An Extended Model of Cybercrime Investigations

Séamus Ó Ciardhuáin

Abstract

A comprehensive model of cybercrime investigations is important for standardising terminology, defining requirements, and supporting the development of new techniques and tools for investigators. In this paper a model of investigations is presented which combines the existing models, generalises them, and extends them by explicitly addressing certain activities not included in them. Unlike previous models, this model explicitly represents the information flows in an investigation and captures the full scope of an investigation, rather than only the processing of evidence. The results of an evaluation of the model by practicing cybercrime investigators are presented. This new model is compared to some important existing models and applied to a real investigation.

Introduction

A good model of cybercrime investigations is important, because it provides an abstract reference framework, independent of any particular technology or organisational environment, for the discussion of techniques and technology for supporting the work of investigators. It can provide a basis for common terminology to support discussion and sharing of expertise. The model can be used to help develop and apply methodologies to new technologies as they emerge and become the subject of investigations. Furthermore, the model can be used in a proactive way to identify opportunities for the development and deployment of technology to support the work of investigators, and to provide a framework for the capture and analysis of requirements for investigative tools, particularly for advanced automated analytical tools. At present, there is a lack of general models specifically directed at cybercrime investigations. The available models concentrate on part of the investigative process (dealing with gathering, analysing and presenting evidence) but a fully general model must incorporate other aspects if it is to be comprehensive.

Such a model is useful not just for law enforcement. It can also benefit IT managers, security practitioners, and auditors. These people are increasingly in the position of having to carry out investigations because of the increasing incidence not only of cybercrime, but of breaches of company policies and guidelines (e.g. the abuse of Internet connections in the workplace).

This paper presents an extended model of cybercrime investigations which identifies the activities of the investigative process and the major information flows in that process, an important aspect of developing supporting tools. Existing models from the literature are described and compared to the new model. Notice that the model described here is broader than those which deal only with digital evidence processing; this model

attempts to capture as much as possible of the entire cybercrime investigative process including the digital evidence processing activities.

Existing Models

There are several models for investigation in the literature. Brief descriptions of the most important ones are given below. These models largely restrict themselves to the investigation of the crime scene and the evidence, and so are less extensive in their scope than the model to be described later.

Lee's Model of Scientific Crime Scene Investigation

Lee et al. (2001) discuss scientific crime scene investigation as a process. This model deals only with crime scene investigation, not with the full investigative process. It identifies four steps within the process.

Recognition is the first step, in which items or patterns are seen to be potential evidence. The investigator must know both what to look for and where it may be found. Recognition leads to two sub-activities: *documentation* and *collection and preservation.*

Identification of the various types of evidence is the next step. This involves the classification of the evidence, and one sub-activity, *comparison*. Physical, biological, chemical, and other properties of the evidence items are compared to known standard ones.

Individualization refers to determining whether items of possible evidence are unique so that they may be linked to a particular individual or event. Within this, the items must be *evaluated* and *interpreted*.

Reconstruction involves bringing together the outputs from the earlier parts of the process, and any other relevant information which investigators may have obtained, to provide a detailed account of the events and actions at the crime scene. This leads to *reporting and presentation*.

Based on the above steps, Lee et al. describe logic trees for several different types of scenes, i.e. a series of related actions which the investigator may use for guidance to ensure the highest probability that all relevant evidence will be recognized, identified and individualized, leading to a useful reconstruction. They do not, however, extend this detailed approach to electronic crime scene investigation.

This model emphasises that the investigation of a crime scene must be systematic and methodical. It is mainly aimed at investigations using physical evidence, but it will be seen below that many aspects of it are reflected in forensic examination of electronic scenes. The major limitation of this model is that it refers only to the forensic part of an investigation and issues such as the exchange of information with other investigators are not addressed.

Casey

Casey (2000) presents a model for processing and examining digital evidence. This has the following key steps:

1. Recognition
2. Preservation, collection, and documentation
3. Classification, comparison, and individualization
4. Reconstruction

The last two steps are the ones in which the evidence is analysed. Casey points out that this is an evidence processing cycle, because the reconstruction can point to additional evidence which causes the cycle to begin again. The model is first presented in terms of standalone computer systems, and then applied to the various network layers (from physical media up to the user applications layer, and including the network infrastructure) to describe investigations on computer networks. Casey's model is quite general and is successfully applied to both standalone systems and networked environments.

DFRWS

The first Digital Forensics Research Workshop (Palmer, 2001) produced a model which sets out the steps for digital forensic analysis in a linear process. The steps are as follows:

1. Identification
2. Preservation
3. Collection
4. Examination
5. Analysis
6. Presentation
7. Decision

The model is not intended as a final comprehensive one, but rather as a basis for future work which will define a full model, and also as a framework for future research. The DFRWS model is presented as linear, but the possibility of feedback from one step to previous ones is mentioned. The DFRWS report does not discuss the steps of the model in great detail but for each step a number of relevant issues are listed, e.g. for *Preservation* the relevant issues are case management, imaging technologies, chain of custody and time synchronisation.

