Establishing Findings in Digital Forensic Examinations: A Case Study Method

Oluwasayo Oyelami, Martin Olivier

Chapter 1

ESTABLISHING FINDINGS IN DIGITAL FORENSIC EXAMINATIONS: A CASE STUDY METHOD

Oluwasayo Oyelami and Martin Olivier

Abstract In digital forensics, examinations are carried out to explain events and demonstrate the root cause from a number of plausible causes. Yin's approach to case study research offers a systematic process for investigating occurrences in their real-world contexts. The approach is well suited to examining isolated events and also addresses questions about causality and the reliability of findings. The techniques that make Yin's approach suitable for research also apply to digital forensic examinations. The merits of case study research are highlighted in previous work that established the suitability of the case study research method for conducting digital forensic examinations. This research extends the previous work by demonstrating the practicality of Yin's case study method in examining digital events. The research examines the relationship between digital evidence – the effect – and its plausible causes, and how patterns can be identified and applied to explain the events. Establishing these patterns supports the findings of a forensic examination. Analytic strategies and techniques inherent in Yin's case study method are applied to identify and analyze patterns in order to establish the findings of a digital forensic examination.

Keywords: Digital forensic examinations, Yin's method, establishing findings

1. Introduction

Causality is about drawing relationships between an observed phenomenon – the effect – and its plausible cause(s) [4, 6, 7, 10, 19, 23]. Establishing these relationships supports the findings of a forensic examination. In establishing cause and effect relationships, a forensic examiner identifies patterns in the evidence that may be used to establish findings and also to attribute the source. Understanding these patterns and how

they can be applied to test hypotheses are central to establishing the findings of a forensic examination.

In order to demonstrate causality, a forensic examiner searches for patterns that support a hypothesis. The more supporting patterns that are found, the more compelling are the causal findings. These supporting patterns ultimately form a web of consistency that provides support for the findings of the forensic examination. The use of a web of consistency is supported by Casey's certainty scale [3], which notes that evidence supported by multiple independent sources has a higher certainty value than information obtained from a single source.

The case study research method proposed by Yin [25] offers a systematic process for investigating occurrences in their real-world contexts. This research method is very popular in the social sciences, where it has a definite focus; in fact, Yin's seminal book on the topic is currently in its fifth edition [25]. An analysis of Yin's approach reveals that it is particularly appropriate for examining isolated events; moreover, it addresses questions on causality and the reliability of findings. The merits of case study research are discussed in earlier work [18], which established the suitability of the case study research method for conducting digital forensic examinations. This research extends the earlier work by demonstrating how the case study method can be applied in digital forensic examinations.

2. Causality and Digital Systems

A digital system contains a complex set of software programs that are executed within the system. The control logic of a program executes and controls the operations of the program. It receives input commands from a user and executes the commands on the computing system. It also controls and executes automated operations that have been structured in the software program.

The execution of input commands and/or automated operations by the control logic causes effects in a digital system. This implies that the control logic is the cause of the effects in the system. An effect triggered by the control logic may be a passive effect or an active effect. A passive effect occurs when control logic execution causes traces or side effects in the digital system; thus, passive effects are referred to as traces or side effects in the system. On the other hand, an active effect occurs when control logic execution triggers further control logic executions in the system; these further executions of control logic correspond to active effects in the system. Active effects may also leave traces that are passive.

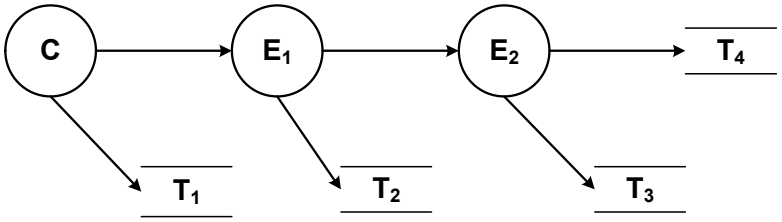

Figure 1. Cause and effect in a digital system.

Figure 1 illustrates a cause and effect in a digital system. A cause C leaves a passive effect or trace T_1 and its execution triggers an active effect E_1. The initiation of the active effect E_1 leaves a trace T_2 and its execution triggers another active effect E_2. The initiation of the active effect E_2 leaves a trace T_3 and the execution of the active effect E_2 leaves a trace T_4. As illustrated in Figure 1, an effect can be an active effect or a passive effect, which is a trace in the system. The active effects – namely, the control logic executions – are transient in the system. In other words, active effects are not observable because the execution of a command itself is invisible in the system. It is the traces that are observed in the system.

