Computer Network Forensics Assistance Methodology Focused on Denial of Service Attacks

Hans Newton Fonseca Cantanhede
Federal University of Maranho (UFMA)
Computer Science Postgraduate Program
Av. dos Portugueses, 1966 Bacanga –
CEP 65080-805, Sao Lus – MA – Brazil

Samyr Beliche Vale
Federal University of Maranho (UFMA)
Computer Science Postgraduate Program
Av. dos Portugueses, 1966 Bacanga –
CEP 65080-805, Sao Lus – MA – Brazil

ABSTRACT

The problem addressed in this paper is the difficulty in criminalizing denial of service attacks in Brazil. With the advent of Law 12.737 of 2012 in Brazil, known as the Computer Crimes Law, these attacks could be considered crimes. However, no procedures were found to support it. This paper proposes a methodology based on the 2012 Computer Crime Law to assist computer networks forensic analysis, focused on charging offenders who commit denial of service attacks, as well as to present a computational architecture to automate its steps. For this purpose, it was promoted a review of related works and also dedicated sections for the clarification of terms needed to contextualize the research. At the end of the article, the methodology and its steps are presented, and also the proposed architecture and the results of experiments performed to validate the proposal. It is concluded that the availability of the information obtained by the aid of the proposed methodology demonstrates that the investigation authority can proceed with the duly substantiated liability of the offending agents.

General Terms

Forensics, Network attacks, Crime detection

Keywords

Forensic network analysis, Assistance methodology, Denial of service, Computer crime law, Computer architecture

1. INTRODUCTION

Nowadays, information is one of the most valuable assets. The advantage of digital production, the connections made through social networks, and the use of software as a service are features of what is called the 4 Industrial Revolution. And all these elements are object of interest to the companies, because the more they understand the customers and their relations with the company, they can increase their outreach, productivity, and efficiency[38]. Internet of Things (IoT), Cyber Physical systems, Artificial Intelligence (AI), Big Data and Cloud Computing are emerging areas with the aim of efficient problem solving, using agility and searching for sustainability[5]. The products of this new revolution involves many network assets and these can be vital for proper functioning of the described areas. These assets can be vulnerable and these vulnerabilities are explored by cyber attacks, and because of anonymity on the internet, there is a sense of impunity. In Brazil, a law was created to try mitigating these criminal activities and enable the possibility to charge offending agents of those activities, and by that ensure the information security

The security information is present in requirements and planning services[23]. The use of techniques or technologies like intrusion detection system (IDS), which is responsible for network monitoring, [32],[11] shows the attempt to ensure the security information principles: confidentiality, integrity, availability.

The companies security infrastructure, built in those principles, is many times tested. Offenders, also known as crackers, take advantage of failures in services, applications or communications that operate over the internet with the aim of damaging, stealing data, causing unavailability of services or even destroying data. The Denial of Service (DoS) and its variation called the Distributed Denial of Service (DDoS) are examples of attacks that have being growing up [27] and many users or service providers, who are suffering these attacks, do not have any information about them because of the lack of monitoring investment.

When some type of monitoring is done to protect the network, a lot of information can be generated, however, perpetrators of malicious activity are rarely charged[9]. The possible reason for that is the lack of mechanisms to assist criminal prosecution like: laws, methodologies or technologies. Therefore, the perpetrators have the feeling of impunity and usually think that they won't be charged by their acts, because of the companies protection mechanisms deficiency or even loopholes in the law that do not typify those activities as crimes.

It has been seen an increase in the number of malicious actives like: exposing personal data, as photos, through security gaps in victims' computer[19]. Since the Law 12.737, called Computer Crimes Law, was approved in 2012 in Brazil, it started to be possible to typify some activities in digital environment as crimes. Not all malicious activities were typified, however, this is considered progress when it comes to charging offenders.

It is know that IDS can track malicious activities, however, these records are lost inside the large volume of data that these tools generate. The clarification of this malicious activity is under responsibility of network expert, that needs to explain through evidences: the author; the cyber attack technique used in which network the fact occurred; who was the destination host; authors intention or motivation; the damage caused, if there were an attempt or actual attack and them react building security directives to protect the network.

The network expert may not hold the necessary knowledge to determine, among all malicious activity occurred, which of them are crime or not. In the investigation process made in forensic analysis it is necessary the communication with that expert in providing the evidence, represented by IDS historical data so this can be analysed searching for criminal offenses. Another problem is that the data can be deleted or lost, eliminating possible evidence for malicious activity, by the dynamism and large volume that happens in network traffic.

Hence the objective of this work is creating a methodology to assist the Network Forensic Analysis, focused on criminalizing denial of service attacks, according to Brazilian Computer Crimes Law. This methodology will be composed by steps: the elaboration of malicious activity behaviour model and of a computer crime model, and also a computer architecture which will automatize those steps. The data model should assist in clarification of malicious activity occurred on the network, by the logs registration and interpretation from security tools like IDS, well as its correlation with the legal elements of malicious activity, provided by the Brazilian penal legislation known as Computer Crimes Law. The proposed architecture will provide assistance in network forensic analysis, in extraction of malicious activity evidence, in correlation of evidence founded that will form the behaviour model of malicious activity, united with the descriptive crime model. Then it will be able to identify the necessary elements of the crime to proceed in a penal prosecution: the source, the author, the time of the fact, making these information available so they can be interpreted by the investigation authority. A series of experiments were conducted, to validate the methodology and computational architecture, using denial of service simulating scenarios.

Section 2 presents a background for the research contextualization, defining basic concepts as well as the presentation of the law used in the research. Section 3 presents the research-related papers. Section 4 presents the methodology to aid computer networks forensic analysis focused on denial of service attacks. Section 5 details the experiments performed as well as the results for validation of the research. In section 6 there is a brief discussion of the results. Section 7 presents the conclusion and future work.

2. BACKGROUND

Since its invention in the 60s, the internet has been evolving, so nowadays it resembles to basic resources like water and electricity. The internet can be used in many areas [22] like: e-commerce, games, education, social networks, hence benefiting like agile information availability, resources sharing and information exchange. However, these scenario also brings appropriate context for criminality. Being used by criminals as a way, as much as a focus for the attack [33]. Cyber attacks, information stealing, information destruction, industrial secrets revealing are more and more common in the news. The next section will bring necessary concepts for the research.

In Figure 1, a typical scenario of a corporate network is presented. This scenario contains network assets that are physical and logical elements in networks like: routers, switches, servers (firewalls, domain name servers (DNS), web servers, email server). The assets usage implies in some sort of storage by them with logs. A log of an event is a record or a set of them, stored in files or database, which contain activity from applications or operational systems[15]. Together they are used to document operations or inside and outside events occurred for maintenance, debug or necessary analysis.

