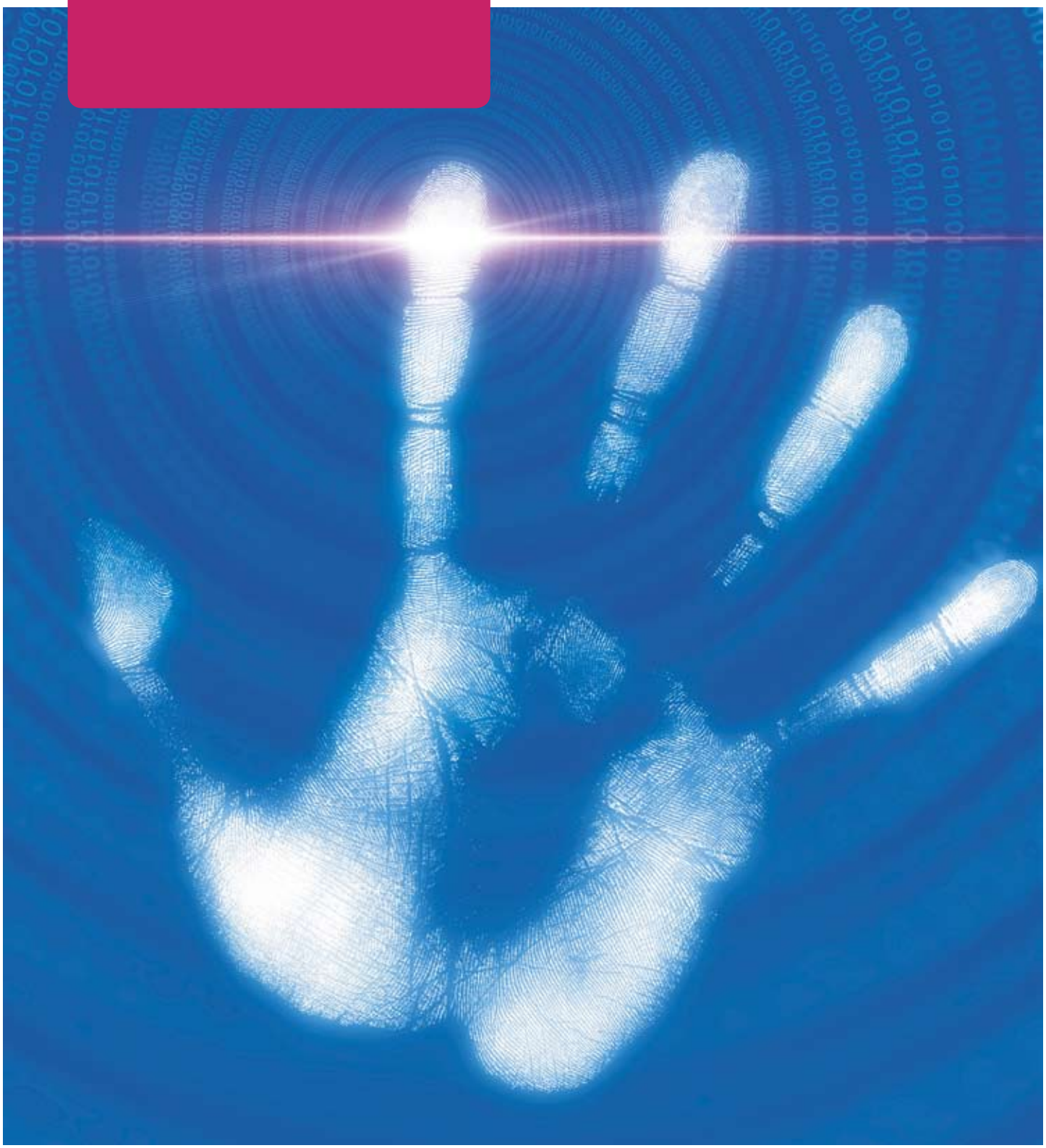
Dell digital forensics solution blueprint



The challenge:

In recent years there has been an exponential rise in terms of volume, velocity, variety and sophistication of digital activity by criminals and terrorist groups around the world. Today, most crimes have a digital component.

