THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 9 | Number 2 Article 6

2014

Multi-Stakeholder Case Prioritization in Digital Investigations

Joshua I. James
Soon Chun Hyang University, joshua.i.james@pm.me

Recommended Citation

James, Joshua I. (2014) "Multi-Stakeholder Case Prioritization in Digital Investigations," *Journal of Digital Forensics, Security and Law*: Vol. 9 : No. 2 , Article 6.
DOI: https://doi.org/10.15394/jdfsl.2014.1171
Available at: https://commons.erau.edu/jdfsl/vol9/iss2/6

MULTI-STAKEHOLDER CASE PRIORITIZATION IN DIGITAL INVESTIGATIONS

Joshua I. James
Digital Forensic Investigation Research Laboratory
Soon Chun Hyang University
Shinchang-myeon, Asan-si, South Korea
joshua@cybercrimetech.com

ABSTRACT

This work examines the problem of case prioritization in digital investigations for better utilization of limited criminal investigation resources. Current methods of case prioritization, as well as observed prioritization methods used in digital forensic investigation laboratories are examined. After, a multi-stakeholder approach to case prioritization is given that may help reduce reputational risk to digital forensic laboratories while improving resource allocation. A survey is given that shows differing opinions of investigation priority between Law Enforcement and the public that is used in the development of a prioritization model. Finally, an example case is given to demonstrate the practicality of the proposed method.

Keywords: case prioritization, digital forensic triage, investigation prioritization, workflow management, risk

1. INTRODUCTION

In recent years there has been a growing awareness of the need for digital investigation. Likewise, with the advancement of technology and an increase in the amount of data produced, the needs of digital investigators have expanded while the resources provided have not kept pace (Casey, Ferraro, & Nguyen, 2009; Gogolin, 2010). A number of prior works have proposed alternative models of investigation, many times looking for more efficient ways to identify devices and data that have some or no relevance to the case. Methods such as digital forensic triage (Koopmans & James, 2013) seek only to sort exhibits by their likely relevance to the case and not exclude exhibits, where methods such as enhanced preview[1] (Shaw & Browne, 2013) seek to filter non-relevant exhibits though a more in-depth but highly automated analysis. Methods such as these essentially attempt to make the overall investigation process model more efficient by implementing stages of investigations of increasing rigor.

Other methods attempt to focus on the identification of where related digital evidence is likely to be located (or not) in a system (Garfinkel, 2006; Rowe, 2014; Rogers, Goldman, Mislan, Wedge, & Debrota, 2006). These approaches help guide an investigator during the investigation, making more efficient use of available resources.

While many of these works attempt to reduce the amount of potentially non-relevant data needing 'hands-on' analysis by a human during the investigation, few have looked at ways to optimize the difficult and timely process of case management before an investigation begins. Casey, et al. (2013) analyzed overall digital forensic processes to determine key decision points for optimization, shifting some of the decision process to the investigator in an effort to improve efficiency and quality of ser-

[1] Also known as 'preliminary analysis'

vice. However, non-optimized case management can also contribute to a reduced investigation throughput, and increase risks to the organization (Jones & Valli, 2011, p.38).

While various works claim that case management is a critical aspect of efficient criminal investigations, few give models for management, and specifically for investigation prioritization. For example, Jones & Valli (2011) claim that "...the type of task that will be accepted into the laboratory and the priority with which different types of cases will be given should be determined". They claim a standardized case prioritization method will help alleviate conflicts between staff and investigators who only want their cases prioritized, but do not elaborate on how prioritization should take place. Similarly, Shaw & Browne (2013) present the concept of 'administrative triage' to sort and/or reject exhibits before receiving an analysis using a point-based 'matrix system'. However, there is no elaboration on the construction or use of such a 'matrix system'.

Fife (2010) gave a discussion on the of prioritization of international criminal cases in which 'key criteria' for prioritization of international crime is loosely defined. However, there is no discussion about how criteria should be implemented beyond simple consideration by a case manager. This situation is slightly improved by the Australian Federal Police (AFP) (Australian Federal Police, 2010), but stops just before providing a practical implementation of a prioritization model. Even if such criteria are considered, such loose definitions may still lead to an organization-centric prioritization that may not accurately reflect the interests of all stakeholders. As stated by Ortmeier & Davis (2012, p.184) "...any change initiative considered by police must address both [organizational and public] perspectives, not just one or the other".

1.1 Contribution

This work contributes to field of criminal justice by proposing a novel, multi-stakeholder case prioritization method that helps reduce risk to the implementing organization, and allows for more efficient resource allocation within the organization during investigations.

While such a method may be applied to criminal case management in general, this work is specifically concerned with criminal cases involving digital evidence. As such, digital forensic investigation laboratories are the primary focus.

2. CASE CATEGORIZATION AND PRIORITIZATION IN PRACTICE

In practice, Law Enforcement (LE) organizations, even within the same country, implement different methods to prioritize investigation resources. With some organizations, general case prioritization may be based on the organization's specific mission. For example, the United States (US) Department of Justice (DOJ) prioritize the following areas, in order (US Department of Justice, 2013):

1. Protecting Americans from national security threats
2. Protecting Americans from violent crime
3. Protecting Americans from financial fraud
4. Protecting the most vulnerable members of society

While a priority of general case types may be dictated by the organization's mission, this does little to instruct case managers and investigators in how to prioritize specific categorizes of cases, leading to prioritization that may be based on subjective feelings of the case managers or superior officers.

