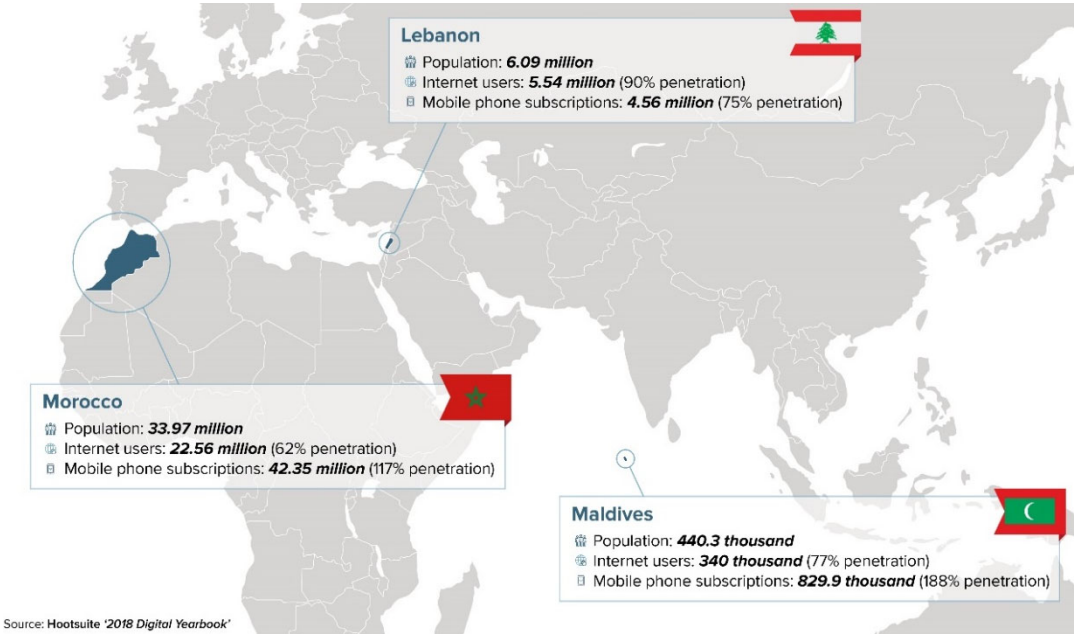
Criminal networks, including terrorists continue to rely on the ability to communicate to achieve their objectives. They are becoming more adept at leveraging technology to mask their activities, avoid detection, making it increasingly difficult for security agencies to counter their illicit activities. The 'Cloud' has fundamentally changed how terrorist material is stored, shared and used operationally, allowing for an almost limitless amount of data to be accessed anywhere and without physical storage on devices. At the same time, the rise of mobile, social media and cloud-based information solutions also gives law enforcement agencies, if properly equipped and trained, the ability to collect, handle, exploit and analyse a wealth of data, identify illegal activities, study networks and linkages and present technical information as compelling probative evidence contributing to fair criminal convictions. In the three focus territories of Lebanon, Morocco and Maldives, internet and mobile data penetration and usage is very high, with an average percentage of internet users of around 76% and average mobile phone subscriptions at 126% (Graphic 1). This presents major opportunities for intelligence and law enforcement to use digital forensics techniques to drive and support investigations, providing high quality evidence which secures fair and transparent CT justice outcomes.



Graphic 1. Mobile and internet usage in target countries

This opportunity, however, also brings with it significant challenges. Exploitation of digital evidence can generate an enormous amount of technical data that is meaningless without timely processing and proper analysis. It is also critically important that Senior Investigating Officers (SIOs) are able to use digital evidence that has been seized, handled, processed, analysed to maintain evidential integrity in the context of complex investigations, alongside other forms of evidence within a wider effective investigative strategy, and in alignment with relevant legal frameworks. ***In other words, technical capacity alone (systems, training) does not automatically translate into investigations capability: solid working practices, codified in policy and integrated into wider forensic and investigative strategy, and compliant with the legislative frameworks of that jurisdiction, is required to generate meaningful CT justice outcomes.***

Our locally-owned approach and strong pre-existing networks support delivery by a team which blends leading technical capability with experienced investigative practitioners, underpinned by agile and responsive project management.