This growth has been exacerbated by dramatic advances in electronic hardware. The growing diversity of consumer electronic devices, all with increasing memory or storage capacity, offer criminals and terrorists a wealth of opportunity to hide harmful information.

It is not uncommon for desktops and laptops to come with hard drives that measure 100's of gigabytes of storage. The latest hard drives include options for 2 or 4 terabytes. Considering that just one terabyte can store 200 DVDs, that's a vast amount of storage and represents a problem that will only keep growing.

From PCs to laptops, mobile phones to thumb drives and even games consoles, police and security forces are being pushed to the limit to clone, ingest (or image), index and analyse growing amounts of suspect data while preserving the digital chain of custody and protect citizens.
When suspected criminals have been charged and PC assets seized, police and agencies are put under enormous pressure to process and analyse potential evidence in a very short space of time and in less than perfect IT environments.

And where whole organisations are suspected of criminal or terrorist activity the number of devices to be analysed, can escalate dramatically

Imaging data takes time

Hard drives first have to be copied or "cloned" so as not to "contaminate" the source of data. This is a major challenge for forces or agencies as, in order to preserve data copied from clones, it requires huge storage requirements.

It can take hours, or even days, to copy and process confiscated hard drives, together with the systems on which they are working. This has to be done with meticulous care and attention to detail.

In order to preserve the chain (or continuity) of custody there are a number of rigid guidelines. Documentation has to include conditions under which the evidence is gathered.

The identity of all evidence handlers must be revealed. The duration of evidence custody, security conditions while handling or storing the evidence, and the manner in which evidence was transferred to subsequent custodians must be stated... that takes time.

The current problems with ingestion and analysis

Once cloned, data is "ingested" by digital forensic experts onto one or several workstations, or high performance PCs. Again this can take a great deal of time depending on the amount of data being ingested before data can be indexed, triaged and analysed.

Due to the large volume of data to be analysed and the risk of losing data, experts have to be at the lab to carry out analysis. In addition local laws may prohibit remote searches of seized hard drives for analysis by high tech crime units.

It's no surprise therefore that there is a huge backlog of seized hard drive – 18-24 months[1] is typical. At best data can be shared across file servers but analysis still has to be done at the lab and requires state-of-the-art network capabilities to transfer data backwards and forwards between centrally held servers and the analysts' PCs. Very often this doesn't allow for data to be shared between analysts working in the same location, let alone at remote sites. Real time sharing across agencies or even borders, between multi-government agencies, is out of the question.

Consequently the only current solution for further analysis requires lab visits. Additionally, if malicious code is contained on the cloned image, this can cause damage to the forensic expert's workstation which could either require a rebuild starting the ingestion process over again, or if left undetected could potentially compromise the chain of custody.

Market Challenges

- Lack of expertise and resources together with exponential volume of suspect data has led to an 18 – 24 month[1] backlog.
- Ad hoc and unstructured IT approach focused on single or multiple PC infrastructure.
- Expensive forensic time focused on managing technology, data duplication and securing chain of custody.
- Offsite access to data is limited. Investigators have to be at the lab to avoid the risk of information leakage.
- Malicious code can corrupt analysts' workstations, which may require system rebuild and possible contamination of evidence.
- Approaches to backing up suspect data vary from force to force. Risks from device/media malfunction over time.

Solution Benefits

- Simplifies imaging, sharing and archiving data across experts and teams which can dramatically increase productivity.
- Standardises forensics IT infrastructure and establishes a clear process for secure electronic information exchange.
- Focuses forensic expertise on the analysis of suspect data by offering a single user interface to a suite of forensic applications.
- Offers either onsite or secure remote analysis and reviewing of suspect data and evidence.
- Ability to run malicious code in a "ring-fenced" environment, without affecting system integrity.
- Optional Back-Up Recovery and Archiving (BURA) and Disaster Recovery (DR) configurations establish a clear process to help secure chain of custody and information sharing and destruction.