Similar to the DOJ, the U.S. Federal Bureau of Investigation (FBI) divide crime into the following general categories in order of priority (FBI, n.d.):

1. Terrorism
2. Counterintelligence

3. Cyber Crime
4. Public Corruption
5. Civil Rights
6. Organized Crime
7. White-Collar Crime
8. Violent Crimes & Major Thefts

As observed, many countries use similar high-level categories of crime; however, even though the DOJ and FBI have prioritized general categories of crime, the reasoning for this prioritization is not given, which makes following their categorization and prioritization model difficult. Further, a lack of objective prioritization can mean undue stress for the organization, and poorly-planned, superficial efforts to 'crack down' on whatever area is currently in the spotlight.

The challenge with not having a fixed prioritization model, among others, is that continually-changing priorities potentially increases the amount of stress put on the investigators while potentially lowering the overall quality of investigation. In the Korean Police, when a particular case type is topical and becomes the priority of a high-ranking official, all groups under the hierarchy must prioritize the problem. This increases stress for all those involved because results must be shown in the newly-prioritized area usually while maintaining the same prior investigation quality and throughput for all case types.

A recent example in Korea involved a child exploitation investigation (Hancocks, 2012). Due to the graphic circumstances of the case, child exploitation became a national focus for approximately 2 months, resulting in crack-down operations. These operations resulted in over 9000 arrests, with less than 200 being convicted on charges of downloading child exploitation material (CEM). While some CEM cases are still investigated as a matter of course, after a large investment in training and resources to combat CEM, investigations rarely went further than naive peer-to-peer network investigations.

Based on the author's observation, once the public shifted their attention to a different social issue, police focus followed. This constant shifting of priority has at least two consequences. First, because of the lack of proper long-term investment and focus on specific types of crime, major incidents happen at least once a year, to which Law Enforcement react by re-prioritizing (and re-investing) in these types of crimes for a short period. Any gained knowledge is usually lost before focus is shifted back to the specific crime type, requiring more training and investment to react to the issue. Second, constantly changing priorities to match current public focus causes the police to have a negative public image. The public expects the Law Enforcement to both prevent crime and react immediately to incidents. However, because of constantly changing priorities and no long-term planning, prevention initiatives are largely non-existent (in Korea's case). Because general crime categories are not a focus throughout the year, when an incident does occur investigators often need to quickly receive training or external guidance before a proper response can be executed.

Some efforts do exist to attempt to objectively prioritize investigation resources. Some organizations in Canada have implemented their own prioritization matrix for their department using tools such as Microsoft Excel to calculate the priority score of each case based on a number of factors such as case type, number of associated digital devices, time since the investigation has been requested, media attention, and a number of others. Many times the case manager is responsible for the matrix. In doing so, it is more difficult for outside groups to affect the system and get their cases prioritized, but also allows bias at the case manager level. These locally-developed prioritization models, and the underlying prioritization algorithms are usually not disseminated.

Ireland is taking a slightly different approach by requiring local investigators to fill out a form accompanying any request for a digital investigation. This form has a number of fields that correlate to different prioritization factors.

While the weight of each factor is not shared, the local investigator, who may be better qualified to report on the situation, can affect the priority of their case. There is, however, still some oversight by the digital investigation case manager.

Prior to the use of this approach, prioritization of cases was specified completely by the digital investigation case manager. One major challenge with investigations within the Irish unit is that prioritized cases would continually be assigned to investigators, some with more than 15 assigned cases at once, all with the 'highest priority'. There were two major reasons for this: first, high-ranking officials would personally request cases to be investigated with a high priority without going through an official request process. Second, media attention would make a case high priority, sometimes even being assigned multiple investigators who then must put all other high-priority cases on hold.

While there was no official prioritization model in Ireland, investigators generally prioritized child exploitation investigations, with approximately 80% of an investigator's time focused on those types of investigations (James & Gladyshev, 2013). Certain 'special circumstances' may see other case types prioritized, such as an immediate threat to life. Investigators often mentioned attempting to prioritize CEM investigations where the suspect has access to children; however, there are too many of these factors for case managers to consistently prioritize with no objective model.

2.1 AFP Case Categorisation and Prioritisation Model

One of the most comprehensive, publicly available case categorization and prioritization models is provided by the Australian Federal Police, with their "Case Categorisation and Prioritisation Model" (CCPM) (Australian Federal Police, 2010). This model defines "major elements" for prioritization that include incident type, impact, type of response, relation to scope of AFP, resources required, budget assigned, duration, value of offense, and case type.

Each major element is divided into well defined sub-categories or sub-considerations. For example, 'Impact' is evaluated with four levels ranging from 'low' to 'very high', with the criteria for each level defined.

While the CCPM may be one of the most comprehensive models publicly available, and does well in defining the factors considered in prioritization, the CCPM does not provide a method for implementation. For example, once impact is evaluated, there is no guide as to how a case manager should include this additional information into their decision-making processes.

2.2 Common Challenges in Observed Case Prioritization

In many Law Enforcement organizations, there are a number of challenges that often times lead to less-efficient resource allocation, increase case time, and increased risk to the organization. One challenge comes from the assumption that LE are managing cases in line with the needs of their clients. Just like any organization, the scope of LE changes over time, and this change is often difficult to identify from within the organization. This means that the scope of work that the organization is conducting may gradually begin to reflect more the organization's wants rather than the client's needs. In these organizations, other stakeholders were rarely identified, and almost never consulted.

