All crime is becoming e-crime

As many investigations now mean seizing any number of suspects' digital devices for examination, forces are coming to terms with the dilemma that is how to manage the rapid growth in data passing through high-tech crime units (HTCUs) without increasing the size of the teams to match the scale of the task.

Ben Chapman, Dell's Government and Defence Marketing Manager, said "Not only is the amount of storage built into consumer electronics devices increasing, irrespective of crime, so too are the number of devices police have to seize. If you multiply one by the other the police are faced with an exponential growth in the volume of digital data they have to investigate".

While it can be argued that being able to access the internet to interact with the rest of the world from anywhere is changing the way we live our lives, it is certainly the case that police forces are being posed a number of challenges to cope with demand.

Police workforces are shrinking to match budgets in an age of austerity, however, few can afford to reduce the size of their digital forensic teams; they just wouldn't be able to cope with the inexorable rise in the number of files to be examined to prosecute many of their serious offenders.

Steve Slater, head of Devon and Cornwall Constabulary's HTCU, believes it is not simply the growth in number of devices, whether that is criminals' use of anonymous pay-as-you-go phones to commit crime or lifestyle changes meaning suspects own many devices, it is also the types of crimes his unit has to deal with.

Paedophilia remains the biggest crime type needing digital forensic examination but almost all other offences, as well as suicide and road death investigations, also have a digital factor. In particular, terrorism, homicides, kidnapping, fraud and drug offences are all responsible for increasing the supply of digital devices to be examined.

It's not just Home Office forces that are seeing the same level of growth in demand. The British Army's Service Police Crime Bureau (SPCB) owned by the Provost Marshal (Army) (PM(A)) deals with all forensic requirements from operational theatres or frontline Royal Military Police (RMP), Royal Navy Police and, if required, the RAF Police (which has its own HTCU) where they require a greater level of analysis. SPCB too has also had to cope with a massive growth in volume of data.

Policing the 330,000 defence community around the world has its own challenges. Technology minded service personnel typically own the latest iPhones, BlackBerrys, tablets, laptops and games consoles, all of which connect to the internet. SPCB's Cyber-Crime Centre (3C) is responsible for the analysis of upwards of 15 devices in each case and it is easy to see why the unit has experienced an average growth in data submissions of 120 per cent a year since 2001.

Major Keith Miller, head of SPCB, says every single device also has much more data storage capacity, multiplying the Gigabytes to examine and creating a massive influx of data into HTCUs.

What can police force and law enforcement agencies do to cope with the wave of demand? Scaling up forensic analysis teams to match the growth in demand is simply not sustainable, or even possible given the three years it takes to train an analyst. Doing

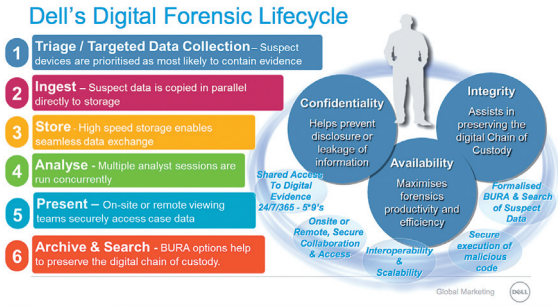
nothing is also not a viable option. So forces must find smarter ways of working if they are to mitigate any of the risks faced by a delay in examining exhibits submitted to the units and manage growing workloads within tight fiscal conditions.

The solution for SPCB and Devon and Cornwall Constabulary has been to take advantage of greater processing power, parallel processing and integrated forensic packages which handle everything from targeted data collection or 'triage' at borders or the scene of crime to managing the analysis of digital evidence and the digital chain of evidence back at the lab.

Parallel processing

Traditionally, forensic analysts in the past completed their work on individual workstations, processing, imaging, indexing and cataloguing the findings of the many devices submitted to their units.

As those workstations are set to work, analysts are dependent on the processing power and speed of that



computer to complete its job. There are a number of disadvantages with the traditional way of handling data. Typically this is because investigators spend much of their time administering, upgrading or maintaining lab hardware. When confiscated devices are being processed it can tie up each workstation for hours and in some cases weeks at a time. Because of the size of data, officers find it difficult to work together on cases because digital evidence cannot easily be shared locally, let alone regionally across the force's network.

While parallel processing has been around since the early days of the first computers, it is only now entering the forensic arena. By harnessing the multi-threaded capabilities of AccessData Lab (AD Lab) running on Dell's Blades, analysts are able to dramatically reduce the time needed to analyse even the multiple, multi-terabyte investigations because they are running them in the data centre or part of the force's private 'cloud'. Each analyst can set about multiple jobs, from the same single workstation, rather than the workstation being taken over by a single task.

