eForensics Magazine

INVESTIGATING FRAUD IN WINDOWS-BASED DRIVING EXAMINATION THEORY SYSTEMS AND SOFTWARE

Fraud can take many forms, can take place practically anywhere, any when and any how. Theoretical driving examinations are now computerized in most parts of the world and the overwhelming majority of such systems tend to have some to no security at all, relying instead on the invigilators of the exam to catch those suspected of fraud. But, what happens when the invigilators fail and you, the digital forensic investigator, is asked to look into the case? Where does one start, where does one go and where does one end up? What do we investigate, how do we go about it and what tools with?

In this article, I will attempt to share my experiences investigating such systems from the point of view of the digital forensic investigator who first arrives in the scene of the crime, from the moment of arrival to the end report submitted to the client.

Let us, then, start our journey from the moment we (the digital forensic investigators) get the fateful call, where we are told it's a case of fraud in the Driving Test Centre and we have been called to investigate it and present a report.

To begin with, it should be stated that, as most driving test centres are part of a country's internal services, we are going to always be dealing with a mixture of government officials (of middle-management persuasion) and local law enforcement, and we are always going to be needing to deal with red-tape -style bureaucracy, where everything is moving much more slowly than when dealing with the private sector.

This means we are going to be dealing with the nightmare scenario where our crime scene is possibly several months old and very seriously tainted (as non-essential government bodies tend to respond fairly slowly and after much red-tape to such cases), and where normal digital forensic processes and practices don't usually work. The nightmare comes from the fact that, in such a scenario, you cannot explicitly trust the data you collect or any information that you are given and cannot corroborate in a straightforward way.

The data has been tainted, the exams are running 2-3 times a week and the test centre cannot be closed down for the duration of the investigation, so we are told we have to release the (many, plus servers) computers within a very specific and finite length of time (1-2 days at most).

So, we arrive in the vicinity of the crime scene (the building).

First and foremost in our minds should be that this is a place where practically everybody has access to the building between government office working hours, and where nowadays Internet access via wireless access points scattered throughout the building is the norm, and they are used by both staff and examination candidates at the same time.

This means we can assume three things:

a. That the test area is not completely isolated.

b. That the fraud may not simply involve the test area's workstations but also the devices of the examination staff and the candidates.

c. If points a and b hold true, there is nothing we, the police or the government body can do about it, nor is there any reliable way for us to find out who did what using the wireless access point, when and how (forget about going through logs (if they exist at all) of the free wi-fi access points in a public area).

So, we map and find the range of the wireless Internet access points, see whether that range extends to the testing room, detail the findings in our contemporaneous notes and move on to the testing room itself.

In an examination environment, the location of everything and everyone in it before, during and after examination time is as important as the actual workstations used in the examination.

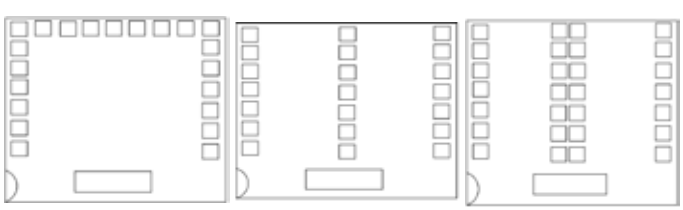

Figure 1: Workstation placement in the examination room.

Figure 1 shows three of the more common workstation placement schemes in an examination room. As we can see, the types of workstations, their placement in the room, the tables they are using for the workstations (e. g. Figure 2), the invigilator's seat & point of view and even their walking patterns are of importance if one is to try to map the scene of crime in this instance. So, we deal with the physical crime scene as we would in a normal forensic investigation in the real world. The reason for this is we want to establish how the alleged crime has been perpetrated, or how it has not been perpetrated (at this point, we either prove or disprove theories).

Figure 2: A typical examination workstation

Some workstations will be full computer systems utilizing touch-screen technology with more conventional input devices (keyboard & mouse) and main processing units hidden away inside panels, such as the system shown in Figure 2. Others will be complete kiosk-style systems with such components integrated to form as small a footprint as possible. The type of workstation used, as well as how the layout of the room is utilized to take this into account, is also very important.

For example, in one of my investigations, I asked a member of the invigilation team to take part in a small experiment where I was the person taking the exam and they were the invigilator in the room, under proper examination conditions. By doing everything I could to gain physical access to the system without being seen by the invigilator (also accounting for the invigilator's heightened perception of the possibility of me committing fraud), I was able to better understand the possible physical access points, barriers to access and subversion mechanisms. Such experiments can give you a better idea of the strengths and weaknesses of certain physical approaches to fraud.

After we detail and provide a set of photographs and drawings of such information on the physical locale of the crime scene, we need to move to the more traditional aspects of a digital forensic investigation, namely the processes of seizure, acquisition, analysis and reporting.

As we discussed before, however, the rules governing such processes, as defined by NIJ (2004) or ACPO (2011) in their good practice guides, have to be applied to a crime scene that has been contaminated repeatedly over a potentially large period of time. Combine the above with the requirement for the seizure of any equipment and the acquisition processes to be performed in the shortest possible timeframe so that the test centre can be up and running, for example, the next day, and you are faced with the nightmarish scenario of having to perform said processes in such a way so as to comply with the requirements of the public body and, at the same time, not compromise whatever shred of evidential value the artifacts may still retain.

