Technical Report:

A preliminary Process Model for Investigation

Stig Andersen

Special Investigator / PhD Researcher

Oslo Police District / NTNU *

May 2019

Abstract

Criminal investigation is an important part of most law enforcement organisations and a vital part of policing and crime-fighting. Yet it is among the least researched topics in police science. Other types of investigations are performed using the same overall methodology, but within different jurisdictions and with different objectives. Experience suggests that there is room for trans-organisational and inter-subject learning between various organisations performing investigations, and the miscellaneous fields of investigation and forensics. This document describes a preliminary investigation process model designed to be applicable in all situations where a systematic examination or study is performed. The model is based on previous work by contemporary scholars and shares similarities with Fahsing's "6 Cs" circular model. Descriptive Business Process Model and Notation 2.0 (BPMN 2.0) is used to visualise the process. The objectives are to express, detail and visualise the various investigation actions and the relationship between them, thus contributing to a greater understanding of the investigation process. The model also provides a framework on which further research can be conducted in this multi-disciplinary field.

Keywords— Investigation, Process model, Forensics, Crime

*Funded by the Norwegian Research Council and Oslo Police District.

Contents

List of Figures

1 Introduction

Criminal investigation is recognised as a process of collecting, processing and presenting information in order to explain the circumstances of a possible crime [12, 30]. The circumstances of an incident are the what, where, when, who, why and how (5WH) of the incident. In order to arrive at an explanation of the incident, investigators must explore the various possible explanations of the event [32]. These various explanations form the different hypotheses of the incident [6] and are sometimes called lines of enquiry. Though criminal investigation is the least researched topic within police science [19], there are a few different models describing how investigation is performed. Fahsing [6] describes investigation as a cyclic process of information collection and hypothesis testing 5WH. His model includes hypothesis-developing steps, but does not show the beginning and the end of an investigation. Nor does it show the relationship between an investigation and the required surrounding activities of incident detection, reactions (e.g. court proceedings) and overall case management. College of Policing in the UK on the other hand adopts a more practical and comprehensive model [4]. They describe various actions in greater detail, and show how a criminal investigation is initiated, conducted and disposed of or transferred to court proceedings. It does not, however, describe investigation in terms of hypothesis testing beyond mentioning how "all reasonable lines of enquiry" should be pursued as dictated by the UK Code of Practice to the Criminal Procedure and Investigations Act 1996.

Studies in the USA in the 60s and 70s concluded that most crimes are solved by patrol officers and the general public [19], and studies from the UK in the 1970s and 1980s showed that information from witnesses is the most significant source of crime solving data [12]. Further more, legal scholars in Norway claim that interviews are the most important source of evidence in criminal investigations [27, 1]. However, while information from people involved with or witnessing a crime obviously contribute vital information to an investigation, information from physical and digital sources is playing an increasingly important role through a criminal case. This increased variety of information and data sources is challenging established norms on how criminal investigation is performed and understood.

Research conducted over the past 10-15 years in both policing and digital forensics points to the hypothetico-deductive model as a methodical standard which investigation should strive to adhere to [6, 24, 3]. This corresponds to Poppers description of the methods of the empirical sciences [23], and to Platt's observations which lead to his "Strong Inference"-model [20]. And both the National Police Directorate and the director of public prosecutions in Norway supports this approach to criminal investigation [21, 26]. The hypothesis driven investigation is also how criminal investigation is currently being taught at the Norwegian Police University College [22].

This document describes a general investigation process model developed based on the hypothetico-deductive model. Though developed from a criminal investigation stand point, this model is applicable in all situations where a systematic examination or study is performed. The objectives are to express, detail and visualise the explicit and implicit

actions of an investigation, the relationship between them, and how investigation relates to surrounding processes. This will contribute to a greater understanding of the investigation process, and provide a framework on which further research can be conducted in this multi-disciplinary field. Descriptive Business Process Model and Notation 2.0 (BPMN 2.0) is used to visualise the process and the text is structured as follows: Section 2 described what a criminal case is and delineates the different parts of a case, including the relationship between crime detection, investigation and prosecution. Section 3 presents the criminal investigation process and describes each step of the process in greater detail. A brief discussion on the implications and use of the process model is offered in section 5, before section 6 outlines possible future research.

2 Criminal case process model

A crime is that which violates criminal law. A criminal case is an incident, or a series of related incidents, and the associated set of circumstances, which constitute a violation of a law. *When* something becomes a crime, for example at what point in time a planned robbery becomes a crime, is a legal matter outside the scope of this text. It is sufficient to recognize that some incidents are crimes, and while these incidents are being processed by the justice system, they constitute a criminal case. Figure 1 shows a general outline of the process a criminal case follows through a justice system. As the figure shows, after an incident has occurred, it must first be detect and identify as a possible crime before investigation begins. If it is found that the incident might constitute a crime[1], a criminal investigation is initiated. The goal of the investigation is to gather sufficient information to determine if anyone can and should be indicted for the crime, and if so, prepare the case for prosecution. The prosecution process might involve several steps including multiple appeals. For a criminal case to be considered completed or solved, it must either be dismissed, or the prosecution process has to end in acquittal, an enforceable verdict or a recognised alternative legal reaction. Each incident which follows this process, i.e. each instance of the process, is called a criminal case.

