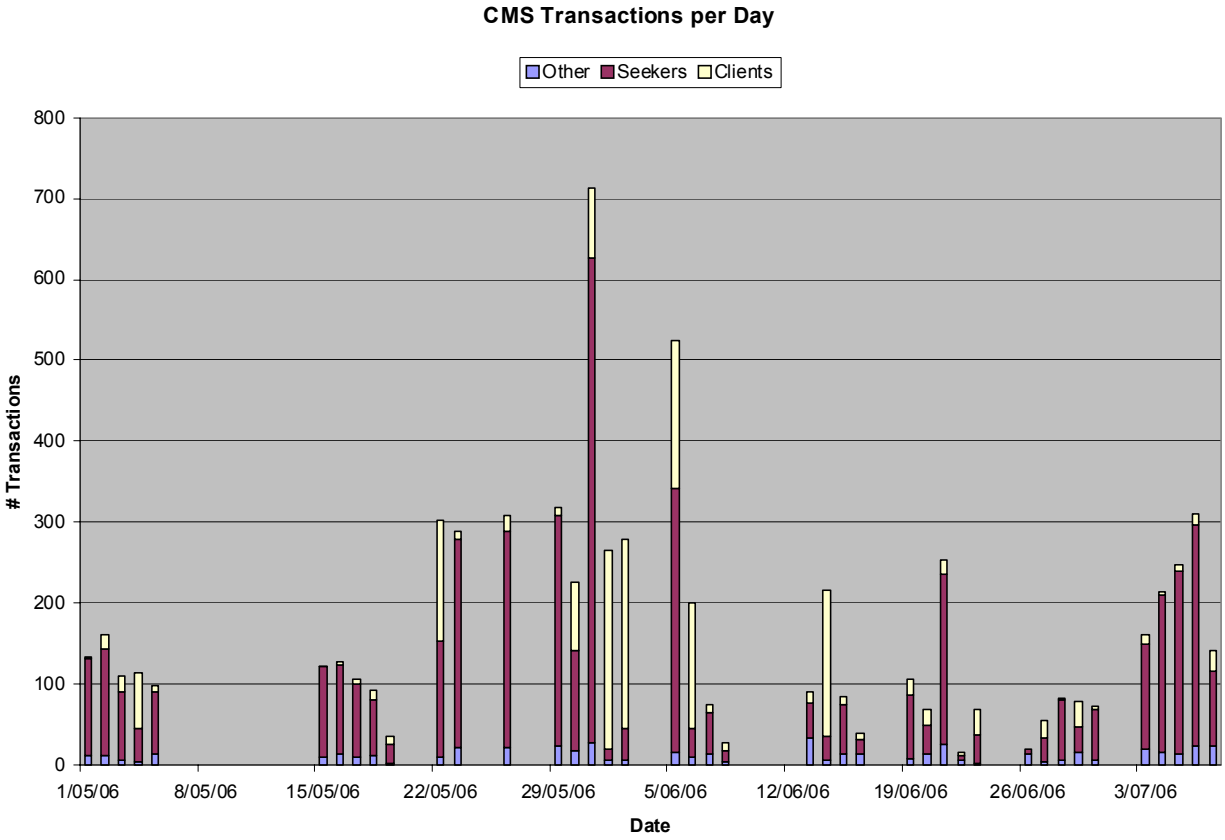


**Figure 2: Showing suspicious CMS access behaviour**

Of course, it is entirely proper that the respondent would have accessed the CMS. We noticed, however, that each URL contained not only the fine details of the transaction, but also a Unix timestamp. We therefore acted on the hypothesis that thetimestamp would reveal abnormal access such as working outside of normal hours.

We extracted many thousands of such URL records, sorting them by date. Interestingly, we noted that several – as many as 30 – copies of each unique URL were stored on the computer. The reason for so many copies is that the web browser keeps copies not only of browser history but also cached copies of the resultant file for subsequent efficient retrieval. We therefore filtered the list of URLs to remove duplication, then analysed the timestamp to break down the CMS access to a day-by-day snapshot.

## 3. ANALYSIS

The CMS access records dated back to late 2004, which we were informed is when the CMS came into operation. We were able to build up a picture of typical usage of the database by analysis of access records throughout 2005:

Figure 1 shows typical access in 2005 at around 50 accesses per day with some significant peaks. Typically there is a consistent ratio of seeker (job seeker) to client (potential employer) accesses of around 5:1 to 10:1. Other transactions include logging on to the CMS, managing personal calendars and a number of other management features.