Dell's digital forensics solution

Dell's approach to digital forensics takes what is effectively a serial process and applies the principles of cloud computing using data centre capabilities to enable simultaneous parallel processing of digital evidence.

Stage 1 (Triage)

Using a combination of Dell's fully rugged Latitude™ E6400 XFR laptop and Evidence Talks' Spektor triage software, digital forensics officers have the opportunity to quickly recover potential evidence from suspect devices for viewing on site. Not only can this save time, all data recovered is evidentially sound, either exported as an EO1 file for loading directly into the data centre or imaged as normal by uploading through via USB interface to central storage for processing back at the lab.

Stage 2 (Ingest)

In common with existing practices, suspect data is cloned but instead of imaging data onto a single workstation, data is ingested onto a central evidence repository rather than an individual analyst's PC.

By ingesting data immediately into the data centre, data transfer from one device to another is minimised, increasing availability of that data to multiple analysts dramatically improving productivity and efficiency.

Stage 3 (Store)

Storing suspect data directly to the data centre enables analysts to focus on analysis instead of being concerned whether there is sufficient hard disk space available on their PCs to store and index data. It also means that they are not slowed down having to backup other forensics work to recordable media such as DVDs.

Storing data centrally also enables data and workloads to be shared more efficiently and also minimises the amount of time needed to copy extremely large data sets from one device to another further increasing productivity. Even over the latest high speed networks this can take hours, inefficiently tying up both PC as well as network resources.

Stage 4 (Analyse)

By centrally storing suspect data it is possible to index and triage data within the data centre on high performance servers instead of using dedicated analyst PCs.

This way, multiple analyst sessions using software such as AccessData FTK and Guidance EnCase can be run concurrently on single or multiple workstations resulting in greatly increased productivity. And of course, analyst time can be devoted to analysing data rather than administering it.

Each application instance is run in an independent server session that helps protect the rest of the system from malicious code and viruses assisting to preserve system integrity. Where malicious code or applications are required to be run for understanding and evidential purposes, analysts can execute them in secure, isolated, "sand-pitted" environments.

Previously, if malicious code had been mistakenly executed, it could compromise the integrity of suspected evidence, chain of custody and the time already spent on analysis. Consequently, this would probably have required a rebuild of the analyst's workstation and starting the imaging and analysis process all over again.

Stage 5 (Present)

Once the data has been processed and potential areas of interest identified, viewing teams involving anything up to 200 police officers (depending on the size of the forensics infrastructure) can be granted real time secure access to potential case evidence. Additionally, the formalised nature of this infrastructure allows for easier secure remote access to qualified experts – reviewing teams do not have to be on site to support larger incidents and there is no need to risk posting out evidence on CDs.

Dell's digital forensics lifecycle

1. **Triage**
   Using Dell's fully rugged Latitude™ E6400 XFR laptop together with Evidence Talks' Spektor triage software, forensics analysts can quickly view more accessible evidence from suspect devices at the scene of crime.

2. **Ingest**
   Once cloned, suspect data is ingested directly onto a central evidence repository instead of onto a workstation. The solution allows for multiple devices to be ingested simultaneoulsy.

3. **Store**
   Copying data direct to high speed Dell™ EqualLogic™ and Compellent storage helps enable seamless data exchange between servers and storage improving productivity.

Fig 1. Breaking down the Digital Forensics process into 5 separate stages.

4. **Analyse**
   Multiple analyst sessions can be run concurrently on single or multiple Dell OptiPlex™ PCs resulting in further increased productivity.

