I. J. Computer Network and Information Security, **2015, 2, 25-32**
Published Online January 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ ijcnis.2015.02.03

PNFEA: A Proposal Approach for Proactive Network Forensics Evidence Analysis to Resolve Cyber Crimes

Mohammad Rasmi
Zarqa University/Department of Computer Science, Zarqa, 13132, Jordan
Email: mr77mr@hotmail.com

Ahmad Al-Qerem
Zarqa University/Department of Computer Science, Zarqa, 13132, Jordan
Email: ahmad_qerm@zu.edu.jo

Abstract—Nowadays, cyber crimes are increasing and have affected large organizations with highly sensitive information. Consequently, the affected organizations spent more resources analyzing the cyber crimes rather than detecting and preventing these crimes. Network forensics plays an important role in investigating cyber crimes; it helps organizations resolve cyber crimes as soon as possible without incurring a significant loss. This paper proposes a new approach to analyze cyber crime evidence. The proposed approach aims to use cyber crime evidence to reconstruct useful attack evidence. Moreover, it helps investigators to resolve cyber crime efficiently. The results of the comparison of the proposed approach prove that it is more efficient in terms of time and cost compared with the generic and the modern process approach for network forensics.

Index Terms—Cyber crime, network forensics, proactive approach, evidence investigation component.

I. Introduction

According to the Cyber Security Watch Survey [1], cyber crime attacks incurred an average monetary loss of $123,000 per organization in the USA in 2011. Ponemon [2] reported that the annual cost of solving cyber crimes is $5.9 million. The Ponemon's study is based on a representative sample of 50 organizations in various industrial sectors in the USA. The cost incurred by cyber crimes per company ranges from $1.5 million to $36.5 million each year. In reality, a strong relationship exists between the time required to resolve a cyber crime and the cost. Based on a previous study [2, 25], cyber crimes could become costly if they are not resolved quickly.

Current investigation techniques are very costly and time consuming because extensive effort is required to analyze the overwhelming amount of evidence presented in each cyber crime case. In addition, gathering useful evidence is difficult because most techniques utilize active and reactive processes to analyze cyber crimes; such processes start right after the detection of the cyber crime.

Network forensic systems can be classified into two approaches: proactive and reactive. Proactive network forensics is a new approach in live investigation that deals with the phases of network forensics during an attack. In contrast, reactive network forensics is a traditional approach that deals with cyber crime cases after a period of time, which consumes a considerable amount of time during the investigation phase. As reported by [4-7], proactive forensic approaches reduce the time and cost of investigation by identifying potential evidence and reducing the resources needed in the investigation phase. These approaches are utilized in the preliminary analysis of a cyber crime and help improve and accelerate the decision making process.

This paper is proposed a new approach to resolve cyber crime for network forensics, the process of the proposed approach will be described in section 3. The approach will be compared with the generic process model for network forensics as mentioned in [8], which will be described in section 4. The next section will present a related work of network forensics approaches.

II. Related Work

The first Digital Forensics Research Workshop (DFRWS) [3] defined the first network forensic reactive approach as a generic investigation framework that can be applied to network environments and to most investigations. The framework includes six classes of tasks, i.e., identification, preservation, collection, examination, analysis, presentation, and decision making. Reith M. refined the DFRWS framework in 2002 and proposed a new model called Abstract Digital Forensics (ADF) [9]. This model consists of nine phases, i.e., identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence. The model creates a standardized framework for network forensics.

The first general process model for network forensics was proposed by [16]. The model includes six steps, i.e., capture, copy, transfer, analysis, investigation, and presentation. A new framework called the step-by-step framework was proposed by [17] to clarify the definition of network forensics. The framework studies previous research to establish a step-by-step framework, which groups all the existing processes in three stages, namely, preparation, investigation, and presentation, which are implemented as guidelines in network forensics. The guideline proposed by [18] based on existing frameworks to integrate forensic techniques into incident response through a set of processes that contains four stages: collection, examination, analysis, and reporting.

The generic process model for network forensic analysis proposed by [8] is based on various existing digital forensic models. The framework, divides the phases into two groups. The first group relies on actual time and includes five phases: preparation, detection, incident response, collection, and preservation. The four phases in the second group act as post-investigation phases, which include the examination, analysis, investigation, and presentation phase.

According to proactive network forensic concepts as mentioned by [6, 21], the first five phases work proactively because they work during the occurrence of the cyber crime. The other four phases of this model work after the investigation phase and act as a reactive process. Given that all the activities of network forensics are included in this model, the present research adopts the phases of this model as a baseline to show how the analysis phase integrates with the other phases.