As previously described, not having an objective case prioritization model to follow can lead to the organization being more reactionary, potentially wasting more resources and generally increasing stress within the organization while having a minimal real impact on the identified problem. In many observed organizations that could be classified as reactionary, the digital forensic laboratory often maintained the most risk in terms of blame for investigations not being completed in a timely manner (reputation). Many times laboratory services were the slowest, and a lack of objective case management meant that cases were consistently prioritized over each other after being assigned to an investigator, exacerbating resource challenges and slowing the time to completion for all cases.

While prioritization was sometimes due to factors such as media attention, the most commonly observed reason that cases would continually be prioritized over previously-assigned cases was because of higher-ranking officers pushing the case. If investigation capacity cannot effectively maintain 'normal' priority cases, then needlessly prioritized cases contribute to delaying all cases. This situation, again, normally increased risk to the laboratory and not the higher-ranking officials, even if the laboratory has no control over the situation.

2.3 Potential Benefits of a Standardized, Multi-Stakeholder Prioritization Method

Many of these challenges can be wholly or partially solved by implementing a multi-stakeholder case prioritization method. First, if the opinions of all stakeholders are included, risks to the laboratory can be reduced. For example, in the previously described child exploitation case, the public normally asks the police why they were not prioritizing these types of cases *before* the incident happened. Currently, many LE organizations have no answer to this question, making the organization look less competent (reputation risk). If an objective, multi-stakeholder prioritization method was created, the organization could potentially show that the stakeholders themselves did not prioritize these types of incidents, and illustrate that if new case types should be prioritized then other case types should receive less resources.

Further, by understanding what the priority areas are, and knowing that priority will not be changed in the short term, investigators will face less pressure to perform under unknown circumstances. If objective case management is in place and thoroughly enforced, it will be more difficult for cases to jump the queue. This could mean that investigators are assigned fewer simultaneous cases, reducing the time needed to jump between and familiarize him or herself with the case.

3. PROPOSED CASE PRIORITIZATION METHOD

The proposed case prioritization method seeks to address the weaknesses identified in Section 2.2. Prioritization is based on the identification and quantification of relevant factors. *Prioritization factors* (factors) are any consideration that may change the priority of a specific investigation request.

The proposed method for the identification and prioritization of cases can be defined as four general steps:

1. Categorize crime types, and acts that fall under each category
2. Identify prioritization factors
3. Determine the priority of factors
4. Assign a weight to each factor based on determined priority order
5. Apply desired prioritization algorithm based on weighted factors

3.1 Categorize Crime Types

In attempting to prioritize types crimes at local, national or international levels, it is important to have crime categories clearly and meaningfully defined. For example, when attempting to gather statistics about national and international digital crime and investigations, the inconsistency in categorization of different acts and how these acts translate into digital crimes makes measurement and analysis of such crimes difficult. The *Comprehensive Study on Cybercrime* (Malby et al., 2014) shows that countries use many different 'divergent' approaches that may consider the object, intent and damage, among others. Further, Douglass & Burgess (Douglas, Burgess, Burgess, & Ressler, 2013) claim that general crime categorization by Law Enforcement is often based on the criminal motivation. Such classification of cybercrime is further examined in (Ghernaouti, 2013). Acts are often categorized first by looking for the most analogous types of 'traditional' crime, and updating or transplanting language from already

implemented legislation (Malby et al., 2014). As observed, the digital component appears to rarely be a factor in categorization, but practical classification instead tends to rely on the motivation of the act and how the act relates to currently implemented legislation.

While many organizations around the world are attempting to create categories of crime, and digital crime specifically, few release details of how these categories are formed. Of the few that have been released, the CCPM (Australian Federal Police, 2010), and Douglas, Burgess, et al. (Douglas et al., 2013) give a more comprehensive overview of how meaningful classification may be achieved. Crime classification is an important first-step to ensuring the most efficient allocation of resources; however, this work focuses more on investigation prioritization rather than the taxonomy of crime.

Categories of crimes are highly specific to the culture and politics of the group implementing the categorization (Rauscher & Yaschenko, 2011). General areas, or even specific acts, may be aligned, but how each country defines and classifies will normally differ. It is difficult to propose a 'standard' method of categorization that would work for every group due to the subjective way in which types of crime may be conceptualized. Practically, this means that each organization will need to adopt or define crime categories that are aligned with their culture and political system.

3.2 Identify and Prioritize Factors

After categorization, an organization must identify prioritization factors (pf) to be considered. Since crime categorization has already been completed, crime categories, or even the acts that fall under each category, may be used as the primary prioritization factor. As such, an organization may begin to determine the priority of the 'case type' factor. As discussed, prioritization should take into account all stakeholders, and also consider special circumstances in which a crime may be given a higher or lower priority. The following are example prioritization factors that will be considered in this work:

1. Use defined crime categories to identify priority of cases for stakeholders (survey):
   - The public
   - Higher-ranking officials
   - The department
   - Other departments, local stations, etc.
2. Use defined crime categories to identify priority of cases based on severity of fine or prison sentence
3. Identify special circumstances that may change the priority of a case
4. Consider the age of the investigation request

Using these factors gives a comprehensive overview of the perspective of each stakeholder, as well as the legal system in general. Further, potential factors – such as threat to life – may also affect prioritization, and is still considered. Many other factors could be included, for example all factors identified in the AFP's CCPM.