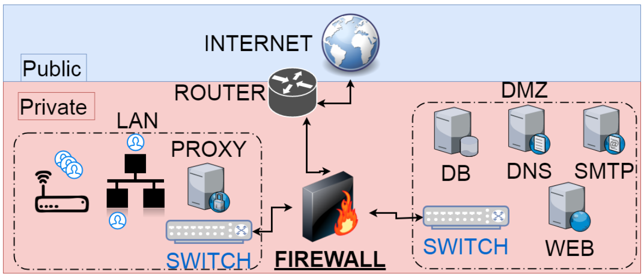


Fig. 1. **Typical scenario of a corporate computer network.**

In the same Figure 1, a division of the network is clear: the public area and a private one. The public represented by the internet link access symbolizes the outside, with network assets that are not controlled by someone in the private network, but controlled by the Internet Service Providers. The router is the gateway between the public and private area. In the private area there is the capacity of control and management, because the assets are under control of a network administrator.

The presence of local networks (LAN) wired or wireless, firewalls, proxy servers, demilitarized areas providing access to database, domain name servers, email servers and web servers, represent the network assets of the private area. These network assets are configured by human, in attempt of assuring data protection and right functioning of network environment, however they are sensitive to failures and vulnerabilities caused by bad management by the responsible administrator.

In both physical (hardware) and logical topology (such as software) there may be vulnerabilities and thus suffer attacks.A vulnerability is defined as a found failure, in other words, system weakness that allow an intruder to execute commands, generally caused by human errors, and the attacks are manifestations of intruders to cause damage to topology by exploring their vulnerabilities[1]. It is necessary to say that in computing area it is hard to find systems one hundred percent fail safe, however, the aim is the possibility to minimize their negative effects, as much as possible.

If the attack is a harmful activity or at least injurious, it can be considered as a criminal activity. In Brazil, a criminal activity has to violate constitutional and penal principles, as the principle of legality, in its 1st article says that *"There will be no crime without previous law that define it. (art 1, Penal Code)"* [40], in other words, crime only exists when there is a law and a typical activity happens after the law creation.

2.1 Computer Crime Law and the elements used by forensic science

The offense according to brazilian law must contain the following elements: typicality, unlawfulness, culpability and be punishable[8]. Typical is the fact that resembles what is described in the law. Unlawful is the act against what the human behavior should be and against the legal system. Culpable is the act occurred where you analyze the intention or not from the offending agent. Punishment is the possibility for the offending agent be punished by your acts, fixed by the law.

The Criminalistics, according to [30], also known as Forensic Science, is the scientific-technical and penal-juridic discipline that aims to solve criminal offenses, in other words, prove its materiality and authorship. The Forensic/Criminal Expertise is the practical and concrete acting of Criminalistics, which from your procedures, techniques, methods and theories to execute forensic analysis on evidences[6], hence the forensic expertise is Criminalistics in practice. According to [42], to solve a crime it is necessary to answer a few questions:

(1) What has happened?
(2) Where has it happened?
(3) How has it happened?
(4) When has it happened?
(5) Who has done that?
(6) Why?

The items 1,2,3 and 4 refer to the materiality, the item 5 refers to authorship, and item 6 refers to the motivation. Knowing the malicious activity, discovered the criminal offender responsible for the activity and knowing that the fact is a typical fact described in the law, the culpability of the agent must be showed. Even if the criminal offender did not have the intention, but if he or she had consciousness of his or her acts, then he or she can be punished. Only the imputable, in other words, the one that can be charged of accusation and have full consciousness of the illegality can be criminally liable for their acts. Hence, the motivation of the offender must be very clear to proceed in the next phases of prosecution.

Brazilian legislation that bases the identification of network crimes is the Law 12.737 of 2012, called Computer Crimes Law, that treats the interruption or disturbing of telegraphic service is presented and it's the legal base used for this research, because it gives support to penal prosecution when detected the malicious activity denial of service has occurred:

> Art. 266. Interrupt or disturb telegraphic service, telegraph, radiotelegraph or phone, prevent or difficult its re-establishment: Penalty - detention of one to 3 years, and penalty. 1 Incurs the same penalty for those who interrupt telematic service or public information utility, prevent or difficult its re-establishment.

In the legal field, the verbs are the principal elements of law that describe the behavior to be verified, hence the presence of those behaviors assure the existence of the offending fact. So if, for example, the verb in the law is "subtract", in this case if this action did not occur, then there is no crime, since the law is clear in the element that follows it.

Knowing the formal base concepts, it is possible to highlight the technical part of the attacks to be focused and that has compatibility with the data security research context. More precisely, it will be discussed about the denial of service attacks, which are the aim of the research for constituting offense that could be charged in Brazil.

2.2 Criminal cyber attacks outside the law

A cyber attack very familiar in the literature is the denial of service attack (DoS). It affects the quality that the network bandwidth can support, of computer network services, through a packet overload, so legitimate requests can not be answered properly [11]. Depending on the strategy used, the DoS can be categorized in Volume Based Attack, Protocol Attack or Application Level Attack [27].

Application based attacks are focused on services that run over the application level of the network, so HTTP, DNS, SMTP, SSL are examples of protocols of that level, or even applications that support or are supported by those protocols, like operating systems, and web servers. The basic idea is to break the server sending as many messages as they can not answer for overload of requests[41]. The web servers are the main focus of this technique and so are the applications that use the web to deliver its services. Examples of the attacks in this category are: slow post, get flood and slowris.

Hence in the most part of the cases, the motivation from offending agents using this kind of technique is the deny legitimate requests of the services, in other words, to cause unavailability. Therefore, ways of effective verifying the occurrence of these attacks must be created. It is also necessary a legal base that assist in charging offenders. Next, is present the discipline to formalize computer crimes, necessary for charging criminals. There will also be ways to find out if the DoS attack happened using the available tools, important step in charging offending agents.

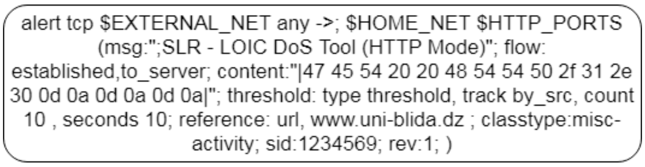
2.3 Computer Networks Forensic Analysis

The use of computer systems as a way or end to committing crimes produces logic or physical evidence [2], [28]. The Computer Networks Forensic Analysis studies the formal procedures to characterize a malicious activity in computer networks and to find the elements that formalize the crime, if it has happened. The procedures involve: the evidence identification, its isolation and preservation, extraction for analysis and correlation and its presentation in forensic report.

