Science & Justice 62 (2022) 594–601

Contents lists available at ScienceDirect

Science & Justice

journal homepage: www.elsevier.com/locate/scijus

Professional Practice Report

The Hierarchy of Case Priority (HiCaP):- A proposed method for case prioritisation in digital forensic laboratories

Graeme Horsman

Cranfield University, College Rd, Cranfield, Wharley End, Bedford MK43 0AL, UK

ARTICLE INFO

Keywords:
Digital forensics
Case prioritisation
Case acceptance
Decision making
Risk

ABSTRACT

The need for digital forensic science (DFS) services has grown due to widespread and consistent engagement with technology by members of society. Whilst digital evidence often plays an important role in many inquiries, available investigative resources have failed to keep pace with such demand for them. As a result, the use case prioritisation models for backlog/workload management are of increasing importance to ensure the effective deployment of laboratory resources. This work focuses on the concept of case prioritisation in a digital forensic laboratory setting, following the submission of exhibits for examination, where this workflow is described. The challenges of case management and prioritisation in laboratories are discussed, with both 'case acceptance' and 'case prioritisation' procedures explained. Finally, the 'Hierarchy of Case Priority' (HiCaP) - a transparent, risk-based approach for the prioritisation of cases for examination, is proposed and described using examples.

1. Introduction

The requirement for digital forensic science (DFS) services has grown due to widespread and consistent engagement with technology by members of society. Subsequently, digital data is often of value to those conducting an investigation as they seek to ascertain both the physical conduct and digital behaviours of any parties subject to an inquiry [12]. The value that digital data can bring to an investigation is now recognised across many jurisdictions [3], where all parts of the investigative workflow have a role to play, starting from first responders attending incidents who may make decisions as to the relevant of digital devices [45], to the practitioners who conduct analysis of them. Such demand raises issues regarding the field's capacity to cope, and its ability to provide both an effective and efficient service to law enforcement and criminal justice systems [6]. This has subsequently led to a much-discussed concern that often digital forensic laboratories (DFLs) operate with case backlogs in place as noted by many academic works [7–11] and vendors of DF tools [12], resulting in slower case turnaround times whereas, in some instances, delays to justice of up to 12 months have been reported [1314]. This position will understandably cause apprehension for all parties involved in the investigatory process [1516] where these backlogs are the result of demand exceeding available resources [17–19]. This is a somewhat familiar problem in regards to the various forensic science fields [20], where Tulley [21] has already raised concern over sustained underfunding and its negative impact on forensic service delivery. Simply put, available resources in DFS have not kept pace with the demand for them through more cases seeking digital forensic examination [17].

Whilst calls may be made to increase the funding which is allocated to the DFS field in order to acquire and sustain a larger and suitably equipped workforce, it cannot be the only solution championed as a way of meeting the demand which is being placed upon it. Not least as a significant and sustained financial investment is not feasible in many cases, nor has it yet been witnessed in many locations. Despite increased resourcing offering greater options for long term capacity-building, it is the development of strategies for the effective management and deployment of current resources where arguably the greatest benefit to DFS's operation will be seen in the immediacy. As DFS moves forward, arguably it must critically evaluate how it is going to organise and deploy its current capabilities in a way that offers the maximum benefit to all parties involved in the investigatory process. This task is far from simple, where the focus of the discussion here will be on methods for backlog management and case prioritisation (CP), sometimes referred to as triage, in the DFL environment.

1.1. A focus on in-lab case prioritisation

As part of any criminal inquiry, an investigative team will want to have the results of any forensic examination of device or data which they submit to a DFL as soon as is practicably possible. Any outcomes are

E-mail address: graeme.horsman@cranfield.ac.uk.

https://doi.org/10.1016/j.scijus.2022.08.008
Received 22 November 2021; Received in revised form 26 August 2022; Accepted 31 August 2022
Available online 6 September 2022
1355-0306/© 2022 The Author(s). Published by Elsevier B.V. on behalf of The Chartered Society of Forensic Sciences. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

likely to inform their future investigative decision making, and, identify appropriate further lines of inquiry and the direction of any additional investigative conduct. If we consider that in many instances the desired and optimal time for examining any case which is submitted to a DFL is 'immediately' (excluding those with are subject to specific time delays/restrictions), then there is a high likelihood that at any given period, a DFL will be operating with a surplus number of cases in need of forensic examination (a backlog). Any devices awaiting examination that exist within this backlog may subsequently cause any wider investigatory processes as part of that case to be paused, subject to the acquisition of results DFS examination.

Whilst the size of any backlog may differ between DFLs, meaning in some situations the '*wait-time until results are provided*' may be less than in others (which an investigative team may still consider acceptable), in many instances, suboptimal case turn-around times are likely to be incurred. It is expected that such delays will never be eradicated from the DFS investigatory process, instead, placing emphasis on the need to manage in-lab case backlogs and case workloads to ensure that maximum resource efficiency is achieved in all instances. Whilst this does not ensure that all investigative teams will receive timely results regarding their case, it does mean that any available DFL resources are deployed in the most effective way possible at all times, ensuring that those cases that 'need' to be processed are done so promptly. The concept of 'need' is explored later in this work, where it includes ensuring the risk of wider harm being incurred in cases that are subject to an examination delay is reduced. As part of achieving this, DFLs require the use of formal CP measures and/or metrics to support lab throughput and backlog/workload management [22].

In the general sense, 'prioritisation' involves determining '*which of a group of things are the most important so that you can deal with them first*' [23]. When considered in the context of DFS, prioritisation may occur at multiple stages of the investigative process and in multiple contexts. To start, prioritisation may occur at the scene of an inquiry where decisions may be made regarding the investigative value of any device identified - often by a first responder [45]. Prioritisation at this point helps to ensure that only devices deemed relevant to an inquiry are submitted and subject to examination, where such processes arguably stem backlog growth by ensuring available resources are only utilised in cases and on devices where there is a real investigative need. Prioritisation may also occur post-seizure inside of a DFL, where this task may be approached in different ways. First, DFLs may deploy technical triage solutions which are designed to quickly determine the potential value of any device's content to an inquiry, in order to prioritise it for a more comprehensive examination [5,12,24]. This is a technically informed approach. Alternatively, a DFL may deploy a '*case-trait*' approach to evaluating a case's priority utilising surrounding case information and intelligence alone to determine which cases must have resources dedicated to them first [25–27]. In either of these approaches, decisions regarding which cases to address first must be made, but the focus here will remain on the latter approach.