The SPCB first took a different route when it saw huge volumes of data being submitted as part of the Iraq Historical Allegations Team (IHAT). It installed Dell's Digital Forensics solution that meant analysts could use the much greater processing capacity of Dell servers, storage and high speed local area to work on more than one job at a time. It soon realised that jobs that were taking individuals weeks or months could now be completed across a team of investigators in days.

With the proliferation of devices now present in its other work, especially public protection, the decision to spread

Ben Chapman – police are faced with an exponential growth in the volume of digital data they have to investigate.

Steve Slater – forensic triage allows us to identify which are the primary exhibits and focus our available resources where they are needed."

the benefits of Parallel Processing to SPCB's entire digital forensics work was an easy one to justify. It is in the middle of installing a 600 terabyte (0.6 petabyte) datacentre with much improved processing speeds to cater for whatever jobs are thrown its way.

Devon and Cornwall Constabulary has taken a strategic, longer-term approach to it's investment in its digital forensics capability. Instead of constantly upgrading individual workstations, Devon and Cornwall concentrated on storage with a Dell datacentre. It now has up to 160 terabytes of storage and backup and, in the last half of 2011, the force switched to Dell's Blade servers to make use of the complete Dell Forensics solution.

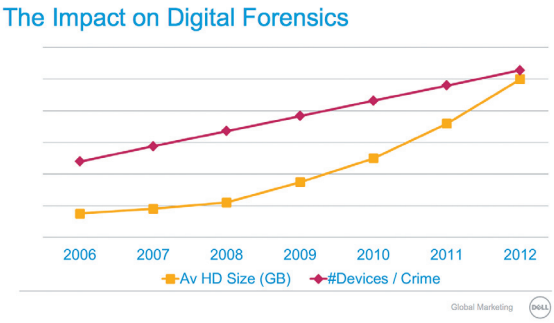
There are many advantages of parallel processing, any analyst will tell you the worst thing they want to see when starting a shift is that their workstation crashed in the middle of the night as a job was running, the first thing they have to do is rebuild their system before they can start the task all over again.

It is easy to see why HTCUs are typically a nightmare for IT support. Workstations need to be replaced every two to three years to take advantage of the latest processor speeds, if they last that long.

Using Dell's solution means each analyst is not dependent on their workstation. The Dell datacentre is where all the work is done making IT management much simpler for the units. Computing resources can be shared across multiple users and not just the analyst with the latest PC. Additionally, any malware or viruses on a suspect device can be contained in a virtual environment which helps ensure the integrity of any evidence as well as the unit's network.

But it is the speed with which investigations can now progress that makes Dell's solution so appealing. Any delay creates risks and, especially in high-profile investigations such as terrorism, the ability to drastically reduce the time it takes to examine huge amounts of data saves that most valuable of commodity – time.

Major Miller explained how the ingestion of terabytes of data can only be done by using something more powerful than an individual workstation.



"In one case, the RMP had to ingest and process eight million files. On a standalone system this traditionally would take eight to nine days whereas on the Forensic solution it was processed in a day and a half. The ingestion phase for IHAT (80Tb of data) took 14 weeks using three persons 24/7 including administration (8,176 hrs); this would have taken upwards of a year, if possible at all, on traditional methods".

"With limited resources, our 15 members of staff will remain and not grow. You have to break away from having an individual analyst with a big tower and screen. The only

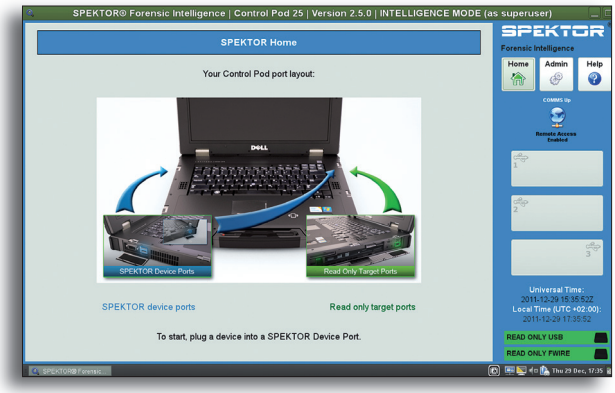
way to be able to do that within national guidelines and be able to stand up in court and say you have looked at 100 per cent of the evidence is to utilise technology. Solutions that ingest large amounts of information, tag it in terms of chain of evidence and then pass it round and distribute that piece of work among a number of people speeds up the process no end."

Major Miller has seen benefits from an HR perspective as well. The previous system saw one individual categorising 850,000 images from one suspect. In future, any case such as this can be distributed around the team safeguarding individuals; by using technology it is possible to share the burden.

Mr Slater said using Blade Servers on its Forensics LAN has revolutionised how the HTCU operates.