For example, you have to immediately discard any (even remote) possibility of getting anything useful from sources such as cache, RAM, page-files and running memory/processes after all the time that has passed since the commission of the alleged crime. That assumption, which is perfectly valid given the circumstances, (and should be clearly stated and the reasons detailed in both your contemporaneous notes and in your report) allows you to reduce the number of artifacts you will seize to just the workstations and servers' hard drives.

Additionally, you should also liaise with the IT department and ask to be given access to the locale where the networking infrastructure for that particular room resides. There you need to identify and photograph any equipment used and assess the evidential value of said equipment. A managed CISCO switch or router, for example, can be of much evidential value, as opposed to an un-managed un-named-brand switch/router. Any "exotic" hardware should also be seized.

What you should also be looking for, while liaising with the IT department, is whether the computer network in the room is completely isolated from the rest of the network (as it should, in an ideal world, be) or not (as the case will more often be) and, if it is not isolated, what the keyholes the IT department

has installed for ease of administration are. As before, note it down in your contemporaneous notes, but be prepared for such information to be either false or not entirely true.
Another point you should consider, while liaising with the IT department, is the possibility of their complicity in the alleged crime. In a lot of cases involving fraud, such crimes are perpetrated through the collusion of the offender with one or more insiders.

So, with the process of seizure complete and the hard-drives in your possession, the acquisition process begins and is conducted in exactly the same way the manual says (image the drives using a hardware and software blocker, hash the images, make copies of the images etc.) and return them, through the proper channels, to the driving examination centre. An important tip, at this stage, is that you should always expect to have to deal with any and all kinds and sizes of storage mediums (IDE, SATA, SSD etc), with any and all kinds of partitioning schemes. And you should always expect to consume more storage space for the disk images than originally given to understand you will require.

The process of analysis when investigating Theoretical Driving Examination centres is both more and less complex than in your average type of casework.
You don't have to deal with very exotic hardware, the Operating System in use is always Microsoft Windows (2000, XP, Vista or 7, depending on the age of the computer systems used by the testing centre), and the filesystem in use is either FAT32 or NTFS. Standard digital forensic analysis methodologies and tools of the OS and the filesystems have been amply documented by such authors as Casey (2011), Carrier (2005) and Carvey (2009, 2011).

One such system can be seen in Figure 3, where we can see the partitioning scheme is split into two partitions, both of which are NTFS, and whereas the first partition is devoted solely to the OS, the other contains the driving examination software.

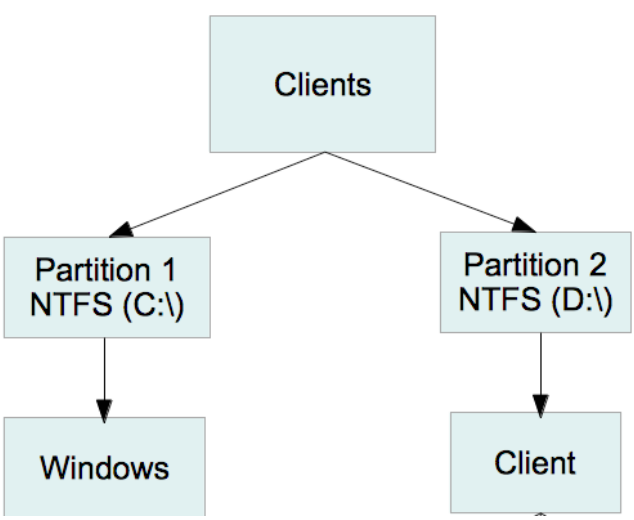

Figure 3: A hypothetical exotic configuration of an examination workstation.

What you do have to deal with, however, are:

a. Exotic driving examination software.
b. Exotic driving examination software update mechanisms.
c. The fact that the information you are trying to find that would prove or disprove the actual commission of the alleged crime has been either:

   a. not recorded in recordable (and thus retrievable) locations;
   b. overwritten by the passage of time and by log-file retention policies;
   c. deleted multiple times through re-formatting of the hard-drive;
   d. do not exist because the hard-drive has been replaced at an unspecified time in the past.

d. The sheer number of hard-drive images that you have to analyze just for this one case.

When it comes to exotic driving examination software, there are a number of things one has to understand and be able to deal with. First of them is the fact that the contract for the development of the driving examination software will have been auctioned off to the bidder with the lowest offer, price-wise. This means that the software itself will not behave in a predictable and identifiable manner (e. g. as identified in the National Software Reference Library *(http://www.nsrl.nist.gov/))* and will have to be analyzed in order to identify any points that the offender(s) will attempt to exploit by themselves, any points that the offender(s) will attempt to exploit through the help of a third-party (insider) and any points that the third-party (insider), or even fourth-party (driving instructor paid off to take the examination on behalf of the interested party) will attempt to exploit by themselves on behalf of the offender, with or without the help of the insider.