5. **Present**
   The solution allows for scalable numbers of on-site or remote viewing teams to be securely granted access to the case data – 24/7/365.

6. **Archive & Search**
   Industry standard BURA options help to preserve the digital chain of custody and securely exchange data and cooperate in a crisis.

Stage 6 (Archive & Search)

The Dell "Blueprint" for modular digital forensic solutions can help provide a modular and scalable environment that can be expanded and upgraded to keep up with the growing demand for processing and exponential storage requirements.

Integrating a formalised Backup Recovery and Archiving (BURA) infrastructure helps to optimise cooperation between agencies and forces and even across borders. Additionally industry standards based BURA facilities help free up analyst administrative burdens, provide consistency between labs especially in times of crisis, and helps minimise the risks to the digital chain of custody where currently suspect evidence is backed up on recordable DVDs and "home type" backup devices. This makes it much easier to move information securely between high tech crime labs.

Additionally, Dell's Digital Forensic Blueprint includes an optional search component that allows for information correlation between ingested data sets. This allows the analyst to be able to quickly perform internet like search capabilities on the entire case data store including both active online content as well as archived material from previous cases.

Analyse data quicker, help secure more convictions

Fig 2. A screen shot of Dell's digital forensics solution showing dual screen enabled workstation running multiple instances of both AccessData FTK (versions 1.8 and 2.2) and guidance encase simultaneously.