The following examples clarify the concepts of cause and effect in a digital system:

- **bash Shell Command Execution:** An example of cause and effect in a digital system is the execution of a `bash` shell command initiated when a certain input is provided by a user. The input to the `bash` shell is stored in the `bash` history and execution is initiated by the control logic. A forensic examiner knows that the control logic initiated the `bash` shell command because of the traces of the command initiation left in the `bash` history. However, the execution of the `bash` command itself is invisible. Therefore, it is not possible to know if the command did execute. It is also possible that environmental variables may have been configured to disable the `bash` history. However, programs that execute may leave traces and a forensic examiner may conclude that the program caused the traces.

- **crontab File Execution:** A second example is the execution of a `crontab` file. A `crontab` is a system service that causes commands to be executed at specified times. The execution of `crontab` is controlled by the `cron` daemon, whose control logic executes the commands in the system background. When the specified time

for a command execution is met, the `cron` daemon initiates the command and passively logs the initiation of the command. The logging of the `crontab` command is a passive effect while the execution of the command is an active effect. However, the command may or may not have executed and may not leave any traces in the system. There may or may not be passive effects to indicate execution success or failure.

- **Database Trigger Execution:** A third example is the execution of a database trigger. A database trigger executes a sequence of commands when a logical condition is met. The initiation of the database trigger may create a log entry (passive effect) and its execution may create another log entry and may also initiate another trigger (active effect) that may, in turn, cause a log entry.
- **Email Arrival at a Mail Transfer Agent:** A fourth example is the arrival of email at a mail transfer agent. Email is forwarded from one mail transfer agent to the next until it is delivered to the recipient's inbox. The arrival of an email at a mail transfer agent causes a log of the email communication to be written, which is a passive effect. The email is then routed to the next mail transfer agent in the delivery path or is delivered to the recipient's inbox. The routing of email is an active effect while the delivery to the recipient's inbox is a passive effect.

Drawing inferences from the above examples, the arrival of an email at a mail transfer agent is similar to a `bash` shell interface waiting for a command from the user. It is also similar to a `cron` daemon waiting until the time arrives to execute a command from `crontab`. It is also similar to a database watching data and waiting for a condition to be met in order to execute an operation. From these examples, it is possible to conclude that a `bash` shell command entered by a user, the logical conditions satisfied in the `crontab` and database trigger examples and the arrival of an email at a mail transfer agent are all forms of input to a system executed by the control logic that causes effects to occur in the system.

A digital system operates in a pre-set mode of execution and system configuration; additionally, as illustrated above, it is programmed to accept certain inputs. Depending on the input that is received, the control logic executes the expected sequence of commands that are predefined by the system. Depending on the system configuration, certain traces are typically left in the system. This implies that, by analyzing the system configuration and the known inputs, a forensic examiner may be able to predict the traces that will be in the system. This can be viewed

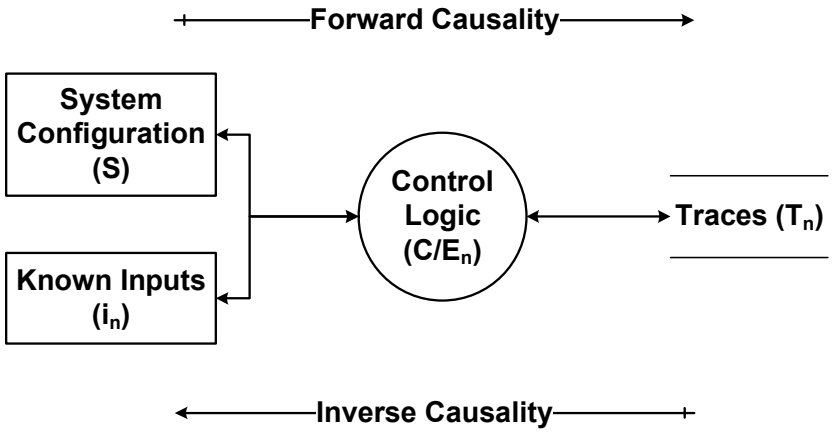

Figure 2. Causality in a digital system.

as "forward causality." On the other hand, a forensic examiner may also be able to use the traces found in a system to predict the system configuration and system inputs at the time; this can be described as "inverse causality."

Figure 2 illustrates the notions of causality in a digital system. Forward causality enables a forensic examiner to predict the traces that are expected based on the system configuration and program input. Inverse causality enables an examiner to predict the plausible causes in the system. Based on the predictions made from the traces by applying inverse causality, an examiner can test the predictions made about the plausible causes by applying forward causality to demonstrate the observed side effects or traces.