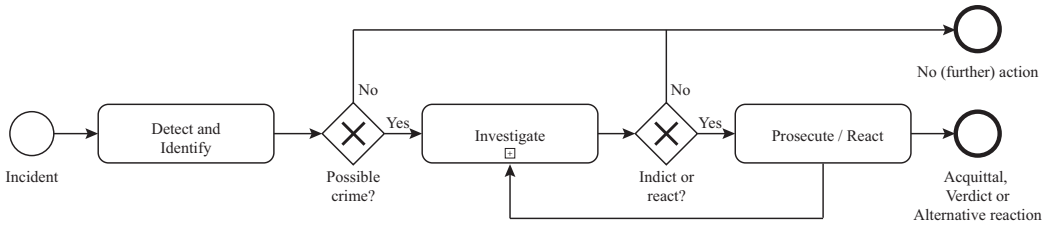

Figure 1: Criminal case process model

[1]Some law enforcement organisations are also tasked with investigating incidents that are not crimes. Such incidents follow the same process but are not subject to prosecution but rather to a different post-investigation treatment.

The first step, *detection and identification*, generally involves an incident being observed by or reported to the police. It is based on the initial information provided in this process that the decision to initiate an investigation or not (the *Possible crime?* gateway) is taken. The last step, *Prosecute / React*, involves court hearings and other resolutions outside the courts, e.g. by the perpetrator accepting to pay a fine. The details of these process steps are outside the scope of this text.

3 Criminal investigation process model

Criminal investigation is performed to determine if a crime has occurred, and to discover, describe, and document sufficient information about the incident. Sufficient information means information which accurately and adequately explains the circumstances of the incident. There are six circumstances to an incident. They are the what, where, when, who, why and how (5WH) of the incident [12, 30, 6]. The information collected to describe these must be of such quality, and collected under such circumstances, that they can prove the incident beyond reasonable doubt in a criminal court [2, 12, 33, 5]. In some jurisdictions, a criminal investigation might also be required to collect other information related to the resolution of the case [30, 25].

Research suggests that for an investigation to be thorough and objective, all the possible hypotheses that might explain the incident should be identified and tested. This should ensure that the investigation arrives at the most probable explanation [6]. This approach is equal to the scientific method [23, 20, 11] and can be described as a process in four steps:

1. Formulate possible hypotheses that can explain the incident
2. Identify what information is required to evaluate the hypotheses
3. Collect data that can inform these hypotheses
4. Evaluate each hypothesis in light of the collected information

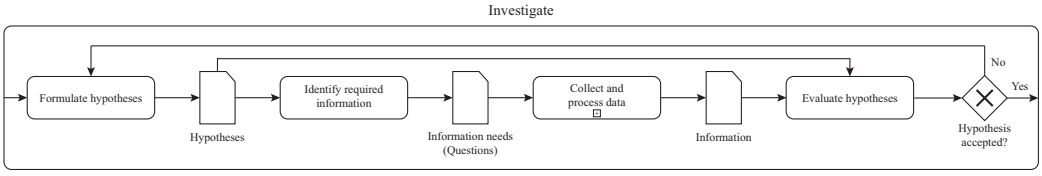

Figure 2: Criminal investigation process model

Figure 2 shows a visual layout of these four process steps and how they relate to each other. The third step is further divided into four steps as shown in figure 3:

1. Identify, locate and gain access to/control over sources of possibly relevant data

2. Acquire human or digital data, or physical traces from a data source

3. Explore and examine the data/traces to identify what data/which traces might be relevant (significant data)

4. Extract or generate information from the possibly relevant data/traces

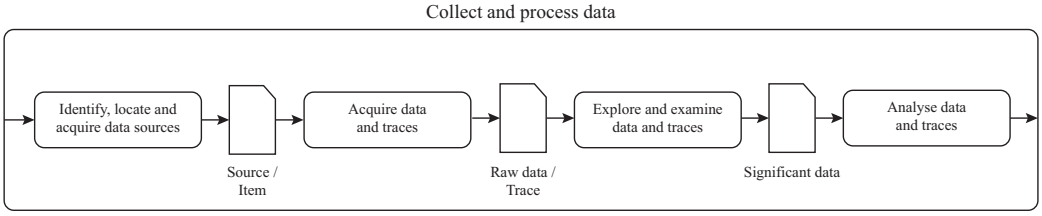

Figure 3: Data collection and processing process model

The criminal investigation process forms a conditionally, continuously and loosely coupled looping process of hypothesis development and data processing. This means that the investigation process continues until the case is resolved[2]. Also, a series of data collection and processing actions can be initiated for each information requirement, and each data collection and processing action can result in information relevant to several hypotheses.