Based on our thorough understanding of CT and wider security governance challenges in the focus regions, we understand that to successfully build practical digital evidence capacity which improves investigation and prosecution of CT cases, HMG requires an Implementing Partner that possesses; the credibility to work quickly to establish trust of end users within tight project timescales; an in-depth knowledge of the target operating environments and pre-existing relations of trust with their security agencies; CT-specific technical expertise that covers all aspects of digital evidence and its application in the criminal justice system; a proven track record of successfully managing simultaneous, complex CSSF programmes to meet and exceed HMG expectations.

Torchlight brings a unique combination of competencies to measurably improve CT justice outcomes in this important project:

1. ***Localised.*** Our participatory approach, making the end users part of the solution and securing full local leadership of implementation, maximises the prospect of embedding a sustainable capability in beneficiaries' long-term business models.
2. ***Connected.*** We will leverage our established relationships with end users, built through sustained and quality engagement in Lebanon and Morocco, to 'hit the ground running' without a requirement for lengthy relationship building, and adopt a highly informed approach to navigating the organisational sensitivities in all three territories.
3. ***Blended.*** Our team offers the highest quality technical expertise in digital forensics and evidence, alongside experienced criminal justice experts who know how to apply digital capability in the practice of complex CT investigations/prosecutions. This team is configured to drive not only outputs (capacity) but outcomes (use in investigations and submission in court).
4. ***Agile.*** Our project management approach is agile, enabling us to remain flexible whilst delivering in complex environments, and fully equipped to manage every component of three concurrent projects with zero draw on HMG resources.

By leveraging these competencies, Torchlight will deliver scoping, design, implementation and exit phases which meet and can exceed the Authority's expectations, while deepening stakeholder ownership and participation in any future phases of UK support to digital or other CT security and justice outcomes in the three territories. We will also use our engagement to support the Authority's political access and influence in these jurisdictions.

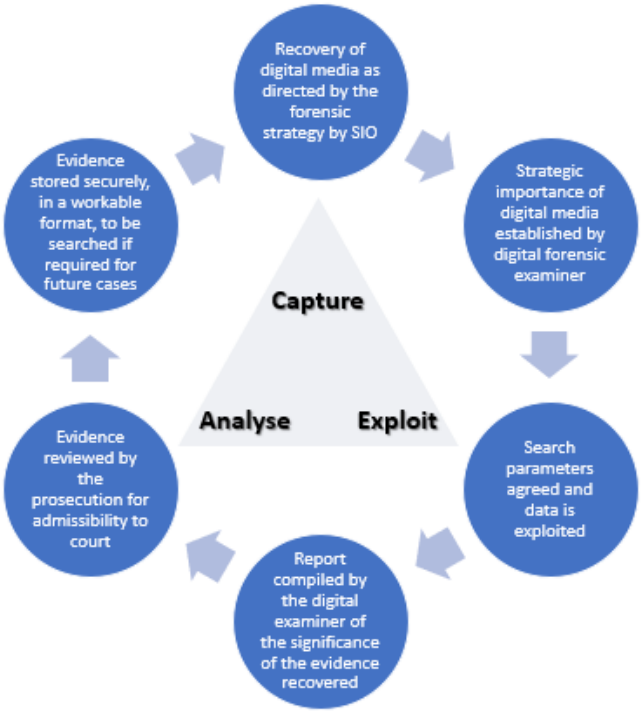
INCEPTION PHASE

OUTPUT 1: A proven scoping process optimising solution development and fostering local ownership for successful implementation

In order to align to tight project timelines whilst delivering to Torchlight's quality standards, we will deploy two Scoping Teams concurrently, with regular lessons sharing between each team throughout the inception and subsequent phases. Digital Evidence Expert Matt Blackband will lead the team covering Lebanon and Morocco, while Digital Evidence Expert Graeme Burridge will lead the team covering the Maldives. Matt and Graeme will maintain these lead roles through the Delivery Phase, providing continuity and maintaining momentum and stakeholder networks from start to finish; while sharing lessons and leveraging any potential synergies and economies (e.g. shared suppliers to maximise VFM) across the project territories. Given the tight timeframe, and mindful of the sensitivities of CT organisations and the possibility of reluctance to allow full access, rapidly developing relationships of trust is key. Our approach is (a) to deploy only the most credible international experts with the proven ability to establish immediate professional credibility; and (b) to adopt a proven *collaborative* rather than *probing* methodology, using the initial scoping as an opportunity to develop relationship with counterparts, identify and address their concerns, and promote inclusivity and trust. In addition to eliciting accurate and complete information, this lays the foundation of local ownership and engagement for success in the Delivery Phase.