3. Using Yin's Method

This section reviews the application of Yin's case study approach as a scientific method for conceptualizing digital forensic examinations [18]. The case study method as described by Yin [25] is suitable for examining isolated occurrences. The process of carrying out a forensic examination involves three main aspects: (i) understanding the body of knowledge in the field; (ii) formulating hypotheses in the examination; and (iii) testing the hypotheses (empirical testing).

3.1 Body of Knowledge

A forensic examiner must have scientific knowledge and experience in the forensic field in order to practice in the field. An understanding

of the body of knowledge in the field is a necessary requirement for all forensic science disciplines [9, 13, 15, 17]. An examiner must have expert knowledge in the field in which the examination is intended to be carried out. Without expert knowledge in the field, an examiner cannot consistently make valid claims nor will the hypotheses be based on the body of knowledge and experience gained from scientific practice within the profession.

3.2 Hypotheses Formulation

Hypotheses formulation is driven by the questions that are asked about the evidence [22, 26]. The formulation plays an important role in the examination of evidence [1, 2, 5]. The process of formulating hypotheses also guides the examination phase. Hypotheses formulation typically yields multiple hypotheses, one is the main hypothesis and the others are alternative hypotheses. The main hypothesis reflects what the examiner expects to observe and demonstrate in the context of the examination. The alternative hypotheses are plausible explanations that oppose the main hypothesis and must be disproved.

In forming a hypothesis, an examiner typically would seek to answer one or two main forms of questions during the examination of the evidence. In its first form, the examiner may be required to address a decision problem [14]. In its second form, the requirement is to address a narrative problem [20, 21].

The decision problem addresses the examination of evidence in terms of the narrative. For example, a generic decision problem in digital forensics may be stated as "Does this sequence occur on the disk?" where the sequence may refer to a software signature, execution of malicious software, downloaded software or evidence of a network intrusion or compromise. A decision problem is usually answered by a yes, no or inconclusive.

The narrative problem, on the other hand, addresses the examination in terms of causality. An example is "What caused this sequence to occur on the disk?" where the sequence is as illustrated above. The narrative problem requires an examiner to examine and explain the facts that support the conclusions that are made. Interested readers are referred to [14, 20, 21] to explore the use of decision problems and narratives in digital forensics.

Hypotheses formulation takes one of the two forms discussed above. While a narrative problem may also be interpreted in the form of a decision problem, both forms serve different purposes, but also achieve the same goal of explaining the findings made from the evidence exam-

ination. Hypotheses formulation should be done before examining the evidence to ensure that the examination is free from bias [8, 9, 13, 16].

It is important to note that, depending on the nature of the examination, it may not be necessary to formulate hypotheses. For example, when measurements are required to determine an outcome, the formulation of hypotheses is not a requirement.

3.3 Hypotheses Testing

The main purpose of the evidence analysis phase is to test the hypotheses. In testing a hypothesis, a forensic examiner has to consider the likelihood of a particular occurrence reaching a definite conclusion. In the example above, which asks the question "Does this sequence occur on the disk?" the examiner may seek to demonstrate the occurrence of the sequence on the disk. The result is usually a yes or no based on the weight of the supporting patterns found in the evidence. The result may also be inconclusive, indicating that what is observed does not provide sufficient proof to confirm or deny the plausibility of the occurrence of the sequence. This may occur in situations involving file deletion, evidence tampering or insufficient evidence.

The question "What caused this sequence to occur on the disk?" examines the occurrence in terms of causality. A forensic examiner may seek to demonstrate that the sequence is attributable to a certain cause and confirm the hypothesis. However in doing this, the examiner must also actively identify evidence that refutes the hypothesis. An examiner may successfully prove that an observed effect is attributable to a cause, but in order to strengthen the finding, the examiner must refute other plausible rival explanations.

A methodical approach must be applied to prove the hypothesis, analyze the evidence, establish causal relationships and demonstrate a web of consistency between the evidence and its plausible causes. A number of techniques proposed by Yin may be applied. The techniques include pattern matching, explanation building, time-series analysis and logic models [18, 24, 25]. Also, when examining complex digital evidence, an examiner may use the cross-case synthesis technique, which applies the logic of replication, namely literal replication and theoretical replication.

The pattern matching technique enables an examiner to compare patterns predicted before an examination against the observed patterns. Predicted patterns are expected findings based on the body of knowledge and apply forward causality [18, 24, 25]. Using the pattern matching technique, an examiner can demonstrate that a set of hypotheses or

explanations E explains a set of observed patterns or observations O, while knowing E but not having observed O at the time.