Note that the transition between each process steps might appear from the model as something which happens explicitly and that each step is time consuming and complex. While this might be true in some instances, it is not necessarily so. Several process steps, at all levels of the model, can occur implicitly in an investigators mind within seconds. In fact, it is probably impossible for a human to become aware of an incident without immediately constructing and evaluating at least one hypothesis about how it came to be.

Investigation is performed by an investigator, data collection and processing is performed by a subject expert. A subject expert is a person with the necessary knowledge and skills to gather, process and interpret data from a data source. This means that an individual can be both an investigator and a subject expert. Whether a person can hold and perform an activity depends on his or her competence. For instance, a person with the competency to perform investigative interviews is an investigative interview subject expert. A person competent to perform autopsies is a medical forensic subject expert. Both can also be an investigator, and an individual can hold all three competencies. What is important is that data must be collected and processed with such confidence and quality that the resulting information can be presented as evidence in a court of law.

[2]A case is resolved when it reaches one of the two end states, see figure 1. Case resolution is also described in section 2.

3.1 Investigation

As mentioned above, investigation involves formulating possible explanations to the incident, identify what information is required to evaluate these hypotheses, collect data which can inform these hypotheses, and finally evaluate the information provided by the data and determine how the information supports or weakens each hypothesis. The following sections describe each part in greater detail.

3.1.1 Formulate hypotheses

The first step of an investigation is to formulate, i.e. express in precise and simple terms, the possible and reasonable[3] hypotheses that can explain the incident. Compared to the scientific method, this first step is equivalent to statement construction [23] or "Devising alternative hypotheses" [20, p.347].

Both hypotheses which imply that the incident was a crime, and hypotheses which explains the incident as not criminal, must be identified. For a hypothesis to be complete it must include all of the six circumstances (5WH) . Some information is always available from the *detection and identification* process step (see figure 1). This initial information is used to formulate the first hypotheses. The initial hypotheses should focus on *what* the incident was, and *where* and *when* it took place. Once more information is available, further details are added to the hypotheses based on this new information. Such hypothesis development can involve formulating new hypotheses, adding details about *who*, *how* or *why* the incident occurred to existing hypotheses, or formulating sub-hypotheses. A sub-hypothesis is a variation of a main hypothesis such that some key details are equal to all the sub-hypotheses while other details vary. Eventually, given that enough information can be collected, one hypothesis will emerge as sufficiently informed to adequately explain the incident thus providing the means to resolve the case.

3.1.2 Identify required information

After formulating the hypotheses, the information that is required to evaluate them must be identified. One way to perform this step is to formulate questions based on what information is missing for each hypothesis. The purpose of this process step is not to predict all the information to be found during data collection. That would be prediction or possibly prophesy. Rather, this step directs the collection of data such that all aspects of the incident, i.e all hypotheses, are covered. Compared to the scientific method, this corresponds to the second step as described by Platt [20, p. 347]:

> Devising a crucial experiment (or several of them), with alternative possible outcomes, each of which will, as a nearly as possible, exclude one or more of the hypotheses

[3] Reasonable in this instance means that supernatural explanations like murderous unicorns and alien abductions are excluded.

Investigations rarely include experiments in the same way as scientific research does. The gist of this step, though, is to determine and plan for the collection of data which is suitable to ”exclude one or more of the hypotheses”. This corresponds to the planning of data collection and processing actions, e.g. interviews, crime scene investigations and forensic examinations, which are performed as part of an investigation.

Some data collection actions could potentially yield a lot of obviously irrelevant information. For instance, gathering data about a witness' entire life when the incident being investigated is a possible theft which took place within the last 24 hours is probably out of scope. However, the fact that the owner of the lost property suffers from amnesia could be very relevant. Hence, care must be taken to ensure that the investigation covers the appropriate scope. This process step aids in that regard.

3.1.3 Collect and process data

The key to any investigation is information, and information is constructed from data. Figure 3 shows the process of how data is collected and processed, and the details are described in section 3.2. This section describes data, metadata and information in general, and how the *Collect and process data* process step relates to the other investigation steps.