Reith, Carr and Gunsch

Reith, Carr and Gunsch (2002) describe a model which is to some extent derived from the DFRWS model. The steps in their model are:

1. Identification

2. Preparation
3. Approach strategy
4. Preservation
5. Collection
6. Examination
7. Analysis
8. Presentation
9. Returning Evidence

This model is notable in that it is explicitly intended to be an abstract model applicable to any technology or type of cybercrime. It is intended that the model can be used as the basis for developing more detailed methods for specific types of investigation, e.g. dealing with fixed hard drives or embedded non-volatile memory, while identifying any commonality possible in procedures or tools.

The Proposed Model

Given that a number of models already exist, what is the motivation for presenting yet another one? The existing models do not cover all aspects of cybercrime investigation; they focus mainly on the processing of digital evidence. Although valuable, they are not general enough to describe fully the investigative process in a way which will assist the development of new investigative tools and techniques. A comprehensive model can provide a common reference framework for discussion and for the development of terminology. It can support the development of tools, techniques, training and the certification/accreditation of investigators and tools. It can also provide a unified structure for case studies/lessons learned materials to be shared among investigators, and for the development of standards, conformance testing, and investigative best practices.

The single largest gap in the existing models is that they do not explicitly identify the information flows in investigations. For example, Reith et al. (2002) themselves have noted the absence of any explicit mention of the chain of custody in their model. This is a major flaw when one considers the different laws, practices, languages, and so on which must be correctly dealt with in real investigations. It is important to identify and describe these information flows so that they can be protected and supported technologically, for instance through the use of trusted public key infrastructures and time stamping to identify investigators and authenticate evidence.

A further issue with the existing models is that they have tended to concentrate on the middle part of the process of investigation, i.e. the collection and examination of the evidence. However, the earlier and later stages must be taken into account if a comprehensive model is to be achieved, and in particular if all the relevant information flows through an investigation are to be identified.

The proposed model is shown in Figure 1 (page 21). The activities in an investigation are as follows:

1. Awareness
2. Authorisation
3. Planning
4. Notification
5. Search for and identify evidence
6. Collection of evidence
7. Transport of evidence
8. Storage of evidence
9. Examination of evidence
10. Hypothesis
11. Presentation of hypothesis
12. Proof/Defence of hypothesis
13. Dissemination of information

These activities are described below. In general, an investigation according to this model proceeds in a "waterfall" fashion with activities following each other in sequence. However, it is possible that an activity may require changes to the results of a previous activity or additional work in that activity, so the sequence of activities shown in the model allows backtracking. In fact, it is to be expected that there will be several iterations of some parts of the investigation. In particular, the examination-hypothesis-presentation-proof/defence sequence of activities will usually be repeated a number of times, probably with increasingly complex hypotheses and stronger challenges to them at each iteration as the understanding of the evidence grows.

The major information flows during the investigation are also shown in Figure 1. Information about the investigation flows from one activity to the next all the way through the investigation process. For example, the chain of custody is formed by the list of those who have handled a piece of evidence and must pass from one stage to the next with names being added at each step. There are also flows to/from other parts of the organisation, and to/from external entities. The information flows are discussed in more detail below.

Awareness

The first step in an investigation is the creation of an awareness that investigation is needed. This awareness is typically created by events external to the organisation which will carry out the investigation, e.g. a crime is reported to the police or an auditor is requested to perform an audit. It may also result from internal events, e.g. an intrusion detection system alerts a system administrator that a system's security has been compromised.

The awareness activity is made explicit in this model because it allows the relationship with the events requiring investigation to be made clear. Most earlier models do not explicitly show this activity and so do not include a visible relationship to the causative events. This is a weakness of such models because the events causing the investigation may significantly influence the type of investigation required, e.g. an

auditor can expect cooperation from a client, whereas a police investigator may not receive cooperation from suspects in an investigation. It is vital to take into account such differences to ensure that the correct approach is taken to an investigation in a particular context.

Authorisation

After the need for an investigation is identified, the next activity is to obtain authorisation to carry it out. This may be very complex and require interaction with both external and internal entities to obtain the necessary authorisation. The level of formal structure associated with authorisation varies considerably, depending on the type of investigation. At one extreme, a system administrator may require only a simple verbal approval from company management to carry out a detailed investigation of the company's computer systems; at the other extreme, law enforcement agencies usually require formal legal authorisation setting out in precise detail what is permitted in an investigation (e.g. court orders or warrants).

Planning

The planning activity is strongly influenced by information from both inside and outside the investigating organisation. From outside, the plans will be influenced by regulations and legislation which set the general context of the investigation and which are not under the control of the investigators. There will also be information collected by the investigators from other external sources. From within the organisation, there will be the organisation's own strategies, policies, and information about previous investigations. The planning activity may give rise to a need to backtrack and obtain further authorisation, for example when the scope of the investigation is found to be larger than the original information showed.