In identification process the interest evidence, logical or physical, are identified like network traffic or even logs of ids tools. In preservation process a hash is generated. The hash is an integrity assurance mechanism that uses cryptography to alert changes in a digital artifact[12]. All found evidences, like logs of any file of interest, must go through this step and have their hashes stored. This is an important requirement when an evidence is presented to an investigation authority. Another way to assure the integrity and authenticity is by using a blockchain. Known as a "confidence protocol", it is a distributed database that uses decentralization as security. It works like an open place, where everyone can publish their data. Forming a structured chain of blocks, where the information of one block is guaranteed by the previous block [16]. The publishing of evidences in this blockchain could increase the guarantee of integrity and authenticity of evidence found.

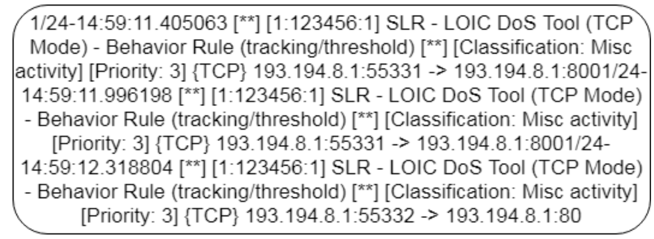
After the identification and preservation of the evidences, a copy of them is made, so there will not be a risk of infecting the original evidence. Many of these evidences, when digital, are unintelligible by man, like bits and bytes. In the extraction process transformations, normalizing and cleaning steps are made, in other words, manipulations that do not affect information, but allow its correlation and also properly visualization.

In the analysis process the knowledge is discovered. A great deal of information can be invisible, and they can be key to penal prosecution, so in this process, by proper examinations for every type of evidence, these pieces of information can lead to discovering the vital information for the investigation. All



```
alert tcp $EXTERNAL_NET any ->; $HOME_NET $HTTP_PORTS
(msg:";SLR - LOIC DoS Tool (HTTP Mode)"; flow:
established,to_server; content:"|47 45 54 20 20 48 54 54 50 2f 31 2e
30 0d 0a 0d 0a 0d 0a|"; threshold: type threshold, track by_src, count
10 , seconds 10; reference: url, www.uni-blida.dz ; classtype:misc-
activity; sid:1234569; rev:1; )
```

Fig. 2. **Denial of service detection rule. Adapted from [35]**



```
1/24-14:59:11.405063 [**] [1:123456:1] SLR - LOIC DoS Tool (TCP
Mode) - Behavior Rule (tracking/threshold) [**] [Classification: Misc
activity] [Priority: 3] {TCP} 193.194.8.1:55331 -> 193.194.8.1:8001/24-
14:59:11.996198 [**] [1:123456:1] SLR - LOIC DoS Tool (TCP Mode)
- Behavior Rule (tracking/threshold) [**] [Classification: Misc activity]
[Priority: 3] {TCP} 193.194.8.1:55331 -> 193.194.8.1:8001/24-
14:59:12.318804 [**] [1:123456:1] SLR - LOIC DoS Tool (TCP Mode)
- Behavior Rule (tracking/threshold) [**] [Classification: Misc activity]
[Priority: 3] {TCP} 193.194.8.1:55332 -> 193.194.8.1:80
```

Fig. 3. **Snort generated alert from correlating the previous rule to the denial of service attack. Adapted from [35]**

knowledge must come from the evidences. In the analysis all the chain of custody, which is the proof of the correlation of the events, showing since they were collected until when the key knowledge was discovered from events occurred, documenting the operations and obtaining the answers to the questions made by the investigation authority[39].

Last, the forensic report is formalized, documenting all steps proceeded, the information extracted, the sources of the information, as well as the procedures done which will allow replicability and serve as free conviction of the judge. In other words, the judge will take the forensic report as base to his decision, but the forensic report will not force him to follow what is in it. This idea shows us how important is presenting the information in the forensic report in a well justified way and the procedures well described, so that the judge can get all the matters of the fact analysed.

2.4 DoS attack alerting

For alerting DoS attack it is necessary to establish an environment to monitor the network traffic or the system at issue. The Intrusion Detection Systems are capable of filtering communications and alerting malicious activity, which try to break the security information principles: confidentiality, integrity, authenticity and availability or the ones that tries to break security mechanisms of a computer or network [4]. IDS has three modules: monitoring module, decoding the traffic from the source, like network packets, the detection machine module that uses correlation rules and matching patterns and the alert module that enables the expert to analyse the information about malicious activity identified[25].

IDS rule writing can be a complex task. It is necessary to acknowledge the communication that occurs, at network protocol level. A computer network expert usually is responsible for writing these rules. In Figures 2 and 3 examples of rules for detecting denial of service attack and its respective alert raised by IDS snort.

The information that characterize the malicious activity as crime can be extracted from the generated alerts. In Table 1 these characteristics are: the source, the technique, the moment, which are extracted and stay in disposal to analysis.

Table 1. **Information extracted from IDS alert**

[redacted] INFORMATION	IDS ALERT INFORMATION EXTRACTION
Source Logical Adrress (IP), Source Physical Address(MAC)	193.194.8.1:55332
Technique used	SLR - LOIC DOS Tool (TCP)
Explain how attack occured	+10 Packets/10 sec
Timestamp	1/24-14:59:11.405063
Destination Logical Adrress (IP), Destination Physical Address(MAC)	193.194.8.1:80
Main element identified: disturb, prevent or hamper connection establishment	DISTURB

Hence, the IDS can be a source of evidences that a malicious activity occurred. These evidences, can be valid to the judge, but there is only one thing that separates the companies to charge the offenders: an expert to extract those evidences using procedures of forensic analysis, ensuring that the probative value of the content presented is licit and that there was no modification in the source of the evidence.

There are other tools that try mitigating the malicious activity in computer networks, like firewalls. These can also be source of evidences, when properly configured to store the evidences that can be analysed for a forensic interest.

3. RELATED WORK

The increase of internet use, provides an interesting scenario for cyber attacks[29]. In this section, related works to information security, DoS identification and typification of digital crimes are presented.

Works interested in classifying cyber attacks were observed. The intrusion detection systems already perform this task, generating alerts of malicious activity on computer network or individual hosts[31]. It is argued that the increase of threats has promoted the search of new ways to identify cyber attacks in computer networks. Using various techniques based on statistics like machine learning algorithms, multivariate correlation analysis, naive bayes classifier, behaviors profiles and data mining generate substantial growth in detection of cyber attacks[24]. The point is to identify the attacks as fast as they can, enabling a faster countermeasure decreasing the effects of the attacks.

DoS victims grow every year. A way to identify this attack is monitoring: the network flow, the memory of the server, the CPU load average, database space or storage disk space. The author [35] used an architecture with Snort IDS and created a more efficient algorithm in detecting DoS and DDoS attacks. He also proposed a model or an architectural change to automatic filtering these attacks in a computer network real time monitoring. The author selected DoS attacks of type UDP, TCP and HTTP implemented in a proper tool to evaluate his proposal, achieving 43.5% improvement in detection of DoS and DDoS attacks.