Information are facts related to the incident being investigated and is constructed from data. Data are ”raw facts” as they are stored in, or transmitted from, a data sources. Data can also be extracted from physical items or traces. Information is constructed by interpreting data in relation to the incident being investigated. The facts used to perform this interpretation is a form of metadata. Information can thus be defined as:

$$Information = Data + Metadata$$

Hence, to get the information required to solve a criminal case, data must be acquired from various data sources. It must be examined and analysed before it can be used to determine which hypothesis is the one most likely to accurately describe and explain the incident(s) of the case. Though far from all data collection and processing steps involves experiments as described above, this step corresponds to observation [23] - the third step of the scientific model [20, p. 347]: “Carrying out the experiment so as to get a clean result”. In other words: Collect and process data to get as objective and relevant information as possible.

The information constructed from Data changes depending on the corresponding metadata. Similarly, the reliability and validity of data can change with attributes of the data source and of the methods used to process the data. From the field of witness psychology, for instance, it is well known that a person can ”recall false facts” as if they were true. This is a risk associated with the human mind and it does not appear in, for instance, digital sources. If, for example, an incident involves a perpetrator dressed as a clown drive away in a green car at 19:32 CET. A witness might supply the following statement: “The perpetrator was dressed as a clown and drove away in a red car.” The witness believes he is speaking the truth, because that is how he remembers it. A video recording of the same event shows a person dressed as a clown walking to a green car and drive away at 18:32.

The video recording data accurately depicts the person and the car, but the time appears to be wrong, suggesting that the data was extracted without time zone information. In effect, the two pieces of data provides information about the same incident, but neither one of them provides a perfect representation of the incident.

This example shows how different inherent risks are associated with different data sources. There are several different ways of classifying data sources. One is by observing where the information is held. This provides three categories of data sources: Human sources, physical sources and digital sources. A human data sources is, in short, the human mind. Cognitive psychology describes how we receive input via the five senses, store this information in memory, and retrieve, act and communicate based this information [9]. A physical source is anything made up of or containing a physical substance or material. This includes all physical items and locations in physical space like a house, a piece of clothing, a corpse or a box. Physical data often takes the form of traces. A fingerprint, epithelial cells or blood spatter are examples of traces that can be acquired. Digital sources are things that can hold digital data like magnetic, optical or solid state storage devices. Digital network communication systems or devices can also be a source of digital data.

Each type of data source contains or produces data of its respective type. Thus, acquiring data from a human data source results in human data, physical data sources results in physical data and digital data sources results in digital data. Each data type can be classified further in multiple ways, but this root classification is sufficient for the purposes of this text. Though data in general is objective and neutral, the different ways in which data can be acquired, examined and analysed depends on the data source. For instance, since no dependable and comprehensive method of mind reading exists, communication through verbal, written, or other nonverbal means is the only way we have of acquiring data from a human data source. Studies on witness psychology and various interview techniques has shown that the reliability and validity of human data varies greatly, both depending on the source it self and the methods used to acquire the data [16, 24, 17]. This affects the level of confidence that can be placed in data acquired from human sources. It also places strict requirements on how human data is acquired, examined and analysed, and how the resulting information is evaluated.

Similar to the issues described with human data, there are a variety of different issues associated with physical and digital data. For instance, a 2016 study shows that identifications based on bite marks are unreliable and unscientific [29]. And studies on the Mayfield-case shows that fingerprint experts, forensic methodology and forensic scientists in general are subject to confirmation bias, which can lead to faulty analysis of data [34, 14]. All these different issues must be treated as risks to the reliability and validity of both data, metadata and the information processed in an investigation. These risks must be understood and they must be treated correctly at the appropriate stage in order for the investigation and the case to reach the required level of quality.

3.1.4 Evaluate hypotheses

Once information has been collected, the significance of each fact and the combined implication of all the available information is evaluated against all the hypotheses. This is done by determining how and if each fact supports or weakens each hypothesis. To accurately perform this task the collected information must be interpreted and understood, then applied through logical and deliberate reasoning to each hypothesis. This mental process requires operations of what Stanovich and West, according to Kahneman [13], describes as System 2 cognitive processes.

We can deduce two key requirements to performing this task:

1. Information interpretation competency
2. Information availability

The information interpretation competency requirement means that the information generated from the collected data must be considered by a person with sufficient knowledge and skill to understand what the information means. This person must also be competent to understand and assess the implications of the information when it is applied to the various hypotheses. This might sound obvious, but as Bloom's taxonomy suggests; knowledge, comprehension and application competency is required before a person is able to analyse and evaluate something [15]. For instance, a timestamp collected from a message sent via an instant messaging service might have different implications when applied to two different hypotheses. The person evaluating this information in reference to the various hypotheses must be able to understand the message-data and the timestamp-data, and to assess the significance of the information in relation to the various hypotheses.

The information availability requirement means that the person performing the evaluation must be aware of and have access to all other information of relevance [4]. The implications of some information can change dramatically when considered together with other information. If the person evaluating the various information and hypotheses "can't see the whole picture", errors can easily occur.