Based on the fundamentals of proactive approach [6, 21], we conclude, that each phase in the first five phases requires a certain amount of time to accomplish its processes. However, each phase works in real time; thus, the phases require the same amount of time and processing cost to accomplish their processes. Given that the other four phases work reactively, we assume that they require more time and processing cost compared with the first five phases. The reason for this assumption is that reactive phases work after the cyber crime happens; therefore, the required amount of time and cost increases during the investigation process.

The study in [22] reviewed the existing frameworks until 2007 to construct the mapping process between the phases of digital forensics frameworks. It summarizes the mapping of processes into five appropriate phases as the following, preparation, collection and preservation, examination and analysis, presentation and reporting, and disseminating the case. The result of this study simplified the overall processes of existing frameworks in order to identify the critical and important phases for any digital forensics framework as the collection and preservation phase, examination and analysis phase, and presentation and reporting phase.

The multi-component view of digital forensics was proposed by [6]. The view includes three components, i.e., proactive digital forensics (ProDF), active digital forensics (ActDF), and reactive digital forensics (ReDF). ReDF includes six sub phases, which are incident response and confirmation, physical investigation, digital investigation, incident reconstruction, presentation of findings to the management or authorities, dissemination of the result of the investigation, and incident closure. ActDF includes four sub phases: incident response and confirmation, ActDF investigation, event reconstruction, and ActDF termination. The ProDF component defines and manages the processes and procedures of the comprehensive digital evidence. The same authors proposed a theoretical framework [7] to guide the implementation of proactive digital forensics and to ensure the forensic readiness of the evidence available for the investigation process. This framework helps organizations reduce the cost of the investigation process because it provides manageable components and live analysis. The reactive and proactive digital forensic investigation process approaches were studied by [4] and generated the Systematic Literature Review (SLR). SLR reports the gap and limitations of the digital forensic investigation process approaches. The researchers mentioned that from 2001 to 2010, 18 research studies that deal with digital forensic phases were conducted. One of these studies focused on the proactive digital forensic approach [6], and the others focused on the reactive approach. This fact indicates the need for more focus on proactive forensics.

The oldest models that were proposed before 2009 have disadvantages that the categories that may be extremely general defined for practical use, which is difficult for testing, and more cumbersome to use. The modern process proposed by [8, 22, 23] conducted through designing a generic process model for network forensic analysis based on various existing digital forensics models. The framework includes the following phases: preparation, detection, incident response, collection, preservation, examination, analysis, investigation, and presentation. In this paper, we determine the phases of this model as a baseline phase for proposing a new approach in analyzing evidence in order to integrate the analysis phase with other phases.

III. PNFEA Approach

This section presents a new approach called Proactive Network Forensics Evidence Analysis (PNFEA), which extended from the proposed approach by [21]. The proposed approach by [21] is characterized as proactive because it retrieves and preserves evidence before and after analyzing the cyber crime. The proposed approach includes five phases, i.e., preservation, capture, classification, analysis, and investigation. The PNFEA supports evidence analysis phase in network forensics. The new approach contains a chain of components; each one includes a set of a process to conduct a useful data for analyzing phase. The process shows the attack intention and strategy analyzing, and present the methods and techniques used for this goal. The approach contains predefined components such as a proactive network

forensics depository, which was ready with previous phases of the general network forensics model. Furthermore, the approach presents the environments of networks and devices, for capturing and monitoring the network traffic.

The first component of the PNFEA is about attack intention will be presented. The second component is about attack strategy. Evidence analysis integrated through a set of components work together to improve the quality of analysis phase outcome in network forensics. The PNFEA approach contains six components, each one divided into a set of the process. This approach aims to present the integration and relationship between the analysis phase in one side with previous phases and the next phases of the general model of network forensics. In general, previous phases are preparation, detection, collection, preservation and examination of evidence, and next phases are investigation and presentation phase. Moreover, The PNFEA approach shows the relation between the analysis phase with the incident response activities.

The PNFEA distributed through a multi type of components as a predefined proactive network forensics depository (component number 1); network capturing, monitoring and network forensics analysis tools as a manageable component to detect and collect cybercrime evidence (component number 2); and an evidence classification (component number 3). In addition, it has an attack intention analysis (component number 4) and strategy analysis (component number 5). Moreover, component number 6 presents the connectivity relationship between analysis and investigation phases through the incident response. Therefore, the retrieval of similar incident response using Cased-based Reasoning (CBR) approach.

