REPUBLIC OF TURKEY
FIRAT UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND
APPLIED SCIENCE

DIGITAL FORENSIC ANALYSIS FOR VOIP

HUSSEIN FAROOQ TAYEB AL-SAADAWI

Master Thesis
Department: Software Engineering
Supervisor: **Prof. Dr. Asaf VAROL**

JULY-2017

REPUBLIC OF TURKEY
FIRAT UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE

DIGITAL FORENSIC ANALYSIS FOR VOIP

MASTER THESIS

HUSSEIN FAROOQ TAYEB AL-SAADAWI
142137103

Submission Date to the Institute: 07 January 2017
Thesis Presentation Date: 04 July 2017

Thesis Supervisor : Prof. Dr. Asaf VAROL (F. U.)
Other members of the jury : Assist. Prof. Dr. Fatih ÖZKAYNAK (F.U.)
Assoc. Prof. Dr. Cihan VAROL (S.H.S.U.)

JULY – 2017

ACKNOWLEDGEMENTS

First of all, I would like to express my greatest gratitude to Almighty Allah for His blessings and guidance throughout my life and especially for accomplishing the task of my Master thesis. I would also like to express my special appreciation and gratitude to my supervisor Prof. Dr. Asaf VAROL for his effort in making this work possible; I highly appreciate his precious advice and mentoring throughout the course of this research work. My thanks and gratitude are also extended to the committee members who took the time to revise and straighten the final version of this thesis. I would also like to thank the Department of Software Engineering/College of Technology staffs for their positive assistance and feedback. My special gratitude is also extended to the Kurdistan Parliament – Iraq for the provided cooperation and support.

I should also mention my thanks to my parents, my wife and kids, my siblings and my friends for their continuous emotional support and prayers; without your support, it would have been impossible. My special thanks are extended Mr. Malek HARBAWI to for his valuable advice and fundamental comments which enriched the final version of this thesis.

Sincerely

Hussein AL-SAADAWI

TABLE OF CONTENTS

Page No

ABSTRACT

DIGITAL FORENSIC ANALYSIS FOR VOIP

Today, communications through various networks are considered as an important indicator for how we conduct our daily lives. This is realized by the massive use of communication applications that require voice, image, video, and data. VoIP technology is regarded as one of the convenient communication services that meet the requirements of individuals and organizations. The growth of electronic devices and VoIP applications have increased the need for a specialized digital investigation. Generally, the digital investigation is creating challenging issues that need to be confronted. Many advanced digital forensic tools have been developed to assist the digital investigation process. Being familiar with the application scope and the limitations of forensic analysis tools is very important for the investigator. This is due to the fact that choosing a random forensic tool might be a waste of time and it may generate misleading results. Essentially, one tool cannot cope with the requirements of digital forensic applications; and with all the available tools, it is difficult to choose the most suitable tool for VoIP applications. It is possible to analyze and recover popular VoIP applications data from the RAM. However, the blind investigation of the digital evidence from unknown VoIP applications can be tedious and time-consuming. In this research, a classification for popular RAM acquisition and digital forensic tools is conducted. The ultimate aim is to help the investigators to properly choose the right RAM acquisition and forensic analysis tools applicable to VoIP. In addition, the research considered the use of unknown VoIP applications during the classification process. The experimental work was achieved by simulating a client-server unknown VoIP communication as well as the use of popular VoIP applications to create the relevant digital trace. The investigation process is made based only on volatile memory analysis. Two RAM sizes are used in this research, namely 4 and 8 GB. Here, RAM artefacts are captured by FTK Imager v3.1, Magnet Capture V1.0, RAM capture.exe, and DumpIt tools. The generated capture files are analyzed by Forensic Explorer, FTK v6.0, X-Way Forensics, Belkasoft, and Magnet IEF 6.8 tools. The obtained results are used for classifying the tools based on analysis duration, interface type and convenience, tool licensing, the ability to present the artefacts, the possible file formats, and the size of output file. The obtained results vary based on the used tool and RAM size, yet the optimal choice will be always case-dependent. Thus, a combination of tools can always be a useful option for VoIP forensic.

Key Words: Analysis Tools, Digital Forensic, RAM Acquisition, Timeline Forensic tools analysis, Unknown application Call over Network, VoIP Forensic.

ÖZET

VOIP İÇİN DİJİTAL ADLİ ANALİZ

Günümüzde çeşitli ağlar sayesinde sağlanan iletişimler, günlük hayatımızı nasıl yürüttüğümüz konusunda önemli bir araç olarak değerlendirilmektedir. Bu iletişim, ses, görüntü, video ve veri gerektiren iletişim uygulamalarının birlikte kullanımı ile gerçekleştirilir. VoIP teknolojisi, bireylerin ve kuruluşların gereksinimlerini karşılayan uygun iletişim servislerinden biri olarak kabul edilmektedir. Elektronik cihazların ve VoIP uygulamalarının büyümesi, özel bir dijital soruşturmanın gereksinimini artırmıştır. Genellikle, dijital soruşturma, karşı karşıya kalınması gereken zorlu konular oluşturuyor. Dijital soruşturma sürecine yardımcı olmak için birçok gelişmiş dijital adli bilişim aracı geliştirilmiştir. Adli bilişim analiz araçlarının kapsamı ve sınırlamaları hakkında bilgi sahibi olmak araştırmacılar için çok önemlidir. Bunun nedeni, rastgele bir adli bilişim aracı seçmenin zaman kaybı olabileceği ve yanıltıcı sonuçlar doğurabileceği gerçeğidir. Esasen bir araç, adli bilişim uygulamalarının gereksinimleri ile baş edemez; ve bütün mevcut araçlar ile VoIP uygulamaları için en uygun aracı seçmek zordur. Popüler VoIP uygulamalarının verilerinin RAM'den analiz edilmesi ve kurtarılması mümkündür. Bununla birlikte, bilinmeyen VoIP uygulamalarından gelen dijital delillerin körü körüne araştırılması bıktırıcı ve zaman alıcı olabilir. Bu araştırmada, popüler RAM erişimi ve adli bilişim araçlarının sınıflandırılması yapılmıştır. Burada nihai amaç, araştırmacılara VoIP için geçerli olan doğru RAM erişimi ve adli bilişim analiz araçlarını doğru bir şekilde seçmelerinde yardımcı olmaktır. Ayrıca, bu çalışma sınıflandırma işlemi sırasında bilinmeyen VoIP uygulamalarının kullanılmasını da dikkate almıştır. Deneysel çalışma, bir istemci sunucu bilinmeyen VoIP iletişiminin simüle edilmesinin yanı sıra uygun dijital izi oluşturmak için popüler VoIP uygulamalarının kullanılması ile gerçekleştirilmiştir. Soruşturma süreci sadece uçucu hafıza analizine dayanmaktadır. Bu araştırmada boyutları 4 GB ve 8 GB olan iki RAM kullanılmıştır. Burada, RAM artıkları FTK Imager v3.1, Magnet Capture V1.0, RAM capture.exe ve DumpIt araçları tarafından yakalanır. Oluşturulan yakalama dosyaları Forensic Explorer, FTK v6.0, X-Way Forensics, Belkasoft ve Magnet IEF 6.8 araçlarıyla analiz edilir. Elde edilen sonuçlar, araçların analiz süresine, arayüz türüne ve kolaylığına, araç lisansına, olguları sunma yeteneğine, olası dosya biçimine ve çıktı dosyasının boyutuna dayalı olarak sınıflandırmak için kullanılır. Elde edilen sonuçlar, kullanılan araca ve RAM boyutuna göre değişir ancak optimal seçim her zaman duruma bağlı olacaktır. Bu sebeple araçların bir kombinasyonu her zaman yararlı bir seçenek olabilir.