"Historically, every two to three years each workstation was replaced. That means one person had the latest processor and the fastest case processing and everyone else hadn't. From a management perspective, that means I can now invest in additional Blades every year as opposed to additional workstations. That means everybody is benefiting from that additional processing power.

"If we have a power cut in the lab, something goes wrong



SPEKTOR Forensic Intelligence – has been adopted as the triage and imaging front-end to feed into the Dell Forensics solution.

with one of the workstations, where the work being done takes hours if not days to complete, that processing isn't lost, it continues to run on the servers housed in a secure server room, UPS protected and environmentally controlled. That means nothing is lost and we don't have to reinvest the ten hours to redo the work again."

This access to high-speed processing also allowed the force to install a secure CESG manual V standard, 256-bit encrypted tunnel across its network, allowing the far geographical reaches of this vast force area to access files remotely.

In cases involving tens or hundreds of thousands of images, police officers around the force help out. A utility called C4P which runs on Guidance Software's enCase investigation suite, which is also supported by Dell's Digital Forensics solution, controls and records exactly what the officer is doing. It then stores the image in a hash database, if it is seen again the system will identify it as already categorised.

"Officers can do a viewing from wherever they are without having to drive three or four hours and then three or four hours back again," said Mr Slater.

Historically, investigation teams had to be co-located, even in the same room. This solution allows organisations to have a virtual team who do not necessarily need to be even in the same country.

Using triage to reduce demand

The number of devices being seized is a challenge for all HTCUs. If only those devices that require forensic analysis were submitted to the units the workload would be significantly reduced.

Devon and Cornwall became the second force in the country to use digital forensic triage, where 38 frontline officers are now trained in scanning devices to make a decision on which ones need to be analysed.

Mr Slater says triage has been a powerful tool in reducing the number of exhibits per case.

"Triage allows us to identify which are the primary exhibits we need to examine and allows us to focus our available resources where they are needed."

Every job passes through triage and over 100 were removed from the queue in 2011 because they did not contain any evidence.

The HTCU controls the software used in the Dell Forensics triage system, such as Evidence Talks' SPEKTOR® Forensic Intelligence, auditing and authoring capture packs for officers to deploy.

The result of triage is not evidence but intelligence to inform investigators' decisions as to whether exhibits should be examined more closely.

The SPCB has also been using triage since November 2011 and 58 analyses have been conducted at forward police stations using Aceso Mobile units from Radio Tactics Ltd for forensic analysis of mobile phones.

Andrew Sheldon, from Evidence Talks, explained that the Dell Forensics solution is a collaborative approach. Evidence Talks' SPEKTOR triage tool enables the examination of all computers, laptops, USB sticks, removable storage and, using a derivative of Athena from Radio Tactics, thousands of different mobile phones.

"Being able to examine items on site or at border controls is particularly helpful when witnesses do not want to give up their computers or mobile phones because it could take upwards of nine months to go through a high-tech crime team," said Mr Sheldon. "They are prepared to do an at source analysis that takes 20 minutes.

"Triage is not a replacement for forensic analysis; triage is a method of allowing people with limited skills to make

Dell's Digital Forensics solution detail

Dell's Digital Forensics solution combines high-performance EqualLogic or Compellent storage, fibre optic cabling attached to servers running AccessData Lab (AD Lab), providing immediate performance benefit to enable parallel processing which dramatically improves the productivity opportunity.

AD Lab enables investigators to share images to scale up an analysis from individuals to teams of tens or even hundreds of people at the same time.The software is multi-threaded to take advantage of multiple cores on the servers. Parallel processing can then reduce the time to index cases from weeks to days.

Once analysed the data can be archived rather than be kept in live storage, which is far more cost-efficient. If data needs to be retrieved at any future point, perhaps for a trial or appeal, it is easily available instead of having to send someone across town to look for an evidence bag. There are significant benefits in terms of how data is handled serving to maintain its long-term integrity; disaster recovery and back-up procedures also preserve the digital chain of evidence.

Major Keith Miller – a 'golf bag' approach using the right tool at the right time will assist in providing solutions that are flexible and reactive to the ever-changing landscape of forensics.

Andrew Sheldon – Triage in isolation is good, but triage as part of a homogenous system is even better.

The power to do more

Case study – Devon and Cornwall

In 2003, Devon and Cornwall Constabulary's HTCU examined 4,500GB (4.5 terrabytes [TB] the equivalent of about 100 DVD movies or over one million digital photographs copied to disc) of data in 93 cases (48GB per case). In 2011, it had increased to 154,716GB (or 154TB) in 370 cases (447GB per case).

The 2011 figures show only the work within the HTCU. Triage has removed hundreds of exhibits and thousands of GB of data before the HTCU examines cases. These figures would have been nearly doubled if we did not use triage.