Situations where these requirements are not met result in an increased information interpretation and -availability risk (IIAR). This risk is an expression of how a possible error lies with the interpretation of or access to information, rather than with the actual execution of the evaluation. The latter is a hypothesis evaluation risk (HER). This risk stems from judgment errors when performing the hypothesis evaluation. Performing such a task involves making judgments based on available information. When performed based on impressions rather than deliberate reasoning, such mental work is subject to a number of risky heuristics like availability bias, confirmation bias, affect heuristic and tunnel vision [13, 10, 6]. As mentioned above, studies have shown how such risks can impact criminal investigations [34, 14, 31]. Consequently, investigators need to apply logical and deliberate reasoning when performing this process step. Note that the risk of data error,

[4] Note that this requirement goes beyond the basic requirement that the information must exist in the first place.

i.e. that the data constituting the information is wrong, is not a part of this process step. Such errors are inherited from the data collection and processing steps. Hence, problems with bad data cannot be corrected during hypothesis evaluation.

3.1.5 Hypothesis accepted?

When all the hypotheses have been updated according to the collected information, a decision is made on whether or not one of the hypotheses have sufficient support (i.e. enough information) to adequately explain the incident beyond reasonable doubt. If not, further investigation is required. If one of the hypotheses does have sufficient support the case moves on, see figure 1. As mentioned above, this decision is performed in much the same way as hypothesis evaluation (see section 3.1.4). However, the objective is different. The goal of the *Evaluate hypotheses* step is to connect all the various information and consider how this affects the various hypotheses. The objective of the *Hypothesis accepted?*-step is to determine if any one of the hypotheses is sufficiently informed. In simple terms: *Is the investigation finished?* In the scientific method, this step - together with parts of the third and first step - is known as re-testing [23], or "Recycling the procedure, making subhypotheses or sequential hypotheses to refine the possibilities that remain" [20, p. 347].

3.2 Data collection and processing

As described by other scholars before [12, 30, 6] and detailed in section 3.1.3, investigations are solved with information and information is generated from data. The goal of the *Collect and process data* process is to gather data from various sources, and process this data into information which informs the hypotheses of the investigation. This key part of an investigation is divided into four process steps (see figure 3):

1. Identify, locate and acquire available and relevant data sources, including physical items
2. Acquire human and digital data, as well as physical data and traces
3. Explore and examine the acquired data to identify significant data
4. Analyse the significant data and traces to generate relevant information

The following sections describe these steps in greater detail.

3.2.1 Identify, locate and acquire data source

The goal of this step is to determine who, what and where data about the incident might be located, and attain access to these data sources. In practice, this may involve finding out who might have witnessed the incident and identify their names and contact details, search for and seize physical items and traces which might be or contain data relevant to

the incident, or ascertain the user account details of social media accounts belonging to possible suspects.

3.2.2 Acquire data and traces

Acquiring data and traces involves gaining control and possession of human and digital data, for instance through communicating with a human or a digital source, and to extract and lift traces from physical objects. While data presented vocally from a person and stored in digital format is data, it can't be used practically by an investigator before it has been properly prepared. For example, data communicated by a witness to a police officer needs to be recorded as precisely and thoroughly as possible to maintain as much of it as possible. Current recommendations include audio and video recordings, and written transcripts or summaries. Similarly, digital data is stored on physical devices using a variety of different technologies and encodings. In order to process this data in a safe and secure manner such that the data isn't altered or lost, it needs to be copied from the original source to a different storage device.

3.2.3 Explore/examine data

Once data has been acquired, it can be examined. The goal is to locate data which responds to the information requirements, or might otherwise influence the investigation. Sometimes referred to as "reviewing" or "reading", data exploration and examination essentially means to locate significant data and traces, that is data of possible relevance. Note that to determine if a piece of data actually is relevant and why, further analysis might be required. For instance, while the content of the message "We'll get him" might appear obvious, the actual implication of the message could change dramatically when shown to have been exchanged between parents rather than between two people suspected of killing a man.

3.2.4 Analyze data

Significant data has to be analysed to have their relevance, reliability and validity determined. Analysis of data often involves performing various scientific examinations using appropriate forensic methods to identify, classify or quantify something [28, 7, 8], to describe and infer possible causal and historical relationships, or to assess the credibility of testimonies or statements. While several studies has found that evidence based on forensic science might not be as perfect as previously assumed [28, 31], data analysis is still an integral and necessary part of an investigation. What these studies primarily shows is that data analysis must be performed by people with the necessary competency, and that care has to be taken when evaluating the resulting information and using it as evidence.