This work focuses on the process of CP in a DFL following the submission of exhibits for examination, where this workflow is described. The concepts and challenges of case management and prioritisation in DFLs are discussed in section 2 and acknowledgement of existing approaches is made. In section 3, the processes of both '*case acceptance*' and '*case prioritisation*' procedures are explained and contextualised. Section 4 focuses on case acceptance and offers some suggested criteria for use when performing this task. In section 5, the 'Hierarchy of Case Priority' (HiCaP) - a transparent, risk-based approach for the prioritisation of cases for examination, is proposed and explained using case examples. Finally, conclusions are drawn.

2. Making prioritisation decisions

Any CP decision should not be made ad hoc in absence of sound reasoning, rather objective case criteria must be assessed and incorporated into any decision making process. Arguably, prioritisation must occur through an evaluation of relevant case factors and the impact that time delays may have upon them [2627]. Such 'criteria may include the nature of the crime, court dates, deadlines, potential victims, legal considerations, volatile nature of the evidence, and available resources.' [28]. Further, whilst any final CP decision may rest with individuals who have lab oversight and management responsibilities, input from those involved in the wider investigative team in relation to any case should be sought to inform this decision [25]. This task carries great responsibility given the extent of possible repercussions incurred from poor prioritisation decision making, making formal guidance for supporting this process important, yet little exists.

There are limited published commentaries and approaches for directing CP activities in a DFL, which offers little opportunity for those in the field to understand how prioritisation is both occurring on a wider scale and for them to evaluate and learn from existing practices. As a result, it is assumed that CP is a concept that is likely interpreted differently by different organisations and as a result, methods for achieving this task are likely to diverge across the DFS sector. The problem this causes lies with the fact that similar case circumstances may be prioritised and dealt with differently across different geographical locations and organisations. In such instances where diverging approaches exist, it is likely that some entities may be failing to fully identify and manage the risk attribute to the case as well as they could.

In seeking to develop appropriate CP approaches, DFS may consider looking towards other investigative disciplines and policing for support in this area, both domestically and internationally where examples include the Case Categorisation and Prioritisation Model [29]. Of the few approaches that are available and take a digital evidence focus, the National Institute of Justice [25] offer the following approach, based on '*case type*'.

'(1) Terrorism or any case where the loss of life is imminent
(2) Violent crimes such as murder, rape, and assault
(3) A child at immediate risk of exploitation or abuse
(4) Child pornography and solicitation
(5) Theft or destruction of intellectual property
(6) Public corruption
(7) Financial crimes
(8) Internet crimes, including network intrusion and unauthorized access
(9) Identity theft
(10)Fraud'

In addition, SWGDE [30] offers the following prioritisation approach.

1. 'An imminent credible threat of serious bodily injury or death to persons known or unknown, including examinations of evidence necessary to further the investigation of an at-large or unknown suspect who poses an imminent threat of serious bodily injury or death to persons known or unknown.
2. The potential threat of serious bodily injury or death to person(s).
3. Sexual crimes against children.
4. Imminent credible risk of loss of or destruction to property of significant value including identity and financial theft, as well as system intrusions.
5. Immediate impending court data, or non-extendable legal deadline.
6. The potential risk of loss or destruction to property or exam is needed to further an investigation.'

The model offered by the National Institute of Justice [25] seeks CP by case type, an approach which has much merit, but is an approach that is difficult to implement in a way that is exhaustive of all possible crime types. For example, there is limited indication as to how cases involving malicious communications may be prioritised. Clearly, cases of a specific type offer greater priority than others on face value, reflected by the

prioritisation of cases of suspected acts of terrorism, violent crimes and crimes involving children. However, it is suggested that additional factors may also increase the priority of a case, such as any suspects deprivation of liberty whilst an investigation is ongoing, or factors internal to any case type which may increase its severity. For example, fraud is considered a low priority case type, however, it is argued that the substantial value of assets involved in a suspected fraud may increase the need to conduct a timely investigation of any casework. Arguably, the point to raise here lies with the need to consider some of the potential risk and harm that exists within each case, and this approach appears to have been taken by SWGDE [30]. Here, SWGDE's CP approach appears driven by risk/harm, prioritising cases based on this factor. It is suggested such an approach may serve a better purpose of protecting society at large by ensuring high risk/harm cases are dealt with first. This six stage approach offers a foundation, but arguably omits some level of detail with regards to cases at the lower end of the severity level. For example, here the approach deals with prioritising particularly severe cases, however, there is limited guidance for prioritising cases which are closer to being considered volume crime.

Whilst both approaches offer a starting point for organisations to consider when developing a CP approach, arguably further elaboration and distinction may be required between prioritisation level types if the full spectrum of case circumstances are to be captured in the prioritisation process.

2.1. Case management and prioritisation

It is argued that effective CP improves backlogs [22]. Whilst approaches to CP often differ between organisations [17] where in Section 1 we considered technical and case-trait approaches, all DFLs prioritise the cases that are received into their laboratory to varying degrees. This may take place via a strictly defined and recognised prioritisation process (a defined strategic methodology for determining the importance of a case based upon information surrounding the case itself, for example, offence severity or the risk that the suspect poses to others) such as those proposed by the National Institute of Justice [25] and the Scientific Working Group on Digital Evidence (SWGDE) [30]. Alternatively, prioritisation may be informal and *ad hoc*, determined by approaches such as 'first come first served' or via a practitioner's subjective judgement where cases are available to choose from in regards to which they intend to examine next [17]. Whilst in both instances, case-level prioritisation occurs, for a DFL to effectively manage case throughput and backlogs, approaches to CP must be deployed consistently using objectively justifiable principles to underpin any decisions made. As a result, there is a need for DFLs to develop and deploy formal CP approaches rather than rely upon impromptu approaches. This sentiment is acknowledged by James [17] who notes that a failure to effectively prioritise case workloads can place undue stress upon both the workforce and organisation. Work by James [17] notes that when organisations lack an 'objective prioritisation model' this was shown to lead to subjective case prioritisation decisions being made which placed stress on the organisation through resource waste without necessarily meeting the needs of the case. In some cases, case prioritisation was shown to be influenced by organisational goals, the media, higher ranking officers [17].