Notification

Notification in this model refers to informing the subject of an investigation or other concerned parties that the investigation is taking place. This activity may not be appropriate in some investigations, e.g. where surprise is needed to prevent destruction of evidence. However, in other types it may be required, or there may be other organisations which must be made aware of the investigation.

Search and Identification of Evidence

This activity deals with locating the evidence and identifying what it is for the next activity. In the simplest case, this may involve finding the computer used by a suspect and confirming that it is the one of interest to the investigators. However, in more complex environments this activity may not be straightforward; e.g. it may require tracing computers through multiple ISPs and possibly in other countries based on knowledge of an IP address.

Collection

Collection is the activity in which the investigating organisation takes possession of the evidence in a form which can be preserved and analysed, e.g. imaging of hard disks or seizure of entire computers. This activity is the focus of most discussion in the literature because of its importance for the rest of the investigation. Errors or poor practices at this stage may render the evidence useless, particularly in investigations which are subject to strict legal requirements.

Transport

Following collection, evidence must be transported to a suitable location for later examination. This could be simply the physical transfer of seized computers to a safe location; however, it could also be the transmission of data through networks. It is important to ensure during transport that the evidence remains valid for later use, i.e. that the means of transport used does not affect the integrity of the evidence.

Storage

The collected evidence will in most cases need to be stored because examination cannot take place immediately. Storage must take into account the need to preserve the integrity of the evidence.

Examination

Examination of the evidence will involve the use of a potentially large number of techniques to find and interpret significant data. It may require repair of damaged data in ways which preserve its integrity. Depending on the outcomes of the search/identification and collection activities, there may be very large volumes of data to be examined so automated techniques to support the investigator are required.

Hypothesis

Based on the examination of the evidence, the investigators must construct a hypothesis of what occurred. The degree of formality of this hypothesis depends on the type of investigation. For example, a police investigation will result in the preparation of a detailed hypothesis with carefully documented supporting material from the examination, suitable for use in court. An internal investigation by a company's systems administrator will result in a less formal report to management. Backtracking from this activity to the examination activity is to be expected, as the investigators develop a greater understanding of the events which led to the investigation in the first place.

Presentation

The hypothesis must be presented to persons other than the investigators. For a police investigation the hypothesis will be placed before a jury, while an internal company

investigation will place the hypothesis before management for a decision on action to be taken.

Proof/Defence

In general the hypothesis will not go unchallenged; a contrary hypothesis and supporting evidence will be placed before a jury, for example. The investigators will have to prove the validity of their hypothesis and defend it against criticism and challenge. Successful challenges will probably result in backtracking to the earlier stages to obtain and examine more evidence, and construct a better hypothesis.

Dissemination

The final activity in the model is the dissemination of information from the investigation. Some information may be made available only within the investigating organisation, while other information may be more widely disseminated. Policies and procedures will normally be in place which determine the details. The information will influence future investigations and may also influence the policies and procedures. The collection and maintenance of this information is, therefore, a key aspect of supporting the work of investigators and is likely to be a fruitful area for the development of advanced applications incorporating techniques such as data mining and expert systems.

An example of the dissemination activity is described by Hauck et al. (2002). They describe a system called *Coplink* which provides real-time support for law enforcement investigators in the form of an analysis tool based on a large collection of information from previous investigations. A further example is described by Harrison et al. (2002). Their prototype system is not real-time, but instead provides an archival function for the experience and knowledge of investigators.

Information Flows in the Model

A number of information flows are shown in the model. First, there is a flow of information within the investigating organisation from one activity to the next. This may be within a single group of investigators or between different groups, e.g. when evidence is passed to a specialist forensic laboratory for examination. This flow of information is the most important in the course of the investigation, but may not be formalised because it is within the organisation, usually within a single investigating team. However, there are benefits to be obtained by considering this information explicitly. By doing so, support can be provided in the form of automated procedures and tools, e.g. case management tools.

However, before the investigation can begin there is a need for information to come to the investigators, creating the awareness that an investigation is needed. This is modelled as being from either internal (e.g. an intrusion detection system alerting a system administrator to an attack) or external sources (e.g. a complaint being made to police).

Obtaining authorisation for the investigation involves further information flows to and from the appropriate authorities, e.g. obtaining legal authorisation for a search or obtaining approval from company management to commit resources to investigating an attack.

The planning activity involves several information flows to the investigating team. From outside the organisation, there will be policies, regulations and legislation which govern how the investigation can proceed. Similarly, there will be the investigating organisation's internal policies which must be followed by the investigators. Other information will be drawn in by the investigators to support their work, e.g. technical data on the environment in which they will be working.

If appropriate to the type of investigation, the notification activity will result in a flow of information to the subject of the investigation; e.g. in civil legal proceedings there will be requests for the disclosure of documents. This information will be subject to controls such as the policies of the investigating organisation.

When the hypothesis based on the evidence must be justified and defended in the proof/defence activity, information will flow into the investigating team from within their organisation and especially from outside (e.g. challenges to evidence presented in court).