Anahtar Kelimeler: Analiz Araçları, Adli Bilişim, RAM Erişimi, Adli Bilişim Araçları Zamanlama Analizi, Ağda Bilinmeyen Uygulama Çağrısı, VoIP Adli Bilişimi

LIST OF FIGURES

Page No

LIST OF TABLES

Page No

ABBREVIATIONS

ATA : Analog Telephone Adaptor
HDD : Solid State Drive
HTTP : Hypertext Transmit Protocol
IETF : Internet Engineering Task Force
IM : Instant Messaging
IMTC : International Multimedia Teleconferencing Consortium
IP : Internet Protocol
IPsec : IP Address Security
ITU : International Telecommunications Union
NVM : Non-Volatile Memory
OSI : Open Systems Interconnection
PBX : Private Branch Exchange
QoS : Quality of a Service
RAM : Random-Access Memory
SCCP : Skinny Client Control Protocol
SDP : Session Definition Protocol
SIP : Session Initiation Protocol
SMTP : Simple Mail Transfer Protocol
SSD : Hard Disk Drive
SSL : Transport Layer Security
TCP/IP : Transmission Control Protocol/Internet Protocol
TLS : Secure Sockets Layer
UA : User Agent
UDP : User Datagram Protocol
VoIP : Voice over Internet Protocol

1. INTRODUCTION

Communication and contact between human beings are considered as a basic need in our life. Many communication features assist in the growth of business popularity by adding the needed infrastructure such as voice, text, video, and etc. Ever since its invention, the voice communication via Public Switched Telephone Network (PSTN) has been an effective form of communication technology evolution. Popular development throughout voice-driven technologies via computers, smartphones, and networks have become an important part of the communication systems.

In 1998, the conceptual realization of Voice over Internet Protocol (VoIP) produced a new equipment unit's hardware and software programs. VoIP applications have allowed the communications between IP networks and PSTN and vice-versa. This had incremented voice traffic usage in the U.S. alone to approximately 2% in less than one year [1]. By the year 2000, the deployment of VoIP as real commercial services took place and it has been widely used ever since. After the emergence of VoIP, the shrinking in PSTN utilization has become obvious in the business sector [2]. Generally, VoIP is perceived by offering different functionalities, dynamic demanded aspects, and cheaper rates than PSTN services. This has been reflected on the popularity VoIP had achieved in its early days [3, 4]. This, in fact, is more useful for small size enterprises as it allows them to compete with a minimal cost [4].

Despite all the advantages offered by VoIP, like all IP-based services, the main disadvantage of using VoIP is represented by the generated risk of abusive and harmful applications as well as the attacks initiated by scammers, blackmailers, and cyber-terrorists. This creates many potential security threats inherited from the Internet Protocol (IP). The vulnerabilities available on the Web are usually affecting VoIP as well and the risk may possibly compromise sensitive or private information related to organizations and/or individuals. In order to alleviate the risk of security issues and optimally respond to the cyber-criminal activities targeting VoIP services, various proposal and solutions have been offered and presented [5]. Essentially, the proposed solutions rely on the use of encryption methods, antimalware programs, and applications that bind with recommended security measures and ethics. However, in the case of criminal activity incidents, there should be a proper way to respond in order to backtrack the attackers.

The best answer for this need is to investigate and detect the legal evidence that can be used in the court of law. This type of procedure is referred to by VoIP forensic. Essentially,

VoIP forensic begins by taking advantage of the digital evidence generated through VoIP transactions and data remnants residing somewhere on the electronic components of the computing devices.

The growth of applications and systems applicable for cyber-criminal activities are continuously increasing. In the same way, traditional forensic techniques are generally inadequate for the autopsy of VoIP information. Consequently, the evolution of communication over the network should grow in line with the development of applications and tools for digital forensic techniques. The applicable VoIP forensic analysis methods present numerous techniques to investigate VoIP forensic as shown in Figure 1.1 [6].

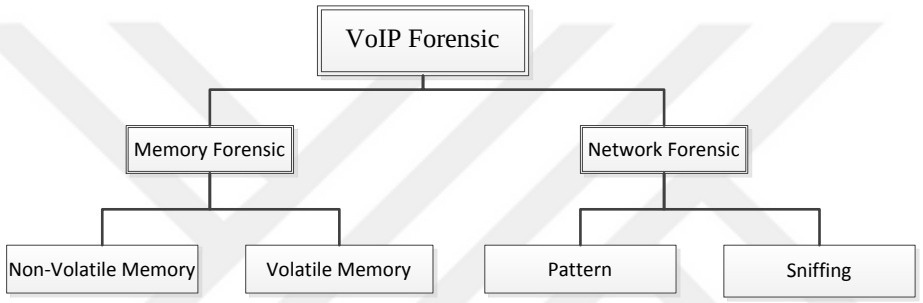

Figure 1.1. VoIP Forensic Types

Many VoIP forensic research attempts have used various methods for investigation. These methods include VoIP forensic network monitoring and traffic capturing to identify evidence related to VoIP by sniffing or by tracking attack patterns. The actual evidence might be extracted using memory forensic applied to VoIP applications. It is equally important to investigate the system after a call termination. This is done using memory VoIP forensic methods such as volatile and non-volatile memory analysis, depending on the available crime scene situation as illustrated in Figure 1.2.