Effective CP methods ensure the effective deployment of available DFL resources in line with the needs of any case and both its surrounding circumstances and requirements. This is important given the impact that case delays can have upon all parties that are involved in it. In turn, any examination delays may heighten the risk of harm being incurred by other involved parties or those in the wider society if those subject to an inquiry either intend to or proceed to carry out illegal conduct during the period that a device is waiting to be processed. Given the importance of CP, any prioritisation methods must be developed formally and subject to rigorous scrutiny as poorly defined and deployed prioritisation methods can be as detrimental as having no methods at all. Following a review of literature, it is suggested that any CP approach must possess the following traits:-.

1. *Be effective*:- Any prioritisation method/strategy must be effective, where effectiveness concerns the ability to appropriately determine the importance of any given case, and when it '*should*' be subject to examination in light of any existing resource demands [36] and subsequent risks posed by those involved. Effective prioritisation also must consider the challenges that limited funding places upon law enforcement agencies [40]. Effective prioritisation means that any case is subject to examination at the first available opportunity that is appropriate for the management of any risk factors attributable to it and any of the parties involved, given available resources [17]. Doing so ensures that taking into account a DFLs capacity, it has processed the case at a point where any attributable risk is at its lowest point, where any further delays merely seek to increase it or the risk of poor case outcomes. As
2. *Be consistent*:- Consistency is a requisite of all forensic processes so as to infer reliability from it [37] where CP is no different. CP is a complex task [40] but it must be conducted in a consistent manner, ensuring that any decisions that are made can, and will be replicated in future situations where the same or comparable circumstances are presented [38]. Consistently applied prioritisation increases both reliance and trust in the system whilst allowing for the effective planning and deployment of any future available investigatory resources as those involved in these decisions understand the circumstances which dictate them. Further, consistent prioritisation decisions allow members of the wider investigative team to plan any further inquiries around justifiable time estimates that are based upon case-examination times. Finally, consistent prioritisation helps to ensure that the public get a consistent level of service [46].
3. *Be transparent and justifiable*:- Transparent processes allow its users to determine its reliability and to evaluate it [39]. Any CP decision must be transparent and justifiable, allowing any investigating team who are submitting a case to a DFL to understand how and when their case will be subject to examination, and the underpinning reasoning for this. Where specific information/metrics/methodologies have been deployed as part of forming any CP decision, such content must be available and accessible to review and evaluation if/when required. The Police Foundation [40] note that being transparent in regards to the priorities being placed upon certain crime types increases the public's understanding of any decisions being made. All prioritisation decisions must have an objective evidence base from which they are based. This is stressed by the National Institute of Justice [25] who state that a 'priority level will be determined based on the facts known about each case when it is submitted to the digital forensic lab and will be updated as relevant information affecting the priority becomes available'.
4. *Be robust*: Case prioritisation decisions are difficult, where often there is more than one possible solution available [47] meaning that any CP methodology must be robust in-process, preventing its manipulation and use to artificially designate the priority of a case. Whilst information supplied by an investigative team will support their case's prioritisation, they must also be prevented from being the only determinative factor where an independent prioritisation decision is required. As a result, whilst an investigative team may not like the priority which is assigned to their case, they should not be able to change it unless there is objective evidence to warrant such a change.

On face value, the concept of CP may appear deceptively simple, where it is necessary to scrutinise how such decisions are made and by whom.

3. Case acceptance vs priorisation

Whilst up to this point, the narrative surrounding the management of case backlogs/workloads within a DFL has focused solely on the concept

of prioritisation, there is in fact a second element to this challenge; 'case acceptance' (CA). When a DFL seeks to manage the cases which it receives, it is important to make a distinction between the processes of CA and CP - these are two distinct challenges that must be addressed [31]. Before any case can be prioritised within the remit of a DFLs resourcing and management structure, it must be accepted by any DFL. This process is acknowledged by Parsonage [32] who notes that a DFL must first determine whether to accept a case through the use of defined criteria that can be used to manage the amount of work entering the lab.

Cases that are accepted by a DFL as done so on the grounds that the lab is capable of conducting the work which has been requested within currently known and accepted circumstances. Any CA process requires the use of criteria from which to base any final case decision, where Interpol [33] suggests this decision is the responsibility of the lab manager [33]. Effective CA processes prevent cases that cannot or should not be prioritised for examination from entering the DFL where such processes will result in a delay to the case being correctly handled and any amendments or further requirements made. In essence, CA acts as the first line of processing for a DFL to use when managing its backlog/workload.

Therefore in a DFL, the backlog management process should be considered a two-step procedure, any case which is brought to the DFL must first pass any CA criteria before it can then proceed to be prioritised in line with cases in the existing backlog (see Fig. 1). Both of these processes will now be considered in turn.

4. Case acceptance

As stated, all cases which are submitted to a laboratory should first be subject to CA criteria. The purpose of a CA is to determine a case's current 'state' in order to assess whether it can and should be handled by the DFL and proceed to its CP process. This requires first assessing the case and all its associated metadata and information to determine whether it is in a position to be examined. This includes as a minimum ensuring any required permissions for the examination are in place, all necessary information and paperwork is supplied and accurate, and relevant instructions are provided and confirmed contractually. Second, a DFL must make an assessment of its capacity and capability in line with the case's requirements. Whilst a case may be in a position to be processed, this does not mean that a DFL can or should process it, where the DFL must determine whether it can provide the service which is requested by the investigation team submitting the case, both technically and legally. CA should not be confused with the development of an investigative strategy where appropriate investigative methods and approaches are determined, it should be considered in parallel, where decisions made in regards to an investigative strategy will impact the outcome of the CA assessment.

Any CA decision must be formed following the use of objectively defined evaluative criteria which can be applied to a submitted case. It is suggested that the following CA criteria offer a minimum standard.