The explanation building technique enables an examiner to develop a narrative of a case by specifying a set of causal relationships about the occurrence, or explaining how and why the occurrence happened [18, 24, 25]. This involves stating an initial hypothesis or explanation about the case and then testing the hypothesis. If the hypothesis is found to be inconsistent, it is revised to reflect the new findings. The revised hypothesis or explanation is then tested again as more observations are made in an iterative manner until an explanation is made that fully reflects the final findings of the case. Using the explanation building technique, an examiner can demonstrate how, from an initial set of hypotheses or explanations E_1, an examiner can iteratively revise and create new explanations E_i that are consistent as the observed patterns O_i are examined.

The time-series analysis technique enables an examiner to bring together key aspects of an occurrence in chronological order. The chronology also reflects the case as a set of causal relationships, showing which key aspects may have caused or contributed to the existence of other aspects [18, 24, 25]. The time-series analysis technique enables an examiner to determine that the observed patterns O_i are not causal effects of other patterns based on their occurrence times.

A logic model enables an examiner to break down a complex occurrence into repeated cause and effect patterns and to demonstrate how the final findings are obtained from intermediate findings [18, 24, 25]. Analysis of the logic model identifies the observed patterns O_i that may have contributed to the occurrence of other observed patterns.

Another important technique is cross-case synthesis, which is mainly applied in multiple case examinations. The cross-case synthesis technique involves multiple case studies that help determine whether the findings from selected cases support any broader or particular conclusions. This technique applies the logic of replication, which has two components, literal replication and theoretical replication. In literal replication, an examiner selects a number of cases with the goal of demonstrating similar findings; this provides a web of consistency. Theoretical replication enables an examiner to select and examine another set of cases while predicting opposing results with the goal of invalidating the opposing results [18, 24, 25].

Whatever the technique or combination of techniques employed in a case, a forensic examiner must consider and address the observed patterns that point to alternative explanations. In doing so, the examiner collects data on alternative explanations and examines them in order

to demonstrate their suitability or unsuitability. Demonstrating the unsuitability of rival explanations can be very helpful in explaining the case.

4. Causal Relationships in Digital Forensics

This section discusses causal relationships in digital forensics and how these relationships can be established.

4.1 Understanding Causal Relationships

Drawing relationships between a cause and its effect requires the identification of patterns during the analysis of evidence. The patterns that are found can be applied to establish and demonstrate various relationships. These relationships include correlations, data consistency and plausible causes. Relationships that form correlations are discerned from patterns that reflect matching data. Consistency relationships are derived from patterns that posit a cause or plausible causes on an effect. Plausible causes are a number of likely mechanisms or actions that can initiate an effect or may have initiated an effect.

A valid user name and its corresponding password are matching data that have a correlation as a login credential. A relationship that demonstrates consistency could be a successful login attempt to a website, which reflects a valid user name and that the corresponding entry in the password database was applied. A successful login attempt to a website may also be achieved via an SQL injection mechanism captured in a database log (that enabled access to login information) or via a brute force attack. Plausible causes of the successful login to the site are the use of an SQL injection mechanism, brute force attack and valid login credentials. By identifying patterns in the evidence, a forensic examiner can posit that an action was taken that caused an effect to occur. Correlating patterns from matching data support the claim of consistency and consistency patterns can be applied to demonstrate causal relationships.

4.2 Establishing Causal Relationships

Establishing causal relationships supports the findings of a forensic examination. It also strengthens the claims of causal inferences made by the examiner. The three main concepts that help establish causal relationships are: (i) specification of the necessary and sufficient conditions for causality; (ii) establishment of a web of consistency in the evidence; and (iii) refutation of alternative hypotheses or explanations.

Necessary and Sufficient Conditions for Causality. An effect may occur under certain conditions and a number of conditions may be necessary for an effect to occur. The existence of a number of causes may not indicate that all the plausible causes contributed to the effect. A cause may be considered to be sufficient to initiate an effect without the participation of other conditions or causes. Thus, a forensic examiner may be required to determine the cause(s) that contributed to the effect observed from two or more plausible causes. The examiner may further determine the conditions under which the effect would be rendered implausible. A condition X is deemed to be necessary for an effect B to occur if and only if the falsification of the condition X guarantees the falsification of B. A condition X is deemed to be sufficient if its occurrence guarantees that the effect B will occur. Necessary conditions are the conditions without which an event cannot occur whereas sufficient conditions are the conditions that guarantee an expected outcome.