To test monitoring architectures, and evaluate the efficiency of ids configuration, it is required a way of simulating the network traffic. Works interested in simulation of malicious traffic and generating data sets, for training and efficiency tests in malicious activity detection[21], were observed. The authors [17], created a data set represented by files in PCAP format, which is a well known extension of packets in network traffic[3], this data set has scenarios of evaluating cyber attacks in computer networks, including DoS and DDoS. The architecture and the network assets of the test environment were presented and the moments of each attack where marked, so it will be possible to visualize the scenarios, as well as to extract characteristics when using it to aid cyber attacks detection. The lack of data sets of denial of service attacks in application layer was the motivation of the authors[14]. The authors [13], [26], [18] presented a detection model based in CUSUM algorithm, that has already been used in detecting of DoS attacks and they aim on DoS attacks that produce a small amount of packets to disturb the network service.

There are also digital crime generic investigation process. Based on DFRWS Framework, a generic road map of base activities, that are: identification, preservation, collection, exams, analysis and presentation, the author [39] define the End-to-End Digital Investigation (EEDI) process, to aid digital investigations. This process contains steps that the investigator must perform to fulfil the base of the framework. The steps of collecting evidences, analysis of individual events, preliminary correlation, events normalization, removing conflict events, second level of correlation, timeline analysis, chain of custody construction and corroboration must be applied in every activity of the base framework, serving as a checklist, assuring the applicability of the process to the base framework. Without giving focus in any specific malicious activity, the author also speaks about techniques to determine: if the attack has really happened, if there was premeditation, in other words, the motivation of the attack or yet if the attack was spoofed so it would not be recognized.

For being a relatively new law, it has been observed works backed to its understand and the reaches that law 12.737 of 2012 can have. However, a gap was found in lack of works backed to criminal typifying, in other words, works that show which malicious activity can be characterized as crimes according to Brazilian computer crimes law. Another gap was the absence of methodologies that make the subsumption between the given computer crimes law, to its characterization and enables its correlation with malicious activity occurred, so a formal document can be presented as forensic report, opinion or technical report. Also there was not found a computational architecture that automates this process and enables a person, without specialized knowledge in computer networks, to succeed in presenting a formal document, with enough evidences to charge offending agents of denial of service attacks or other malicious activities that could be framed in this penal legislation.

4. PROPOSED SOLUTION

The approach for solving this problem involved the definition provided in the legal provision to characterize cyber crime, an analysis to identify the compatible malicious activity to this legal base, the subsumption of the fact to the legal regulation, in other words, the violated elements of the law, extracting this elements which are necessary for classifying the malicious activity of denial of service and by that generating a correlating model between what is defined as crime and the suspicious activity.

The methodology to assist computer network forensic analysis focusing on denial of service attacks is proposed, following the protocol of Standard Operational Procedure[10], with the aim to serve as complementary resource to beginners as much as to experts, acting like a checklist that makes this methodology applied to the identification of evidences, its preservation, collection procedures, exams, analysis and formal presentation.

It will be proposed the creation of a computational architecture that automates the process made by the expert in computer networks responsible for writing the forensic reports that serve for judges appreciation and reasoning of investigation authority to its convincing. Then, the experiments made for validating the proposed solution are presented, showing the applicability of the solution in simulated situation close to the reality. The phases of the methodology are detailed in the next subsection.

4.1 Applied Methodology

The methodology to assist the forensic analysis in Computer Networks must comply with the fundamental principles of forensic computing, with a focus on criminalizing denial service attacks.

This methodology assumes in practice the format of protocols procedures, in other words a Standard Operational Procedure[36], the use of experimental controls and extensive bibliographic research made before the experiment[7]. The proposed steps to the process to be followed for denial of service analysis are:

—**Identify the malicious activity that resembles the violation of computer crime law**: In this step, studies are done to define what can be criminalized from the law;

—**Identifying and recording the elements of the crime**: knowing the legal legislation that helps charging the offenders, a threshold can be set for tracking the crime in malicious activity.

—**Creating the behavior data model and crime model**: knowing the malicious activity that can be criminalized and its respective legal provision it is possible to measure in a data model way so the important behavior elements of the evidence can be monitored and stored until they reach the minimum needed to be considered relevant, in other words, to be considered crime;

—**Capture ids events**: The ids events become clues of attacks, so that must be captured for later analysis;

—**Data preservation and its analysis**: the events as any other evidence related to the crime must be preserved to maintain the integrity and specialized exams must be used for correlating facts, extraction of necessary information for crime solving;

—**Fact subsumption with the legal base described in the law**: correlation between the malicious activity and what it is considered crime;

—**Providing evidence to the investigation authority**: it is necessary to set the information and formalize it for the investigation authorities.

4.2 Model proposition

Two models will be defined: the one about crimes and another one about malicious activity behavior.
The crime model serves as parameter to alert the elements of malicious activity that characterize the crime and must become from computer crime law requirements, as it defines what is crime. From these requirements it is possible to identify the characteristics that must be observed in malicious activity behavior.

As shown in Table 2, the elements for defining the denial of service attack are: the interruption, the disturbing, prevent or difficult the establishment of the service, causing service unavailability to legitimate requests. Then, the malicious activity that achieve

Table 2. **Mapping malicious computer law verbs to malicious activities, their results and motivations**

[redacted] *BASE*	*VERB*	*MALICIOUS ACTIVITY*	*RESULTS*	*MOTIVATION*
Article 266	Interrupt	http slowris slowhttptest	OVER LOAD THE SERVER	DENY SERVICE TO LEGITIMATE REQUESTS MAKING SERVICE UNAVAILABLE
Article 266	Disturb	http DoS goldeneye	UNABLE TO RESPOND TO REQUESTS FOR LACK OF RESOURCE	
Article 266	Prevent or hamper	syn flood hping3	PREVENT RESPONSE TO REQUESTS	

Table 3. **Crime characterization model**

[redacted] *(METRICS)*	*TYPE*	*DESCRIPTION*
TOTAL REQUESTS	number	total number of requests on the experiment
DENIED REQUESTS	number	number of requests with status code 408
TOTAL IPS DISCOVERED	number	amount of IPS found in the requests
TOTAL IPS REPEATED	number	of all IPS, this metric tells how many times the same IP appear in requests
UNAVAILABILITY TIME	number	difference between first and last generated alert, considering unavailability occured during alert generation
ALERTS ON IDS	number	evidence of cyber attack occurence
AVERAGE OR REQUESTS	number	the average number of requests in the unavailable interval

Table 4. **Model for characterization of malicious activity behavior**

[redacted] CRIMINAL TYPE	COMPUTER NETWORK INFORMATION
Author(who)	Source Logical Adrress (IP), Source Physical Address(MAC)
Materiality(what)	Technique used
Facts(how)	Explain how attack occured
Time(when)	Timestamp
Victim(where)	Destination Logical Adrress (IP), Destination Physical Address(MAC)
Penal type(why)	Main element identified: disturb, prevent or hamper connection establishment

service unavailability, in other words, that perform denial of service attacks, have singular characteristics which defines it. These characteristics must be monitored and then defined thresholds to alert relevant variations in that monitoring.