1. Does the DFL have a contractual agreement with all relevant parties outlining the scope of all tasks which the DFL is permitted to carry out?
   a. And, can the DFL fulfil the requirements of this contractual obligation?
2. Does the submitted case contain all relevant paperwork to allow for an examination to be conducted?
   a. This includes continuity statements and exhibit information.
   b. Is the information accurate?
3. Have case instructions been provided?
   a. And, are these understandable by the DFL?
4. Can a suitable investigative strategy be developed by the DFL?
   a. Any laboratory should determine whether there is an existing and appropriate investigative strategy determined or whether there is sufficient information to devise one. This requires the ability to converse with the wider investigative team in order to establish a robust understanding of the case circumstances and requirements.
   b. Are the expectations of the investigatory team understood and manageable by the DFL?

The application of CA criteria should be transparent and documented, where the outcome of this process may not be a binary decision of 'accept' or 'reject', instead it is suggested that CA can lead to cases being placed into one of the following three '*case-state categories*'.

Case progress:- Any case following CA which is deemed to be in a state where all necessary information and resources are available which permits the laboratory to conduct an examination of it without any additional requirements. These cases can be subjected to CP.

Case Reject:- Any case following CA which is deemed as being unsuitable for examination within the DFL. A rejection status may be given for a number of reasons including both issues arising from the wider investigatory team and any in-lab concerns. In addition, cases that have been subject to additional inquiries may be rejected if any case issues cannot be resolved. Cases that are rejected must be returned to the submitting authority with an accompanying justification for adopting this stance.

Case paused:- Any case following CA which is deemed to be in a state where further investigatory progress cannot be made currently, however it may be possible to meet the expectations of the investigatory team subject to further inquiries being made by the DFL. This may be due to an absence of any required information needed to conduct an effective examination, or where legal/procedural omissions or irregularities exist and further clarification is needed. Cases in this state cannot proceed under current laboratory conditions and therefore should be placed into a state of pause while those factors preventing progress are rectified. This may be as a result of further requirements needed from the wider investigatory team, or due to in-lab issues (for example, if the purchase of additional equipment is required). The duration of any pause period should be monitored to prevent undue delay, where it may be necessary to define threshold times for both case review and to determine the period of time where it becomes untenable to continue to house the case without any indication of directions for progressing it. Cases that are paused may ultimately move to a case rejection status if a resolution cannot be found within a suitable time frame. Further, cases may be proceedable once any resolution is found. Paused cases cannot be prioritised by a DFL, rather they should exist within a hypothetical 'holding pen' which should be monitored until a solution is established.

On completion of the CA, only those cases in a proceedable state should continue to be managed through a DFLs prioritisation process.

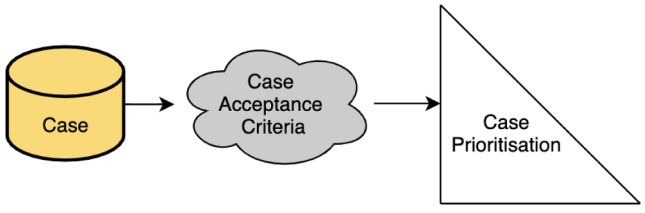


Fig. 1. The backlog management process.

5. Case prioritisation

CP processes attempt to effectively allocate resources to a case in a manner that reflects how and when it should be subject to forensic examination. At the foundation of any prioritisation decision lies the concept of 'need' - i.e. '*when does this case need to be examined in order to ensure an effective outcome for all parties involved is achieved*'. An effective outcome takes into account factors that include the needs of any alleged victim, ensuring they are not unnecessarily exposed to further harm or

undue levels of stress through investigative delays. In addition, the needs of any individual(s) subject to an inquiry must be considered and both the disruption to life which is caused whilst investigative procedures are undertaken, as well as an assessment of any potential further harm such an individual(s) may seek to inflict. CP in DFS is a difficult task requiring the assessment and evaluation of a number of case factors, which when considered in totality allow a prioritisation to be made. Arguably, this process could become paralysing due to the complexity involved and lack of widely available published supporting guidance, where this work seeks to propose a risk-based strategy for CP - the 'Hierarchy of Case Priority' (HiCaP).

5.1. The 'Hierarchy of Case Priority' (HiCaP)

The HiCaP approach takes a '*risk of harm*' approach to CP in DFLs where using HiCaP, cases are assigned one of 16 prioritisation 'levels', which indicates the case's priority position in a DFLs backlog/workload. HiCaP's 16 levels are arranged from level 1 (where cases can be considered the highest priority) to level 16 (where cases can be considered the least priority). The hierarchical ordering of the 16 levels is based upon the size of the 'risk of harm' which those involved in any case are exposed to whilst the investigation is ongoing. HiCaP considers cases where there is a high and unmanageable risk of serious harm being incurred by any parties involved as being of high priority for a DFL where it is suggested that these cases be allocated DFL resources with relative immediacy. As any risk of harm decreases or the management of it becomes more feasible, such cases are considered less of a priority, receiving level allocations which are an appropriate reflection of the level of harm perceived to be present. Applying HiCaP to a DFL backlog/workload allows cases to be processed in order of their HiCaP allocated level. Fig. 2 demonstrates the formation of a DFL case 'priority queue' due to HiCaP CP. In this hypothetical example, a DFL maintains two cases at level 1 which require immediate processing, followed by cases ordered by priority at levels 4, 8 and 16. It is necessary to state that in a real operational environment, it is likely that multiple cases will exist at any single HiCaP level, as shown in Fig. 2.

The HiCap approach is shown in Fig. 3 where each of its levels is defined and explained below.

Level 1: 'There is an immediate threat to the life or wellbeing of others':- Any case where as part of its circumstances there is an immediate threat to the life or wellbeing of others must be prioritised for the immediate allocation of resources by a DFL. In such cases, the risk of harm being immediate is arguably too great to manage, providing an arguable justification for cases in this category to be a top priority for a DFL.

Level 2: 'The device(s) is linked to a serious crime where a high risk of further significant harm being caused exists':- This category includes those inquiries where devices have been seized as part of inquiries linked to serious crimes where the risk of further serious harm being caused is high. In such cases, harm may occur to both persons or property, however, for cases to be classified at level 2, any potential harm inflicted must be both significant, and with a high likelihood of it occurring making the management of it potentially infeasible/too great of a risk. Any decision regarding harm must be based on objectively evidencable information. Such a scenario may be more likely to occur in instances of serious crime, defined under Police Act 1997 Section 93(4)(a) as any act which 'involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose'. South Yorkshire Police [34] note that examples of serious crime include cases of abduction, human trafficking, child sex offences, murder and terrorism offences (a non-exhaustive list). However, some cases surrounding volume crime types may be justifiable under this category if the requisite harm requirement can be evidenced.