Consider a simple example where X implies visiting a web page and the side effects B_i of X may be the HTML file displayed on the screen, followed by subsequent connections to retrieve images for the page, followed by requests to retrieve the linked web pages. The action of X may also cause the source IP address to be logged on the server, the web page to be logged in the browser web history, the file to be cached at the source system, and so on.

Suppose that X and Y are two events where a web page was visited and assume that a defendant has acknowledged X and denied Y. It is sufficient to prove that Y occurred if the forensic examiner can show that the conditions necessary for Y to have occurred are observed and the effects that can be attributed to the occurrence of Y are also observed. The demonstration of these conditions establishes a web of consistency in the evidence, which shows that the claim is backed by multiple sources of evidence that support the findings. A finding made in an examination without the necessary conditions of the hypothesis being met refutes the validity of a hypothesis.

Web of Consistency. A web of consistency is established when evidence from various sources are found to corroborate and, therefore, create a convincing argument for the findings. The specification of the necessary and sufficient conditions of a case supports the establishment of a web of consistency. The more tightly coupled the evidence, the less likely that there will be several plausible causes.

In the case of the example above, where the defendant denied that a web page Y was visited, establishing a web of consistency requires that devices such as a firewall, proxy server and/or intrusion detection system

in the network have activity logs that validate the fact that the web page was visited. Examining the defendant's computing device may also provide evidence from the browser web history, web cache, search history, cookies and web beacons that stored information about the defendant's online activities. It is also possible that the defendant may have cleared the cache and deleted web history records. The examiner may then have to show that deletions occurred. In essence, the examiner expects to see traces or signs of deletion in order to make justified inferences about the case. When there are limited or no traces, justified inferences cannot be made about the case.

Alternative Hypothesis and Explanations. As stated above, plausible alternative explanations may be found that explain an occurrence. These explanations may be eliminated or at least considered doubtful by showing that one or more conditions necessary for the effect to be considered attributable to the alternative cause were not found. A statement by Campbell [24, 25] demonstrates the significance of alternative rival explanations in the examination of occurrences: "More and more I have come to the conclusion that the core of the scientific method is not experimentation *per se*, but rather the strategy connoted by the phrase 'plausible rival hypothesis'."

The refutation of rival explanations can be used as a criterion for interpreting the findings of an examination. When rival alternative hypotheses are refuted, the findings of an examination are strengthened. The forensic examiner must demonstrate that a certain rival cause does not fully address the conditions present in the case and, therefore, cannot be an attributable cause. This provides a more convincing argument for the findings. The greater the number of rival explanations that are addressed and excluded, the stronger the findings of the case.

In summary, when establishing causal relationships, the specification of the necessary and sufficient conditions, the creation of a web of consistency and the examination of alternative explanations enable a forensic examiner to demonstrate sufficient proof of the hypothesis and to strengthen the findings of the examination.

5. Lottery Terminal Hacking Incident

This section illustrates the application of the case study method to demonstrate causality in a lottery terminal hacking incident [11]. The incident involved the manipulation of a lottery game system known as 5 Card Cash [12]. The 5 Card Cash game is based on standard poker with a digital 52-card playing deck. A player purchases a system-generated ticket that has five randomly-selected cards. The player can win up to

two times. The first win is an instant prize based on the composition of the cards on the player's ticket. The second win is when the lottery organizer randomly draws five cards from a deck that evening and the player is able to match two or more cards on the purchased ticket with the five randomly-drawn cards.

5.1 The Case

The 5 Card Cash game was suspended after it was suspected that lottery terminals may have been manipulated. Specifically, the game winnings were observed to be much larger than the game parameters should have allowed.

5.2 The Investigation

An investigation determined that some lottery ticket operators were manipulating their terminals to print more instant winner tickets and fewer losing tickets.

An investigator determined that an operator could slow down a lottery terminal by requesting a number of database reports or by entering several requests for lottery game tickets. While the reports or requests were being processed, the operator could enter sales for 5 Card Cash tickets. However, before a ticket was printed, the operator could see on the screen if the ticket was an instant winner. If the ticket was not a winner, the operator could cancel the sale of the ticket before it was printed.

5.3 The Examination

The examination focuses on testing the inferences made by the investigator. This is done by applying the principles and techniques of the case study method. The goal is to demonstrate how the inferences may have been determined and the certainty with which the inferences can be considered to be reliable.

Because the case itself does not provide much information about the design of the 5 Card Cash game, a generic design is used to illustrate the examination and the assumptions about the workings of the game system. The generic game system configuration presented in Figure 3 provides the context for the examination.