The HTTP type of DoS attack, focus on HTTP communications, performing a large volume attempts of connections thought HTTP protocol, overloading the server, so the monitored element in this type of DoS attack must be the number of missed requests, highlighted by the code 408 - REQUEST TIMEOUT. A large volume of this kind of answer in a web server can be a clue that it is under DoS attack. Unfortunately it was not found in the literature an exact definition of how many requests are necessary to make a service unavailable, it is possible that this value can variate given that the infrastructure available can contain more or less capacity of processing. Here, the considered amout will be the minimum amount necessary to make the server unavailable, in other terms, the much request it received that were possible to answer properly until it started to deny requests for not having enough capacity of processing to answer them properly, causing unavailability of the service. The presence of the alerts on IDS enriches the analysis and gives more information about the attack. If the attack is made directly, this is to say, the IP of the source is not spoofed, the IP address will repeat itself, proving the intention of the source to cause unavailability. However, it is known that crackers mostly use a technique of spoofing their IP. In this case many different IPs will be candidates to be the source, so the difference between the request times can be an element to notice the attack and reduce the search space of possible addresses from offending agents. In Table 3, the model of denial of service crime characteristics is presented.

From the overall requests received in an interval of time, the average requests per second can be calculated. It is possible to notice abnormal variation of requests, and estimate when the attack was started, building by that the chain of custody of the events, seeking to explain the truth in the evidence found.

For characterization of malicious behavior it will be necessary information which alert the presence of malicious activity occurred in the network. The alerts given by an IDS signal that information. Then, in Table 4 it is found that the information in computer network are elements that characterize the malicious activity behaviors, forming the representative malicious activity behavior model.

4.3 Architecture

To achieve the objectives and activities defined in this methodology, it will also be proposed a development of a computational architecture to assist the forensic expert that, preserving the clues given by the IDS and by mapping the security incidents characterized as crime, interpreting its penal elements in accordance with Brazilian Computer Crimes Law, will help the generation of forensic reports, in the context of forensic computer networks analysis. The proposed architecture is presented in Figure 4.

The first phase, called Pre-processing, contemplates the capture of data, storage and primary data normalization. The second phase, called Processing, has as its main steps the interpretation, accounting and correlation. The third phase, called Presentation, consists of the formalization and the provision of the data, in an organized way, through an interface, so the investigation authority can have them.

Initiated by IDS monitoring in step 1.1, log files will be generated with malicious activity alerts. Assisted by computer network forensic captor in step 1.2 to record this information in an alert database. In steps 2.1 to 2.3 there will be interpretation, accounting and correlation with the base of crimes typified by the Brazilian Computer Crime Law with malicious activities using the technique of views in the database. The crime base will be pre-configured with the rules used to identify criminal activity on computer networks.

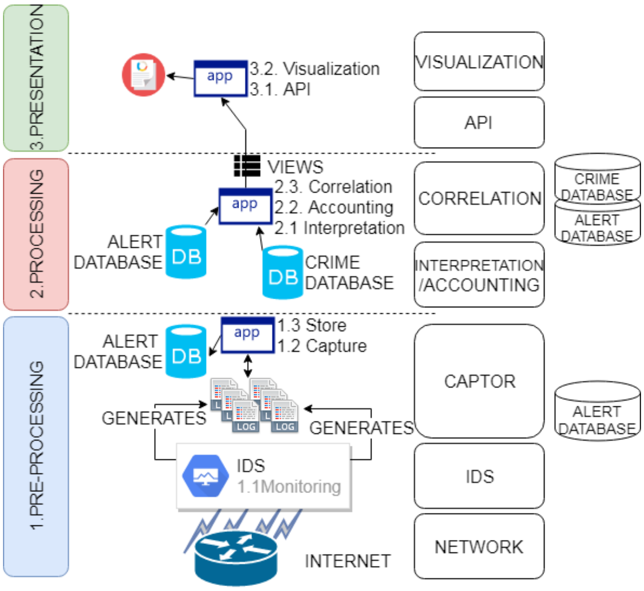


Fig. 4. **Proposed Solution Architecture**

Finally, in step 3, the exposure of the data through a Computer Network Forensic Application Programming Interface (APIForNet) to consult in the views provided by Phase 2, thus being able to generate activity reports, to assist in the charging of malicious activity in the context of computer networks properly supported by Brazilian computer crime law.

4.4 Identification of malicious activity and capture by IDS

This step consists of using an IDS to generate alerts of malicious activities that occur on a computer network. Among the available IDSs, Suricata was chosen because it is a free tool that provides not only flagged alerts, but various information about the origin of alerts as well, such as network traffic packets, network status information during monitoring and other information that can be used in a forensic analysis.

Writing rules for running IDS is usually the work of a specialist in charge of computer networking, such as the network administrator, who has the necessary knowledge to do so. Suricata already offers a set of free rules written by your community and can be used to detect some attacks including denial of service attacks.

Once the IDS is configured, alerts will be flagged and it will be made available in tool log files and these should be stored. Integrity assurance mechanisms, such as hashes, must be applied following the principle of information security integrity. It is also suggested that these logs can be published to a block-chain network, as it is quoted by [37],[20] this block network is also used for data integrity assurance. This information forms the basis of malicious activity behaviors.

4.5 Correlation of malicious activity with the model

After configuring the IDS, having the database of suspicious malicious activity, and the database of predicted crimes, it is possible to make the correlation between the two databases, and thus report the crimes occurred in an automated and intelligent way. An example of rules that could be used:

—If there are denial of service attack alerts, AND there are logs of type 408 server REQUEST TIMEOUT, it can be concluded that a crime has occurred.

4.6 Typifying

Article 266 of Law 12.737 of 2012 provides the legal basis for the research. In Table 2 the mapping of verbs related to the Brazilian Computer Crime Law with malicious activities that may occur on a computer network and its result is based on the goal generally proposed by the malicious activity of denial of service. This will serve as a reference for future reference by the law enforcement operators, to typify malicious activity in the context of computing.