IV. Comparisons with Generic Network Forensics Approach

The effectiveness of PNFEA approach is minimizing the time and the cost of the investigation process in advance to improve the quality of decision-making. The quality conducted when resolves the criminal case through passing network forensics phases with a minimum time and low cost. The time and cost are management issues, which try to find an efficient path that could be reduced the time and cost. In general, to identify this path the critical path method implemented, which uses one time estimate to identify the duration of each phase to accomplish its activity. The critical path is a path which there phase activities accomplished without any delay. The delay of any phase, activity will be delayed the resolution of the criminal case. Accordingly, the critical path used when the management level sure about the duration of each phase. The alternative way to identify the critical path is used Program Evaluation and Review Technique (PERT) method. The PERT used in a more uncertain situation to identify the time and cost of resolving the criminal case.

This paper applies PERT analysis as a stochastic method for handling uncertainties in time and cost planning. The PERT method used to calculate the variation in cost and time needed to resolve the criminal case through the network forensics approach phases. This research assumes that the criminal case passes to the all phases of the network forensics approach. The PERT estimates the critical path as an optimal solution to resolve the criminal case, which requires the most time to manipulate with the criminal case from the first phase to the final one. The evaluation of the analysis phase as an individual phase it doesn't make any sense without other phases. Hence, the PNFEA approach compared with the generic process model of network forensics, which proposed by [8]. The reason for the choice the generic process model that it is based on various existing digital forensics frameworks proposed till 2010. The generic process model has a nine phases (preparation, detection, incident response, collection, preservation, examination, analysis, investigation and presentation) acts as a combined of reactive and proactive activities. The PNFEA approach has a five phases (preservation, capturing, classification, analysis and investigation) work proactively as described previously.

V. Experimental Results And Analysis

The experiments used to evaluate the proposed approach depend on the backdoor and worm attacks as a case study. However, each criminal case acts as an individual problem needs to resolve using the network forensics approach. The PERT method estimates the critical path for resolving the criminal cases of backdoor and worm attacks as individual criminal cases, which manipulated through all phases of both PNFEA and generic approaches. Moreover, each case will be compared with a real statistical analysis data based on the time and cost in each case as mentioned in [2]. The three values estimation form used in PERT time and cost criminal case analysis. The three values present the best, expected and worst case scenarios either for time or cost estimation. The values combined to compute the expected average value of time or cost to find the critical path of resolving the criminal case.

The main assumption in this evaluation that the estimated time and cost values depends on the experience and the judgment of the network forensics approach manger. This assumption built on the fundamental of the PERT three time estimations. Thus, the evaluation estimate the best case scenario of the time and cost that needed for each phase, and the other two estimations computed depending on the best case value to increase the reliability of the evaluation. Obviously, the estimated value of proactive activities will take less than of reactive activities value. To be more reliable, the same best case scenario estimation values will assigned to proactive activities on both approaches.

A. Time Estimations Analysis

The time needed to accomplish each phase activity of network forensics depends on some of criteria such as the network forensics infrastructure like hardware and software. In addition, it depends on the human resource and how they will be responding to the criminal case. However, the three times estimate for each phase used to compute the expected average time to accomplish activities of each phase of the network forensics approach. The first estimation time called the optimistic time, which can define for each phase based on the PERT three time estimation method, as the following:

Definition 1: Given a minimum time period called a_t, which can be in microsecond, second … day, week, months to accomplish all the activities of one phase of the network forensics approach (In this paper the time will be measured in days).This time presents a best case scenario for the duration of the phase that everything proceeded better than expected.

The second estimated time is the most likely time value, which called m_t. It estimates the expected average time period to accomplish one phase activities when it's requested. This value presents the expected average scenario. Accordingly, this value is greater than or equal to the optimistic time. So, in this evaluation the most likely time can be calculated using this formula:

$$m_t = (1+v) * a_t, \text{ where } v \in \mathbb{R} \text{ and } \geq 0 \quad (1)$$

The third estimated value is a pessimistic time, which is called b_t. It is the maximum time period to accomplish one phase activities and presents the worst case scenario. This time estimated when the phase or one of it is actively not works properly and something wrong happened such as user error, hardware or software stop working. In fact, this value is greater than or equal to the expected average estimated value. So, in this evaluation the pessimistic time can be calculated as the following:

$$b_t = (1+v) * m_t, \text{ where } v \in \mathbb{R} \text{ and } \geq 0 \quad (2)$$

From the above three time estimation the expected duration time, which called t_e for each phase will be estimated based on the PERT method as the following:

$$t_e = (a_t + (4 * m_t) + b_t) / 6 \quad (3)$$

The variance (σ^2) (descriptive measurement) of optimistic and pessimistic time measures the degree of uncertainty, which associated with the duration time distribution for each phase. The variance for each activity calculated as the following:

$$\sigma^2 = ((b_t - a_t) / 6)^2 \quad (4)$$

Table 1 and Table 2 show the instance three time estimations and the variance for each phase of the both generic network forensics, and PNFEA approach respectively.

