

Unlock the *power* of digital forensics

The future of Digital Forensics is fast, powerful,
scalable and secure



Accelerate investigation times with rapid digital forensics analysis

Transform digital evidence analytics with a powerful, scalable and secure data platform.

The growth of digital technology and the rise of cybercrime, has created new and complex challenges for police forces in investigating and prosecuting criminal activity.

Digital evidence has become a critical component of many criminal investigations, from terrorism and organised crime to cyberbullying and online harassment.

As the volume and complexity of digital evidence continues to grow, a new approach to digital forensics platforms and data is vital to deliver the required performance to:

- accelerate the investigative process
- improve the victim experience
- increase public safety.

In collaboration with police forces we've developed a technology blueprint that addresses the challenges Digital Forensics Units (DFUs) face today, that can easily scale and adapt to meet the growth of demand in the future.



“The sheer scale of the information held on mobile devices today presents one of the greatest challenges to law enforcement’s ability to secure and preserve evidence.”

HMICFRS Report

An inspection into how well the police and other agencies use digital forensics in their investigations.

The Future of Digital Forensics is:

Fast | Powerful | Scalable | Secure | Controllable

...with predictable costs



Solving the unique challenges facing Digital Forensics Units

High performance for forensics data ingestion

In any investigation time is of the essence. Digital forensics architectures need to be built with speed in mind and ensure that police forces have high performance where they need it, for ingesting and processing forensics data in real time.

Scale-out file storage platforms are tuned to optimise performance and capacity with a choice of all-NVMe or hybrid SSD and HDD systems. This combination ensures data exists on the right tier at the right time, always.

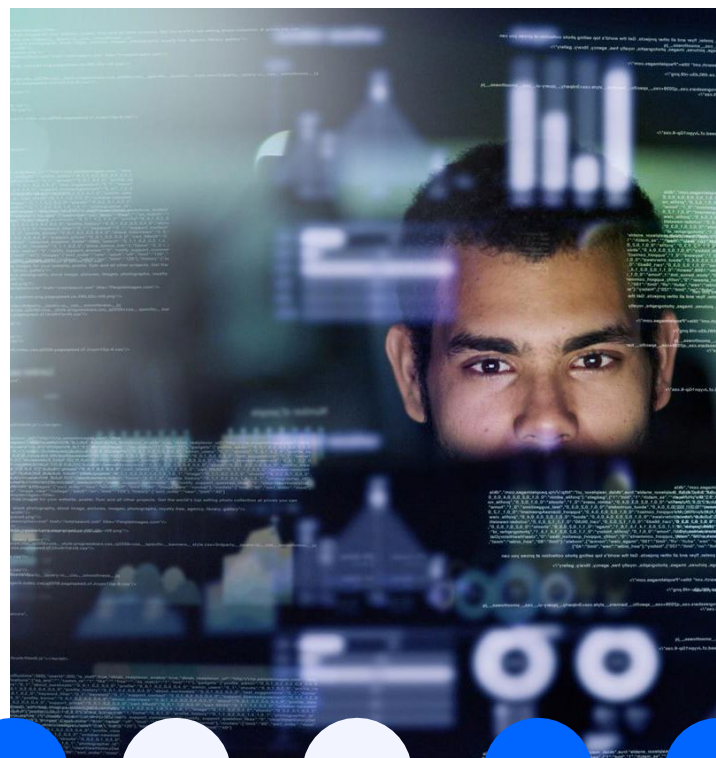
In addition to optimising the performance of file data, the solution needs to address the Digital Forensics Unit's unique requirements around security for sensitive data, compliance requirements, and a mandate to move to the cloud.

Real time analytics for visibility and control

New types of cybercrime, fraud and digitally enabled sexual exploitation illustrate a fundamental change in the profile of demand placed on the police service. It's critical that information and evidence is gathered quickly and accurately from multiple data sources.

Data management goes much wider than a single storage platform or piece of software. It is impacted by people, processes, tools, governance and more.

Digital forensics architectures of the future must have a solid foundation. One that's built on intelligent hardware platforms and includes holistic management and data analytics. Once in place, the Digital Asset Management (DAM) and forensics insights platforms and databases can really get to work in achieving the level of results the public demands.





Massive scalability

The scale of information that can be recovered from the examination of digital devices can be huge, with some mobile phones now able to store 130,000 digital images and other data.

HMICFRS Report

An inspection into how well the police and other agencies use digital forensics in their investigations.

Data has exploded and is growing exponentially with the current increase in demand for digital forensics unlikely to stop. For Digital Forensics Units it's crucial to have the ability to store more data than ever before, and to be able to scale the storage platform simply and cost-effectively.

Scalable file storage is able to effectively meet the demands of digital forensics. It provides the right-level of performance and it's inherently designed to scale predictably and almost without limit.