Denial of service attacks must comply with the rule described for them to be held liable. If any malicious activity that causes harm to the service is mapped, but not in accordance with the law, it may not be classified as a crime but only as harmful activity. Having the article defined, it is necessary to characterize the malicious activity and analyze the elements needed to its criminal prosecution, as well as the purpose of the offender to continue a criminal prosecution and propose the perpetrators indictment.

Thus, it is important to define the following points to characterize the malicious activity: the origin or authorship (who performed the cyber attack), the destination or victim (who suffered the cyber attack), the technique used (materiality), the crime time (when it occurred), the motivation for the crime, and a law that defines malicious activity as crime [34]. Table 5, shows the information needed to characterize the crime with the available data from the occurred activity in computer networks.

Table 5. **Model for characterization of malicious activity behavior**

[redacted] TO CRIMINAL TYPE	MALICIOUS ACTIVITY BEHAVIOR ELEMENTS	EXTRACTION OF IDS ALERT
Author(who)	Source Logical Address (IP), Source Physical Address (MAC)	193.194.8.1:55332
Materiality(what)	Technique used	SLR - LOIC DOS Tool (TCP)
Facts(how)	Explain how attack occured	+10 Packets/10 sec
Time(when)	Timestamp	1/24-14:59:11.405
Victim(where)	Destination Logical Address (IP), Destination Physical Address (MAC)	193.194.8.1:80
Penal type(why)	Main element identified: disturb, prevent or hamper connection establishment	DISTURB

Table 5 shows the elements for subsumption of information required for criminal typifying, in a computer network context. This information is extremely important, as after identifying the malicious criminal activity, the preparation of the report must be proceeded to demonstrate the violation of the law elements for accountability of the authors.

5. RESULTS

In order to validate the methodology, some test scenarios were proposed, simulating a forensic analysis from the occurrence of malicious activity, through the collection of evidence to the

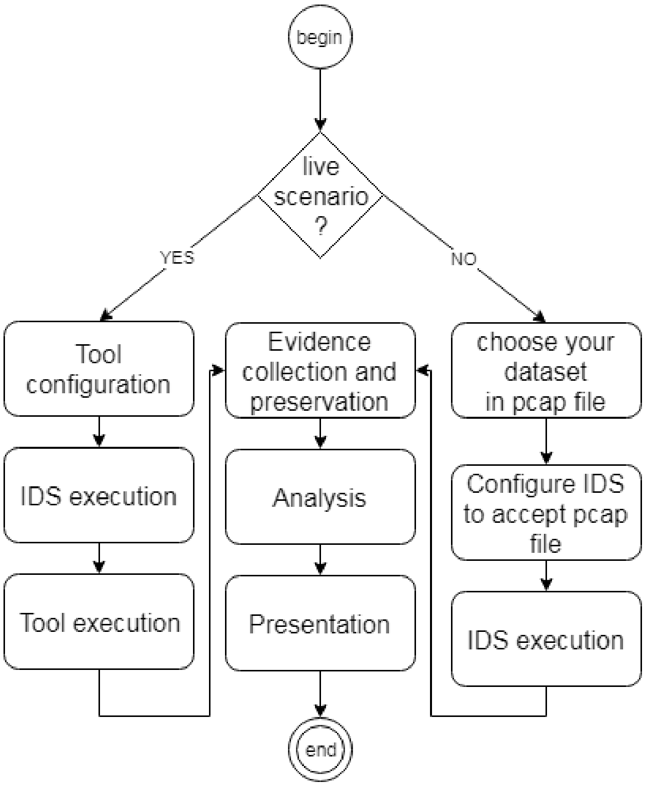


Fig. 5. **Experiments workflow**

presentation of information obtained, through the proposed steps. The tests were conducted on a Macbook Pro type computer with 256GB of storage, 8GB of RAM and the Macosx operating system to be named host. The following test architecture was created, as shown in Figure 6, 2 (two) virtual machines using the virtualbox tool called guests, as follows:

—1 attacker (using KaliLinux OS 2019.2)

—1 victim (apacher server 2.4) running a wordpress application (v5.2.3) simulating a service over the internet

On the host computer, an IDS Suricata (v4.1.2) was configured for network monitoring. Although it is possible to use the rules of the community, it was decided to create a specific rule for monitoring denial of service attacks. The rule used is shown in Figure 7.

Suricata configuration allows all network flow to be stored. This step is fundamental, because in addition to starting the process of evidence preservation, it ensures replicability, as others may have access to this file and perform other analyzes and methods that they consider necessary. The following paragraphs explain the scenarios performed, and their results obtained in the following section.

—Scenario - SLOWRIS: Using the slowhttptest[1] tool, a denial of service attack was performed on the victim guest computer.

—Scenario - SYNFLOOD: Using the hping3[2] tool, a denial of service attack was performed on the victim guest computer.

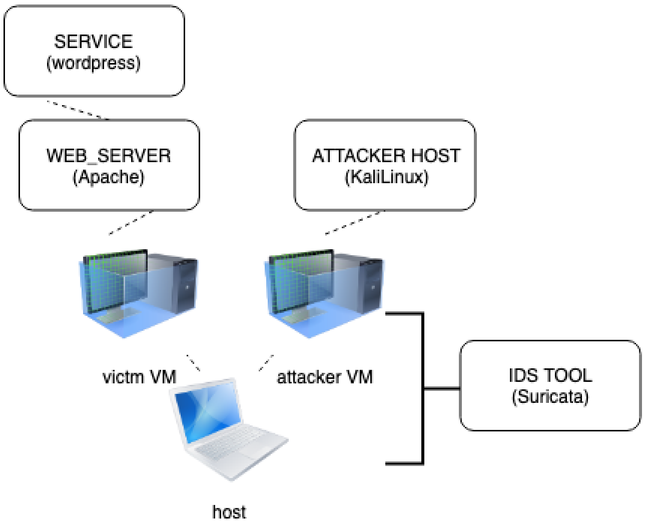
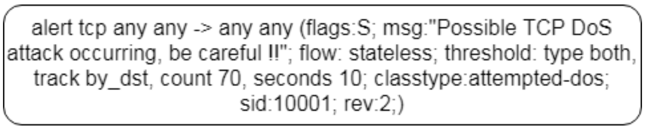


Fig. 6. **Architecture used in experiments**



```
alert tcp any any -> any any (flags:S; msg:"Possible TCP DoS
attack occurring, be careful !!"; flow: stateless; threshold: type both,
track by_dst, count 70, seconds 10; classtype:attempted-dos;
sid:10001; rev:2;)
```

Fig. 7. **Rule for capturing malicious activity events**

—Scenario - Goldeneye: Using the goldeneye[3] tool, a denial of service attack was performed on the victim guest computer.

—Scenario - CIC DoS data set (CICDOS2017[4]): Using the CIC DoS data set [14] a behavioral check of the proposed architecture was performed.