One way of analyzing the driving examination software is to reverse-engineer it, which is a very long and arduous process that may or may not be a waste of time in terms of what its outcome will be but can potentially give us easily verifiable data of evidential value. It should be noted, here, that the process of reverse-engineering the actual software is not only time-consuming but also requires a very good knowledge of reverse-engineering principles and methodologies and a very good knowledge of low-level computer programming and debugging.

Another way of analyzing the driving examination software is to use a copy of the server and workstation disk images, convert said copies into virtual machine disk images and recreate either the entire or part of the network in a virtualized environment (through VirtualBox or VMWare, for example). Then, using the credentials previously supplied by the IT department of the examination centre and all the information you have gathered about the network topology and the operation of the network, attempt to simulate a full theoretical driving examination, at the same time monitoring the network through the use of such tools as registry change/modification viewers, system resource/modification viewers and packet capturing solutions (eg. wireshark *(http://www.wireshark.org))*.

The advantages of this analysis method is that, through simulation and observation, you will gain a deep enough level of understanding of the network in question and its operation, and you will have the opportunity to observe, record and analyse all the effects the operation of this piece of software has on the workstations and the network in general, thus identifying the points made earlier in the article. Another advantage of

this analysis method is that it will allow you to also identify, at the same time, the updating mechanism the software has for updating the driving examinations. The major disadvantage of this approach, however, is that it will effectively destroy the evidential integrity of all the copies of the disk images acquired in the previous step of the investigation, and should only be attempted when multiple copies of those disk images have been made.

A third approach to analyzing the driving examination software is to also acquire the program itself through a request made through the law enforcement body. However, the major stumbling block I've run across in my attempts to do that comes from the way the software tends to be distributed to the driving examination centres, namely through subcontracting the task to private IT businesses, who then image the system the software is installed and install the image on a number of workstations and servers which they set up in the test centres themselves. Attempting, thus, to acquire an intact copy of the software in question, involves any number of red-tape riddled steps and have an equal chance of being a waste of time and completely fruitless as they have of actually allowing you to acquire the software in a reasonable timeframe.

With regards to the rest of the points (points c and d, specifically) made earlier in terms of what you have to deal with when dealing with this kind of a case, the major stumbling block of any analysis process is the time-frame in which you have to perform the investigation. In my personal experience, the usual time-frame you are given to conduct the investigation ranges between one and two months from seizure to filing your expert witness report. Any analysis, thus, that is to be attempted should mainly concentrate on the retrieval of any possible information that can be readily retrieved through standard digital forensic methodologies in the slice of time the alleged crime has been committed, and the analysis of the actual driving examination software in so far as possible. You are, after all, dealing with information that has been tainted by time and by further use of the workstations before the digital forensic investigation has begun, and you don't have either unlimited time or resources at your disposal.

Also, any analyst working on the case should expect and be prepared to have to work with little in the way of retrieved/carved information (regular files or log-files) aside from the actual driving examination software. After all, it is easily possible for the hard-drives of some (or even all) the workstations to have been replaced in the time between the alleged crime and the beginning of the investigation and the previous hard-drives destroyed before the alleged crime has been reported.

All this information, and the various reasons for the lack of available data due to the time between the commission of the alleged crime to the time the investigation of said crime has begun has to be very clearly stated in the reporting process.

As you have seen, heard and/or know, a digital forensic investigation is normally a relatively lengthy and difficult process, in the best of cases, that is highly dependent on the length of time between an offence and the beginning of the investigation. As you can see in this article, the difficulty of processing cases such as those of fraud in theoretical driving examination tests is twofold: not only do you have to deal with a red-tape-derived increased time-frame between the offence and the investigation, but you also have to deal with issues ranging from time-constraints in the seizure, acquisition and release of the artifacts to issues such as completely custom and unpredictable software whose behavior is non-consistent and non-standards-compliant. But it is my hope that this article will give you a few pointers as to where to start looking and what to look for when such casework falls in your lap.

References

ACPO, (2011), "Good Practice Guide for Computer-Based Electronic Evidence, Association of Chief of Police Officers, UK, (http://www.7safe.com/electronic_evidence/#), Last seen: 10/07/2012

Carrier B., (2005), "File System Forensic Analysis", March 2005, Addison-Wesley Professional Series, UK, ISBN-10 0321268172

Carvey H., (2009), "Windows Forensic Analysis DVD Toolkit, Second Edition", June 2009, Syngress, UK, ISBN-10 1597494224

Carvey H., (2011), "Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry", Syngress, UK, ISBN-10 1597495808

Casey E., (2011), "Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers and the Internet", May 2011, Academic Press, UK, ISBN-10 0123742684

NIJ, (2004), "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", April 2004, National Institute of Justice, US, (http://nij.gov/nij/pubs-sum/199408.htm), Last seen: 10/07/2012

Author Bio

George Chlapoutakis is a Network Security and Digital Forensic researcher, developer, investigator and consultant working in both the academic sector, as a part-time lecturer in Teesside University, UK, and in the business sector through his private business, SecurityBible Networks (http://www.secbible.com), which is based in Greece but operates in the European Union.