Table 1. Instance of Three Time Estimations and Variances for Generic Approach Activities

Activity ID	Activity(Phase)	a_t	m_t	b_t	t_e	σ^2
A	Preparation	3	6	12	6.5	2.25
B	Detection	3	6	12	6.5	2.25
C	Incident Response	3	6	12	6.5	2.25
D	Collection	3	6	12	6.5	2.25
E	Preservation	3	6	12	6.5	2.25
F	Examination	2	4	8	4.333333	1
G	Analysis	2	4	8	4.333333	1
H	Investigation	2	4	8	4.333333	1
I	Presentation	2	4	8	4.333333	1

Table 2. Instance of Three Time Estimations and Variances for PNFEA Approach Activities

Activity ID	Activity(Phase)	a_t	m_t	b_t	t_e	σ^2
A	Preservation	2	4	8	4.333333	1
B	Capturing	2	4	8	4.333333	1
C	Classification	2	4	8	4.333333	1
D	Analysis	2	4	8	4.333333	1
E	Investigation	2	4	8	4.333333	1

The frequency of occurrence the average expected time (t_e) for each approach is close to the most likely estimation time (m_t), as shown in Fig. 1. That means to accomplish the activity phase it needs the average expected time. Accordingly, the expected time presents the approximately of the duration time for each phase.

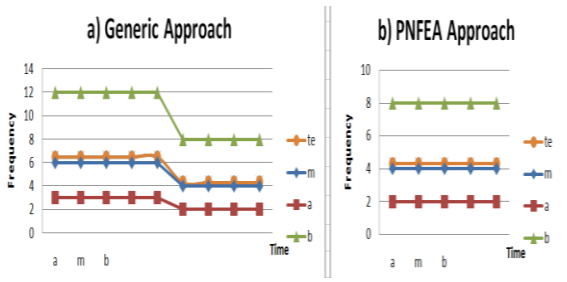

Fig. 1. The frequency of Occurrence the Average Expected Time (te)

Basic on the above information, which conducted from PERT method, it is important to extend more information as the most likelihood time to resolve the criminal case. To analyze the probability of accomplish time on the path to resolving the criminal case; this paper used the normal distribution pattern. First of all, the criminal case resolving variance, which named (σ^2_c) computed as the sum of all the variances of phases for each approach, as the follows:

$$\sigma_c^2 = \sum \sigma^2 \quad (5)$$

To measure the confidence of time resolving the criminal case, the standard deviation, which called (σ_c) will be computed as the follows:

$$\sigma_c = \sqrt{\sigma_c^2} \quad (6)$$

The standard deviation means that the time needed to accomplish the resolving of criminal case need (± σc). To achieve acceptable value, the result of experiments in this paper will be on both plus and minces standard deviation, and always it finds the same duration to accomplish resolving the criminal case. The probability of accomplishing the resolving the criminal case conducted from the formal normal distribution table, after converted and computed the z-score as the follows:

$$z = (Due\ Date - Expected\ \ Date) / \sigma_c \quad (7)$$

Where the Due Date is the time duration to accomplish resolving the criminal case which equal the sum of all expected average time (t_e) for all phases. The Expected Date presents the Due Date plus or minus the standard deviation (σ_c). Table 3 shows the instance of the research experiments that shows the duration and normal distribution of all phases for both PNFEA and generic approach.

It is a uniform for both PNFEA and general network forensics approaches had the probability 84.13% chance to accomplish resolving the criminal case. This ratio is acceptable in this evaluation that depends on uncertainty values and methods to estimate the time. Taking in the account there is 15.87% risk to uncover the resolving the criminal case at the average expected time. From the experimental results the PNFEA approach minimizes the time by the average 59.45%. The experiment related to the backdoor and worms attack, the PNFEA minimize the time by 55.04% and 56.43 respectively, with error ration equal to 0.0005% and 0.0028% from the expected average time.