The system has six components, which perform functions such as generating lottery tickets, processing payments for tickets, printing tickets and generating reports. The output of one system component may also be an input to another component. This implies that certain system components must execute before another component can begin to exe-

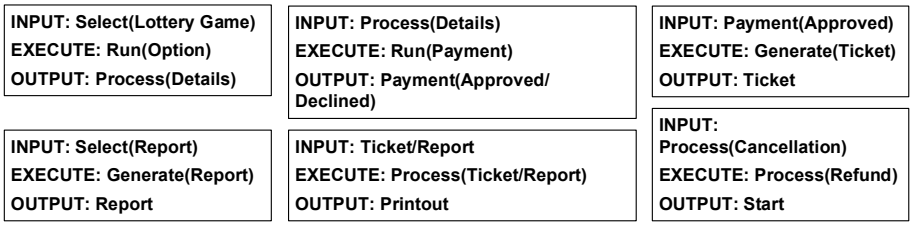

Figure 3. 5 Cash Card game system.

cute. For example, a ticket has to be generated before it can be displayed or printed. Also, reports have to be generated before they can be printed.

5.4 Hypotheses Formulation

From the initial investigation described above, the questions that the examiner may be asked can be framed as a decision problem and as a narrative problem. The decision problem addresses the examination in terms of the narrative and the narrative problem addresses the examination in terms of causality.

The two problems are stated as follows:

- **Decision Problem:** Are transactions deliberately canceled after the results are known?
- **Narrative Problem:** What enables the cancellation of transactions after the results are known?

The case study based on these two questions tests the hypothesis:

- **Hypothesis:** The terminal was manipulated in order to display the results in a manner that provided the operator with an undue advantage in determining favorable results and enabling the cancellation of unfavorable transactions.

The expected outcome of testing the hypothesis is to confirm its claim. In order to do this, the examination must demonstrate that unfavorable transactions were canceled after the results were known and that transactions considered to be favorable were allowed to continue. The alternative rival hypothesis is:

- **Rival Hypothesis:** The terminal was not manipulated in any way and the winnings are the result of legitimate transactions obtained within the scope of the game parameters.

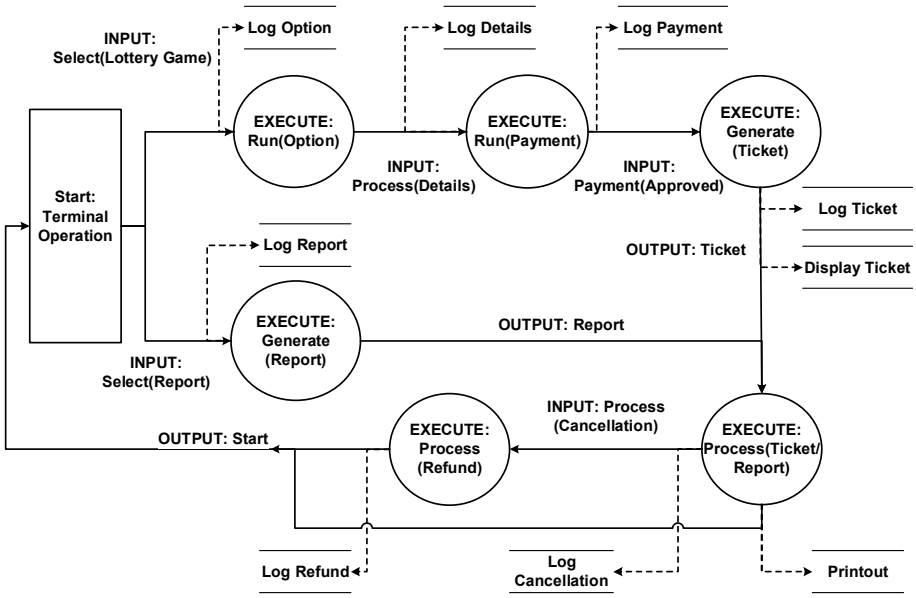

Figure 4. Cause and effect pattern (logic model).

5.5 Hypothesis Testing

Based on the game system configuration in Figure 3, a forensic examiner can express the system in terms of the cause and effect pattern or logic model shown in Figure 4. Figure 4 models the game system in terms of input, execution and output. An input to query the database using Select(Report) triggers the control logic to initiate the generation of the report; this initiates a passive effect to print the report.

Another pattern is observed in ticket generation. The selection of the lottery game triggers the program control logic to initiate the payment module, which issues the ticket and sends it to the printer without prompting the user. The ticket is also displayed as a passive effect.