When the investigation concludes (whether the outcome is successful from the investigators' point of view or not) there will be information flows as the results are disseminated. These flows are again subject to controls; e.g. names may have to be withheld, or certain technical details may not be made known immediately to allow solutions to problems to be implemented. The information produced by the investigators may influence internal policies of the organisation, as well as becoming inputs to future investigations. It may also be passed through an organisation's information distribution function to become available to other investigators outside the organisation, e.g. in the form of a published case study used for training investigators, or as a security advisory to system administrators.

At all times during the investigation, information may flow in and out of the organisation in response to the needs of the investigators. These general information flows are subject to the information controls put in place by the investigating organisation. In an abstract model it is not possible to identify clearly all the possible flows and therefore, further research is needed to refine this aspect of the model for particular contexts.

Comparison with Existing Models

Table 1 gives a comparison of the activities in the proposed model with those in the models described earlier. It may be seen that there are a number of activities in this model which are not made explicit in the others. Information flows are not explicitly addressed by other models. The correspondence between the activities is not always

one-to-one, but the overall process is similar. Table 2 cross-references the terms used for the activities in the proposed model to those found in the other models discussed above, as there is some variation in the terms used.

Table 1. Comparison of activities in the models discussed

Activity in new model	***MODEL***			
	Lee et al.	Casey	DFRWS	Reith et al.
Awareness				✓
Authorisation				
Planning				✓
Notification				
Search/Identification	✓	✓	✓	✓
Collection	✓	✓	✓	✓
Transport				
Storage				
Examination	✓	✓	✓	✓
Hypothesis	✓		✓	✓
Presentation	✓		✓	✓
Proof/Defence			✓	
Dissemination				

Table 2. Comparison of terminology in models

Term in new model	***MODEL***			
	Lee et al.	Casey	DFRWS	Reith et al.
Awareness				Identification
Authorisation				
Planning				Preparation
Notification				
Search/Identification	Recognition, Identification	Recognition	Identification	
Collection	Collection and Preservation	Preservation, Collection, Documentation	Preservation, Collection	Preservation, Collection
Transport				
Storage				
Examination	Individualization	Classification, Comparison, Individualization	Examination	Examination
Hypothesis	Reconstruction	Reconstruction	Analysis	Analysis
Presentation	Reporting and Presentation		Presentation	Presentation
Proof/Defence			Decision	
Dissemination				

Advantages and Disadvantages of the Model

This model has the advantages obtained from previous models, but extends their scope and offers some further benefits. A reference framework is essential to the development of cybercrime investigation because it allows for standardisation, consistency of terminology, and the identification of areas in which research and development are needed. It can also provide a pedagogical tool and a basis for explaining the work of investigators to non-specialists, whether they are jurors or company management.

The most important advantage of this model in comparison to others is the explicit identification of information flows in the investigative process. This will allow tools to be specified and developed, dealing with case management, examination of evidence, and the controlled dissemination of information. The model can also help capture the expertise and experience of investigators with a view to the development of advanced tools incorporating techniques such as data mining and expert systems.

Inevitably, the generality of the model presents some difficulties. It must be applied in the context of an organisation before it will be possible to make clear the details of the process. For example, the model shows an information flow between activities which includes the recording of the chain of custody, but the procedures for this can only be

specified in detail when the organisational and legal context of the investigators is known.

Evaluation of the Model

The approach adopted for initial validation of the model was to obtain the views of the intended user community, i.e. investigators, in some depth. This was done by presenting the work to a number of experienced police investigators (from 2 to 10 years of experience in computer crime investigation) in Ireland and discussing it with them in a "focus group" format. In addition, another experienced investigator was interviewed separately. All the participants in the evaluation exercise were given explanatory material based on the descriptions of the model above. The views expressed during the interviews were noted and the investigators completed a questionnaire, which is shown in the Appendix.

This approach to validation has the following advantages:

- The interview and questionnaire format takes full advantage of the experience of those participating by being more open than a narrowly-focused survey.
- Participants have a clearer understanding of the subject, because they can ask questions about the work rather than simply responding to a fixed set of questions.
- Participants can raise and discuss points which might not be identified by a simple survey. Any such issues can be explored at once in some detail.

Completeness of the Model

The investigators' response to the model of investigations was very positive. The group stated in response to Question 1 (Did you feel that the model of investigations adequately represented the structure of investigations in your organisation?), "The model is an excellent representation of the various actions and information sources that are utilised during the course of a police investigation." It was their view that the model had more general applicability than just for computer crime investigations; it could be used to describe any police investigation. It also brought out activities which they had not considered as separate parts of an investigation, particularly hypothesis and dissemination. The backtracking inherent in the model was noted as important, because real investigations do not proceed in a simple linear manner.

The group felt that no part of the model could be omitted for their work (Question 3). In response to Question 2 (Did you think that any major elements were omitted from the model?), they felt that no major elements were missing from the model but they said: "… we felt that there should be a greater crossover between the information controls and dissemination." When questioned further on this point, the group members suggested the additional information flows as follows:

- Make explicit the influence of external policies, regulation and legislation on the policies of the investigating organisation.
- Link the external policies, regulation and legislation, and the organisational policies to the information controls.

