



Income Tax Raid

The Income Tax Department Is Much Smarter Than You Think.

Nothing can be hidden from their investigations: passwords, encryptions, deletions. They have a solution for everything. Learn all about how the Income Tax Department retrieves digital data to collect evidence.

An income tax raid! The mere mention of that phrase sends shivers up any businessman's spine. It has always been a hush-hush topic and people often stay tight-lipped when the subject comes up. Misusing technology to hide evidence is the new reality of today's business. Increasingly, a lot of people are getting convicted on the basis of the evidence collected from their digital data. Their own computers betray them. Government forensic labs in Hyderabad and Chandigarh specialise in investigating digital data. The courts now accept digital evidence and the cyber expert's testimony. An expert's testimony in court, along with whatever digital evidence was found, supports the case and is instrumental in convicting the suspect.

Let's demystify the entire procedure that shrouds an income tax raid—where

digital data is investigated to the core. We caught up with Samir Datt, Director, Computer Forensics and Investigation, Foundation Futuristic Technologies(P) Ltd. and he divulged some very interesting details.

Modus operandi

To begin with, the Income Tax Department identifies every location of a business that could hold potential evidence. When a raid is planned, the forensic department is contacted to prepare all the necessary equipment that will be required to investigate the digital data from confiscated computers, laptops, etc. The experts informed us that before the raid, hard drives are prepared to collect the evidence. For this, clean hard drives are required because if there was already data on it, it gets difficult to distinguish

between the old data and that of the suspect's. Also, the suspect can very easily claim that any incriminating evidence was already on the IT department's drive. So the first thing that is done is to prepare a destination drive. There are specialised tools that are used for this process. DriveWiper Voom hardware is used to wipe off all the past data. It also generates reports to ensure that the hard disk is clean. This hard disk is used as the destination or target drive.

Once on the destination drive, it is the choice of the investigating officer whether to seal the equipment on the spot or bring it to the IT department's office. The entire data from the suspect's computer is digitally imaged on to the target drive. When a forensic imaging process is carried out, the bit-by-bit clone of the original hard drive is prepared using specialized tools. The hard drive contains all the files that you can see, including the operating system files, deleted files, files that someone has accidentally or intentionally deleted, encrypted files, misnamed

files, password protected files, hidden files and partially hidden files. Data hidden surreptitiously within other files is also retrieved. These tools are OS independent and work without the need of a dedicated drive. All this happens at a very fast pace. The original hard drive is then sealed.

Also it is important to know that the data copied from the source drive to the cloned drive is the same. Similar to human beings who have distinctive fingerprints, in digital investigation, a unique fingerprint is created for each hard drive. This is also known as hashing. Two hard drives can have the same hash value only if they have the same content. "During investigation, when a hard drive is collected from the destination, we have to prepare documentation that certifies that the suspect's hard drive has been seized along with the hash value. The suspect has to know the hash value when his drive was seized. If the hash value changes, this means that the hard drive



This clones your hard drive data @ 5.5GB/min

has been tampered with," explains Samir Datt.

Now even if a bit of the content on the hard drive changes, the hash value will change. This ensures a fair procedure of investigation. In a court of law, if the hash value of the hard drive is different from the hash value recorded at the time when it was seized, it can be challenged. The defendant can plead innocence, claiming that the law enforcement agencies are trying to frame him. In order to prevent this, proper procedures and technologies are adopted.

The obtained data is then write-protected using write-protect bridges. Now, the hard drive is connected and files can only be read but not written to. This guarantees that the purity of the evidence is intact.

They cannot be fooled

The forensic department cannot be fooled. Today, businessmen use removable drives like USB drives, pen drives, digital cameras, iPods and MP3 players—all of which can also be used as movable storage devices. The suspect might try to move away with pen drives that are as inconspicuous and look similar to a pen, but the forensic department keeps a close tab on all movements. These drives are seized too.

In some cases, suspects try to outsmart the authorities and misname files. For example, they rename their confidential file as the Windows file and



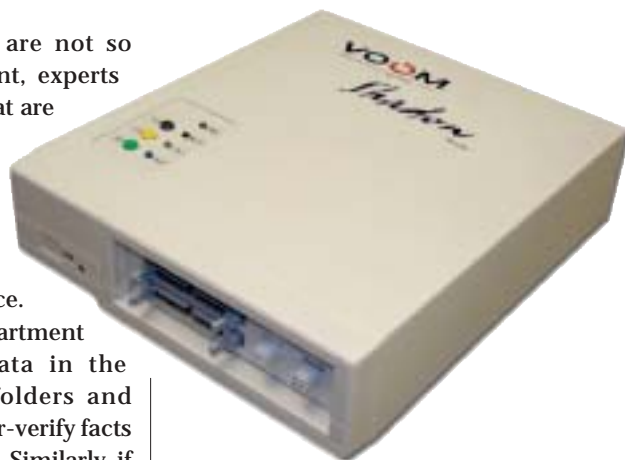
Samir Datt

copy it to the Windows folder. They're confident that an investigator is not going to open the thousands of files inside the computer and would obviously leave the system files alone. That is where they are wrong. Investigating officers have specialised tools that scan the whole hard drive and classify each file, according to category. So these tools identify the encrypted, password protected files, the misnamed files, the image files and the compressed files. Normally data is compressed only when someone is backing it up or transmitting it to another drive to make it easy to carry, which is again a piece of evidence to be checked on. This can take four to eight hours for the case to be set up.

Once the password-protected files are identified, password-cracking tools

in court, where people are not so technologically conversant, experts use specialised devices that are plugged between the CPU and hard drive. This allows the computer to be booted up and will show what the suspect sees, without contaminating the evidence.

The investigating department cross-checks all the data in the inventory, the e-mail folders and accounts details to counter-verify facts and to pinpoint anomalies. Similarly, if during a raid they uncover significant amounts of unaccounted cash, then data from other sources, such as e-mails, inventory and databases, is sifted through to assist in auditing the cash. The case of a property consultant in Gurgaon was investigated. While



This examines imaged hard disk

Your rights

Although it is the investigating department's decision to tackle the evidence, they seize the drives in the presence of witnesses and those seized



Hardware and Software used to examine acquired data

are used to unlock them. Steganography is the art of storing files in another file. There was a case in which a coded message was passed on behind a forwarded funny picture. Investigative tools can very easily track all these hidden messages. These tools conform to the judicial and evidential requirements.

When the evidence is to be shown

examining the data in his Tally software, his assessments of his income totalled approximately Rs 2 crores, which was not too much. However, when the forensic department examined his data more thoroughly, they found a number of deleted Tally files. When these were recovered, his income assessments went up to 130 crores, which proved him guilty of tax evasion.

drives are taken to the income tax department. The person or company being raided, however, can request for a copy of their data or for the original drive after the IT department's work is done.

This article is to make you aware that no matter how hard anyone tries, the income tax department is superiorly equipped and will take no



Data investigation tools

time to dig out your deepest hidden secrets. The solution is extraordinarily simple, according to the Income Tax department: Just pay your taxes! ■

—Kalpana Sharma,
Kumar Anshuman,
BenefIT Bureau