Table 3. Duration and Normal Distribution for PNFEA and Generic Approach

Exp#		σ^2_c	σ_c	Due Date	Expected Date	Z	Proba_ bility
1	PNFEA	1.25	1.118034	10.83333	9.715299	1	0.8413
	Generic	6	2.44949	30.33333	27.88384	1	0.8413
2	PNFEA	0.217014	0.465847	7.708333	7.242486	1	0.8413
	Generic	1.041667	1.020621	21.58333	20.56271	1	0.8413
3	PNFEA	0.868056	0.931695	15.41667	14.48497	1	0.8413
	Generic	2.647569	1.627135	35.45833	33.8312	1	0.8413
4	PNFEA	5	2.236068	21.66667	19.4306	1	0.8413
	Generic	15.25	3.905125	49.83333	45.92821	1	0.8413
5	PNFEA	0.3125	0.559017	5.416667	4.85765	1	0.8413
	Generic	1.5	1.224745	15.16667	13.94192	1	0.8413
6	PNFEA	0.054253	0.232924	3.854167	3.621243	1	0.8413
	Generic	0.260417	0.51031	10.79167	10.28136	1	0.8413
7	PNFEA	0.138889	0.372678	4.166667	3.793989	1	0.8413
	Generic	0.666667	0.816497	11.66667	10.85017	1	0.8413
8	PNFEA	6.805556	2.608746	11.66667	9.057921	1	0.8413
	Generic	32.66667	5.715476	32.66667	26.95119	1	0.8413
9	PNFEA	31.25	5.59017	37.5	31.90983	1	0.8413
	Generic	80.55556	8.975275	80	71.02473	1	0.8413
10	PNFEA	0.555556	0.745356	25	24.25464	1	0.8413
	Generic	1	1	50	49	1	0.8413
11	PNFEA	0.004253	0.065219	1.079167	1.013948	1	0.8413
	Generic	0.012028	0.109672	2.400067	2.290395	1	0.8413
12	PNFEA	0.003668	0.06056	1.002083	0.941523	1	0.8413
	Generic	0.011134	0.105516	2.300013	2.194497	1	0.8413

B. Cost Estimations Analysis

The cost analysis aims in this evaluation to estimate the amount of money (USA Dollar currency) spend it to resolve the criminal case. The same rules of time analysis as described above will apply to the cost estimation. The PERT method used a form of three cost estimates combined by formula into an expected cost similar to determining expected time in PERT time.

The three cost estimate form is subject to probabilistic analysis in advance to identify the expected cost for each phase in network forensics approach. The three cost estimate is an optimist, most likely, and pessimistic cost estimate, which presents the best, expected average and worst cost scenario for each phase. This evolution values will be based on the information listed in [2], which indicate that the average cost to resolve the cyber attack is 22,986 USD per day. This evaluation assumes that this value presents the best cost case scenario to accomplish the phase activities. In other word, it presents the optimistic cost estimate, which named (c_o). The cost includes the estimation of the direct, indirect and opportunity costs, which associated with the criminal case resolving. In addition, it distributes to all the activities of network forensics centers as detection, analysis, recovery and preservation, and presentation activities as well as the cost of hardware and software.

The second estimated cost is the most likely cost value, which called (c_m). It estimates the expected average cost value to accomplish one phase activities. This value presents the expected average scenario. Accordingly, this value is greater than or equal to the optimistic cost (c_o). So, in this evaluation the most likely cost can be calculated using this formula:

$$c_m = (1+v) * c_o, \text{ where } v \in \mathbb{R} \text{ and } \geq 0 \text{ and } c_o = 22986 \quad (8)$$

The third estimated value is a pessimistic cost, which is called (c_p). It is the highest cost value to accomplish one phase activities and presents the worst case scenario. This value estimated when the phase or one of it is actively not works properly and something wrong happened such as user error, hardware or software stop working, This cause the necessity to use other resources which raise the resolving the of the criminal case. In fact, this value is greater than or equal to the expected average estimated value. So, in this evaluation the pessimistic cost can be calculated as the following:

$$c_p = (1+v) * c_m, \text{ where } v \in \mathbb{R} \text{ and } \geq 0 \quad (9)$$

From the above three cost estimation the expected cost, which called (c_e) for each phase will be estimated based on the PERT method as the following:

$$c_e = (c_o + (4 * c_m) + c_p) / 6 \quad (10)$$

The variance (σ^2) (descriptive measurement) of optimistic and pessimistic cost measures the degree of uncertainty, which associated with the expenditure distribution for each phase. The variance for each activity calculated as the following:

$$\sigma^2 = ((c_m - c_o) / 6)^2 \quad (11)$$

Table 4 and Table 5 show the instance three cost estimations and the variance for each phase of the both generic network forensics and PNFEA approach respectively.