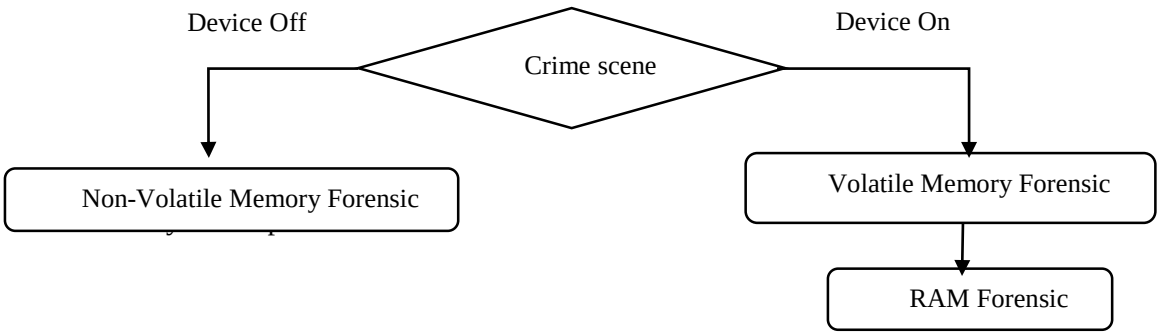

Figure 1.2. Applicable VoIP forensic based on the crime scene

Fortunately, digital forensic tools can be used for investigating and analyzing systems through software and hardware. This is generally done to recover and extract information from the network or memory. The idea is that non-volatile memory stores the information for a long time with or without electric power being on. However, the volatile memory depends on the electric power supply where data gets lost after the power goes off. VoIP forensic through non-volatile memory is usually done by extracting the information of VoIP applications, such as Skype, from the hard disk. These applications do keep a copy of their files on the hard disk which can be used for investigation purposes. The information here can be directly related to the media and caller ID information, etc. [7]. Obtaining the actual pieces of evidence from VoIP data remnants residing on the Random-Access Memory (RAM) is conducted to provide legitimate evidence to be used in the court of law. RAM forensic techniques cover a wide area in the forensic analysis due to their useful outcomes. Therefore, VoIP forensic through RAM requires higher attention than other techniques.

1.1. Research Problem and Significance

There are numerous forensic tools applied for digital forensic cases including live memory acquisition tools and forensic analysis tools, yet only one tool cannot solve all forensic cases. On the other hand, none of the available forensic analysis tools can directly solve unknown VoIP applications forensic. In addition, the digital investigators may get confused about choosing the right tool that can be used for analyzing unknown VoIP applications cases.

1.2. Research Objectives

The main objective of this research work is to provide a better understanding of the digital forensic analysis applicable for VoIP. However, this objective can be elaborated to the following sub-objectives:

- To review and investigate the literature related to VoIP forensic and come up with a reliable solution to VoIP forensic based on based on the volatile memory analysis.

- To test and classify the prominent forensic tools that can be used for VoIP forensic investigation, then present the best tools that are relevant to VoIP forensic.
- To establish a proper classification for the used tools based on their analysis results**.**

1.3. Thesis Organization

This thesis is organized as follows:

Chapter I: Presented the needed introduction for communication and the concept of volatile VoIP forensic. Besides, it explained the research problem and its significance along with the objectives of the thesis.

Chapter II: Presents the literature review which contains several VoIP forensic and RAM forensic related work, and the principals behind developing forensic techniques for VoIP applications.

Chapter III: Provides a general overview of VoIP communication with a focus on different practical VoIP forensic issues.

Chapter IV: Discusses the computer memory and its relationship to VoIP forensic.

Chapter V: Presents the methodology followed by this thesis to conduct the research work.

Chapter VI: Provides the experimental results as well as the analysis of these results.

Chapter VII: Presents the final conclusions and recommendations for future work.

2. LITERATURE REVIEW

Investigating the attacks targeting VoIP applications is mainly referred to by VoIP forensic. This area of research is still progressing as various VoIP applications and tools have come into the existence. Essentially, securing VoIP applications is at an extreme importance as vital and confident information can be compromised via these applications. This fact has been drawing the attention of many researchers who have realized their work to academic publications. In order to throw light on several forensic tools relevant to VoIP including memory acquisition and forensic analysis tools. The followings present a thorough revision of the most relevant methods and developed techniques of VoIP forensic.

Nick *et al*. [8] presented different methods for automatically deriving digital aim definition as well as forensic tools related to volatile memory that assist the investigators. In their work, they used Forensic Analysis Toolkit (FATK) to process system memory images. In addition, they developed a filtering process to extend FATK functionality using Python programming language to expand their analysis results. However, standard digital forensic methodologies principally focus on the familiar VoIP applications and don't take into the consideration unknown applications use. Similarly, Manson *et al*. [9] presented a valuable overview of forensic tools and challenges to investigate the digital evidence. They conducted comparisons between forensic tools such as Forensic Toolkit (FTK), Autopsy and Sleuth Kit, and Encase, to present a description of these tools applicable to data collection and analysis. They developed a Graphical User Interface (GUI) that facilitates the application of FTK in order to save time and reduce the needed effort.

Leong and Chan took a lead on contemplating and developing an idea based on Skype forensic [10]. They set up the needed Skype event path and they formulated the needed framework for evidence extraction and analysis. They succeeded in detecting sockets associated with active Skype and provided recommended steps for further analysis. This work is considered as one of the early attempts in the field of VoIP forensic. The attempt could provide some answers to whether it is possible to forensically analyze an encrypted peer-to-peer communication. Also, it addressed how the possible future developments and the needed effort could be. In the same context, Simon and Slay [7] provided a valuable review of the physical memory to assist investigating the targeted pieces of evidence that represent the artefacts. In addition, they used Skype as an application for recovering and analyzing the data related to Skype. Then, they obtained the data related to VoIP which

included: five-point history, content, passwords and encryption keys. However, the work did not provide a complete VoIP forensic tool to be used in a broader sense. Pelaez and Fernandez [11] had presented an attempt to formulate a method for VoIP network forensic. Their idea was essentially based on creating an applicable framework for VoIP forensic. In their work, they proposed VoIP collector design pattern for evidence collection and VoIP evidence analyze pattern for evidence analysis. These two patterns combined were called VoIP forensic pattern and it was presented in UML for further development. This work was generally useful as a pioneer attempt in the field; however, it did not actually offer any practical implementation nor did it provide any experimental testing. In fact, the idea of this research attempt was initiated from a previous research proposed by Fernandez *et al*. [12].