Although this method attempts to take the opinions of multiple-stakeholders into account, some stakeholders opinions may be of greater importance to the department than others. In these cases, a subjective 'weight' of the stakeholders opinion is given. A weight is defined by the person or group creating the prioritization model, and cannot be objectively defined.

3.2.1 Stakeholder Survey

As discussed, in many organizations the opinion of the public was rarely considered in investigation prioritization, and was normally assumed to be in line with the organization's goals. This assumption, however, was not substantiated, and directly led to increased risk for the laboratory. Further, it was often observed that laboratories were more reactionary when these risks were not considered and planned for before an incident occurred.

Each stakeholder should be surveyed by group (public, department, high-ranking officials, etc.) concerning the priority of investigation for crime categories and specific criminal

actions, and the differences in group prioritization should be noted. For example, the department may find particular types of crime to be priority areas, where higher-ranking officials may have a slightly different view. At the same time, the opinion of the public may also be integrated to ensure that the views of the organization at least somewhat reflect the expectations of external stakeholders.

When attempting to measure the priority of stakeholders, there are at least two ways to assign values to priority. The first, and arguably easiest, is to order crime categories by priority, and use the order as the priority measure. For example, if there are 9 crime categories, the highest priority crime could be assigned a value of 9, and the lowest priority crime could be assigned a value of 1.

Instead of simply assigning a value based on priority order, an organization could also consider the raw values provided by the stakeholders. For example, when a group is surveyed the average priority value for a particular crime, even the highest priority, will be less than the maximum possible value, unless everyone agrees. By using the set of average values, an organization can identify how much a certain stakeholder prioritizes case type X over case type Y. If there is a big difference between case type X and case type Y, then more resources should be allocated to the case type with the higher priority. However, if there is a small difference, the organization may consider assigning similar resources.

3.2.2 Severity of Fine or Sentence

To help reflect the priorities of the legal system, one factor that may be considered is the severity of the fine or sentencing associated with particular types of crime. There are at least two ways in which measurement of punishment severity can take place: charge based or category based. The method can consider each specific action (charge) on a case-by-case basis, or the overall punishment severity of crimes under a specific category can be combined to give any crime under that category a certain priority.

For example, Ireland's *Child Trafficking and Pornography Act, section 5 (1998)* states that conviction for producing, distributing, etc., child pornography leads to "...imprisonment for a term not exceeding 14 years". The *Criminal Damage Act, Section 5 (1991)* states that conviction for a person who "without lawful excuse operates a computer" shall be liable for "...imprisonment for a term not exceeding 10 years". In this case, based on Irish law, the legal system appears to lead to the prioritization of CEM investigations over basic hacking investigations, and this is informally reflected in the digital forensics laboratory (James & Gladyshev, 2013). Alternatively, Korea's *Act on the Protection of Children and Juveniles From Sexual Abuse, ch. 2, article 8 (2011)* specifies a maximum of 10 years for the production of CEM, while the *Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. Article 72 (2010)* specifies a maximum of 3 years for network intrusions, with the latter being the prioritized focus area.

While a thorough review of all applicable acts would need to be conducted, prioritizing by the punishment severity can help ensure that an organization is focus on crimes that are considered more serious by the legal system.

3.2.3 Risk Assessment for Special Circumstances

Previously discussed prioritization factors and their associated priorities are being considered under nominal circumstances. There are, however, a number of circumstances under which a case should be categorized as top priority regardless of case type, punishment, etc. These are situations in which the investigation priority should be increased (or decreased) independent of all other factors by using a *risk modifier* (rm).

Ireland, for example, adds additional priority (weight) to situations where there is an immediate risk to life; a matter of national security; a serious crime; a query from court for a re-examination; operations; the suspect on bail; the suspect is known to victim; the suspect is a repeat offender, or (informally) media atten-

tion, among others. Australia assesses what is defined as the "impact of a matter", assessing similar circumstances as Ireland. Each special circumstance can be assigned a particular value in a range based on the 'seriousness' of the circumstance. For example, Australia uses four levels of 'impact', from 'very high' to 'low'. In this case, a 1 to 4 scale could easily be implemented.

The organization must determine the protocols for handling special circumstances in regards to cases currently in progress. Some circumstances may take precedence over cases in progress that have a lower priority, while others may not take precedence over cases in progress, but go to the top of the queue.

3.2.4 Age of Request

So far, this work has looked at case category, punishment severity and special circumstances as prioritization factors. However, if only these static priorities are considered, it is possible that low priority cases may never be investigated as higher priority investigations continue to be requested. To help with this situation, the length of time since the investigation request may also be considered. For example, by considering time, a case with a priority of 1 (lowest priority) out of 9 (highest priority), would eventually reach a priority of 9 if left unassigned for a certain period of time (defined by the organization). The threshold for increasing priority should be as long as possible, so cases do not normally receive the majority of their priority from the time value.

