The many companies that sell software for computer forensics have developed products for analysing satellite navigators. Police high tech crime units and independent laboratories now use this software on an industrial scale. Computer technicians conduct the analyses. This is home territory for them, since the biggest component of a vehicle satellite navigator is a computer, often running the Linux operating system, and with access via a USB connection or an SD card. The analysis software extracts addresses which it plots using tools such as Google Maps. Specialists extract similar data from satnavs built into vehicles.

But many investigating officers find the results disappointing: “it’s just a list of addresses!” Unlike CCTV, ANPR and witness evidence, there are rarely times or dates to fit into a chronology. And anyway, the addresses are simply destinations for planning routes. The defence will point out that no-one can say who entered them, or at what time on what date, or whether a route was planned to them, or whether the satnav ever went there, let alone in a specific vehicle driven by a their client!

Another problem is that the investigating officer may simply not be able to understand the data provided. What are all these addresses? Were they recorded by the device itself or input by a user? Was that inputting an intentional action? The sense of frustration is enhanced by the quality of reports generated by much commercial software. The best packages provide at least some explanation of the data they contain, the worst none at all. The technicians who conduct the analyses often have neither the time nor the training to help. This leaves the officer with the prospect of presenting and defending poorly understood data in court. Some just give up!

But the addresses may at least have intelligence value. Police in a UK Midlands force seized TomToms from the vehicles of four armed robbery suspects who claimed, unsurprisingly, that they barely knew one another. Each suspect’s satnav turned out to hold the addresses of all the other suspects as recent destinations, showing association between them. And more: the addresses listed there included those of banks where the gang had committed armed robberies!

Another force in the North of England was investigating cases in which women had been trafficked from Eastern Europe for prostitution. When interviewed, the women barely knew which city they were in. But they could describe their clients and details of the houses they had been taken to. The heavies who drove them there had used a satnav to find the clients’ addresses. The list of destinations it held identified the clients, corroborated the women’s statements and helped lead to prosecutions.

An expert in GPS who understands the operation of satellite navigators and examines stored addresses will ask: who, or what, put them there and how did they do so? Figure 1 shows a point found in a TomTom seized from a member of a gang suspected of conducting a cash-in-transit hijacking. This location had to have been entered into the TomTom by someone taking it there and saying “add my present location to the Favourites list” or by their touching a map on the screen and saying...
“record this point”. In either case there was *mens rea:* a clear intention to mark and record the location and then to label it “A”. The point was there to show the driver of a bulldozer the exact location at which to lie in wait. When the target cash vehicle approached the junction nearby, he drove the bulldozer forward, crashing into it and damaging it so seriously gang members could climb inside and make off with the cash. Presented alongside other testimony, this single point in a satnav made powerful evidence.

![Figure 1: Just a single point in a long list of addresses](image)

Another similar marker, in a TomTom in Wales, turned out to be a murderer’s reminder to himself of precisely where he had buried his victim’s body for when he returned months later to dig it up again. He had labeled it neatly with her initials.

Sometimes the greatest evidential value comes from locations entered not by a user, but by the satellite navigator itself. A Scottish police force, investigating a series of sex attacks and robberies, seized a suspect’s TomTom. Their High Tech Crime Unit ran commercial analysis software that produced thousands of addresses, most of them multiple repeats; the printout was an overwhelming 104 pages long, even without maps! A GPS expert witness called in to examine the report identified the tiny number of locations that the satnav itself had recorded, proving that it had actually been there. He gave the jury a clear explanation of how GPS works, how one could be certain the TomTom had started or ended a journey at those points, and how accurate the location measurements would have been. When the prosecution showed that there was a TomTom fix like that close to the scene of offence after offence, the evidence proved compelling and the suspect was convicted.

None of the locations I have cited was timed or dated. Each was simply an item in “just list of addresses!” On their own, most of them had very limited evidential value. But each of them proved to be of great significance when carefully presented in combination with other material. Good forensic software packages will extract these locations. But to detect and demonstrate their importance in a case requires much
more: someone with an understanding of the modes of use of the satnav clear enough to explain these matters to a jury and robust enough to withstand hostile cross-examination.