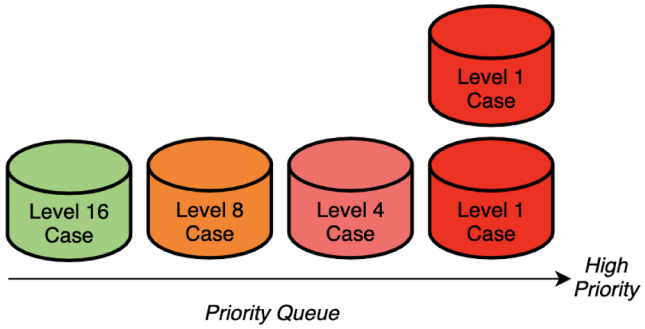


Fig. 2. A DFL priority queue formed by HiCaP allocation.

Level 3: 'A suspect(s) is deprived of their liberty whilst awaiting the results of the inquiry.':- Here, where a suspect is remanded in custody subject to an investigation where the results of any digital examination are fundamental to any decision to release or charge them, such cases are considered of high priority and are placed at level 3 in HiCaP.

Level 4: 'Any potentially relevant digital data exists in a volatile state and is vulnerable to change/loss if actions are not carried out.':- Cases falling into level 4 concern information that may be lost if action is not taken immediately or within a specific time frame, and such information in important to the inquiry taking place. The failure to act promptly may result in the inability to conduct an effective investigation and poor case outcomes.

Level 5: 'A defined, impending and non-movable deadline exists with punitive measures attached if missed for any/all parties including a suspect/victim.':- Examples here include cases where legal deadlines may be set that are unmovable, and failure to adhere to them may compromise an investigation or carry a penalty for any/all involved, or where contractual deadlines are set out in regards to any examination requirements or tender. What is considered an 'impending non-movable deadline' must be subject to scrutiny as in some cases a deadline may be emphasised as non-moveable where in reality it is one which would merely be beneficial to the client.

Level 6: 'The investigation being conducted is likely to lead to the discovery of exculpatory evidence.':- Where information contained on a device is believed to absolve an individual with regards to a suspect event/action, these cases are considered a level 6 priority.

Level 7: 'The device(s) being examined belongs to a victim/witness/3rd party in the case.':- Where devices may contain information relevant to an inquiry, but the device owner is not believed to have committed any unlawful act, level 7 priority is assigned where efforts should be made to ensure the timely processing and return of any equipment in order to limit any disruption/detriment.

Level 8: 'There is an immediate risk of damage to property or of substantial financial and/or reputational detriment being incurred by others.':- Cases where financial detriment or harm to property belonging to another is immediate, such cases are prioritised at Level 8.

Level 9: 'The device(s) is linked to a serious crime where a low or manageable risk of further significant harm being caused exists.':- Cases prioritised at level 9 are distinguished from those at level 2 in that although a serious crime has been committed, the risk of further harm is low and manageable.

Level 10: 'The device(s) is linked with a volume crime offence where there is a high risk of additional harm being caused.':- At level 10, cases are associated with an inquiry into a potential volume crime incident and the risk of further harm being caused is considered high. Any further harm should not be considered serious for the case to be assigned at this level, where indications of more severe harm suggest the commission of additional more severe offences. In these instances, the HiCaP level should be reconsidered to one with a higher priority.

Level 11: 'The digital investigation contains a device which is linked to other wider inquiries.':- Here, where the results of any device examination are also pertinent to wider inquiries taking place and may influence/guide further investigative actions, a level 11 is assigned.

Level 12: 'The suspect(s) is subject to oppressive/invasive bail conditions whilst a device examination and inquiry takes place.':- Cases prioritised at