Priority based on time could be modeled in at least two ways. Either linearly where each minute/hour/day adds a certain priority measure, or by modeling a particular curve. By modeling priority based on a curve, organizations can consider things like 'grace periods'. For example, in South Korea cases should be concluded in less than three months. If, however, there was a request for investigation, and this case had not been assigned after a certain period (two months, for example) then by modeling a curve, the first two months may have no affect on the priority, but afterwards the priority could increase rapidly.

3.3 Prioritization Formula

Once factors have been ordered in terms of priority, an organization may assign a measure to each factor based on its determined priority. For example, a priority measure may be assigned for each case type; a weight to each stakeholder; a priority measure to identified risk (risk modifier); a priority measure modifier based on time (increasing with time). The way priority measures are assigned will depend on how the organization has decided to measure each prioritization factor.

Different prioritization factors may call for different weightings if one factor should have more influence over the final prioritization than others. For example, an organization may want to take public opinion into account, but not as much as high-ranking officials within the organization. In this case, each stakeholder (specific prioritization factor) may have an associated weight modifier that changes the weight of the stakeholders input. For example:

- pp, dp and hp are ordered sets of crime category priorities from public, department and high-ranking surveys, respectively
- Each i-th object in an ordered list correlates to the same case *crime category*. For example, child exploitation may be the third crime category, meaning that $pp[3]$ and $dp[3]$ would correspond to the public and department child exploitation priorities, respectively.
- pp^m, dp^m and hp^m are weight modifiers for the public, department and high-ranking stakeholders, respectively
- $P(i)$ is the overall priority of the i-th crime category, where $P(i) = ((pp[i] * pp^m) + (dp[i] * dp^m) + (hp[i] * hp^m))$

Consider an example where the public, department and high-ranking officials prioritized CEM cases as 9, 5 and 1, respectively. Further, they ranked drug investigations as 1, 4

and 9, respectively where 9 is the highest priority and 1 is the lowest priority. Assume the organization wants public responses to have less weight, and responses from high-ranking officials to have more weight:

- $pp^m = 0.5$; $hp^m = 1.5$
- $pp = [9, 1]$; $dp = [5, 4]$; $hp = [1, 9]$

$P(i) = ((pp[i] * .5) + (dp[i]) + (hp[i] * 1.5))$
Before stakeholder weighting: CEM=15; Drugs=14
After stakeholder weighting: CEM=11; Drugs=18

If only one prioritization factor, or prioritization factors of the same type are being considered, no scaling procedure may be necessary. However, if multiple prioritization factors, or factors of a different type are being considered that must represent equal weights, then scaling within a range will be necessary. Using a linear scaling model, the results of each prioritization factor can be scaled within some range. This example will use the range 0 to 1, with 1 being the highest priority.

If $P\min = 11$, and $P\max = 18$, $Scale\min = 0$ and $Scale\max = 1$, the following formula for scaling can be used:

$$f(x) = Scale\min(1 - \frac{x - P\min}{P\max - P\min}) + Scale\max(\frac{x - P\min}{P\max - P\min})$$

Because the chosen scale is 0 to 1, the formula reduces to: $f(x) = (x - 11/18 - 11)$, or CEM=0 and Drugs=1. Each independent prioritization factor should be scaled to the same scale before comparing with other factors.

The prior example can be expanded by considering the crime's associated fine or length of sentence. In this case using a priority measure based on the priority order of the severity of sentencing.

There must also be some consideration whether such a prioritization factor should be equal to the weight of one stakeholder, or the group of stakeholders. In this work, it will be equal to the weight of all stakeholders, therefore scaling of each independent prioritization factor is necessary. Scaling, as discussed, will be denoted as $scale()$. After scaling, the overall maximum priority is equal to a factor's maximum priority multiplied by the number of independent prioritization factors.

Using the prior example, if the sentencing priority (sp) for CEM and Drugs is 6 and 3, respectively where 9 is the highest priority and 1 is the lowest priority, then the priority (P) of the i-th crime category can be written as:
$P(i) = scale((pp[i] * .5) + (dp[i]) + (hp[i] * 1.5)) + scale(sp(i))$

Note that if two independent prioritization factors with a $P\max$ of 1. Overall maximum priority equals $P\max \cdot factors$.
Assume: $sp = [6, 3]$, then
CEM $= P(1) = (0 + 0.625) = 0.625$
Drugs $= P(2) = (1 + 0.25) = 1.25$

3.3.1 Example Prioritization Formulas

The following is a list of example prioritization formulas not including time, followed by an example of how each prioritization model would change the priority of different cases.
Case priority with only unweighted stakeholders:
$P_1(i) = ((pp[i]) + (dp[i]) + (hp[i]))$
Case priority with only weighted stakeholders:
$P_2(i) = ((pp[i] * pp^m) + (dp[i] * dp^m) + (hp[i] * hp^m))$
Case priority with only sentencing:
$P_3(i) = (sp[i])$
Case priority with sentencing same base weight as each weighted stakeholder:
$P_4(i) = ((pp[i] * pp^m) + (dp[i] * dp^m) + (hp[i] * hp^m) + (sp[i]))$
Case priority with sentencing same weight as combined stakeholders:
$P_5(i) = scale((pp[i] * pp^m) + (dp[i] * dp^m) + (hp[i] * hp^m)) + scale(sp[i])$
Case priority with stakeholders and risk modifier:
$P_6(i, rm) = scale((pp[i] * pp^m) + (dp[i] * dp^m) + (hp[i] * hp^m)) + scale(rm)$
Case priority with stakeholders, sentencing and risk modifier:
$P_7(i, rm) = scale((pp[i] * pp^m) + (dp[i] * dp^m) + (hp[i] * hp^m)) + scale(sp[i]) + scale(rm)$

P	Priority of $i = 3$ (0 to 1 scale)
P_1	1.00
P_2	0.60
P_3	1.00
P_4	0.81
P_5	0.62
P_6	0.36
P_7	0.53

Table 1 Priority of $i = 3$ for each previously given formula

Notice, scaling is only necessary when comparing independent prioritization factors, however, all results below will be scaled to a 0 to 1 scale for consistency and comparison.