—Scenario - Intrusion Detection Evaluation data set (CICIDS2017[5]): Using the CICIDS2017 data set [17] a behavioral check of the proposed architecture was performed.

To perform the first three experiments, the following steps were followed according to the proposed architecture. First configuring the respective tool needed for attack simulation and setting parameters. Then running Suricata IDS for network monitoring with the rule configured for denial of service attacks and alert generation parameters. The tool command was executed simulating the denial of service attack. The generated evidence such as server logs files, generated alerts records, PCAP files, were preserved. For project decisions these artifacts were analyzed using JAVA programming language, as well as crime metrics and information extracted and saved in MYSQL database for its easy and agile practice of usage. Finally conclusions using correlation rules as described in section 4.5, about crime occurrence can be compiled and made available through reporting interfaces like an API for the investigating authority.

For the last two experiments the difference is that the attacks have already been simulated and are in the form of a PCAP file. It is possible to start the IDS tool by configuring the input as the PCAP file (which simulates network traffic), and thus generate

[1] https://tools.kali.org/stress-testing/slowhttptest
[2] https://tools.kali.org/information-gathering/hping3
[3] https://github.com/jseidl/GoldenEye
[4] https://www.unb.ca/cic/datasets/dos-dataset.html
[5] https://www.unb.ca/cic/datasets/ids-2017.html

evidence in the IDS alert format. Its possible that some metrics can't be measured in this type of scenario(not_applicable label), like information of web server (total requests, denied requests and average of requests) aren't available. However it is still possible to measure the other metrics (IPS discovered, repeated IPS, alerts on ids and the unavailability time) and so this type of experiment can help measure the quality of the rule used for the IDS, and allow adjustments for new runs with cyber attacks data sets that were validated by the literature. A fluxogram of the steps performed in the experiment scenarios is presented in the Figure 5 and the summary of the results of the experiments can be seen in Figure 8.

6. DISCUSSION

Although the last two experiments contain scenarios similar to the first two experiments, there is no evidence of web server monitoring from these two experiments, which would deplete a formal document of accountability of infringing agents. These were, therefore, made to verify as much information as possible for formalization.

In the first 3 experiments, the monitoring was stored in a PCAP file that would allow a full replication of the experiment. However, in the last two, this storage was not necessary since they already originate from PCAP files with hash information of integrity. The first 3 experiments were performed until the server would not respond. The first SLOWRIS experiment behaved as expected, generating strong evidence of malicious activity interrupting the service and enabling a forensic investigation to be carried out to hold offenders liable. In the second experiment SYN FLOOD there was no evidence generation, but it was noticed a change in CPU usage of the attacking machine during its execution, it is likely that the IDS rule created will not be applied for this experiment and a new rule that considers its particularities to be applied. The third experiment behaved partially as expected, generating evidence in the web server's log, but no alert from the IDS, possibly due to the IDS rule not applying to this attack, however a request was unavailable which partially indicated the occurrence of the denial of service attack so there was only service disturbing. In the last experiments, it is proposed the execution of the architecture in a database already known in the literature and demonstrating the generation of alerts that would be indicative of the occurrence of crimes, that is, the malicious activities in the last experiments can be considered as harmful to the server.

7. CONCLUSION

This paper has presented a methodology for computer network forensic analysis, focusing on denial of service attacks and aims at assisting the forensic expert interested in solving such crimes, in terms of the Brazilian Computer Crimes Law N. 12.737/2012.

This methodology was also based on the legal formalism of the search for constituent elements of cyber attacks, as well as on the existing legal bases. In addition, it provides a set of activities that, following the computer forensics principles, allows the crimes typification committed, the identification of their source, author, time of crime, target, "iter criminis" (crime path), as well as the patrimony achieved. The results show positive impressions of the study with its necessary elements for individualization found, to proceed with the charge of the offenders.

The study has also showed the need to evaluate more elements that can be used to hold offenders accountable, since at times the experiments only partially correlated with those required to pursue offenders. The effectiveness of the rule used should also be considered, as the architecture proposed will be directly proportional to the number of evidence founded by the ids.

As an indication of future works, it is suggested to observe and store the physical state of the experiment machines to analyze changes in the use of resources such as memory, processing and storage. It is also suggested that the collected evidence be published in a block-chain and so that its validity to the judge increases. Other type of crimes that could be considered from the computer crime law should be pointed to increase the charging of offenders.

8. REFERENCES

[1] Mohamed Abomhara and Geir M. Kien. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 4(1):65–88, 2015.

[2] W.H. Allen. Computer forensics. *IEEE Security and Privacy Magazine*, 3(4):59–62, jul 2005.

[3] Izzat Alsmadi and Mamoun Alazab. A model based approach for the extraction of network forensic artifacts. In *2017 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, nov 2017.

[4] Douglas J et al. Brown. A survey of intrusion detection systems. *Department of Computer Science, University of California, San Diego*, 2002.

[5] Yubao Chen. Integrated and intelligent manufacturing: Perspectives and enablers. *Engineering*, 3(5):588–595, oct 2017.

[6] Ari Cover and Ricardo Deitoz Posser et al. Methodology of communication between a criminal database and a virtual reality environment for forensic study. In *2017 19th Symposium on Virtual and Augmented Reality (SVR)*. IEEE, nov 2017.

[7] Alexandre Alberto Gonalves da Silva. *A percia forense no Brasil.* PhD thesis, USP, 2009.

[8] Marcelo Xavier de Freitas Crespo. *Do conhecimento da ilicitude em face da expanso do direito penal.* PhD thesis, USP, 2012.

[9] Ali Reza Arasteh et al. Analyzing multiple logs for forensic evidence. *Digital Investigation*, 4:82–91, sep 2007.

[10] Denis Trek et al. Advanced framework for digital forensic technologies and procedures. *Journal of Forensic Sciences*, 55(6):1471–1480, aug 2010.

[11] Eldow et al. Computer network security ids tools and techniques (snort/suricata). *Int. J. Sci. Res. Publ*, 6(1):593, 2016.

[12] Emmanuel S. Pilli et al. Network forensic frameworks: Survey and research challenges. *Digital Investigation*, 7(1-2):14–27, oct 2010.

[13] Haining Wang et al. Detecting SYN flooding attacks. In *Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 3, pages 1530–1539. IEEE, 2002.

[14] Hossein Hadian Jazi et al. Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. *Computer Networks*, 121:25–36, jul 2017.

[15] Hudan Studiawan et al. A survey on forensic investigation of operating system logs. *Digital Investigation*, 29:1–20, jun 2019.

[16] Igor Zikratov et al. Ensuring data integrity using blockchain technology. In *2017 20th Conference of Open Innovations Association (FRUCT)*. IEEE, apr 2017.