In order to test the hypothesis that the terminal was manipulated, the examiner has to first specify the conditions that are necessary and sufficient to demonstrate the manipulation of the terminal. Specifying these conditions enables the examiner to know what to test. As stated above, necessary conditions are those without which an event cannot occur whereas sufficient conditions are those that guarantee the expected outcome.

The necessary conditions required to support the hypothesis that the terminal was manipulated are:

- There were sold tickets within a short time period before the transaction deadline.
- The terminal was busy or delayed during the time that the winning tickets were printed.
- Only unfavorable tickets during terminal busy/delay times were canceled.

These conditions are necessary in order for the operator to have an undue advantage in determining the results and cancelling unfavorable transactions.

The sufficient conditions are expected to provide a definite indicator of malicious activity. Specifically, it is sufficient to prove the hypothesis if it can be shown that:

- The activities specified under the necessary conditions occurred at numerous times.
- There is a consistent pattern with which these activities occurred.

In essence, the forensic examiner is required to demonstrate that, if there were late ticket sales and the terminal was busy, then the ticket sales made mostly involved winning tickets and the ticket sales canceled mostly involved unfavorable tickets. Also, the examiner may be able to show that this pattern occurred at numerous times in a consistent manner. Proving the hypothesis in this way eliminates the chance of having an alternative hypothesis that would take into consideration the necessary and sufficient conditions highlighted in the case. A hypothesis that cannot explain these conditions is excluded. Note that sufficient conditions may only be found if the hypotheses made are narrowed down to plausible explanations.

The specification of the necessary and sufficient conditions also helps establish a web of consistency. After observing the logs of system activities, the forensic examiner may be able to conduct a time-series analysis that displays the transactions along with their occurrence times.

Querying the log of generated tickets helps the examiner determine whether or not tickets were sold within a specified time period before the transaction deadline. The query provides the examiner with data that can be further analyzed to determine if tickets were processed when the terminal was busy or delayed. To do this, the results from querying the sold ticket log are compared with the results from the log of reports generated. This analysis is based on the knowledge that the terminal would be busy or delayed when the suspect tickets were generated and when

the reports were being processed. The analysis provides the examiner with a smaller set of tickets that were generated when the terminal was busy or delayed. Using this set of tickets, the examiner would expect to discover that winning tickets were printed and unfavorable tickets were canceled. To determine whether only unfavorable tickets during terminal busy times were canceled, the set of tickets is compared with the log of canceled transactions. This could enable the examiner to show that a larger number of unfavorable tickets were canceled and the remaining tickets that were not canceled were primarily winning tickets.

The examiner successfully demonstrates the correctness of the hypothesis when the necessary conditions for the case have been proved. This indicates that the terminal could have been manipulated such that the results were known before the transactions were completed and unfavorable transactions were deliberately canceled.

In order to demonstrate sufficient proof of the hypothesis, the examiner may widen the scope of the analysis to other time frames for the same terminal, demonstrating that manipulations occurred multiple times and, thus, establishing a web of consistency. It may also be sufficient to demonstrate that the unfavorable tickets sold when the terminal was not busy were legitimate transactions conducted on behalf of a lottery user by the operator.

Using replication logic, the examiner can also expand the scope of the examination to consider multiple cases. By applying literal replication, the examiner could examine a number of suspected terminals using the same conditions and sufficiently demonstrate that manipulations occurred on the suspected terminals. This would further confirm and strengthen the hypothesis while enabling a web of consistency to be established.

By applying theoretical replication, the examiner can select another set of suspected terminals and examine them to invalidate the alternative hypothesis (i.e., falsify the hypothesis that the terminals were not manipulated). Another theoretical replication approach is to select a number of known "clean" terminals and show that the type of manipulation found on the suspected terminals could not be found on the clean terminals.

The identification, testing and validation of the necessary and sufficient conditions of a hypothesis and the application of analytic techniques and strategies in the case study method strengthen a forensic examination. In particular, demonstrating causal relationships and establishing a web of consistency ensure that the findings of the examination are consistent and reliable.

This case study has used a logic model to illustrate the application of an analytic technique in a forensic examination of a digital system. Other analytic techniques, namely pattern matching, explanation building, time-series analysis and cross-case synthesis, can also be applied to establish findings in digital forensic examinations.

6. Conclusions

This chapter has sought to demonstrate the practicality of the case study method in digital forensic examinations. The focus has been on applying the case study method to establish the findings of a forensic examination. The research clarifies the relationship between digital evidence – the effect – and its plausible causes, and how patterns can be identified and applied to demonstrate the findings. By applying Yin's case study method, an examiner can establish the relationships that support and validate the findings of a forensic examination.