Our scoping methodology, proven across numerous impactful missions for HMG and other donors, has **five key components**:

1. Preparation. In preparation for the scoping, we will conduct stakeholder mapping and establish a stakeholder engagement plan with the Authority. Working through the Authority Project Manager, this will enable us to identify "who's who" within the stakeholder organisations, determine incentives, recognise potential blockers and maximise the Authority's continued ownership of these relationships. A thorough review of the existing capability assessment reports produced by the in-country CTPLOs will also be conducted, enabling our Scoping Teams to develop strategies for each country, for sign-off by the Authority prior to deployment and to act as a handrail for baselining of end user capabilities.
2. Strategic Engagement. During the initial stage of in-country deployment the Scoping Teams will meet with Embassy stakeholders to finalise strategy, review the stakeholder engagement plans and finalise scoping timelines. In close coordination with Embassy relationship owners, we will engage with the senior leadership from the beneficiary organisations to ensure agreement on the objectives for the scoping mission, lay the foundations for delivery, and align all stakeholder expectations.
3. Baseline Workshop. The first stage of capability assessment is an interactive workshop with beneficiary digital examiners and CT investigators. We use the steps for examination of digital evidence (Graphic 2) as a refence guide for this workshop, for each step in the cycle unpacking current practices, analysing examples where possible, looking at strengths and assessing gaps in technical, human resource or procedural capability. This proven process generates insights into their capability (technical, human, procedural), provides a forum for discussing challenges implicit in the wider justice system, obstacles for the use of digital evidence, and interagency and cross-sector working; whilst maximising ownership and buy-in through broad participation in the beneficiary agency.



Graphic 2. Basic steps in the examination of digital evidence

Creating a Learning Environment to Conduct a Needs Analysis

During a scoping of the Punjab Forensic Science Agency's (PFSA) digital capabilities, our Digital Forensic Expert (Matt Blackband, a proposed expert on this project) opened with an engaging workshop based on case studies and mini-exercises so that he could baseline participants' abilities. This approach enabled us to understand the ground truth, determine the gaps and reinforcing the benefits to PFSA officers and leaders of engagement with the project, deepening participation and ownership.

4. Site Visits. Following the Baseline Workshop, the scoping will continue through a series of site visits that will be guided by the workshop findings. We recognise that beneficiary agencies may not grant full access, but site visits will include engagement in operational headquarters, field offices (e.g. police stations, intelligence stations).

Data capture during site engagement is through:

- Formal interviews and informal discussions with senior management and at the tactician level (practitioners)—this will allow us to understand the challenges and expectations at both levels as often they have differing views;

- Scenario-based questions which elicit responses that allow the end users to demonstrate processes—this will allow us to see, first-hand, the procedures that they utilise, the workflow process, their equipment, storage considerations, etc;
- Creating a learning environment—through use of mini exercises, we can observe how cases are handled, identify existing gaps, etc whilst also transferring knowledge and educating the end users;
- Providing opportunities to seek technical advice—this can be done through informal interactions with staff, asking them about recent cases that have challenged them and advising on different possible approaches they might wish to consider in the future.

This will enable us to examine specific aspects that include: Human Resources (skills, capacity, development); Technical Resources (equipment, tools; procurement); Policies and Procedures (SOPs, legislative frameworks); Leadership and Incentives (at tactical, operational and strategic levels). Combined with the initial workshop, we will provide a full baseline assessment of the following functions:

Security
Access control – who has access to the evidence; how is control maintained
Network security – IT security tools used
Cyber security awareness – measures to ensure safe cyber practices; cyber security training
Exhibit storage – how is evidence being stored; how long must evidence be stored
Interoperability
Interagency practices - interactions between CT investigators, digital unit and prosecutors; presentation of technical data to non-technical audiences (ie in court); use of expert witnesses
Forensic strategies – who develops the strategy to direct investigations
Joint activities – training, case reviews, MOUs
Processes
Submission process – evidence seizure and packaging; how is it handed over to the examiner; what information is provided; what requests are made for exploitation of the item
Workflow process practices – how is evidence received, handled, triaged, processed
Existing SOPs – effectiveness, processes for implementation, reflective of international best practice and ISO standards
Exhibit handling and storage – evidential practices being followed, evidence storage facilities, access
Local legislation *(this is of particular importance as it will not only vary in each jurisdiction but can also be obstructive in use of digital evidence)* - legal frameworks concerning capture, handling, exploitation and storage of digital evidence; data protection
Capacity
Audit of available hardware/software, IT infrastructure, periphery items – IT systems (capacity, processing, security); specialist digital forensic equipment (versions); IT network security; basic forensic consumables
Digital evidence capabilities – basic competency in use of equipment, use of advanced techniques such as 'Chip Off' forensics
Caseload and capacity of the units (ie number of dedicated staff)
Current processing timelines – turnaround times for routine evidence and fast-tracked submissions
Common evidence types – the format of the evidence being submitted

5. Verification Workshop. We will use the final day of the scoping to hold a workshop with the same participants from the Baseline Workshop where we will summarise our findings with the end users, refining and stress-testing the information, and seeking clarification on any gaps. In the Verification Workshop we begin work with counterparts to jointly develop a proposed solution, using the opportunity to develop an outline implementation plan (see below) for refinement in line with the selected technical solution. We will test the concepts within the plan with them. This initial plan will be refined and presented in a report (one for each country) to the Authority. *The ability to jointly develop the solution and test the plan will expedite the process for gaining acceptance of the implementation plan by the stakeholders, maximising results in the Delivery phase.*

OUTPUT 2: A rigorous, objective framework for assessing the equipment solutions against a fully worked-up scope

Torchlight is equipment agnostic— we will only recommend equipment options that fit the solution. All potential suppliers undergo rigorous due diligence checks to ensure that we mitigate any risks that may affect delivery of outputs and outcomes. We maintain strong relationships with a wide variety of forensic equipment suppliers so that we can select the right solution for the requirement, and these established relationships also allow us to negotiate discounts, which we will pass on to the Authority to achieve VfM. For example, our market relationships and buying power recently enabled us to include a 10% discount for the purchase of digital forensic software to the British Embassy Amman. We will give due consideration to end user technical capability levels, maintenance requirements and fiscal sustainment needs (e.g. ongoing costs for licences, maintenance, software updates, patches etc) to ensure the equipment will continue to be used in a self-sustaining manner independent of project support and be supported into the future.

In-region sourcing for VFM

In delivering over 30,000 items of specialist communications equipment for a CSSF partner country, we used a variety of suppliers to maximise the efficiencies offered to HMG, achieving an average saving of 25% on a contract worth over £15m. Wherever possible, we prioritise local and regional procurement (subject to strict quality standards) to leverage maximum VFM and support local economies.

This is particularly critical because digital device technology is continuously advancing, and criminal actors are quick to adopt new technology solutions—*law enforcement must therefore be equipped with a solution which can keep pace with these advances.*

For Output 2, we will follow the first stages of our proven procurement processes, linking supply market analysis directly to delivery. This involves: (a) Define scope – what functions the equipment needs to perform; at what scale, e.g. how many users; what level of expertise; interoperability with existing kit or that of other partners agencies; ease of transition from legacy equipment; within what cost; sustainability, e.g. level and extent of systems admin and maintenance needs etc; required timescale for implementation; licencing issues; (b) develop scoring matrix in line with scope; (c) whole-of-market review and scoring against matrix; (d) present scored recommendations, pros and cons, selected solution and justification.

OUTPUT 3: Robust plans, approved by host agencies to maximise local commitment to delivery and uptake

As set out above, an initial outline implementation plan will be developed with host agency stakeholders in the Verification Workshop, securing the strongest possible ownership for solution implementation. Following agreement by the Authority of the equipment solutions for each country, our experts will refine and finalise the implementation plans, which will include the following key components: development programme, risks and mitigations, responsibilities and reporting.