Khan *et al*. [13] approached VoIP forensic from an important aspect that is detecting caller identity from an encrypted traffic. The idea of this attempt is interesting and so is the implementation. The authors used Artificial Intelligence (AI) in the form of machine learning regression model for training the machine on various packets to detect the possibility of the attacker. In their work, they succeeded in detecting anonymous attacker with a success rate of 70-75%. However, such results will not build a legal case, rather, it may be used as a complementary approach to verify other extracted evidence.

Francois *et al*. [14] proposed a generic method for conducting digital forensic in VoIP networks. They focused on detecting the used device specifications from the captured traffic. Their work was based on only signaling protocols and considered all other data irrelevant to the analysis. Although the idea of extracting device specifications is useful in forensic analysis, as it can assist in backtracking, yet, it is generally neither enough for VoIP forensic nor is it providing an adequate information for legal cases. Irwin and Slay [15] presented one of the most useful attempts up to that time. In their work, they proposed the idea of volatile analysis for discovering evidence related to VoIP usage. This is, of course, based on the used protocols, especially UDP and RTP in this case. The work here is assuming that the device is maintained on, otherwise, the contents of the volatile memory, RAM, will not be kept. They also managed to create a basic GUI for the tool that they developed and performed the analysis based on special selective criteria such as the memory and protocol to be analyzed. The presented work was able to retrieve information of a VoIP call from the RAM with high true rate (97.4% for a Skype call over a period of 3 minutes and 99.7% for an X-Lite call over the same period). The main limitation of this work is the status of the analyzed device, as switching off the device means ignoring the possibility of applying this method,

which might be the case. In addition, the study focused only on retrieving the call rather than other embedded evidence that may be more necessary than the call itself. Moreover, there is no enough information on the claimed implemented forensic tool and its interface in order to inspect, investigate and validate its usability. Interestingly, the same thoughts stimulated Irwin *et al*. [16] to come up with a comparative approach in order to measure the feasibility of forensically extracting VoIP evidence from the virtual hard disk and RAM at the same time. Yet, the result of virtual environment forensic did not provide any valid evidence related to VoIP calls.

Hsu *et al*. [17] investigated and proposed a collaborative methodology for VoIP forensic. The core concept in this research effort is based on including all possibilities for evidence residing on the network operator components as well as the Internet Service Provider (ISP) servers. The authors also proposed the idea of active forensic by discovering any forgotten header information available in the Session Initiation Protocol (SIP) requests. The proposed work considered critical steps in developing VoIP forensic; however, the effort was guided only to discovering fraud information embedded in SIP which is usually extremely tricky and may cause misleading results. Hongtao [18] analyzed the contemporary working principles of VoIP forensic. He tried to modify VoIP forensic methods via encryption algorithms and legal monitoring system. He explained the steps for enhanced cyber-criminal investigation deploying gateways in foreign countries. The research presented interesting ideas and useful thoughts, yet it did not offer a concrete methodology since it was still in progress.

Stefan and Felix [19] reviewed techniques for gathering information from computer memory. In their work, they illustrated the benefits of improving the information security field. According to their study, they showed that volatile memory assists in giving a plethora of information which has a high impact on the result. Although, the VoIP forensic has regularly developed with the evolvement of communication technology, yet this development should progress faster to satisfy the forensic investigation need. Apart from the work of Stefan and Felix, Su and Wang [20] presented a study on the meaningfulness of the artefacts that come from the physical memory. The study presented a statistical analysis that measures the degree of memory change in order to reach the final estimation.

Ibrahim *et al*. [21] developed a model for VoIP evidence based on gathering attack information from different parts of VoIP application system. The main argument of the proposed work is that gathering attack information from different components of VoIP will

definitely further assist in extracting more readable digital evidence pieces for the legal case. Even though the idea of the attempt sounds logical, however, the practical implementation and experimental testing were totally missing in the proposed research. This has obviously made the work incomplete and could only be used for further development and investigation rather than practical applications.

The study conducted by Leonardo *et al*. [22] provides a comparison between RAM capturing tools and presents the capability of operation including the interface, capturing operation time, artefacts, and the orientation of the tool (commercial or open source). In the same way, Dave *et al*. [23] deployed the volatile memory analysis and techniques of RAM acquisition. They also presented how live forensic is important for digital forensic investigation. In their study, they managed to extract useful information which is not residing on the hard drive. In addition, the study discussed the capability of capturing and analysis tools. Nonetheless, this work had focused on RAM acquisition more than other forensic issues.

Le-Khac *et al*. [24] conducted an experimental research on Tango forensic where they used real-life data to prove the feasibility of their work. Their idea was based on the argument that Tango had a high number of users and it could be targeted by attackers. They employed an iOS mobile device as well as an Android device for the experimental work. The main aim of their study is to investigate Tango forensic and compare it with both WhatsApp and Viber. The authors did elaborate a lot of details in their paper, yet, there is no enough information on the followed methodology, the developed forensic tool as well as the future possibility of enhancement.

Katosl *et al*. [25] presented an extensive work on VoIP forensic using SIP and Session Description Protocol (SDP). They also proposed a framework for considering the readiness of VoIP forensic for attacker identification based on volatile memory analysis. They managed to formulate a generic framework for VoIP forensic which was able to extract information about the possible attackers such as IP addresses, used devices, and network topology. In addition, their readiness model helped in identifying possible threats and attackers. It also helped in guiding the network administrator for the potential risks and the available ways of combating/blocking them. The main limitation of the developed work is its complexity. Moreover, in this framework, there are privacy concerns generated by the fact that the application may be misused for revealing private information of the legitimate users. Apart from that, Zhang *et al*. [26] had looked at the effectiveness of methods that can

display the artefacts of cyber-criminals. They used volatile memory images for testing and finding the efficient actions for the investigation procedure. However, the result of the virtual environment did not provide adequate evidence related to the VoIP calls.