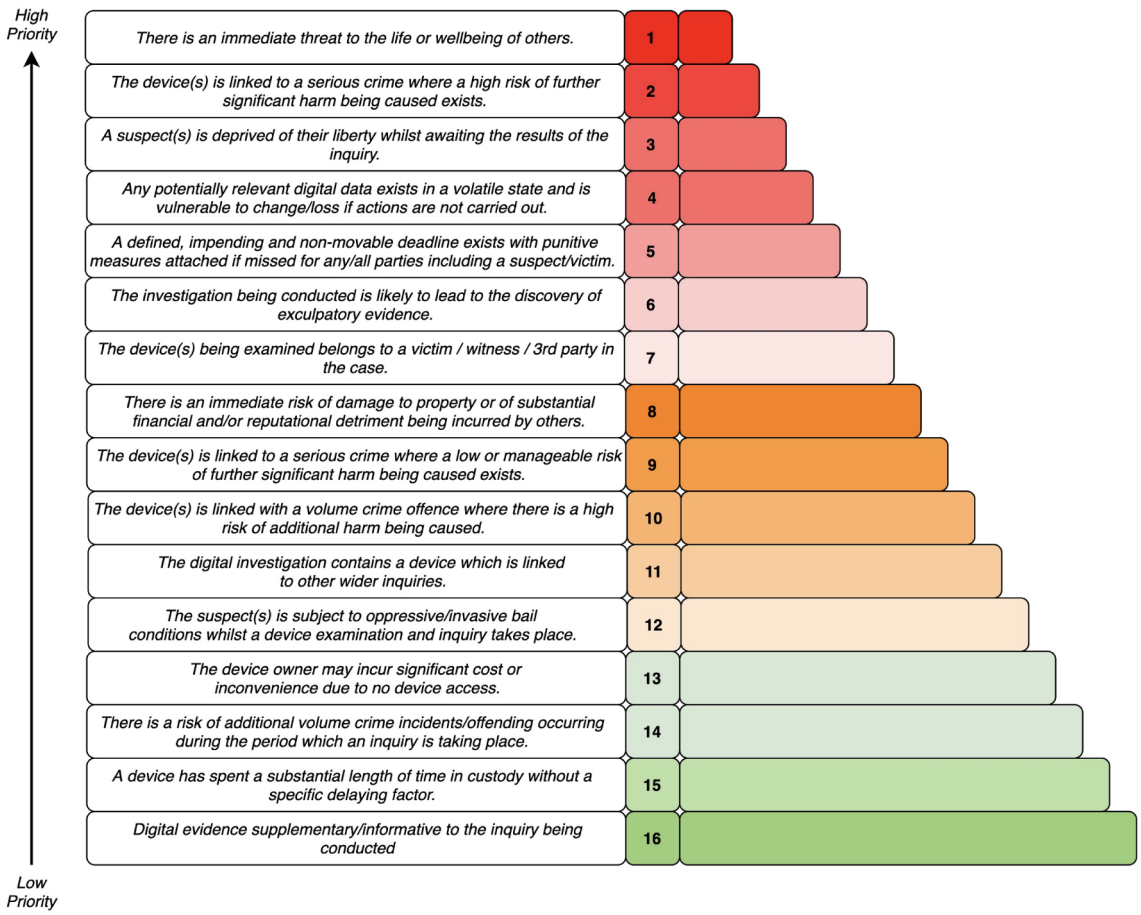


Fig. 3. The HiCaP.

level 12 concern devices where the owner and their actions are strictly regulated subject to the outcome of the digital device examination.

Level 13: 'The device owner may incur significant cost or inconvenience due to no device access.':- Unlike at level 12, cases at level 13 concern individuals who as a result of the examination may incur inconvenience or cost. For example, consider those who have devices seized and as a result are unable to use them, where the impact of this may be that they are still incurring contractual costs associated with the device's usage or the contents of the device is important to their daily life (for example, business-critical information).

Level 14: 'The device(s) is linked with a volume crime offence where a low/moderate and manageable risk of further significant harm being caused exists':- Level 14 priority cases are distinguished from level 10 in that while there is a risk of additional volume crime incidents occurring, the risk of them occurring and any harm as a consequence is not high and therefore deemed unlikely to occur during the period of device examination delay encountered by the investigative team.

Level 15: 'A device has spent a substantial length of time in custody without a specific delaying factor.':- At level 15, the length of time a device has been in the possession of those subjecting it to examination is considered where devices that have been stored for long and potentially unjustifiable periods must be prioritised. Time delays may also increase the presence of risk, a point discussed further in Sections 5.3.1 & 5.4.

Level 16: 'Digital evidence supplementary/informative to the inquiry being conducted':- Cases where any device data is merely supplementary or informative as part of an inquiry are considered priority level 16.

5.2. Flexibility

It is important to note that prioritisation should be considered a task that is flexible, and this is particularly emphasised in relation to the use of the HiCaP model. Therefore whilst a case may be initially assigned a prioritisation level, this level may be subject to change should additional case intelligence be made available which may influence or change any originally made priority level decision. In order for this to be practical, frequent case management reviews must take place within a laboratory in order to ascertain factors that may change a case's priority. Decisions to change a case's priority level should be made by those with oversight and appropriate permission and governance of the laboratory's management and only once clear evidence of a need to change a case's priority is made available. This is emphasised by the National Institute of Justice [25] - 'all exceptions and/or modifications to CP shall be made by the lab director, or with the approval of the lab director, and include all documentation relevant to the change in case priority'. This is particularly important if priority levels are intended to be reduced, where the associated risks associated with these actions and the potential for delayed results must be scrutinised.

5.3. How do you assign a 'level'?

Using HiCaP, each case is assigned a specific level due to the traits that a case maintains. For example, where case information is clear and reliable that any device is linked to a case where there is an immediate threat to the life or wellbeing of others, such a case will be prioritised as level 1. Whilst this may be considered a relatively straightforward process, achieving this effectively requires ensuring that any underpinning case information is evaluated for accuracy and reliability to ensure any prioritisation decisions made are justifiable. HiCaP is designed to prioritise cases based solely upon the risk factors associated with it. Whilst HiCaP does not incorporate any other form of prioritisation

factors, DFLs may prioritise based upon cost and effort required [35], organisation agendas and key performance indicators [32] and capability. These factors are not considered CP factors, instead, information that should form part of any initial CA procedures.

5.3.1. What if a case concerns multiple levels?

In some instances, a case may maintain traits that allow it to be categorised at multiple HiCaP priority levels, where in such circumstances, the highest priority level applicable should be assigned to the case. Consider the scenario where a device belongs to a victim (level 7) and the circumstances involve an immediate threat to the life or well-being of others (level 1). In this circumstance, the case must receive a priority level 1 ranking. Cases may also change priority level due to time delays, where currently level 15 is for devices that have spent a substantial length of time in custody without a specific delaying factor. However, over time, delays may also lead to other case developments and the need to factor in other prioritisation levels, for example where a delay begins to cause significant cost or inconvenience due to having no device access (level 13), then the case priority level may increase to level 13. Consider also cases that are originally prioritised at level 11 (the digital investigation contains a device which is linked to other wider inquiries), however, it is subsequently acknowledged that the wider inquiry involves an incident where there is an immediate threat to life, then it is argued that such a case be moved and prioritised as a level 1 case.

5.4. Why 'time delay' should not be a sole indicator of priority

The length of time a device/case has spent within a DFL gives rise to a number of moot points when considered in relation to prioritisation. Whilst all DFLs seek to provide a prompt service in terms of examination completion times, it is inevitable that some cases will take longer to process. It is suggested that time be a prioritisation factor that is considered incremental. In HiCaP, cases that have spent a substantial length of time in custody without a specific delaying factor are considered a level 15 priority. However, as new cases enter a DFL which contains risk factors that place them at a higher priority level in HiCaP than these cases, then further delays may be experienced. Therefore it is suggested that cases which are prioritised in a DFL at level 15 are subject to consistent review to ensure that they are not kept within a DFL indefinitely. In turn, case delays may subsequently lead to other risk factors emerging which subsequently cause a case to rise in priority. A DFL must exercise caution and strict oversight of the management of cases prioritised at level 15 to make sure that cases that have been delayed have not caused furthermore serious issues.

5.5. HiCaP levels and a hierarchical 'shuffle'

The HiCaP intends to provide a risk-based method of CP within DFLs where it is acknowledged that different organisations and jurisdictions may seek to accept and manage risk differently. Therefore it is recognised that whilst it is argued that the proposed HiCaP offers a viable hierarchical ordering of risk factors, others may place different values of priority upon these levels. In addition, the levels within HiCaP should be considered a base, where any organisation seeking to adopt it may expand upon the existing levels as new and emerging threats become apparent within case work which require prioritisation.