Consider the following example:

- $pp[i] = [1, 4, 9]$, scale 1 to 9
- $dp[i] = [3, 6, 4]$, scale 1 to 9
- $hp[i] = [3, 8, 5]$, scale 1 to 9
- $sp[i] = [5, 4, 6]$, scale 1 to 9
- $rm = (1, 1, 2)$, scale 1 to 10

Assume $i = 3$. As shown in Table 1, consideration of multiple prioritization variables can greatly affect the associated priority value for a given case type. When to scale is an important consideration. For example, if each stakeholders priority measure was scaled before comparing, the overall priority measure for P_1 would be lower.

One final consideration are circumstances where a case that has yet to be assigned, takes priority over cases that are already assigned. In a normal case queue, it is not usually desirable for newly assigned cases to be prioritized over cases in progress. To avoid this situation, a priority buffer can be used that is priority added to cases in-progress. In this work, the priority buffer (P^{buff}) will be equal to the maximum possible priority. In the prior example, the maximum possible priority is 1, therefore $P^{\text{buff}} = 1$. The priority of the case then would be calculated as $P + P^{\text{buff}}$, which will always be greater than the maximum value of P.

Consider again P_7. In this case the risk modifier is used to increase the priority of the case, but the priority will be limited to a maximum of 1. This happens when all prioritization measures associated with P_7 are scaled together. However, if kept independent, the risk modifier could be used to dictate when cases with particular risks should be prioritized over cases in progress. The resulting formula is given below (P_8).

$P_8(i, rm) = scale(scale((pp[i] * pp^m) + (dp[i] * dp^m) + (hp[i] * hp^m)) + scale(sp[i])) + scale(rm)$

If case A has a priority of 0.9, and is assigned to an investigator, it's priority measure becomes $0.9 + 1 = 1.9$. Assuming case B is the highest priority (1.0), and there is also a risk to life which is the highest risk modifier (1.0) then the unassigned priority of case B is above the assigned priority of case A. Once case B has been assigned, then it's priority is effectively 3.0, the $P + rm$ value should be rescaled for all assigned cases, adding P^{buff} again after scaling is complete. This will reduce the priority of already assigned cases to accommodate the newly assigned priority case while ensuring that cases with little or no associated risk do not get prioritized above cases already in progress. When risk modifiers are implemented in this way, they should be carefully planned and rarely used to ensure new cases are not constantly being prioritized over already assigned cases.

A practical implementation of these ideas is best described with a real-world example.

4. EXAMPLE CASE

The following example case illustrates the proposed case prioritization method. Defined general case categories are based on the Irish computer crime categorization, as follows:

- Murder
- Child Abuse/Exploitation
- Organized Crime

Crime Category	Average ranking (1 to 9)	Rank Order (1 to 9)
Adult Abuse/Exploitation	4.96	5
Child Abuse/Exploitation	7.13	8
Drugs	3.91	4
Fraud	3.83	3
Hacking/Intellectual Property Crime	3.03	1
Murder	7.16	9
Organized Crime	5.94	7
Terrorism	5.84	6
Theft/Damage to Property	3.21	2

Table 2 Crime category priority ranking based on a survey of the Irish public, where 1 is the lowest priority and 9 is the highest priority

Crime Category	Average ranking (1 to 9)	Rank Order (1 to 9)
Adult Abuse/Exploitation	3.34	5
Child Abuse/Exploitation	4.79	7
Drugs	2.48	3
Fraud	2.0	1
Hacking/Intellectual Property Crime	3.07	4
Murder	6.28	8
Organized Crime	4.45	6
Terrorism	6.79	9
Theft/Damage to Property	2.21	2

Table 3 Crime category priority ranking based on a survey of the Korean public, where 1 is the lowest priority and 9 is the highest priority

- Terrorism
- Adult Abuse/Exploitation
- Drugs
- Fraud
- Theft/Damage to Property
- Hacking/Intellectual Property Crime

Once general crime categories were defined, a survey of the public was conducted concerning the preferred investigation priority of each crime category, resulting in 119 responses[2]. The majority of the responses were from Ireland and South Korea, with the rest of Europe, North America and the Middle East represented as a minority.

Table 2 and Table 3 show that while lower-priority case types are largely the same between Ireland and South Korea, top-priority case types are somewhat different between the countries. For example, Ireland prioritizing Murder and Child Exploitation, and Korea prioritizing Terrorism and Murder.