There is a number of techniques developed for VoIP forensic based on specific VoIP protocols such as SIP and Real-time Protocol (RTP) for analysis purposes. For instance, Manesh *el al*. [27] proposed the idea of reordering the sequence of the generated RTP packets. In their study, they used Wireshark and Ethercap along with their developed Network Forensic Analysis Tool Kit (NFATK) for this purpose. The developed system here aims at collecting any possible information on unauthorized VoIP activities, tracing the illegal or malicious content source and then generate the needed report to the proper authorities. The attempt represents a considerable effort for VoIP forensic investigation. However, the main issue here is the lack of extensive testing based on various VoIP applications. In addition, the study did not consider internetworks scenario to verify the basic obtained results and validate the usability of the proposed framework. Similarly, Mohemmed *et al*. [28] proposed what is called VoIP forensic analyzer as a modified solution of their former work. However, the adequacy of testing and validation results remain questionable. Khac *et al*. [24] studied the effect of memory acquisition on the memory contents. They paid attention to how it is important to process and analyze the pool allocation memory acquisition of Windows operating system and reuse them based on their extent and a Last-in-First-out (LIFO) schedule method.

Carvajal *et al*. [29] approached VoIP forensic from a different perspective where they conducted a research on how to improve VoIP security by detecting the unprotected SIP-based VoIP. Here, the idea is based on the detection rather than tracing. This can be useful for protection and early prevention of any risk. In simple words, the analysis was based on inspecting SIP header to confirm the status and then a warning should be sent if the results indicate that the traffic, in this case, is unprotected SIP type. This work can be considered as an Intrusion Prevention System (IPS) which improves the security and reduces the vulnerabilities; yet, it doesn't provide any mechanism for VoIP forensic analysis.

Robert *et al*. [30] had provided a comparative research on volatile memory that uses RAM acquisition based on open source tools. In addition, their study used seven shareware open source RAM acquisition forensic tools that are compatible to work with the latest 32-bit and 64-bit Windows XP machines. Apart from that, Kumari and Mohapatra [31] discussed in their study the lack of digital forensic tools and the challenges of the

investigation process. They tested the ability of various tools that are useful for forensic research and issues in cybercrime forensic. In a different maneuver, Joseph and John [32] proposed models and technology platforms for improving network and computer forensic which can be applied to VoIP forensic. In addition, they classified the literature related to digital forensic, including computer, network, acquisition as well as the analysis of evidence.

In general, the reviewed methods have clarified and improved a number of issues related to VoIP forensic. Nevertheless, there is still a research gap in VoIP forensic improvement that should be tackled. Essentially, there are a lot of VoIP applications as well as various digital forensic tools and techniques. However, finding the optimal forensic tool for a specific VoIP application may be cumbersome and time-consuming for the investigator. Therefore, a proper classification study should be presented in this field.

3. VOICE OVER INTERNET PROTOCOL

3.1. The Concept of Voice Communication

There has been an increasing demand for the possible ways of transferring voice calls between parties. This has led to the invention of the concept of voice call communication. This idea was officially launched as a telephone system by G. Bell. In his work, Bell presented the theory of the movement of sound frequencies that go through carbon wires to transfer sound using operator between the caller and receiver. When sound waves come out from the human throat and touch the lining small pieces inside the microphone, they activate these small pieces of carbon which shake due to the sound waves vibration at different frequencies [33]. The produced electric signals from sound waves here are small in amplitude. Thus, they are modulated and amplified in order to be transferred through telephone wires to the end users. This old technique of voice communication is based on Public Switched Telephone Network (PSTN). PSTN is the most famous communication system in the world. The working technique is presuming that two or (more than two) devices share a single iron wire [34]. PSTN is considered as a legacy network [35]. With the popularity of Internet-based applications, researchers have invented a way to transfer voice over the Internet. This application is called Voice over Internet Protocol (VoIP).

3.2. History of VoIP

The idea of VoIP was officially launched in February 1995. It was initially generated by connecting two points of computers with all needed call devices where both of them used the same application software [35]. The benefits of VoIP stimulated the rise of its commercial applications. In 1998, the conceptual realization of VoIP was produced. Further, modern equipment unit's hardware and software programs, which have allowed the communications between IP networks and PSTN and vice-versa, were also produced. This had incremented voice traffic usage in the U.S. alone to approximately %2 in less than one year [1]. By the year 2000, the deployment of VoIP as a real commercial service took place, and it has been widely used ever since. After VoIP was born, the shrinking in PSTN utilization has become obvious, especially in companies and big organizations [2]. So far,

the evolution of VoIP is dramatically increasing. A general comparison between PSTN and VoIP is provided in Table 3.1 [34].

Table 3.1. VoIP vs. PSTN

Criterion	PSTN	VoIP
Path channel	Dedicated lines	One channel path and many protocols used for voice communication over the Internet
Compression outbound direction	Each direction can get 64 kbps	Each direction can compress to get up to10 kbps
Upgrading	Upgrading requires dedicating a new line and material	Upgrading requires updating the software and increasing the bandwidth
Calling cost	The cost depends on the distance and the call duration	Mostly fixed price depending on a monthly fee
Power supply	Telecommunication companies provide the needed electric power	Operates in conjunction with the operational process of the device attached to it. The lack of power supply means service termination

3.3. The Concept of VoIP

The idea was initiated when the communication over the Internet became possible in the form of email; which was quickly developed to real-time messaging in the form of online chatting by texts. Not much later, the idea of online messaging or Instant Messaging (IM) went further to support voice and video communication which was the initiative of VoIP generation [34]. Basically, VoIP is transferring voice data packet over the Internet based on IP address (from one point to another). Traditional telephony, PSTN, employs switching circuits in order to transfer the voice from one point to another; thus, the signals are arranged over channels throughout the switching network. However, in IP networks, voice data must be digitized and transmitted as packets format. These packets recognize their destination and may be rerouted using certain protocols based on the network traffic. The main keyword that

is always appended to VoIP is the IP which has made VoIP possible [34]. Apart from IP, VoIP needs various protocols to from the necessary signaling, establishment, maintenance, and termination of the connection between the two or more parties in real-time across the network. In addition, there are other protocols for monitoring the Quality of a Service (QoS), booking resources, etc.