This suggestion was motivated by concern about "leakage" of information from the investigation to the world outside the investigating organisation, and to inappropriate parts of the investigating organisation itself. Preventing this requires strict controls on the flows of information. Police investigators are particularly sensitive to this "leakage" because of the need for confidentiality which is imposed on them by the external policies, regulation and legislation, and by practical considerations in successfully carrying out the investigation as is seen in the application of the model to a real investigation (Application of the Model, below).

This suggested modification does not cause any substantial change to the basic model. It does, however, emphasise the importance of capturing the information flows in an investigation using a model of the type proposed in the present work, and demonstrates the utility of the model for understanding the investigative process.

Relevance of the Model

The participants in the group were asked to consider how relevant to their work they found the model of investigations (Question 4). The group's assessment of the relevance of the activities is shown in Table 3. On a scale of one to five, with five being most relevant, most activities were considered to be "very relevant." However, four activities were considered "not relevant," namely:

- Awareness
- Transport
- Storage
- Dissemination

Table 3. Relevance of activities in model to their work as rated by participants

ACTIVITY	RELEVANCE				
	1	2	3	4	5
Awareness	✓				
Authorisation					✓
Planning					✓
Notification					✓
Search/Identification					✓
Collection					✓
Transport	✓				
Storage	✓				
Examination					✓
Hypothesis					✓
Presentation					✓
Proof/Defence					✓
Dissemination	✓				

In discussion, it was found that they considered awareness unimportant, because at present they have more than enough work and it is not necessary for them to make significant efforts to achieve awareness of potential investigation. Complaints are made to them, usually including considerable detail of the events. Under-reporting is a concern which will have to be addressed and awareness would then be a more important activity. This activity could, for the present, be considered more relevant to, for example, systems administrators who must maintain and monitor an intrusion detection system in order to be aware of events requiring investigation.

The transport and storage activities were considered to be of no relevance, because at present they are essentially trivial, consisting of the removal and storage of PCs, disks, and similar material. There is no use made of network transport of possible digital evidence at present. However, the participants agreed that this was likely to become an issue of concern in future as the scope of investigations becomes larger.

The participants acknowledged the importance of the dissemination activity, but assessed it as not being relevant to them, because they do not undertake any significant dissemination of the results of investigations. They saw this as a weakness, but no mechanisms exist at present to support dissemination of such information. Computer security professionals already have a culture of sharing information on incidents and vulnerabilities, and this activity would be more relevant to them.

Conclusions about the Model

Based on the above evaluation, it can be concluded that the model provides a good

basis for understanding the process of investigations and captures most of the information flows. Some additional emphasis needs to be placed on the control of the information flows in the law enforcement environment.

The model allowed some interesting conclusions to be drawn about the state of computer crime investigations at present:

- Awareness of a need for investigation is not an issue which police investigators see as problematic; they have a steady supply of work.
- Transport and storage of digital evidence are still at a basic level.
- Dissemination is understood to be important but is still limited.

Forensic computing platforms will need to address the dissemination activity in the model in order to make it more effective, perhaps learning from the computer security professionals' experiences in sharing information. There is scope for significant advances to be made in the transport and storage activities as technology develops.

Application of the Model

In this section a case study of a real investigation is presented. The conduct of the investigation is considered in terms of the new model. This investigation is described in (Ó Ciardhuáin & Gillen, 2002, §5.6).

Description of the Investigation

This investigation began when a bank in Ireland received an email claiming to have found a vulnerability in an online service operated by the bank. The email offered to provide details of the vulnerability in return for payment. On checking their logs, the bank concluded that an unauthorised access had been made to their web server. They received further emails threatening to disclose the vulnerability to the press, including a link to a website which the suspect intended to use to publicise the vulnerability. The bank then reported the matter to An Garda Síochána (Irish police) who began an investigation. It quickly became clear that the compromised computer system was located in a different jurisdiction (London, UK) from the bank's headquarters, and that the source of the emails was in Belfast. Therefore, the investigation was taken up by another police force (the RUC, now Police Service of Northern Ireland). By examining the emails and log files, they were able to identify a suspect and a search warrant was obtained for the premises of the suspect's employers. During the search a computer was seized for examination. Using EnCase, the investigators found copies of all the emails and some other relevant information, which led to a successful prosecution.

Application of the Model

From the description it can be seen that there were three investigating organisations (two police forces and the bank) in two jurisdictions. This shows the importance of capturing the information flows between organisations in a general model. The

investigation as a whole consisted of three overlapping investigations, each involving the activities of the model and the exchange of information with the others. This is shown in Figure 2 (page 22).

Awareness: The Awareness activity can be seen to have occurred three times in this investigation:

1. when the bank received the email.
2. when the bank reported it to the police.
3. when the investigation was passed to a second police force.

Authorisation: The initial authorisation for the investigation by the bank is implicit, because they were investigating their own servers. There was then a second implicit authorisation as the Garda investigation began, followed by the realisation that in fact they were not authorised to carry out the investigation and had to pass it on to another police force who were authorised. The search warrant is a clear example of obtaining external authorisation.