Table 4. Instance of Three Cost Estimations and Variances for Generic Approach Activities

ID	Activity (Phase)	c_o	c_m	c_p	c_e	σ^2
A	Preparation	$68,958	$137,916	$275,832	$149,409	1188801441
B	Detection	$68,958	$137,916	$275,832	$149,409	1188801441
C	Incident Response	$68,958	$137,916	$275,832	$149,409	1188801441
D	Collection	$68,958	$137,916	$275,832	$149,409	1188801441
E	Preservation	$68,958	$137,916	$275,832	$149,409	1188801441
F	Examination	$45,972	$91,944	$183,888	$99,606	528356196
G	Analysis	$45,972	$91,944	$183,888	$99,606	528356196
H	Investigation	$45,972	$91,944	$183,888	$99,606	528356196
I	Presentation	$45,972	$91,944	$183,888	$99,606	528356196

Table 5. Instance of Three Cost Estimations and Variances for PNFEA Approach Activities

ID	Activity(Phase)	c_o	c_m	c_p	c_e	σ^2
A	Preservation	$45,972	$91,944	$183,888	$99,606	528356196
B	Capturing	$45,972	$91,944	$183,888	$99,606	528356196
C	Classification	$45,972	$91,944	$183,888	$99,606	528356196
D	Analysis	$45,972	$91,944	$183,888	$99,606	528356196
E	Investigation	$45,972	$91,944	$183,888	$99,606	528356196

The frequency of occurrence the average expected cost (c_e) for each approach is close to the most likely estimation cost (c_m). That means to accomplish the activity phase it needs the average expected cost. For that the expected cost presents the approximately of the cost value for each phase.

Basic on the above information, which conducted from PERT method, it is important to extend more information as the most likelihood cost to resolve the criminal case. To analyze the probability of expenditure cost on the path to resolving the criminal case, this research used the normal distribution pattern as well as used in time analysis. First of all, the criminal case resolving variance, which named (σ^2_c) computed as the sum of all the variances of phases for each approach, as the Equation (5). To measure the confidence of expenditure cost to resolve the criminal case, the standard deviation, which called (σ_c) will be computed as the Equation (6).

The standard deviation means that the expensive cost needed to accomplish the resolving of criminal case need ($\pm\ \sigma_c$). To achieve acceptable value, the result of experiments in this paper will be on both plus and minces standard deviation and always find that the same expensive cost needed to accomplish resolving the criminal case. The probability of accomplishing the resolving the criminal case with this expenditure cost conducted from the formal normal distribution table, after converting and computed the z-score as the following:

$$z = (Actual\ Cost - Expected\ Cost) / \sigma_c \qquad (12)$$

Where the Actual Cost is the cost value needed to accomplish resolving the criminal case which equals the sum of all expected average cost (c_e) for all phases. The Expected Cost presents the Actual Cost plus or minus the standard deviation (σ_c). Table 6 shows the instance of the research experiments that shows the expenditure cost and normal distribution of all phases for both PNFEA and generic approach.

Table 6. Instance Experiments of the Expenditure Cost and Normal Distribution(P:PNFEA, G: Generic Approach)

Ex#		σ^2_c	σ_c	Due Date	Expected Date	Z	Proba_ bility
1	P	660445245	25699.13	$249,015	$223,316	1	0.8413
	G	3170137176	56303.97	$697,242	$640,938	1	0.8413
2	P	114660632.8	10707.97	$177,184	$166,476	1	0.8413
	G	550371037.5	23459.99	$496,115	$472,655	1	0.8413
3	P	458642531.3	21415.94	$354,368	$332,952	1	0.8413
	G	1398859720	37401.33	$815,045	$777,644	1	0.8413
4	P	2641780980	51398.26	$498,030	$446,632	1	0.8413
	G	8057431989	89763.2	$1,145,46	$1,055,70	1	0.8413
5	P	165111311.3	12849.56	$124,508	$111,658	1	0.8413
	G	792534294	28151.99	$348,621	$320,469	1	0.8413
6	P	28665158.2	5353.985	$88,592	$83,238	1	0.8413
	G	137592759.4	11729.99	$248,057	$236,327	1	0.8413
7	P	73382805	8566.376	$95,775	$87,209	1	0.8413
	G	352237464	18767.99	$268,170	$249,402	1	0.8413
8	P	3595757445	59964.63	$268,170	$208,205	1	0.8413
	G	17259635736	131375.9	$750,876	$619,500	1	0.8413
9	P	16511131125	128495.6	$861,975	$733,479	1	0.8413
	G	42562026900	206305.7	$1,838,88	$1,632,5	1	0.8413
10	P	293531220	17132.75	$574,650	$557,517	1	0.8413
	G	528356196	22986	$1,149,30	$1,126,31	1	0.8413
11	P	2247348.403	1499.116	$24,806	$23,307	1	0.8413
	G	6354997.878	2520.912	$55,168	$52,647	1	0.8413
12	P	1937764.695	1392.036	$23,034	$21,642	1	0.8413
	G	5882501.453	2425.387	$52,868	$50,443	1	0.8413