4 Generalising the model

While the process model is described in terms of criminal investigation, it can easily be adopted and applied to any incident response situation. By making the following small adjustments to the case process model, it becomes a general, all-purpose model for investigation and incident response (see figure 4):

1. Change *Possible crime* to *Possible unwanted incident*
2. Reduce *Indict or react* to *React*
3. Change *Prosecute / React* to *Resolve / Implement Change*
4. Change *Acquittal, Verdict or Alternative reaction* to *Resolution implemented*

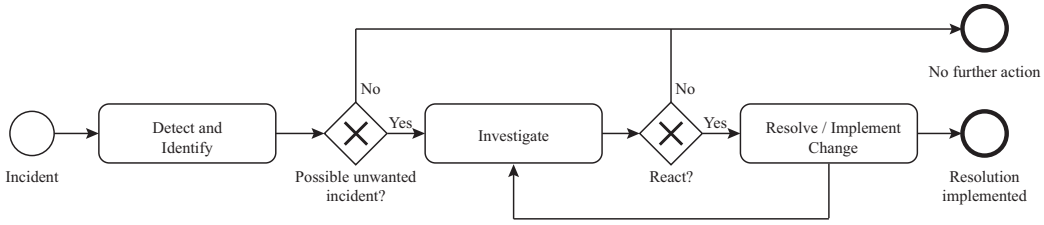

Figure 4: General case process model

No changes are necessary to the *Investigate* and *Collect and process data* processes as they are described in this text. However, different rules govern different actions depending on which context they are executed in. For instance, while law enforcement organisations often have the authority to seize and search both physical and digital data sources as part of a criminal investigation, different rules and regulations govern the authority of private and military organisations. Private or military investigations might not have the same authority to execute investigative actions without consent. This does not render the action irrelevant to the investigation or the case, but might call for a different execution.

5 Discussion

The process model for investigation described here is a development of Fahsing's "6 Cs" circular model [6], and it shares several aspects with his model. They both recognise investigation as an information-based cognitive process, much like what Innes, Stelfox and others have found [12, 30]. As such, both see cognitive bias and other cognitive risks as important factors to manage in order to ensure an acceptable level of quality. Further, both models list access to, and the ability to understand and explore information, as key requisites. However, as mentioned above, while Fahsing's model is clearly fundamentally based on a hypothetico-deductive approach, it fails to show the beginning or entry point

of an investigation, and there is no end or exit point. Nor does it provide a clear discern between the data-oriented phases, and the hypothesis-oriented phases of an investigation. This leaves little room to distinguish between the various subjects and methods employed to acquire and examine data. Without these demarcations, it is hard to describe and specify precise requirements for each method, and for each role in an investigation. The process model described here provides just such a distinction while at the same time providing a clear link between the two aforementioned phases. Also, this process model maintains the overall circular design, and it shows how investigation is a part of a larger process.

In the description of this process model, investigation is compared to the scientific method as described by Popper and Platt [23, 20]. There are some obvious similarities between investigation and the scientific method, and indeed Platt suggests that the scientific method and his method of "strong inference" might be applicable to intellectual work beyond science [20]. Hence, this text supports Platt's assertion. Though his method has been criticised for, among other things, assuming that there is (only) one scientific method [18], it is important to remember that in this model investigation only ever *follows* an incident, i.e. something which *has happened*. Hence, the problem being investigated is always of the same type (prove, describe and classify the incident). Also, all investigations of this type follow a set of predetermined rules. The objective of an incident investigation like this is to prove the incident according to the requirements of the jurisdiction within which the investigation takes place. For instance, the usual requirement in criminal cases are "beyond reasonable doubt", while civilian jurisdictions might simply require above 50% probability. Scientific endeavours, on the other hand, strive for universal or general truths which are vastly harder - probably impossible - to prove.

This model might seem too broad and general for practical application. At this stage, that is by intention. This process model is not designed for direct application. Rather, its objective is to show investigation in a broader context, and to establish that the general process and overall methodology is equal to the well known and thoroughly documented scientific method. Finally, this model provides a framework for future research on topics closely related to investigation, e.g. within forensic science.

6 Future work

Being a preliminary model, work will continue on testing and confirming the reliability and validity of the model. The applicability of the model in various contexts and jurisdictions should also be conducted. Further, the different methods for data collection and processing should be compared to the relevant parts of this model in order to validate its relevancy and suitability. As a general model it might also be appropriate to attempt to expand the model in order to make it more practical, and possibly to develop a set of checklists to support investigators and case managers in the use of this model.