Head of unit Steve Slater said: "The unit continues to experience an average of 30 per cent increase in submissions to the unit each year while not receiving any increase in staff, relying on smarter ways of working to keep up with the demand."

Its eight members of staff examined the following in 2011 (does not include items triaged or mobile phones examined outside of HTCU):

370 suspects
560 computers
724 hard drives
339 mobile phones
192 USB devices
154,716GB of data

Case study – SPCB

The Service Police Crime Bureau (SPCB) has seen an average increase of 120.82 per cent per year in data to be examined in the past ten years. In 2010, the unit received 73,742GB to be examined at an average 1,500GB per case.

One basic indecent images case cost 290 hours at £9,500 when dealt with by an analyst with a standard tower. Run through Dell's Digital Forensics solution, the cost reduced to £3,200, using just over 100 hours.

Major Keith Miller firmly believes that the use of a variety of technologies, in concert, and at the right time (the 'golf bag approach') will assist in providing solutions that are flexible and reactive to the ever-changing landscape of forensics – Dell's solution is one of these.

informed decisions about the next steps they take on site.

"Whilst triage capabilities are improving all the time, it is the forensic experts who can take the decision as to how the evidence came into being, or whether it is indeed evidence. Just like in the medical environment, triage is a way of routing and filtering out the unnecessary. It is not a replacement for forensic analysis by any means. It is less about the technology and more about the process of delivery of triage in the hands of non-experts. You have to ensure that what is done in triage mode is acceptable and poses minimum risk to your evidence.

"SPEKTOR was designed by using the processes used in Evidence Talk's forensic laboratory so when it is deployed there is full traceability of their actions and full audit trail and contemporaneous logging of what's performed. And it is done to the same standards as a good forensic laboratory.

"SPEKTOR as part of the Dell solution has been built as an end-to-end process where you have continuity from the point at which the box is opened to the point at which the potential evidence is ingested into the Dell back-end solution where the AccessData FTK (Forensic ToolKit) software can analyse it."

Triage technology must support frontline officers who are being asked to use it and limit any potential for mistakes to the minimum. It has to reduce the risk of damage to the evidence to nil and it has to be supportive as a forensic process.

SPEKTOR also benefits from remote access allowing forensic experts in the lab to reach out to the frontline and immediately view the evidence on devices. It also allows an operator, without forensic skills, to make a decision on whether a device may contain evidence and, if required, they can use it to take an evidential image; the system guides them through the process.

"Triage in isolation is good, but triage as part of a homogenous system is even better," added Mr Sheridon.

RAM

One of the biggest challenges to digital forensics is the handling of volatile data and encryption used on computers. The content of random access memory (RAM) which is only accessible while a device is powered on is particularly critical and can reveal a considerable amount of data or intelligence including passwords, remote internet or IP addresses accessed among others.

Adrian Culley, Global Engineer of Dell Forensic's partner AccessData Group, believes it is not possible to overstate how important it is to capture the contents of the RAM on an individual machine.

Adrian Culley – it is not possible to overstate how important it is to capture the contents of the RAM on an individual machine.

Twenty years ago, advice to law enforcement officers was to pull the plug on a computer and bring it in for examination if they didn't know what to do with it. That is now the last thing they should be doing.

RAM is fundamental to evidence. As part of the Dell mobile solution, the user can plug a SPEKTOR collector into a running computer and perform a full memory dump as part of the triage process.

"The important thing is the process is recorded and managed. Plugging a device into a Windows computer will make some changes and we have gone to the nth degree to make sure that is recorded and logged so when it is analysed by forensic experts, they can identify those changes," said Mr Culley.

"If a device or computer is switched on and you don't have triage available, don't touch it, get someone who knows what they are doing to deal with it. The best chance to deal with encryption and the only chance to capture the contents of RAM, is keeping power in that machine."

Implementation

As the SPCB continues to set up its latest Forensics LAN, it believes that the use of this type of technology will continue to pay huge dividends down the line in reduction of delay and better use of resources.

Major Miller said that the SPCB uses a raft of innovative technologies across its capability areas. As with SPCB's other relationships, Dell has ensured a collaborative and consultative approach throughout, with much of the testing taking place in Dell's test labs before installation.

He is confident in a successful implementation having seen how it has worked on a smaller system used by the IHAT.

Mr Slater is also complimentary of the way issues have been resolved with Dell technicians quickly on site or in conference calls to discuss and resolve glitches.

The force was looking to deploy C4P, its counting and categorising software, on the Blade servers through a Citrix solution, and Dell tested the implementation on its test datacentre before a contract was even signed.

About Dell Forensics

For further information, please see **dell.com/forensics** or contact your account representative.