[2]Survey questions and results can be found at http://digitalFIRE.ucd.ie

Crime Category	Public Rank Order	Law Enforcement Rank Order
Adult Abuse/Exploitation	5	4
Child Abuse/Exploitation	7	7
Drugs	2	5
Fraud	1	2
Hacking/Intellectual Property Crime	4	3
Murder	8	8
Organized Crime	6	6
Terrorism	9	9
Theft/Damage to Property	3	1

Table 4 Crime category priority ranking based on a survey of the Korean public and Law Enforcement stakeholders, where 1 is the lowest priority and 9 is the highest priority

This example, however, will consider two stakeholders from the Korean case: the public and Law Enforcement. From the survey, 16 respondents categorized themselves as non-Law Enforcement, and 13 respondents categorized themselves as Law Enforcement. Each stakeholders priority ranking is given in Table 4. In this case Law Enforcement prioritization does not reflect the actual priority of any organization, but only the respondents personal opinion.

Table 4 shows that both the public and Law Enforcement agree on the type and order of the top 4 priority areas – Terrorism, Murder, Child Abuse/Exploitation and Organized Crime – but begin to diverge with lower-priority areas. A reason for this could be that the public perceives more risk in certain categories, such as hacking, whereas LE observe more risk in certain areas, such as Drugs. In this example, the observation of LE will carry only a slightly higher weight than the perception of the public, where $pp^m = 0.8$.

There is now enough information to prioritize cases in a queue based on these two stakeholders, however, it may also be useful to integrate punishment severity. In this case crime types with a more severe punishment are prioritized over cases with little or no punishment.

In this case one act per category was selected from Korean legislation to use for ordering.

Assuming we are considering three prioritzation factors – public, LE and legislation – priority of each case type can be calculated as so:

- Public: $pp = [5, 7, 2, 1, 4, 8, 6, 9, 3]$
- Public weight modifier: $pp^m = 0.8$

Crime Category	Punishment	Rank Order
Adult Abuse/Exploitation	(Production of images against will) 5 years[3]	3
Child Abuse/Exploitation	(CEM production) 5 years[4]	3
Drugs	(Usage) 10 years[5]	7
Fraud	(Computer fraud) 10 years[6]	7
Hacking/Intellectual Property Crime	(Intrusion) 3 years[7]	1
Murder	(Murder) life/death[8]	9
Organized Crime	(Organizes) life/death[9]	9
Terrorism	(financing) 10 years[10]	7
Theft/Damage to Property	(theft) 6 years[11]	4

Table 5 Crime category priority ranking based on a survey of Korean Law, where 1 is the lowest priority and 9 is the highest priority. Where the punishment was the same, the same priority was given.

Crime Category	Priority (0 to 1)	Rank Order (1 to 9)
Adult Abuse/Exploitation	0.32	3
Child Abuse/Exploitation	0.49	5
Drugs	0.52	6
Fraud	0.38	4
Hacking/Intellectual Property Crime	0.13	1
Murder	0.94	9
Organized Crime	0.80	7
Terrorism	0.88	8
Theft/Damage to Property	0.21	2

Table 6 Crime category priority ranking where the priority is calculated using identified priorities from multiple stakeholders and rank order is the order of priority where 9 is the highest priority and 1 is the lowest priority.

- LE: $dp = [4, 7, 5, 2, 3, 8, 6, 9, 1]$
- Legislation: $sp = [3, 3, 7, 7, 1, 9, 9, 7, 4]$

$P(i) = scale(scale((pp[i] * pp^m) + (dp[i] * dp^m)) + scale(sp[i]))$

The results of prioritization for each category using this formula are given in Table 6.

While this example determines priority case categories based on the input of multiple stakeholders, specific cases can now be prioritized by considering specific risks, as well as request times associated with the case to further sort individual cases.

4.1 Discussion

This study has shown that different stakeholders may have different opinions about crime priorities, and that the opinions of other groups cannot be assumed. By looking at different countries (Table 2 & Table 3), or stakeholder groups within countries (Table 4) the difference in opinion of crime priorities can be identified. Prioritization, however, can consider more that just the opinions of stakeholders. By considering legislation within Korea, it is shown that the priorities of stakeholders do not necessarily reflect priorities in legislation in terms of severity of punishment. For example, while both the Korean public and LE identified terrorism as the highest priority, if legislation is also considered (based on the small sample of laws) then murder becomes the highest priority. Also, while the Korean public and LE ranked child abuse as the third highest priority, the legislation does not reflect this, bringing the priority of such crimes lower in favor of higher-punishment crimes such as drugs, and even fraud (which as ranked very low by stakeholders).

The example case was not comprehensive, but gives a general idea of how real-world data can provide a base for understanding the needs and wants of particular organizations and cultures. Now that a basic formula has been provided, organizations can begin to identify potential prioritization factors that are relevant to them, and more objectively classify the priority of incoming cases.

4.2 Weaknesses

Just like crime classification, case prioritization is inherently subjective. The proposed method attempts to formalize prioritization based on multiple priority opinions, however, a purely objective prioritization is impossible without eliminating things like stakeholder opinion weights. Such subjective weightings, however, are necessary for a practical implementation. Allowing this subjectivity, however, allows for unfair model creation. For example, the person creating the prioritization model may weigh their department's opinions so far above other stakeholders that other opinions become negligible. However, even in these cases there are at least two benefits. First, the prioritization process is defined and is audit-able, where normally no definition would exist. Second, even if the creator of the model is unfair to other stakeholders, they still receive benefit from a more formalized prioritization model that ensures cases are more effectively assigned needed resources.