Acronyms

5WH what, where, when, who, why and how. 4, 6, 8

BPMN 2.0 Business Process Model and Notation 2.0. 1, 5

HER hypothesis evaluation risk. 11

IIAR information interpretation and -availability risk. 11

Glossary

Competence Knowledge to understand a certain subject and the skills to perform a particular action. 7

Crime That which violates criminal law, i.e. an act for which someone can be punished according to law. 4, 5

Criminal case An incident, or a series of related incidents, and the associated set of circumstances, which constitute a violation of law. 4, 5, 9

Criminal investigation Systematic inquiry and examination to determine whether an incident constitutes a crime, and to sufficiently discover, describe and document the particulars of the incident in order to prepare for a legal resolution. 4–6

Data Facts observed by a human, stored in a human brain, on a physical item or on a digital storage device, or transmitted by communication. 7, 9, 12, 13

Data source Something containing data, e.g. a person, a digital storage device or a physical object. 4, 7, 9, 10, 12

Evidence Something submitted or presented to a court of law to ascertain (a part of) the truth about an incident or topic of interest. 7

Hypothesis evaluation risk (HER) Risk of erroneous evaluation of a hypothesis due to errors in judgement. 11, 16

Incident An event, something that happens. 4, 5, 8, 9

Information Data in context, i.e. data and meta-data. 4, 5, 7, 9

Information interpretation and -availability risk (IIAR) Risk of erroneous evaluation of a hypothesis due to lack of information interpretation competency or missing access to relevant information. 11, 16

Investigation Systematic inquiry or examination to determine the circumstances of an incident. 4, 5, 8

Investigator Person who formulates and develops hypotheses, evaluates information in the context of these hypotheses, and manages an investigation. 4, 7, 13

Metadata Facts about other data, e.g. the information that '112' is the common, pan-European emergency telephone number. 9

Perpetrator A person who has caused an incident. 6

Process A series of related activities or actions performed to achieve a specified goal. 1, 5

Process model A visual representation of a process. 1, 4

Relevance A measure of how or to what degree something relates to or can impact something else. 11, 13

Reliability A measure of how trustworthy or dependable something is. 13

Significant data Data which might be of relevance, i.e. impact the evaluation of one of more hypothesis, influence hypothesis formulation, provide information on a possible data source, or which might be used directly as evidence. 7, 12, 13

Subject expert a person with the necessary knowledge and skills to gather, process and interpret data from a data source with sufficient quality to present the resulting information as evidence. 7

Trace A physical substance or mark, e.g. a fingerprint, blood, epithelial, tool mark, etc. 9, 10, 13

Validity A measure of how acceptable or coherent something is. 13

Witness A person who has information about an incident. 4

References

[1] Johs. Andenæs and Tor-Geir Myhrer. *Norsk Straffeprosess*. Universitetsforlaget, 2009. ISBN: 978-82-15-01154-7.

[2] Ole Thomas Bjerknes and Ivar A Fahsing. *Etterforskning: Prinsipper, metoder og praksis*. Bergen: Fagbokforlaget, 2018. ISBN: 978-82-450-2335-0.

[3] Brian D. Carrier. "A hypothesis-based approach to digital forensic investigations". PhD thesis. Purdue University, 2006, p. 169.

[4] College of Policing. *Investigation process*. 2019. URL: https://www.app.college.police.uk/app-content/investigations/investigation-process/.

[5] European Court of Human Rights. *European Convention on Human Rights*. English. 2010. URL: http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[6] Ivar Fahsing. "The Making of an Expert Detective Thinking and Deciding in Criminal Investigations". English. PhD thesis. Gothenburg, Sweden: University of Gothenburg, 2016. ISBN: 978-91-628-9972-1.

[7] Katrin Franke and Sargur N Srihari. "Computational Forensics: An Overview". In: *Computational Forensics: Second International Workshop, IWCF 2008, Washington, DC, USA, August 7-8, 2008. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 1–10. ISBN: 978-3-540-85303-9. DOI: 10.1007/978-3-540-85303-9{_}1. URL: http://dx.doi.org/10.1007/978-3-540-85303-9_1.

[8] Jim Fraser and Robin Williams. *Handbook of Forensic Science*. English. New York, USA, 2009.

[9] Ken Gilhooly, Fiona Lyddy, and Frank Pollick. *Cognitive Psychology*. Maidenhead: McGraw-Hill Education, 2014. ISBN: 9780077122669.

[10] Jelle Groenendaal and Ira Helsloot. "Tunnel vision on tunnel vision? A preliminary examination of the tension between precaution and efficacy in major criminal investigations in the Netherlands". In: *Police Practice and Research* 16.3 (2015), pp. 224–238. ISSN: 1477271X. DOI: 10.1080/15614263.2014.928622. URL: http://dx.doi.org/10.1080/15614263.2014.928622.

[11] Ray Hilborn and Marc Mangel. *The ecological detective : confronting models with data*. Princeton, New Jersey: Princeton University Press, 1997. ISBN: 978-0-691-03497-3. URL: http://web.b.ebscohost.com/ehost/ebookviewer/ebook/bmxlYmtfXzUyOTQ4MV9fQU41?sid=dde8b29e-375c-41fc-9bd3-e25d806bbe9a@sessionmgr104&vid=0&format=EB&rid=1.

[12] Martin Innes. *Investigating murder : Detective Work and the Police Response to Criminal Homicide*. Oxford: Oxford University Press, 2003.