Dell's digital forensics solution

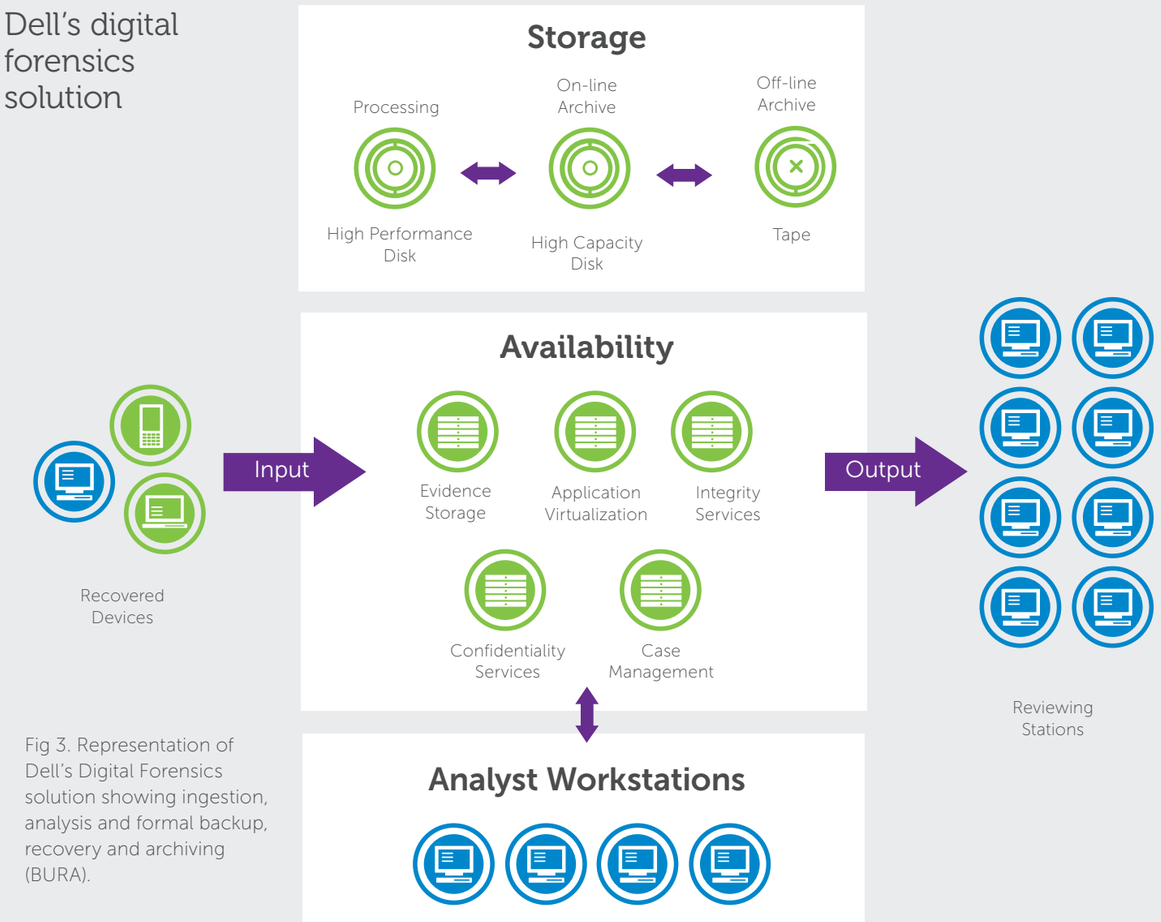


Fig 3. Representation of Dell's Digital Forensics solution showing ingestion, analysis and formal backup, recovery and archiving (BURA).

Summary

The forensics framework is a highly available suite of server, storage and software services that is designed to process and store digital forensic data whilst protecting the security and integrity of that data throughout its life cycle. Solution elements outlined in Fig 3 include:

- Evidence storage – A common modular storage platform that is comprised of a mixture of both high-performance and high-capacity storage devices.
  This allows for data to be processed quickly and seamlessly transferred onto less expensive storage mediums for near-term (Online) and long-term (Offline) retention.
- Application Services – All core forensics applications are run in the data centre allowing for reduced network activity / latency and enhanced performance. This allows the forensic analyst to run multiple instantiations of applications from a single workstation without any degradation in performance.
- Integrity Services – A suite of customised COTS software products that protect the applications and data contained within the system from rogue or malicious code; however, still allowing an examiner to execute suspicious code/ applications in a secure sandpit area.
- Confidentiality Services – A security perimeter helping to eliminate unauthorised data leakage. (This can be configured to UK Government standards).
- Case Management – Optional integration with existing agency or force case handling software.
- Additional Services – Dell can add additional services to the solution framework, such as translation (both text, audio and video) and enterprise search.

About Dell

Dell was founded in 1984 by Michael Dell based on a simple concept: by selling computer systems directly to customers, we could best understand their needs and efficiently provide the most effective computing solutions to meet those needs. Our evolving business strategy combines our revolutionary direct customer model with new distribution channels to reach governmental, commercial customers and individuals around the world.

Dell is working together with police forces, security agencies, Systems Integrators (SIs) and specialist solution providers to simplify the complexities involved with current handling and processing of suspect data and information.

Dell designs, manufactures and customises products and services from in-vehicle mobile solutions to scalable enterprise-class digital forensics solutions. We can provide police and security agencies secure, remote and real time access to essential information and collaborative working.

For better decisions, more timely actions and improved agility, Dell's products include:

- Latitude™ laptops for mobile and flexible working including in vehicle solutions for real time communications.
- Dell™ Precision™ workstations and PowerEdge™ servers for compute intensive applications like Digital Forensics, simulation and modelling energy efficient data centres and command and control infrastructure.
- Dell EqualLogic™, Compellent and PowerVault™ storage solutions that provide scalable, protected and interoperable access as well as Backup, Recovery and Archiving (BURA) solutions for sensitive information and intelligence.
- Dell Global Services can deliver a set of practical and executable plans for simplifying IT that include Infrastructure Consulting Services, Deployment Services, Managed Services and Dell ProSupport.

1. Police want new remote hard drive search powers The Register Posted on 29th April 2009 www.theregister.co.uk/2009/04/29/remote_hard_drive_forensics

Dell Corporation Limited, Reg. No. 02081369, Dell House, The Boulevard, Cain Road, Bracknell, Berkshire RG12 1LF.