In regards to the existence of the levels in HiCaP, their positioning should be underpinned by robust reasoning and evidence of a prioritisation need. One option is for an organisation deploying HiCaP to order its levels based upon available crime statistics that give an indication into crime areas that are both increasing and posing a threat to the wider society [41]. For example, information provided by bodies such as the Office of National Statistics [42] in regards to crime trends may influence policy decisions and justify the prioritisation level of certain case types. Such an approach also raises another prioritisation challenge in that geographical regions may face different criminal threats. As a result, the position of levels in HiCaP may not be suitable for every police force, where geographical factors impacting prioritisation may include metropolitan vs rural areas, and where specific crime types are found to be consistently more prominent in certain areas. Linked to this theme is the concept of case 'solvability', where offences that are typically difficult to attribute to a perpetrator or where a lack of evidence commonly exists, such factors may influence the priority given to a case. Conversely, if case 'turnaround' times are seen as a metric of performance, the priority level a case may be given could be influenced by how quickly it can be dealt with [43].

Prioritisation levels may also be influenced by overarching legal governance that dictates how specific offences should be processed. In some cases, specific time limits may dictate how quickly a case should be processed, naturally raising the priority level of certain cases where expected processing times are short. This may be the case where any ongoing investigation is particularly onerous for an alleged suspect or they are imprisoned pending the outcome of inquiries. Finally public perceptions and expectations may also shape the priority of specific case types [44] in regards to identification and development of appropriate police responses.

In any instance, it is argued that even if a hierarchical 'shuffle' were to take place in HiCaP, providing any ordering is justifiable (through evidence) and remains consistent in its deployment, then it may still remain a viable approach to CP in DFLs. Similar prioritisation challenges occur in fields such as medicine [45] where multiple pathways for case prioritisation may exist, placing emphasis on the need to evidence sound and justifiable principles for which any final prioritisation decision has been based.

6. Conclusion

As DFLs are likely to continue to see large volumes of cases requiring the services of DFS professionals, CA and CP methods will play an important role in ensuring that available resources are deployed effectively. Yet, in light of limited formal guidance, those operating in DFLs may find that they are restricted in their construction of CA and CP approaches without the ability to assess the current state of the art and best practice approaches. For this reason, it is suggested that as the DFS progresses, the production and dissemination of formal CA and CP research should be encouraged. This work has discussed the challenges surrounding backlog/workload management in DFLs and proposed the HiCaP as a method for CP. It is argued that HiCaP offers an evidencable, concise and justifiable approach to CP through the use of '*risk of harm*' as a principle prioritisation metric. HiCaP and its 16 priority levels have been described along with specific deployment challenges including the need for a flexible, evidence-based approach to level allocation.

Future work includes the planned deployment of HiCaP in a laboratory setting in order to appraise its impact and ascertain its performance under real-world conditions. Trial data would allow a critical evaluation of this approach in order to determine its potential value, issues with its deployment and also support future refinement.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A.M. Alrumaithi, Prioritisation in Digital Forensics: A Case Study of Abu Dhabi Police, Liverpool John Moores University (United Kingdom), 2018.
[2] Forensic Capability Network, 2020. "Digital Forensic Science Strategy 2020" https://www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf (Accessed: 24 June 2021).