[13] Daniel Kahneman. "A perspective on judgment and choice: mapping bounded rationality". In: *American Psychologist* 58.9 (2003), pp. 697–720. DOI: 10.1037/0003-066X.58.9.697. URL: https://www.ncbi.nlm.nih.gov/pubmed/14584987.

[14] Saul M. Kassin, Itiel E. Dror, and Jeff Kukucka. "The forensic confirmation bias: Problems, perspectives, and proposed solutions". In: *Journal of Applied Research in Memory and Cognition* 2.1 (2013), pp. 42–52. ISSN: 22113681. DOI: 10.1016/j.jarmac.2013.01.001.

[15] David R Krathwohl. "A Revision of Bloom's Taxonomy: An Overview". In: *Theory into practice* 41.4 (2002), pp. 212–218. ISSN: 10994130. DOI: 10.1207/s15430421tip4104{_}2.

[16] Svein Magnussen. *Vitnepsykologi 2.0*. Oslo, Norway: Abstrakt forlag AS, 2017, p. 361. ISBN: 9788279353881.

[17] C Meissner. "Interview and Interrogation Methods and Their Effects on Investigative Outcomes". In: (2012). DOI: 10.4073/csr.2012.13. URL: https://campbellcollaboration.org/library/interview-interrogation-effects-on-investigations.

[18] William O'Donohue and Jeffrey A Buchanan. "The Weaknesses of Strong Inference". In: *Source: Behavior and Philosophy* (2001).

[19] Martin O'Neill. *Key challenges in criminal investigation*. Bristol, UK: Policy Press, 2018. ISBN: 9781447325772. URL: https://doi.org/10.1093/police/pay040.

[20] John R. Platt. "Strong inference". In: *Science Science* (1964). ISSN: 00368075. DOI: 10.1126/science.146.3642.347.

[21] Politidirektoratet. *Etterforskningen i politiet*. Tech. rep. 2013, pp. 1–57.

[22] Politihøgskolen. *Rammeplan for Bachelor – politiutdanning*. Tech. rep. Oslo: Politihøgskolen, 2018. URL: https://www.phs.no/Documents/2_Studietilbud/1_Bachelor/Rammeplan%20Bachelor%20politiutdanning_godkjent%202018.pdf.

[23] K. R. Popper. *The Logic of Scientific Discovery*. 1959. ISBN: 0415278449. DOI: 10.1016/S0016-0032(59)90407-7.

[24] Asbjørn Rachlew. "Justisfeil ved politiets etterforskning". PhD thesis. Oslo, 2009.

[25] Riksadvokaten. *Etterforskning*. Norwegian. Tech. rep. 1999. URL: http://www.riksadvokaten.no/filestore/Dokumenter/Eldre_dokumenter/Rundskriv/Rundskrivnr3for1999-Etterforskning2.pdf.

[26] Riksadvokaten. *Statsadvokatenes kvalitetsundersøkelse 2016 – voldtekt og mishandling av nærstående*. Tech. rep. 2016.

[27] Jon Petter Rui. "Straffeprosessen i perspektiv". In: *Jussens Venner* 49.november (2016), pp. 382–443.

[28] Michael J Saks and Jonathan Koehler. "The Coming Paradigm Shift in Forensic Indentificaion Science". In: *Science* 309.5736 (2005), pp. 892–895. DOI: 10.1126/science.1111565. URL: http://www.ncbi.nlm.nih.gov/pubmed/16081727.

[29] Michael J. Saks et al. "Forensic bitemark identification: weak foundations, exaggerated claims". In: *Journal of Law and the Biosciences* 3.3 (Dec. 2016), pp. 538–575. ISSN: 2053-9711. DOI: 10.1093/jlb/lsw045. URL: https://academic.oup.com/jlb/article-lookup/doi/10.1093/jlb/lsw045.

[30] Peter Stelfox. *Criminal Investigation : An introduction to principles and practice*. English. First. Devon, UK: Willan Publishing, 2009, p. 248. ISBN: 978-1-84392-337-4.

[31] Nina Sunde and Itiel E. Dror. "Cognitive and human factors in digital forensics: Problems, challenges, and the way forward". In: *Digital Investigation* (2019). ISSN: 17422876. DOI: 10.1016/j.diin.2019.03.011.

[32] Stephen Tong, Robin P Bryant, and Miranda A H Horcath. *Understanding Criminal Investigation*. Ed. by Wiley Series. Oxford, UK: Wiley & Sons Ltd., 2009.

[33] United Nations General Assembly. *Universal Declaration of Human Rights*. English. 1948. URL: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.

[34] U.S. Department of Justice and Officer of the Inspector General. "A Review of the FBI's Handling of the Brandon Mayfield case". In: *Organization* (2006).