The model also attempts to help reduce the number of cases that are prioritized over the currently-assigned queue. The model, however, cannot stop high-ranking officials from forcing cases to jump the queue. If the case manager cannot, or will not, force case requests through the model, then this situation will not be helped. However, by implementing the proposed model, a laboratory can better estimate the time for case completion for all requests. If the laboratory is transparent in its case prioritization model (and current queue), then the entire organization will be able to see when high-ranking officials are delaying their case requests. This will offset reputational risk away from the laboratory. If the reputational risk is transferred to high-ranking officials, they may be less willing to jump the queue, improving the overall process.

Finally, this work assumes a laboratory provides a defined set of services to defined stakeholders. In those cases, regardless of business sector, there will be a priority of one type of case over another. However, if another department either offers a different service or caters to different stakeholders, a model specific to that department will need to be created. There is a certain level of abstraction that can be built into the model (general organizational level), but at a practical level each department may need to identify their own specific prioritization model.

5. CONCLUSIONS

While many works are focusing on helping the investigator to make conclusions more efficiently, many organizations have challenges with case management that can cause delays and inefficiencies in investigations regardless of the process implemented. While some works, such as the APF's CCPM, have already identified various factors for considering how to handle incoming cases, little work has been done on formalizing the prioritization of such factors, including measurement, weighting and comparison. This work has proposed a method for identifying and measuring the priority of factors based on the input from multiple stakeholders that can directly be used for calculating the priority of incoming cases based on an organization's specific needs. Such work can help laboratories to better understand and integrate the expectations of other stakeholders (such as high-ranking officials and the general public) into their investigation work flow.

5.1 Future Work

While a well defined case prioritization model may help in managing the queuing of cases to be investigated, case prioritization may be neglected once a case has been assigned to one or more investigators who may be working multiple cases at the same time. In situations such as these, a quantitative approach to resource allocation may help to ensure that priority of cases is fairly considered and maintained between all assigned cases, not just the pre-assignment queue. Future work will examine formal models for resource allocation for already assigned cases.

REFERENCES

Australian Federal Police. (2010). *Crime Categorisation and Prioritisation Model* (No. May).

Casey, E., Ferraro, M., & Nguyen, L. (2009). Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence. *Journal of forensic sciences*, *54*(6), 1353–1364. doi: 10.1111/j.1556-4029.2009.01150.x

Casey, E., Katz, G., & Lewthwaite, J. (2013, September). Honing digital forensic processes. *Digital Investigation*, *10*(2), 138–147. doi: 10.1016/j.diin.2013.07.002

Douglas, J., Burgess, A. W., Burgess, A. G., & Ressler, R. K. (2013). *Crime Classification Manual: A Standard System for Investigating and Classifying Violent Crime* (3rd ed.). John Wiley & Sons Inc.

FBI. (n.d.). *FBI - What We Investigate.* Retrieved 8 Dec. 2013, from `http://www.fbi.gov/about-us/investigate`

Fife, R. E. (2010). Criteria for Prosecution of International Crimes: The Importance for States and the International Community of the Quality of the Criminal Justice Process for Atrocities, in Particular of the Exercise of Fundamental Discretion by Key Justice Actors. In M. Bergsmo (Ed.), *Criteria for prioritizing and selecting core international crimes cases* (2nd ed., pp. 15–25). Olso: Torkel Opsahl Academic EPublisher.

Garfinkel, S. L. (2006, September). Forensic feature extraction and cross-drive analysis. *Digital Investigation*, *3*, 71–81. doi: 10.1016/j.diin.2006.06.007

Ghernaouti, S. (2013). *Cyber Power: Crime, Conflict and Security in Cyberspace* (1st ed.). EFPL Press.

Gogolin, G. (2010). The Digital Crime Tsunami. *Digital Investigation*, *7*(1-2), 3–8. doi: 10.1016/j.diin.2010.07.001

Hancocks, P. (2012). *7-year-old girl abducted and raped in South Korea, police say.*

James, J. I., & Gladyshev, P. (2013, September). A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. *Digital Investigation*, *10*(2), 148–157. doi: 10.1016/j.diin.2013.04.005

Jones, A., & Valli, C. (2011). *Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility.* Butterworth-Heinemann, Elsevier Inc.

Koopmans, M. B., & James, J. I. (2013, April). Automated network triage. *Digital Investigation*, 1–9. doi: 10.1016/j.diin.2013.03.002

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, E. (2014). *Comprehensive Study on Cybercrime* (Tech. Rep. No. February). United Nations Office on Drugs and Crime (UNODC).

Ortmeier, P., & Davis, J. J. (2012). *Police Administration: A Leadership Approach.* McGraw-Hill.

Rauscher, K. F., & Yaschenko, V. (2011). *The Russia-US Bilateral on Cybersecurity - Critical Terminology Foundations* (Tech. Rep.). East West Institute.

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law*, *1*(2), 27–40. doi: 10.1.1.169.1878

Rowe, N. C. (2014). Identifying forensically uninteresting files using a large corpus. In *Digital forensics and cyber crime.* Springer.

Shaw, A., & Browne, A. (2013, April). A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. *Digital Investigation*, 1–13. doi: 10.1016/j.diin.2013.04.003

US Department of Justice. (2013). *Smart on Crime: Reforming the Criminal Justice System for the 21st Century* (Tech. Rep.). US Department of Justice.