The probability of resolving the criminal case with the expected average of expenditure cost both PNFEA and general network forensics approaches is 84.13%. This ratio is acceptable that based on the uncertainty values and the methods to estimate the cost, which depends on the time. Therefore, there is a probability of 15.87% as a risk to uncover the criminal case at the average of the expected cost. However, the experimental results of the PNFEA approach minimize the cost by 59.45% of the average as shown in Fig. 2. The experiment related to the backdoor and worms attack, the PNFEA minimize the expensive cost by 55.04% and 56.43 respectively, with the error ratio between 0.0005% and 0.0028% from the expected average cost.

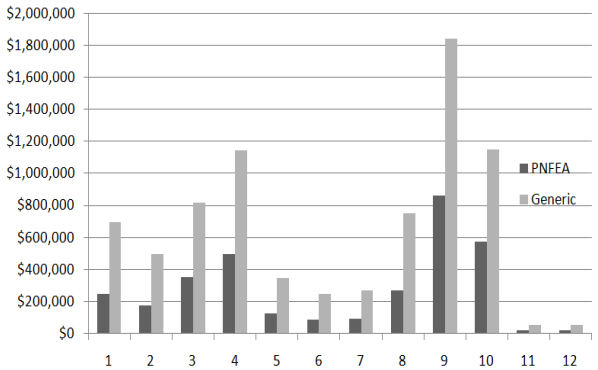

Fig. 2. The Experimental Results of the Cost Average

VI. Conclusion And Future Work

Most existing frameworks and models in network forensics serve as a guideline in the investigation of cybercrimes without enough information or details on how to analyze the evidence. In addition, the vagueness of each phase process is a gap exists in the network forensic phases of these frameworks and models. This gap exists because investigators have difficulty understanding how the phases work and how the outcomes for each phase are achieved. Considerable time is consumed to understand the phases as the researchers focus on the number and ordering of phases rather than the core operations inside these phases

Cyber crimes produce a large volume of evidence through network monitoring and capturing tools. Nevertheless, a significant amount of time is required to discover the real perpetrator. In general, the current network forensic investigation approach, which is reactive, is time consuming, costly, and error prone as it requires much effort to analyze the overwhelming amount of evidence presented in each case. Moreover, gathering useful evidence through the reactive approaches is difficult because the evidence is collected right after the detection of the cyber crime. Thus, a new approach is needed to analyze evidence and enhance the investigation process. In this paper, we proposed a new approach, which employs the proactive process to resolve cyber crime for network forensics. The results of the comparison of the proposed approach prove that it is more efficient in terms of time and cost. Furthermore, the results proof the controversy, which is the time needed to resolve or contain the criminal cases increases the cost.

Acknowledgment

This research is funded by the Deanship of Research and Graduate Studies in Zarqa University /Jordan.

References

[1] CERT, CSO & SERVICE, U. S. S. (2011) 2011 Cyber Security Watch Survey. Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte.

[2] Ponemon (2011) Second Annual Cost of Cyber Crime Study. Ponemon Institute.

[3] Palmer, G., A Road Map for Digital Forensic Research, in Report from DFRWS 2001, F.D.F.R. Workshop, Editor 2001: Utica, New York. p. 27–30.

[4] Alharbi, S., et al., The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review Information Security and Assurance, 2011, Springer Berlin Heidelberg. p. 87-100.

[5] Garfinkel, S.L., Digital forensics research: The next 10 years. Digital Investigation, 2010. 7, Supplement (0): p. S64-S73.

[6] Grobler, C.P., C.P. Louwrens, and S.H. von Solms. A Multi -component View of Digital Forensics. in Availability, Reliability, and Security, 2010. ARES '10 International Conference on. 2010.