Planning: This activity occurred in the bank's investigation when they decided to undertake an examination of the logs with the possibility of contacting the police, depending on what was found. The two police investigations involved planning the approach to be taken to identify the suspect and collect the necessary evidence.

Notification: This activity occurred when the RUC was informed of the investigation. Note that this notification is the external event causing the awareness activity within the second investigating police force. In this investigation it was not appropriate to inform the subject of the investigation that it was taking place. In fact, care was taken to avoid letting the suspect know of the investigation by not visiting the web site which he had set up.

Search/Identification: This occurred initially when the bank identified their log files as a way of deciding what had happened. Later, both police forces carried out similar activities to locate the source of the emails, and a physical search resulted from the information gained in the earlier searches. It may also be seen that the search/identification activity and the later examination activity may interact, as the examination of the logs led to further searches.

Collection: This activity occurred when the search of the employers' premises led to the seizure of a computer, and in the preservation of email messages and log files as evidence.

Transport: This activity clearly occurred in the transport of the seized computer. However, it can also be seen in the transfer of log files from the server to the police for examination, and in the transfer of emails from the bank to the police.

Storage: This activity can be seen in the retention of the seized computer by police and in the imaging of the disk of that computer. It may also be seen in the storage of the log

files and emails.
Examination: This activity occurred in the bank's examination of their log files. It also occurred in the police examinations of the log files and emails and of the seized computer.

Hypothesis: This activity occurred in the bank's investigation when they concluded from the logs that an unauthorised access had taken place. In the police investigations, an initial hypothesis was formulated for the identity of the suspect, which led to the seizure of the computer to obtain more evidence. This involved backtracking in the model, and resulted in a more detailed hypothesis which was then presented in court.

Presentation: This activity occurred a number of times:

1. within the bank, before a decision was made to approach the police, when the evidence was examined by management and perhaps legal advice was sought.
2. when the bank presented their evidence of an incident to the police investigators.
3. when one police force passed the investigation to another.
4. when evidence was presented to obtain a search warrant.
5. when the police evidence was presented in court.

Notice that the formality of the presentation increases as the investigation proceeded.

Proof/Defence: The proof/defence activity also occurred when the case was presented in court.

Dissemination: The dissemination activity took place with the publication of descriptions of the investigation and its outcome (Ó Ciardhuáin & Gillen, 2002). Initial publication took place before the completion of the trial, so that information controls had to be in place to remove sensitive data from the disseminated information, as suggested by the model.

Future Work

The model described above can be used to define requirements for supporting investigations, e.g. for tools to support the information flows identified in the model. The application of the model should be studied in different types of investigation in order to verify its viability and applicability as a general reference framework. Contexts which are of interest include:

- police (criminal) investigations;
- auditors;
- civil litigation;
- investigations by system administrators;
- judicial inquiries.

The characteristics of different investigation types need to be captured, e.g. the applicable evidence standards, and detail added for different types of investigation. This is a general model which can be refined and extended in particular contexts. There is

also a need to identify the actors in investigations and their roles more clearly in each context.

The additional information flows suggested by the interviewees need to be examined and incorporated in the model, taking into account their interactions with other aspects of the model.

The full lifecycle of information derived from investigations needs to be considered. Although some efforts have been already made in this direction (Patel & Ó Ciardhuáin, 2000), there is a need to develop a more general and comprehensive model of how this type of information can be handled to the best advantage while still meeting the complex constraints imposed by considerations such as privacy and the protection of sensitive data.

Conclusion

A new model of cybercrime investigations has been described. The inclusion of information flows in this model, as well as the investigative activities, makes it more comprehensive than previous models. It provides a basis for the development of techniques and especially tools to support the work of investigators. The viability and applicability of the model now needs to be tested in different organisational contexts and environments.

Acknowledgements

The input to the evaluation of the model by members of An Garda Síochána is greatly appreciated. Detective Inspector George Clydesdale of the Police Service of Northern Ireland kindly gave permission to use the case study for this paper.

About the Author

Séamus Ó Ciardhuáin was formerly a researcher in the Department of Computer Science, University College Dublin, Ireland. His research interests include forensic computing and computer security. He has worked as a researcher and technical manager on a number of national and international research projects and as a systems administrator. He has been involved in the development of training for investigators in forensic computing and was co-editor of the reports from a project in the European Union's FALCONE programme which defined a syllabus for the training of cybercrime investigators in Europe. He can be contacted by email at seoc@iolfree.ie.

References

Casey, E. (2000). *Digital Evidence and Computer Crime*. San Diego: Academic Press.

Harrison, W., Heuston, G., Morrissey, M., Aucsmith, D. Mocas, S. & Russelle, S. (2002). A Lessons Learned Repository for Computer Forensics. *International Journal of Digital Evidence*, Vol. 1 No. 3. Online: http://www.ijde.org/docs/02_fall_art2.html [visited 30 June 2004]

Hauck, R. V., Atabakhsh, H., Ongvasith P., Gupta, H., & Chen, H. (2002). Using Coplink to analyze criminal-justice data. *IEEE Computer*, Vol. 35 No. 3 pp. 30–37.