It can be quite straightforward to tie a satellite navigator to a specific individual. The owner’s name may be recorded and usually a Home Address. Even the hardest-hearted criminal may name family members: a mother may be “Mum” and where she lives identified. Addresses visited frequently will be in a record of “Favourites”. In the “Settings” menu users reveal something of themselves and their lifestyles by their choices: the language they speak, decimal or imperial units, international travel. Many commercial forensic packages ignore this information. If the navigator has been used with a hands-free phone, the telephone number will be shown, and lists of calls made and received. Satnavs may even contain photographs or videos showing the owner and family members.

But the greatest evidential value often comes, not from routine locations, but from the unexpected, the entries that cause investigating officers to catch their breath! Suddenly, they spot a known criminal, a wholly unsuspected associate of the owner, a name that produces multiple hits in police databases. There may be complete networks of such unexpected associates. The destinations can deliver surprises too: journeys to Holland are found and a whole new line of enquiry opens up. These unexpected destinations are then linked to ANPR hits or CCTV images. Intriguing intelligence becomes powerful evidence.

Figure 2: Tracking data from a satnav in a car approaching a fatal accident
Few would doubt that the most valuable GPS data comes from tracking systems which can deliver accurate records of journeys, each point timed and dated. Some records will come from covert trackers deployed by law enforcement agencies. Others will show the journeys of vehicles seized by the police that just happen to be fitted with commercial vehicle location devices. And occasionally, an ordinary car satnav in the hands of an expert will unexpectedly deliver top-quality tracking data. The plot in Figure 2 was extracted from a satnav recovered from deep within the crushed wreckage of a car that had been in a fatal head-on collision with a truck. The device itself was damaged, but still working. Inside it was a file that recorded the track of the car, with timed and dated locations every few seconds, together with speeds and headings. It leads right into the scene of the collision. Even the verbal instructions the satnav would have given the driver immediately before the accident could be reproduced. This evidence played an important role at the inquest.

Handling tracking evidence is especially demanding. Although a plot on a map will appear convincing – and will certainly appeal to a jury – it can come under strong attack on grounds of accuracy and reliability. A case may turn on the exactness of GPS fixes. Claims such as “95% of measurements fall within 5 metres of the true position” are correct when the GPS receiver is located on a clear, open site. But what about a covert tracker, hidden deep inside, or even underneath, a vehicle? And in a city centre urban canyon, the satellite signals that reach a GPS receiver may have been blocked and reflected by tall buildings, giving errors of 300 metres. A stationary receiver there will appear to move constantly. The defence will quote such examples to discredit all the tracking evidence. So, one of the skills of a GPS forensics expert is to analyse crime scenes with an understanding of radio propagation and explain where and why there will be substantial errors.

To prove that tracking evidence is sound means recognising the weaknesses of tracking systems, especially low-cost commercial ones. GPS satellites can and do fail and solar weather can cause their signals to be lost; evidence from the nearest official monitoring station will demonstrate that all was well with GPS at the time and place of a crime. Data sent from a vehicle to a tracking centre can be lost or corrupted in the communications channel; this must be audited to show that error detection is in place. Criminals now use jammers to disrupt tracking systems; the evidence must be analysed for indications of this. And some tracking companies do terrible things to forensic data: truncating latitude and longitude readings to save communications charges; altering GPS fixes by map-matching; making mathematical mistakes in processing locations; and failing to understand about geodetic datums so that suspects are shown hundreds of metres from the crime scene! Careful auditing of the system by a navigation expert can show that the tracking results are sound. That done, a jury will be impressed by tracks that fall on highways and stationary data that clusters in a tight area.

We have come a long way from just using software to extract addresses from satnavs! That is still essential work - and it must be done well. But GPS forensics also needs GPS experts to explain the results. They bring an understanding of the radio propagation of signals between satellites and receivers, the factor which dominates accuracy. They know about the handling of navigation data, latitudes, longitudes, heights and datums.
GPS Forensics is developing rapidly and growing in importance. The results are increasingly being presented, challenged and defended in test cases in the courts. But one thing is now certain: given competent analysis and in the hands of GPS forensics experts and detectives keen to make maximum use of this new information, it is certainly a great deal more than “just a list of addresses!”