[7] Grobler, C.P., C.P. Louwrens, and S.H. von Solms. A Framework to Guide the Implementation of Proactive Digital Forensics in Organisations. in Availability, Reliability, and Security, 2010. ARES '10 International Conference on. 2010.

[8] Pilli, E.S., R.C. Joshi, and R. Niyogi, Network forensic frameworks: Survey and research challenges. Digital Investigation, 2010. 7(1-2): p. 14-27.

[9] Reith M, C.C., Gunsch G An Examination of Digital Forensic Models. International Journal of Digital Evidence, 2002. 1(3): p. 12.

[10] Carrier, B. and E.H. Spafford, Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, 2003. 2(2): p. 20.

[11] Stephenson, P., A COMPREHENSIVE APPROACH TO DIGITAL INCIDENT INVESTIGATION, in Information Security Technical Report, E.A. Technology, Editor 2003. p. 42-54. ICIT 2013 The 6thInternational Conference on Information TechnologyMay 8, 2013

[12] Baryamureeba, V. and F. Tushabe. The Enhanced Digital Investigation Process Model. in Proceeding of Digital Forensic Research Workshop. 2004. Baltimore, MD.

[13] Carrier, B.D. and E.H. Spafford, An event-based digital forensic investigation framework, in Proceeding of the 4th Digital Forensic Research Workshop DFRWS20042004. p. 11-13.

[14] Rogers, M.K., et al., Computer Forensics Field Triage Process Model. Journal of Digital Forensics, Security and Law, Vol. 1(2), 2006. 1(2): p. 19-37.

[15] Ciardhuáin, S.Ó., An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 2004. 3(1): p. 1-22.

[16] Wei, R. and J. Hai. Modeling the network forensics behaviors. in Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on. 2005.

[17] Kohn, M., J. Eloff, and M. Olivier, Framework for a digital forensic investigation, in Proceedings of Information Security South Africa (ISSA) 2006 from Insight to Foresight Conference2006.

[18] Kent, K., et al., Guide to Integrating Forensic Techniques into Incident Response, 2006: p. 1-121.

[19] Ricci S.C, I., FORZA - Digital forensics investigation framework that incorporate legal issues. Digital Investigation, 2006. 3, Supplement(0): p. 29-36.

[20] Yong-Dal, S. New Digital Forensics Investigation Procedure Model. in Networked Computing and Advanced Information Management, 2008. NCM '08. Fourth International Conference on. 2008.

[21] Mohammad Rasmi, A. Jantan, and Hani Al-Mimi. (2013) A New Approach For Resolving Cyber Crime In Network Forensics Based On Generic Process Model. The 6th International Conference on Information Technology (ICIT 2013).

[22] Siti Rahayu Selamat, R.Y., Shahrin Sahib, Mapping Process of Digital Forensic Investigation Framework. IJCSNS International Journal of Computer Science and Network Security 2008. Vol. 8(No. 10): p. 163-169.

[23] Pilli, E.S., et al., A Framework for Network Forensic Analysis, Information and Communication Technologies, 2010, Springer Berlin Heidelberg. p. 142-147.

[24] Pilli, E.S., R.C. Joshi, and R. Niyogi, A Generic Framework for Network Forensics. International Journal of Computer Applications, 2010. 1(11): p. 1-6.

[25] K. K. Sindhu,B. B. Meshram,"Digital Forensic Investigation Tools and Procedures", IJCNIS, vol.4, no.4, pp.39-48, 2012.

Authors' Profiles

Mohammad Rasmi is currently serving as an assistant professor in the Faculty of Science, Departments of Computer Science, Zarqa University. He received his PhD in Network Security from Universiti Sains Malaysia in 2013. He received M. Sc. in computer information system from the Arab Academy for Banking and Financial Sciences in 2004, and .Sc. degree in computer science from Zarqa Private University in 1999. His research interests include network forensics, web security, E-government strategy, cloud computing and software engineering.

Ahmad al-Qerem obtaining a BSc in 1997 from JUST University and a Masters in computer science from Jordan University in 2002. PhD in mobile computing at Loughborough University, UK in 2008. He is interested in concurrency control for mobile computing environments, particularly transaction processing. He has published several papers in various areas of computer science. After that he was appointed a head of internet technology Depts. Zarka University.

How to cite this paper: Mohammad Rasmi, Ahmad Al-Qerem,"PNFEA: A Proposal Approach for Proactive Network Forensics Evidence Analysis to Resolve Cyber Crimes", IJCNIS, vol.7, no.2, pp.25-32, 2015.DOI: 10.5815/ijcnis.2015.02.03