Lee, H. C., Palmbach, T. M., & Miller, M. T. (2001). *Henry Lee's Crime Scene Handbook*. San Diego: Academic Press.

Ó Ciardhuáin, S. & Gillen, P. (eds.) (2002) *Guide to Best Practice in the area of Internet crime Investigation*. Report from EU FALCONE Project No. JAI/2001/Falcone/127 "Training: Cyber Crime Investigation — Building a Platform for the Future." Dublin, Ireland: An Garda Síochána.

Palmer, G. (ed.) (2001). *A Road Map for Digital Forensic Research: Report from the First Digital Forensic Workshop*, 7–8 August 2001. DFRWS Technical Report DTR-T001-01, 6 November 2001. Online: http://www.dfrws.org/dfrws-rm-final.pdf [visited 30 June 2004]

Patel, A. & Ó Ciardhuáin, S. (2000). The impact of forensic computing on telecommunications. *IEEE Communications*, Vol. 38 No. 11 pp. 64–67.

Reith, M., Carr, C. & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, Vol. 1 No. 3. Online: http://www.ijde.org/docs/02_fall_art2.html [visited 30 June 2004]

Appendix: Questionnaire used in evaluating the model

1. Did you feel that the model of investigations adequately represented the structure of investigations in your organisation?

2. Did you think that any major elements were omitted from the model? If so, please describe them briefly.

3. Were there parts of the model which you felt could be omitted for your organisation? If so, what were they?

4. Please indicate which activities in the model most closely relate to your own work and experience.

   Please tick 1 = not relevant, 5 = very relevant.

ACTIVITY	RELEVANCE				
	1	2	3	4	5
Awareness					
Authorisation					
Planning					
Notification					
Search/Identification					
Collection					
Transport					
Storage					
Examination					
Hypothesis					
Presentation					
Proof/Defence					
Dissemination					