[17] Iman Sharafaldin et al. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. SCITEPRESS - Science and Technology Publications, 2018.

[18] K. Narasimha Mallikarjunan et al. A survey of distributed denial of service attack. In *2016 10th International Conference on Intelligent Systems and Control (ISCO)*. IEEE, jan 2016.

[19] Khan et al. Network threats, attacks and security measures: A review. *International Journal of Advanced Research in Computer Science*, 8(8):116–120, aug 2017.

[20] Konstantinos Koumidis et al. Optimizing blockchain for data integrity in cyber physical systems. In *5th International Symposium for ICS & SCADA Cyber Security Research 2018 (ICS-CSR 2018)*. BCS Learning & Development, aug 2018.

[21] Mahbod Tavallaee et al. A detailed analysis of the KDD CUP 99 data set. In *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*. IEEE, jul 2009.

[22] Mahdi Miraz et al. Internet of nano-things, things and everything: Future growth trends. *Future Internet*, 10(8):68, jul 2018.

[23] Max Landauer et al. Dynamic log file analysis: An unsupervised cluster evolution approach for anomaly detection. *Computers & Security*, 79:94–116, nov 2018.

[24] Nikhil S.Mangrulkar et al. Network attacks and their detection mechanisms: A review. *International Journal of Computer Applications*, 90(9):37–39, mar 2014.

[25] Roesch et al. Snort: Lightweight intrusion detection for networks. In *Lisa*, volume 99, pages 229–238, 1999.

[26] Tiago Perlin et al. Deteco de anomalias em redes de computadores e o uso de wavelets. *Revista Brasileira de Computao Aplicada*, 3(1):2–15, 2011.

[27] B. B. Gupta and Omkar P. Badve. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. *Neural Computing and Applications*, 28(12):3655–3682, apr 2016.

[28] The British Standards Institution. Information technology. security techniques. guidelines for identification, collection, acquisition and preservation of digital evidence.

[29] A R Jayakrishnan. Empirical survey on advances of network forensics in the emerging networks. *International Journal of Cyber-Security and Digital Forensics*, 7(1):38–46, 2018.

[30] Vera Kaiser Sanches Kerr. *A disciplina, pela legislao processual penal brasileira, da prova pericial relacionada ao crime informtico praticado por meio da Internet.* PhD thesis, USP, 2011.

[31] A. Kumaravel and M. Niraisha. Multi-classification approach for detecting network attacks. In *2013 IEEE CONFERENCE ON INFORMATION AND COMMUNICATION TECHNOLOGIES*. IEEE, apr 2013.

[32] S. Latha and Sinthu Janita Prakash. A survey on network attacks and intrusion detection systems. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, jan 2017.

[33] Pei-Ting Lee and Baijian Yang. Indexing architecture for file extraction from network traffic. In *Proceedings of the 6th Annual Conference on Research in Information Technology - RIIT '17*. ACM Press, 2017.

[34] Mrunal H. Mate and Smita R. Kapse. Network forensic tool – concept and architecture. In *2015 Fifth International Conference on Communication Systems and Network Technologies*. IEEE, apr 2015.

[35] Mehdi Merouane. An approach for detecting and preventing DDoS attacks in campus. *Automatic Control and Computer Sciences*, 51(1):13–23, jan 2017.

[36] Antnio De Jesus Neres and Clives Pereira Sanches. Procedimento operacional padro na PMGO. *Revista Brasileira de Estudos de Segurana Pblica*, 11(1), aug 2018.

[37] Brian Ray. Extending the blockchain: Ensuring transactional integrity in relational data via blockchain technology. Technical report, aug 2019.

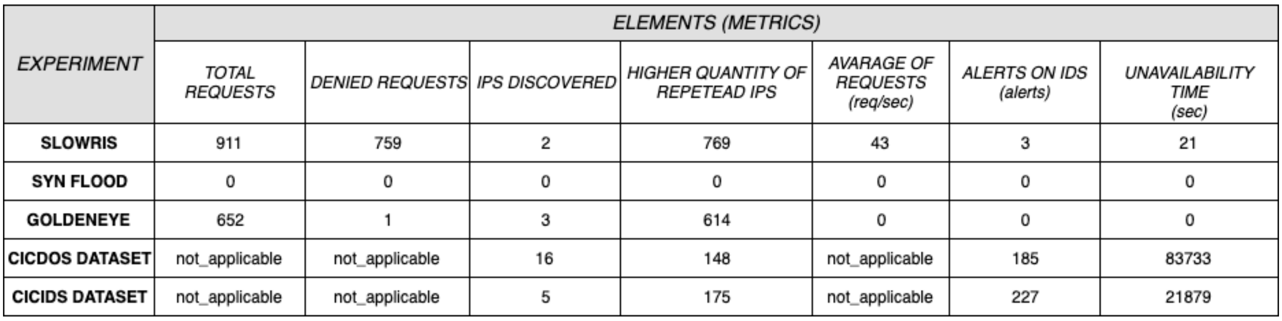
[38] Klaus Schwab. THE FOURTH INDUSTRIAL REVOLUTION (INDUSTRY 4.0) a SOCIAL INNOVATION PERSPECTIVE. In *Journal of Ethnic Minorities Research*, number 23. Vietnam National University Journal of Science, sep 2018.

[39] Peter Stephenson. Structured investigation of digital incidents in complex computing environments. *Information Systems Security*, 12(3):29–38, jul 2003.

[40] Gisele Truzzi and Alexandre Daoun. Crimes informticos: O direito penal na era da informao. In *Proceedings of The Second International Conference on Forensic Computer Science*. ABEAT, sep 2009.

[41] Hanqing Wu and Liz Zhao. Application-layer denial-of-service attacks. In *Web Security*, pages 343–368. Auerbach Publications, mar 2015.

[42] Alec Yasinsac and Yanet Manzano. Policies to enhance computer and network forensics. In *Proceedings of the 2001 IEEE workshop on information assurance and security*, pages 289–295, 2001.



EXPERIMENT	ELEMENTS (METRICS)						
	TOTAL REQUESTS	DENIED REQUESTS	IPS DISCOVERED	HIGHER QUANTITY OF REPETEAD IPS	AVARAGE OF REQUESTS (req/sec)	ALERTS ON IDS (alerts)	UNAVAILABILITY TIME (sec)
SLOWRIS	911	759	2	769	43	3	21
SYN FLOOD	0	0	0	0	0	0	0
GOLDENEYE	652	1	3	614	0	0	0
CICDOS DATASET	not_applicable	not_applicable	16	148	not_applicable	185	83733
CICIDS DATASET	not_applicable	not_applicable	5	175	not_applicable	227	21879

Fig. 8. **Summary of metrics collected from performed experiments following the crime data model**