[3] P. Reedy, Interpol review of digital evidence 2016-2019, Forensic Science International: Synergy, 2020.
[4] G. Horsman, The COLLECTORS ranking scale for 'at-scene' digital device triage, J. Forensic Sci. 66 (1) (2021) 179–189.
[5] G. Horsman, Decision support for first responders and digital device prioritisation, Forensic Sci. Int.: Digital Invest. 38 (2021), 301219.
[6] G. Horsman, Defining 'service levels' for digital forensic science organisations, Forensic Sci. Int.: Digital Invest. 38 (2021), 301178.
[7] R.B. Van Baar, H.M. van Beek, E.J. Van Eijk, Digital Forensics as a Service: A game changer, Digital Invest. 11 (2014) S54–S62.
[8] D. Lillis, B. Becker, T. O'Sullivan, M. Scanlon, Current challenges and future research areas for digital forensic investigation, 2016, arXiv preprint arXiv: 1604.03850.
[9] M. Scanlon, August. Battling the digital forensic backlog through data deduplication, in: 2016 sixth international conference on innovative computing technology (INTECH) (pp. 10-14), IEEE, 2016.
[10] X. Du, N.A. Le-Khac, M. Scanlon, Evaluation of digital forensic process models with respect to digital forensics as a service, 2017, arXiv preprint arXiv:1708.01730.
[11] R. Montasari, R. Hill, January. Next-generation digital forensics: Challenges and future paradigms, in: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) (pp. 205-212). IEEE, 2019.
[12] ADF Solutions, 'ADF as an Innovator in Digital Forensic Software' Available at: https://www.adfsolutions.com/news/innovating-digital-forensic-triage-software (Accessed: 24 June 2021), 2021.
[13] London.gov.uk, 'Backlog of mobile phones and computers awaiting forensic analysis', 2019, Available at: https://www.london.gov.uk/questions/2019/12159.
[14] Police Professional, 'Forensic delays 'deeply concerning' as case backlog grows', 2019, Available at: https://www.policeprofessional.com/news/forensic-delays-deeply-concerning-as-case-backlog-grows/ (Accessed: 24 June 2021).
[15] John Simpson, 'Backlog of devices awaiting police analysis leaves trials facing collapse', 2019, Available at: https://www.thetimes.co.uk/article/backlog-of-devices-awaiting-police-analysis-leaves-trials-facing-collapse-bgb6zft9x (Accessed: 24 June 2021).
[16] Jane Reader, 'Police 'overwhelmed' by backlog of digital devices waiting to be examined', 2020, Available at: https://www.bournemouthecho.co.uk/news/18425051.police-overwhelmed-backlog-digital-devices-waiting-examined/.
[17] J.I. James, Multi-stakeholder case prioritisation in digital investigations, J. Digital Forensics, Security and Law 9 (2) (2014) 6.
[18] Parliamentary Office of Science & Technology, 'Digital Forensics and Crime', 2016, Available at: https://researchbriefings.files.parliament.uk/documents/POST-PN-0520/POST-PN-0520.pdf (Accessed: 29 June 2021).
[19] B. Rappert, H. Wheat, D. Wilson-Kovacs, Rationing bytes: managing demand for digital forensic examinations, Policing and Soc. 31 (1) (2021) 52–65.
[20] K.J. Strom, M.J. Hickman, Unanalyzed evidence in law-enforcement agencies: A national examination of forensic processing in police departments, Criminology & Public Policy 9 (2) (2010) 381–404.
[21] Gillain Tulley, 'Annual Report 17 November 2018 – 16 November 2019', 2020, Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/877607/20200225_FSR_Annual_Report_2019_Final.pdf (Accessed: 21 June 2021).
[22] J.I. James, P. Gladyshev, Challenges with automation in digital forensic investigations, 2013. arXiv preprint arXiv:1303.4498.
[23] Cambridge Dictionary, 'Prioritize', 2021, Available at: https://dictionary.cambridge.org/dictionary/english/prioritize?q=prioritisation (Accessed: 24 June 2021).
[24] V. Jusas, D. Birvinskas, E. Gahramanov, Methods and tools of digital triage in forensic context: Survey and future directions, Symmetry 9 (4) (2017) 49.
[25] National Institute of Justice, 'DIGITAL EVIDENCE POLICIES AND PROCEDURES MANUAL', 2020, Available at: https://www.ojp.gov/pdffiles1/nij/254661.pdf (Accessed: 24 June 2021).
[26] H.A. Hansen, S. Andersen, S. Axelsson, S. Hopland, Case study: a new method for investigating crimes against children, 2017.
[27] I.M.S.H. Alawadhi, Methods and Factors Affecting Digital Forensic Case Management, Allocation and Completion (Doctoral dissertation, University of Central Lancashire), 2019.
[28] U.S. Department of Justice, 'Forensic Examination of Digital Evidence: A Guide for Law Enforcement', 2004, Available at: https://www.ojp.gov/pdffiles1/nij/199408.pdf (Accessed: 24 June 2021).
[29] Australian Federal Police, 'Case Categorisation and Prioritisation Model', 2020, Available at: https://www.afp.gov.au/what-we-do/operational-priorities/case-categorisation-and-prioritisation-model (Accessed 4 October 2021).
[30] SWGDE, 'SWGDE Model Standard Operating Procedures for Computer Forensics', 2012, Available at: http://www.irisinvestigations.com/wp-content/uploads/2016/12/ToolBox/04-ISO%20QUALITY%20MANAGEMENT%20SYSTEM/SWGDE_Model_SOP_for_Computer_Forensics_091312.pdf (Accessed: 24 June 2021).
[31] M.R. Hirst, 'Hi Tech Crime Unit Final with responses Report ', 2014, Available at: https://www.northyorkshire-pfcc.gov.uk/content/uploads/2016/10/Hi-Tech-Crime-Unit-Final-with-responses-Report.pdf (Accessed: 24 June 2021).
[32] Harry Parsonage, 'Computer Forensics Case Assessment and Triage- some ideas for discussion', 2009, Available at: http://computerforensics.parsonage.co.uk/triage/ComputerForensicsCaseAssessmentAndTriageDiscussionPaper.pdf.
[33] Interpol, 'GLOBAL GUIDELINES FOR DIGITAL FORENSICS LABORATORIES', 2019, Available at: https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf (Accessed: 27 June 2021).
[34] South Yorkshire Police, 'Pi9.12 - Crime Management - Crime Allocation Instruction', 2017, Available at: https://www.southyorks.police.uk/media/3436/20182041-pi912-publish.pdf.
[35] M.W. Gielen, Prioritizing computer forensics using triage techniques (Master's thesis, University of Twente), 2014.
[36] R.E. Overill, J.A. Silomon, K.A. Roscoe, Triage template pipelines in digital forensic investigations, Digital Invest. 10 (2) (2013) 168–174.
[37] H. Arshad, A.B. Jantan, O.I. Abiodun, Digital forensics: review of issues in scientific validation of digital evidence, J. Inf. Process. Syst. 14 (2) (2018) 346–376.
[38] G. Horsman, Triaging digital device content at-scene:-Formalising the decision-making process, Sci. Justice 62 (1) (2022) 86–93.
[39] R. Stoykova, K. Franke, May. Standard representation for digital forensic processing, in: 2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE) (pp. 46-56), IEEE, 2020.
[40] The Police Foundation 2017, Available at: Police prioritisation: How should the police choose what matters most in a changing world? https://www.police-foundation.org.uk/2017/wp-content/uploads/2017/09/police_policy_dinners_prioritisation.pdf.
[41] Police Federation, 2019, Stats show need to prioritise crime and policing. Available at: https://www.polfed.org/news/latest-news/2019/stats-show-need-to-prioritise-crime-and-policing/.
[42] Office of National Statistics 2022, Crime and justice. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice.
[43] Home Office 2020 Crime outcomes in England and Wales 2019 to 2020, Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/901028/crime-outcomes-1920-hosb1720.pdf.
[44] College of Policing 2013, Engagement, Available at: https://www.college.police.uk/app/engagement-and-communication/engagement.
[45] J.C. Moskop, K.V. Iserson, Triage in medicine, part II: Underlying values and principles, Ann. Emerg. Med. 49 (3) (2007) 282–287.
[46] National Policing Improvement Agency 2009, Practice advice on the management of priority and volume crime, Available at: https://zakon.co.uk/admin/resources/downloads/volume-crime-practice-advice-on-the-management-of-priority-and-volume-crime-2009-1.pdf.
[47] Mayor's Office for Policing and Crime 2022, Police and Crime Plan 2021-25. Available at: https://www.london.gov.uk/publications/police-and-crime-plan-2021-25.



https://dspace.org/

The Hierarchy of Case Priority (HiCaP):- A proposed method for case prioritisation in digital forensic laboratories

Horsman, Graeme

2022-09
Elsevier
https://doi.org/10.1016/j.scijus.2022.08.008
Horsman G. (2022) The Hierarchy of Case Priority (HiCaP):- a proposed method for case prioritisation in digital forensic laboratories. Science & Justice, Volume 62, Issue 5, September 2022, pp. 594-601

Downloaded from a DSpace repository. https://dspace.org/