VoIP utilizes IP to transmit voice signals over the Internet and or any IP-based network. VoIP environment presents a potential real life scenario such as sharing information between large companies, universities, etc. [33, 35]. This implies the need for Transmission Control Protocol/Internet Protocol (TCP/IP) which is important for collecting information to present many protocols in one frame. The IP frame header has a total size of 58 Bytes. The followings are the main protocols within the IP frame: Ethernet header (14 Bytes), IP header (20 Bytes), UDP header (8 Bytes), RTP header (12 Bytes), and Ethernet Trailer (4 Bytes). The two layers of TCP and UDP compose an interface to the hardware. They are sub-divided into four different layers. TCP supports signal transmission while UDP supports media transmission. All these protocols support the use of VoIP services [33].

3.4. VoIP Operational Principles

VoIP requires a sort of proper conversion to transfer the spoken words from their audio nature to digital signals. In fact, the conversion here is done using the common sampling, quantization and digitization processes followed for converting the analog voice to digital sequences. However, this method is used for converting and storing the voice where some compressing techniques are used to reduce the size of the consumed memory. In the case of VoIP, special compressing/decompressing (CODEC) algorithm is used to provide a real-time compressing/decompressing in order to shrink the needed transmission bandwidth [36]. The whole mechanism is provided in Figure 3.1 for the ultimate benefit of the reader. As shown in Figure 3.2, the packetized data is transmitted over an IP network, mostly the Internet, and for ensuring the transmission process, there is a number of protocols to be used for this purpose, presented in section 3.6, as well as different gateways to leverage the transform between networks (IP-based, Analog Telephone Adaptor (ATA), PSTN, Private Branch Exchange (PBX), etc.) [37].

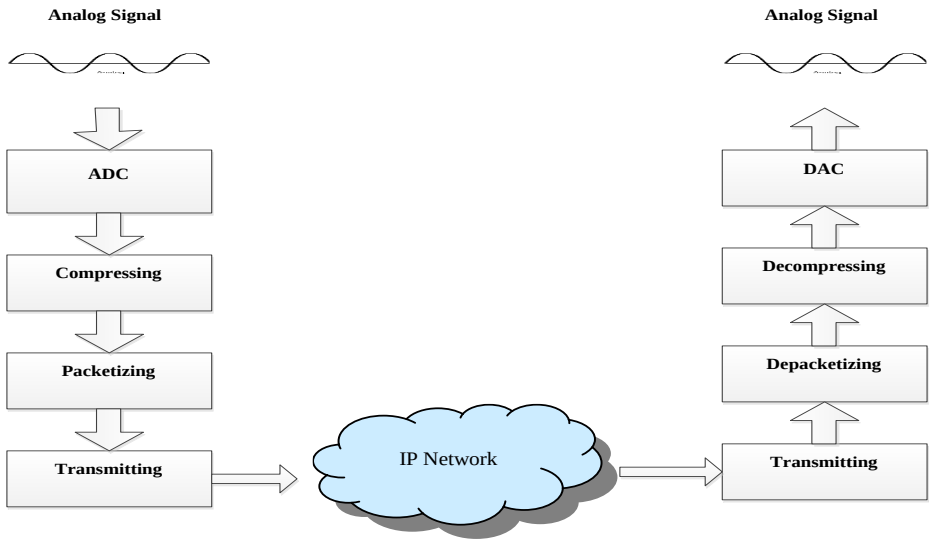

Figure 3.1. Transmission of voice over network

3.4.1. Voice Traffic over VoIP

There are three different ways to establish a call over the network connection, through several methods depending on the condition and effects.

3.4.1.1. PC-to-PC VoIP

This method is typically simple and free of charge. It needs a computer connected to the Internet and a headset or an integrated audio built-in or peripheral devices (microphone and speaker). It also needs a special software to be installed in order to establish the communication between the parties. Definitely, this style works if and only if it has an Internet Protocol (IP) address to establish the connection. It is not limited to the Internet; it can be used in a Local Area Network (LAN) as well. This network must be IP-enabled, i.e. the IP needs to be active to manage packet movements on the network. It is easy, using this way, to connect with another person on the same network. It should be noticed that this method needs to have a relatively high bandwidth. In order to establish the connection, generally, around 50 kbps should be maintained. However, for ensuring a good quality voice, the minimum bandwidth should be 100 kbps [38].

3.4.1.2. Phone-to-Phone VoIP

This kind of style is very helpful but it is not cheap and simple to setup. It implies the use of a phone set on both sides to communicate. The essence of this method is taking the advantage of VoIP as it has a lower cost than regular telephone calls, especially for overseas destinations. Generally, there are two methods use phones to make VoIP calls [38].

- IP Phone:

The IP phone, as shown in Figure 3.2, is similar to the standard phone; the difference here is the used standard where the normal phone uses PSTN network while IP phone is based on a router or gateway. The mechanism that operates VoIP on IP phone imposes plugging in the phone to the RJ-45 socket not to RJ-11socket (which is smaller than RJ-45) as shown in Figure 3.3. The established connection, in this case, can be used for creating local connections based on wireless technologies like Wi-Fi. The device offers cable connection either by USB or 'RJ-45' to other devices [38].

Figure 3.2. IP Phone device

Figure 3.3. RJ-45 Network socket

- Analog Telephone Adapter:

ATA is a device that enables the standard PSTN telephone to directly connect to the Internet or via a PC as shown in Figure 3.4. ATA converts the voice acquired by normal telephone to digital data and sends it through the network. ATA is usually provided along with some VoIP service packages. VoIP providers claim the provided ATA when the service is being terminated. ATA is very simple and straightforward to use; all needs to be done is purchasing a VoIP service package and plugging the ATA to the phone line or connecting it to a computer. With the proper software installed, VoIP calling service will be ready to use [38]. The installation of ATA is explained in the four following steps:

1. Plugging in the power socket.
2. Plugging in the computer line RJ45 sockets.
3. Plugging in the telephone line RJ11 sockets.
4. Plugging in the DSL line RJ45 socket.