Further research is required to demonstrate how the case study method can be applied to strengthen the findings of a forensic examination. The suitability and applicability of the four validity tests of Yin's method and the tactics applied to satisfy these tests need to be investigated for use in a digital forensic environment. Strengthening the findings of a forensic examination would ensure that a logical approach has been followed and that the findings follow from the underlying hypotheses.

References

[1] M. Bunge, *Philosophy of Science: From Problem to Theory, Volume One*, Transaction Publishers, New Brunswick, New Jersey, 1998.

[2] B. Carrier, A Hypothesis-Based Approach to Digital Forensic Investigations, CERIAS Technical Report 2006-06, Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, Indiana, 2006.

[3] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, Waltham, Massachusetts, 2011.

[4] F. Cohen, *Digital Forensic Evidence Examination*, ASP Press, Livermore, California, 2010.

[5] S. Garfinkel, P. Farrell, V. Roussev and G. Dinolt, Bringing science to digital forensics with standardized forensic corpora, *Digital Investigation*, vol. 6(S), pp. S2–S11, 2009.

[6] P. Gladyshev and A. Patel, Formalizing event time bounding in digital investigations, *International Journal of Digital Evidence*, vol. 4(2), 2005.

[7] C. Grobler, C. Louwrens and S. von Solms, A multi-component view of digital forensics, *Proceedings of the IEEE International Conference on Availability, Reliability and Security*, pp. 647–652, 2010.

[8] L. Haber and R. Haber, Scientific validation of fingerprint evidence under Daubert, *Law, Probability and Risk*, vol. 7(2), pp. 87–109, 2008.

[9] K. Inman and N. Rudin, *Principles and Practice of Criminalistics: The Profession of Forensic Science*, CRC Press, Boca Raton, Florida, 2000.

[10] M. Kwan, K. Chow, F. Law and P. Lai, Reasoning about evidence using Bayesian networks, in *Advances in Digital Forensics IV*, I. Ray and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 275–289, 2008.

[11] Lottery Post, Six now face charges in CT lottery scheme (`www.lotterypost.com/news/301512`), March 23, 2016.

[12] Maryland Lottery, What is 5 card cash? Baltimore, Maryland (`www.mdlottery.com/games/5-card-cash`), 2017.

[13] National Institute of Justice and National Research Council, *Strengthening Forensic Science in the United States: A Path Forward*, National Academies Press, Washington, DC, 2009.

[14] M. Olivier, On complex crimes and digital forensics, in *Information Security in Diverse Computing Environments*, A. Kayem and C. Meinel (Eds.), IGI Global, Hershey, Pennsylvania, pp. 230–244, 2013.

[15] M. Olivier, Combining fundamentals, traditions, practice and science in a digital forensics course, presented at the *South African Computer Lecturers' Association Conference*, 2014.

[16] M. Olivier, Towards a digital forensic science, *Proceedings of the Information Security for South Africa Conference*, 2015.

[17] M. Olivier and S. Gruner, On the scientific maturity of digital forensics research, in *Advances in Digital Forensics IX*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 33–49, 2013.

[18] O. Oyelami and M. Olivier, Using Yin's approach to case studies as a paradigm for conducting examinations, in *Advances in Digital Forensics XI*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 45–59, 2015.

[19] J. Pearl, *Causality: Models, Reasoning and Inference*, Cambridge University Press, Cambridge, United Kingdom, 2009.

[20] M. Pollitt, Digital forensics as a surreal narrative, in *Advances in Digital Forensics V*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 3–15, 2009.

[21] M. Pollitt, History, historiography and the hermeneutics of the hard drive, in *Advances in Digital Forensics IX*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 3–17, 2013.

[22] S. Tewelde, M. Olivier and S. Gruner, Notions of hypothesis in digital forensics, in *Advances in Digital Forensics XI*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 29–43, 2015.

[23] S. Willassen, Hypothesis-based investigation of digital timestamps, in *Advances in Digital Forensics IV*, I. Ray and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 75–86, 2008.

[24] R. Yin, *Applications of Case Study Research*, Sage Publications, Thousand Oaks, California, 2012.

[25] R. Yin, *Case Study Research: Design and Methods*, Sage Publications, Thousand Oaks, California, 2013.

[26] T. Young, Forensic Science and the Scientific Method, Heartland Forensic Pathology, Kansas City, Missouri (`www.heartlandforensic.com/writing/forensic-science-and-the-scientific-method`), 2007.