Scale across on-premises and Public Clouds

At some point the physical limits of a data centre or computer room will impact on capacity. In this instance, native integration with Public Cloud services such as Amazon AWS S3 and Microsoft Azure Blob storage can alleviate the pressure.

Using the in-built analytics of scale-out file storage platforms and holistic data analytics, Digital Forensics teams can move data to Public Cloud cold storage tiers that is no longer required in an investigation. Safe in the knowledge that it won't need to be accessed for a long period of time, if ever again.

Utilising Public Cloud services for storing all Digital Forensics data can be risky, unpredictable from a cost perspective and impact the speed of investigations. A blend of on-premises, managed and Public Cloud services in the right combination provide the best results.

"Storing the evidence from digital forensic examinations is a big problem for the police service and it is getting worse. The old ways of storing evidence don't work in this digital age. Policing must move to a cloud-based system of storing digital evidence if it is to become more efficient and effective."

HMICFRS Report

An inspection into how well the police and other agencies use digital forensics in their investigations.

Data governance and security

Data security and governance has never been higher up on the agenda. By its very nature, Digital Forensics data is some of, if not the, most sensitive data in existence and therefore how it is secured and governed needs the utmost focus.

Digital Forensics storage platforms provide encryption for data in flight and at-rest. Integrated data protection is also included via snapshot replication for simple, cost-effective data protection.



Predictable cloud-like consumption

The way in which IT infrastructure and services is purchased and consumed has changed forever. Large CAPEX investments are dwindling in favour of pay-as-go consumption-based procurement models, whether that be month-by-month or over a period of multiple years.

The huge increase in data storage growth and the variety and complexity of the data stored by Digital Forensics Units means that the traditional approach of purchasing platforms is no longer viable. Police Forces would often have to purchase 5X – 10X more capacity than is required on day one.

Pay-as-you-go models enable spend to be aligned to what is needed today and offers the ability to grow in smaller increments as required. Plus pay as you grow over time, can help free up finances for parallel initiatives and projects.



Built-in buffer capacity eliminates the risk of over provisioning by ensuring you'll be able to handle any unexpected demand.



Our Digital Forensics Blueprint delivers:

-  More speed
-  More security
-  More control
-  Improved service



Secure End User Computing



High performance and scalable file data platforms with data analytics



Robust data protection



Right-sized private cloud infrastructure



Best in class networking and connectivity

Key Features

Forensics tuned performance

Optimised for forensics data ingestion and processing performance via a choice of all NVMe or hybrid SSD/HDD platforms

Scale beyond traditional limits

Predictable and almost limitless scale on-premises

Visibility and control

Simple and easy to use data storage platforms and file data analytics

Integrated with public cloud

Utilise Public Cloud for cold tiers of data and REST APIs so users can build and manage a modern digital forensics application stack

Pay per use consumption model

Pay per use consumption models for on-premises infrastructure means you only pay for what you need today. No need to over-provision –and you can scale in smaller increments, which helps to free up funds for other initiatives.

Why Telefónica Tech

A flexible, trusted partner

From our heritage and expertise to our strong leadership team, from partnerships and accreditations to passionate customer focus, there are many reasons we're the right partner. At the heart of it are our people. People who have a huge variety of specialist skills, allowing you to take advantage of our flexible resourcing service as and when you need them. People who are security-vetted and cleared, from technical specialists to delivery teams. People who bring business analysis, project management and support to help you manage dynamic IT demands. Most importantly, they're people who listen and understand the complex needs of police forces. People you can rely on. With Telefónica Tech, it's a partnership of trust.

Contact our Police Sector Specialist for more information:

Ed Taylor

T: 0845 605 2100

M: 07788 293587

E: Ed.Taylor@telefonicatech.uk

About Telefónica Tech

Telefónica Tech is the leading company in digital transformation. The company offers a wide range of services and integrated technological solutions in Cyber Security, Cloud, IoT, Big Data and Blockchain.

With our worldwide presence and strategic hubs in Spain, Brazil, the UK, Germany, and Hispam, our capabilities reach more than 5.5 million B2B customers in 175 countries every day.

We unlock the power of integrated technology for all businesses, bringing together a unique combination of the best people, with the best tech and the best platforms, supported by a dynamic partner ecosystem and strategic agreements with all market leaders. We do this in a simplified manner, to facilitate and accelerate tech adoption and make a real difference every day, to every business.

Telefónica Tech
We're here to **help**.

Visit telefonicatech.uk for more information.



[@TefTech_EN](https://twitter.com/TefTech_EN)



[in Telefónica Tech](https://www.linkedin.com/company/telefonicatech)



[Telefónica Tech](https://www.youtube.com/TelefonicaTech)

About Telefónica Tech

Telefónica Tech UK&I is a key holding of the Telefónica Group. The company offers a wide range of integrated technology services, reaching more than 5.5 million customers in 175 countries every day.