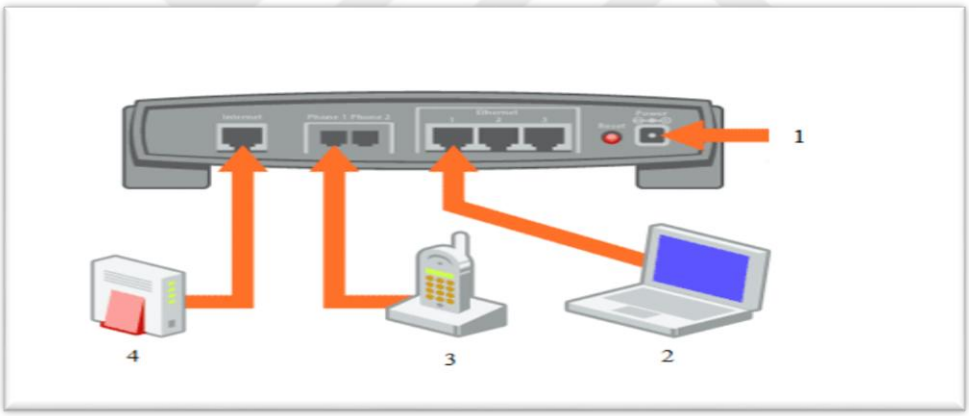

Figure 3.4. ATA device

3.4.1.3. Phone-to-Computer VoIP

Phone to computer communication can be made via VoIP services as well. In addition, it is possible to make a computer to the phone call using the same principle, as the service allows routing the call from the Internet to PSTN and vice-versa [38].

3.5. Open Systems Interconnection

Open Systems Interconnection (OSI) is developed by the International Organization for Standardization (ISO) in 1977. The main aim of OSI is to unify the communication in terms of both software and hardware standards. OSI supports protocols in different layers and it is used as a reference by engineering to the network to determine the error and repair it.

OSI reference model was set as a primary step on the way of organizing the communication between two units. The conceptual essence of OSI is based on setting up a standard framework that addresses network through seven standard layers, and the needed protocols for establishing the communication for each one of these layers. This implies that OSI is providing a role to be done at each layer. Here, it is more convenient for a specific protocol to cope with the needed role or function in a much simpler way than considering all layers at once. This concept is clearly applied in TCP/IP for instance [34]. This research work focuses exclusively on signaling protocols and voice. To comprehend the way OSI works along with the communication protocols, a description of the different layers and their included features are given in the following points:

- *Application Layer*: Representing the interface layer or the part that deals with the user directly. For example, when a browser is opened, this layer deals with HTTP or FTP for achieving web page access or reaching out certain resources. In addition, it is used for identifying communication protocols types and facilitating the authentication [34].
- *Presentation Layer:* This layer serves as an interpreter for the information. It is also responsible for the translation between different protocols [38].
- *Session Layer*: This layer is set for controlling the device number, address and whether the information has been successfully sent or not. The session layer is used for organizing sessions and connections [34].
- *Transport layer*: This layer performs data transfers between computers without errors. It also maps protocols such as TCP, UDP, and RTP [34]. This layer is also responsible for separating long messages to numerous (short and small) messages known as “segments” as shown in Figure 3.5.
- *Network Layer*: This layer is responsible for converting the logical names of devices, such as physical addresses. This message address translation is done by converting the logical title such as e-mail or IP address of a packet [34]. For example, if the physical

address is 10.10.10.10, the network layer will convert it to 20.1A.3B.C2.D1.AD as shown in Figure 3.5.

- *Data Link Layer*: This layer is responsible for providing error detection/correction at the first layer "physical". This layer also adds specific heads and tails to the packets. These attached parts contain the needed information for ensuring the integrity of the frames, as shown in Figure 3.5.
- *Physical Layer*: This Layer represents both the network and modem cards, it also deals with hardware and electrical devices, as shown in Figure 3.5. Physical layer allows passing a bit stream or electrical pulses over the network [34].

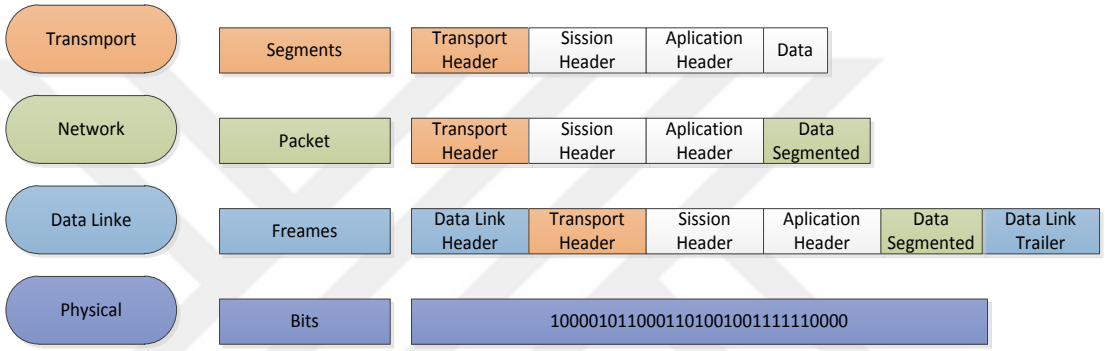

Figure 3.5. Media Layers

3.6. VoIP Protocols

VoIP service has been known as a popular IP-based calling service for a relatively long while. VoIP as network-based service needs certain protocols in order to establish the proper connection over the network as well as ensuring smooth communication with other telephony services such as PSTN, PBX, etc. The methodology of VoIP regularly regards protocols and technologies for transmitting packets over the Internet traffic. Understanding and introducing these technologies come from the explanation of all VoIP protocols, but it is difficult to fully grasp all these protocols in this thesis. Therefore, the focus will be guided towards the most commonly used protocols for forensic purposes which are shown in Figure 3.6. In the following sub-sections, a short needed brief about the main VoIP protocols is given [40].