While incomplete (we did not have the time to relate specific client and seeker record access, for example) the pattern of behaviour was clear. In particular, we noted that all database access occurred during normal weekday hworking hours, and that while there was some significant variation in access rates, there was little to suggest suspicious activity. However, our analysis of access in 2006 revealed very different behaviour, particularly in the period of January to May on specific days. Figure 2 is offered as an example:

The week of 29 May 2006 is of particular interest. Not only is the volume of access abnormally high (at least twice the normal rates of access), but it can also be seen that for this week, and occasionally on subsequent days, the rate of access to client records was much greater than access to job seeker records, suggesting a systematic downloading of client records. There are also clear examples of abnormally high rates of seeker records being accessed during other periods. Furthermore, a review of the access behaviour on a small number of specific dates showed systematic trawling through the database in alphabetical order.

What makes this circumstantial evidence particularly compelling, however, is that our client then checked his personal diary and was able to demonstrate that on days of abnormally high access, he was not in the office.

## 4. MEETING THE ANTON PILLER TEST

Although the test for an Anton Piller order makes explicit reference to a prima-facie case, we were able to establish a sufficiently compelling circumstantial case to justify the issuing of the order, which we then presented in a report to the Court.

That circumstantial case included some conventional evidence which is outside of the scope of this paper. The evidence related to our investigation included:

- Suspicious deletion of logs, including access and security records
- Suspicious gaps in email records
- Incomplete log files suggesting the mounting of an external storage device
- Complete evidence of access to the Customer Management System, timestamped to the nearest second, over a period of nearly two years, inadvertently stored in the form of temporary cached files used by the web browser software.
- Analysis of the access records which clearly demonstrated a significant change in access behaviour in the early part of 2006, including systematic (such as alphabetical order) trawling through the database on specific dates with particularly high levels of access.
- Alignment of dates derived from our analysis with the diary records of our client, showing that on days of high access, he was consistently out of the office.

The case for test 3(a) was substantially weaker, that is to demonstrate "clear evidence that the defendent ha[d] in his possession incriminating documents or things." However, the Court was satisfied that the nature of the evidence, in conjunction with the actions of the defendent in his new business, was sufficient to meet this test.

## 5. OUTCOME

Our client presented our report to the Court and was successful in obtaining an Anton Piller order. We attended the respondent's business premises with supervising lawyers. A number of computers, discs and printed records were seized and subsequently examined.

The authors understand that our client and the respondent have reached a confidential settlement out of court.

## 6. CONCLUSIONS

Our investigation was successful for three reasons: the fortunate implementation of our client's CMS database URLs which incorporated a timestamp; our ability as investigators to recognise the timestamp as a means of analysing an overwhelming volume of digital evidence; and the fact that our data could be presented in such a way that our client could corroborate times with his own personal diary. Without the timestamp, we would likely not have been able to identify suspicious behaviour, and we note, furthermore, that a brute-force automated approach to analysis would likely not have yielded a compelling, if circumstantial, analysis.

It should be clear, however, that the existence of the evidence we recovered was more due to fortuitous circumstances than appropriate record-keeping. Our client recognises that much better record keeping is required in the implementation of the next generation of the Customer Management System. That implementation will include not only a detailed and secure record of all accesses to the CMS, it will also alert the administrator of abnormal activity, and in particular abnormally high rates of access.

While similar monitoring is well established in the banking and telecommunications industry, the focus has traditionally been on monitoring for financial theft or managing credit risk. This case highlights the need for similar monitoring, even within a small enterprise, to mitigate the risk of loss of confidential information. The risk for our client was not only that the client database was potentially being used by a competitor, but also that there was a risk of losing client faith, and therefore business, in the handling of confidential information.

## 7. REFERENCES


[1] Supreme Court of South Australia, 2000, "Practice Direction No. 48 – Anton Piller Orders" (4 October 2000). DOI = http://www.courts.sa.gov.au/lawyers/practice_directions/civil_pd_pdfs/civil_pd_48.pdf

[2] Anne Staines, 1983, "Protection of Intellectual Property Right: Anton Piller Orders", The Modern Law Review, Vol 46, No. 3 (May 1983), pp. 274-288. DOI = http://links.jstor.org/sici?sici=0026-7961%28198305%2946%3A3%3C274%3APOIPRA%3E2.0.CO%3B2-C

[3] "Technical Note TN1150 – HFS Plus Volume Format", Mar 05, 2004, DOI = http://developer.apple.com/technotes/tn/tn1150.html