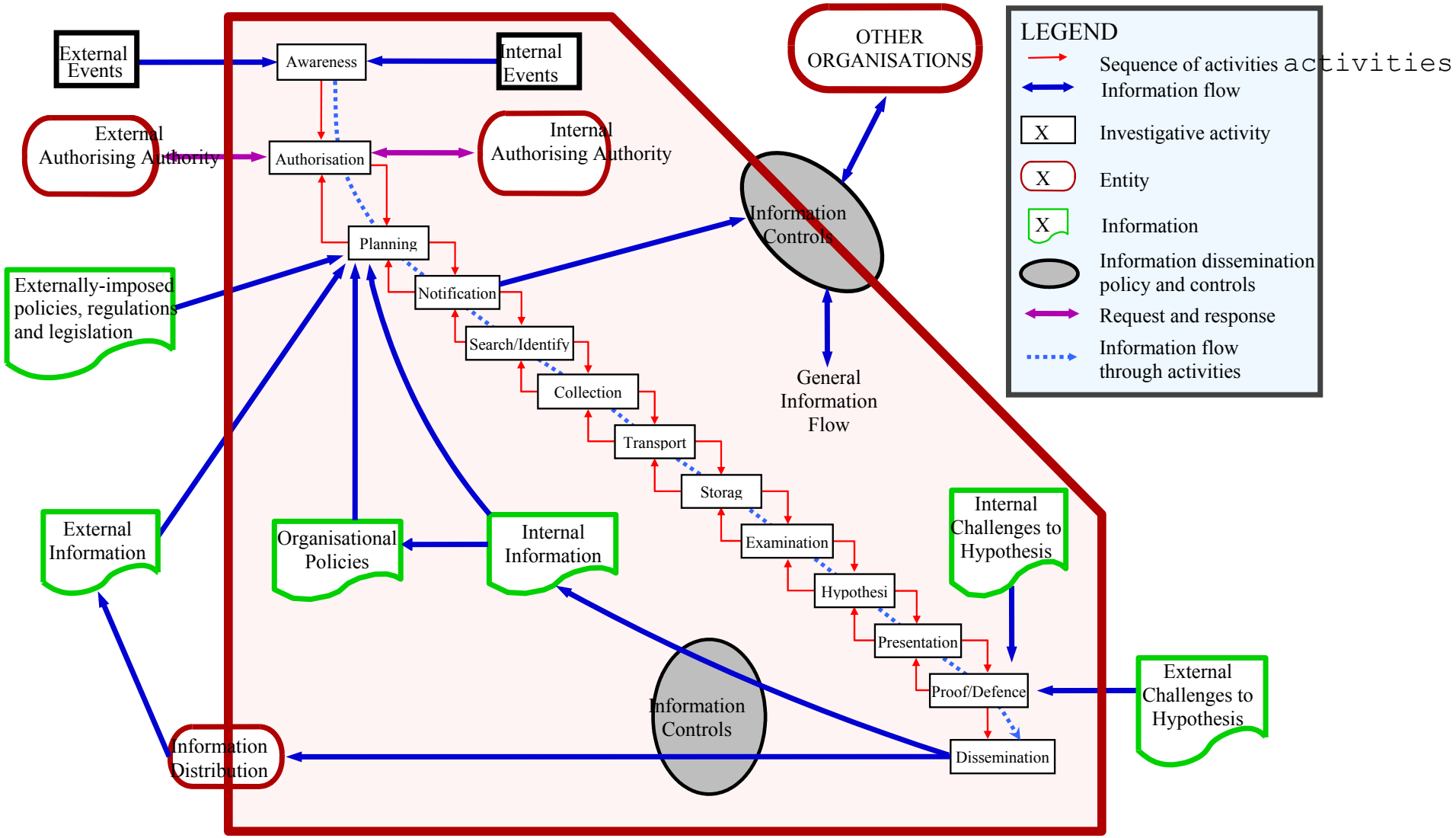

Figure 1. The proposed model of cybercrime investigations.

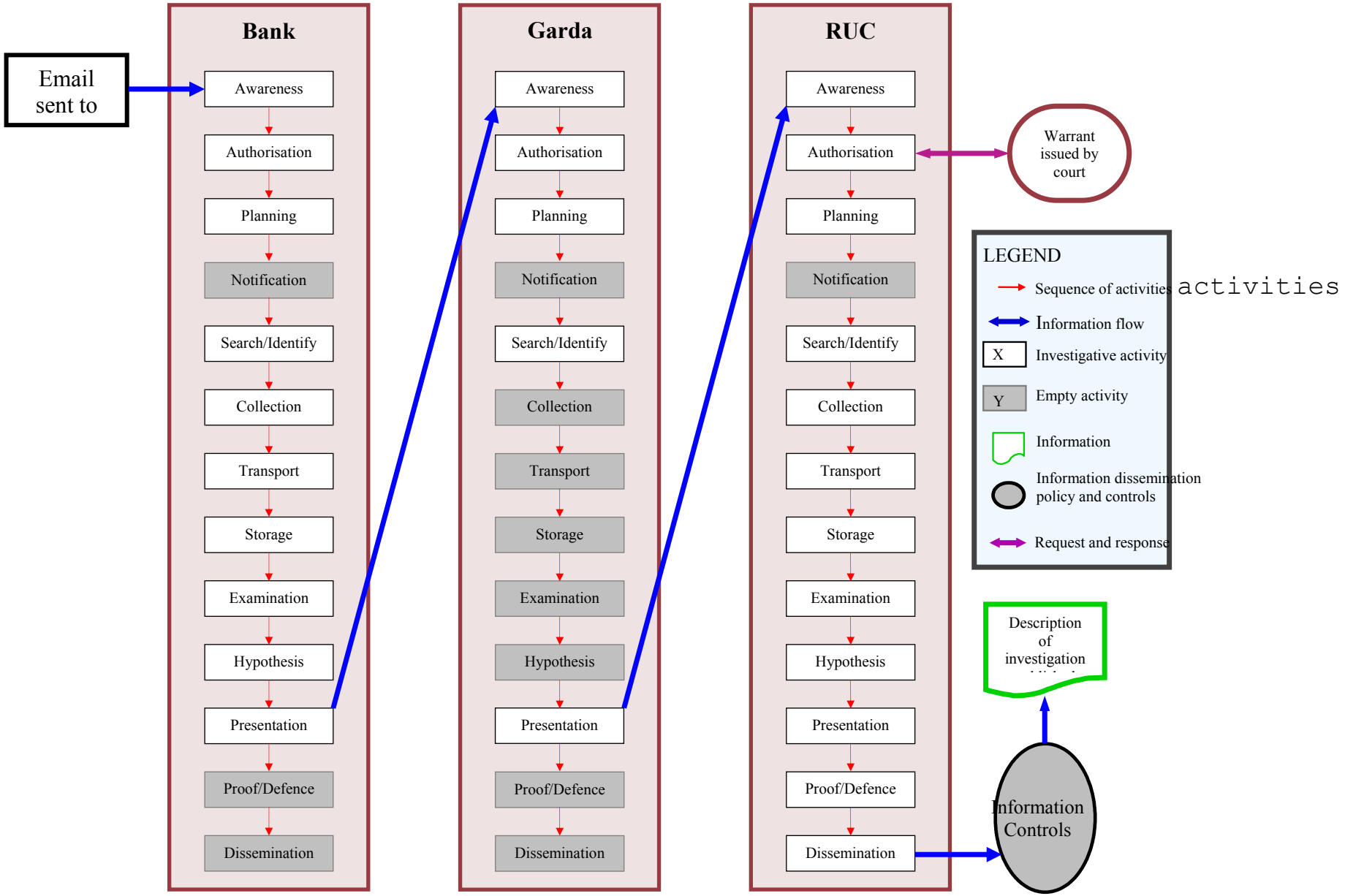

Figure 2. The model applied to a real investigation.