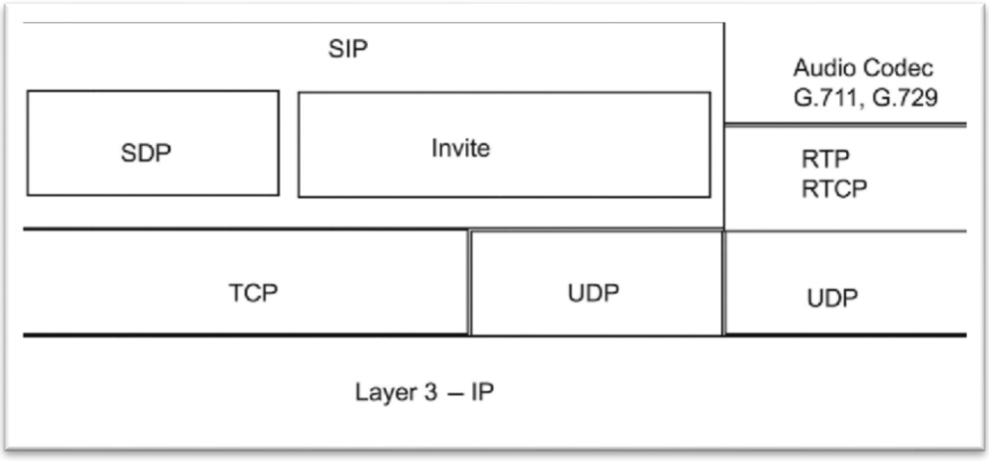

Figure 3.6. Common VoIP protocols arrangement

3.6.1. Real-time Protocol

This protocol is utilized in real-time to transport voice and video to maintain media transfer over IP network and to establish the time continuity. The main duties accomplished by this protocol are detecting packet loss and dynamic media adjustment to compensate for payload encodings such as G.729 sound [41].

3.6.2. G.729

A standard design of algorithm used for audio data compression. It is also a standard for the International Telecommunications Union (ITU) [41].

3.6.3. Real-time Transfer Control Protocol

Real-time Transfer Control Protocol (RTCP) is a protocol given to the endpoints to control the delivery of service and obtain the needed feedback on QoS, inter-media synchronization, identification, and session control. RTCP is widely used for maintaining audio-video packet transport sessions. It works in conjunction with other protocols and provides information about the payload description of RTP, monitoring the delivery, etc. [41].

3.6.4. Secure Real-time Protocol

Secure RTP (SRTP) is used for controlling RTP and ensuring the voice broadcast protection. Basically, SRTP may provide the needed security measures such as authorization, encryption and anti-reply to voice traffic in order to maintain the integrity of the packets. SRTP is also used in conjunction with RTCP and SRTCP which does almost the same task that SRTP performs with RTP. SRTP is generally a collaborative protocol and needs to be used in conjunction with other protocols based on the needed security features [41, 42].

3.6.5. Real-time Streaming Protocol

Real-time Streaming Protocol (RTSP) is a client-server protocol that is used for controlling real-time media delivery [43].

3.6.6. H.323

This type of the protocol is set and specified by the ITU. It sets a foundation for IP-based real-time communications containing audio, video, and information. Usually, in VoIP applications, the controlling and signaling of multimedia information is done through H.323 [34].

Signaling protocols are used during VoIP packets exchange. Basically, these protocols are divided into two categories: session controllers and media controllers. There is a number of session control protocols such as H323, Session Initiation Protocol (SIP), etc. [41]. However, when audio data, such as voice, is moved in the form of packets over the network between two points, there are some other protocols govern the process [41].

3.6.7. Session Initiation Protocol

SIP is established by the Internet Engineering Task Force (IETF) and it is designed for initiating or setting up and tearing down the session between two parties on IP networks [41, 42]. SIP is a text-based control protocol designed for creating, modifying, and terminating

sessions with one or more members. These sessions involve Internet multimedia conferences, Internet telephone calls, and multimedia communications.

SIP is operated with different protocols; applying the TCP allows the use of cryptographic protocols such as Secure Sockets Layer and Transport Layer Security SSL/TLS. Cryptographic protocols provide a lot of security measures whereas UDP allows a faster communication to reduce latency in connections. The main parts of SIP are User Agent (UA), register, server, and the redirect server. UA software includes the client and server elements. The primary issues of SIP security are confidentiality, non-repudiation, message safety, and authentication. SIP is used in both Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP) and IP Address Security (IPSec). The architecture of HTTP has the same client-server protocol with SIP, but this protocol supports mostly similar functionalities of H.323.

3.6.7.1. SIP Components

SIP is developed to work in conjunction with other communication protocols and specific server's communication. Communication mechanism in huge network systems such as the Internet is usually very complex. For this reason, some protocols are designed to facilitate the interface between software and hardware components, which is partially done by SIP [38]. SIP is set to control many protocols related to sending and receiving between two points (client and server). UA may operator with two types of components [44]:

- User Agent Client (UAC): which initiates the requests to be sent to the server.
- User Agent Server (UAS): which receives the requests, processes those requests and creates responses.

UAC and UAS can operate either solely or in a mutual cooperation phase. SIP is compatible with numerous applications, leads eventually to simplify and preserve the functionality of SIP [46].

3.6.7.2. SIP Mechanism

SIP standard is developed to support five special elements with the ability to establish and terminate call communication over a network. The supported facets of the protocol are [34]:

- *User Location*: Provides the determination of the destination of the session that has been established.
- *User Availability*: Supports the ability to register the caller that prefers to communicate over a network.
- *User Capabilities*: Supports the choice of media options that will be applied to the communication such as voice encoding.
- *Session Setup:* Calling parties are using Session Definition Protocol (SDP). The parameters of the session are allocated for establishing the session, such as a video and/or voice encoding that apply to the communication.
- *Session Management*: Supports modifying session parameters and call termination.

In addition, SIP is used for identifying the address, time, call beginning and some other information which can be used for digital forensic investigation.

3.6.7.3. SIP Message Signaling

SIP communication signaling is a text-based messaging similar to HTTP. SIP assists the troubleshooting in a more convenient way than H.323. Also, it transmits information between two endpoints (user and service), as well as the service of request and answers [41]. It is easier to describe this procedure in points as well as on a graph as shown in Figure 3.7.

- *Register*: Initiates a message when a user agent registers SIP address and the proxy server.
- *Invite*: Initiates a message to establish a call to another user.
- *Bye*: The command used for terminating the session initiation protocol and end the call.
- *Cancel*: The command used for abandoning the call connection request that has not yet been finished.
- *Ack*: The acknowledgment command used for accepting and beginning the call session.

In addition, there are lists of code responses applicable for identifying the process. Some of these response codes are shown in Table 3.2 [41].

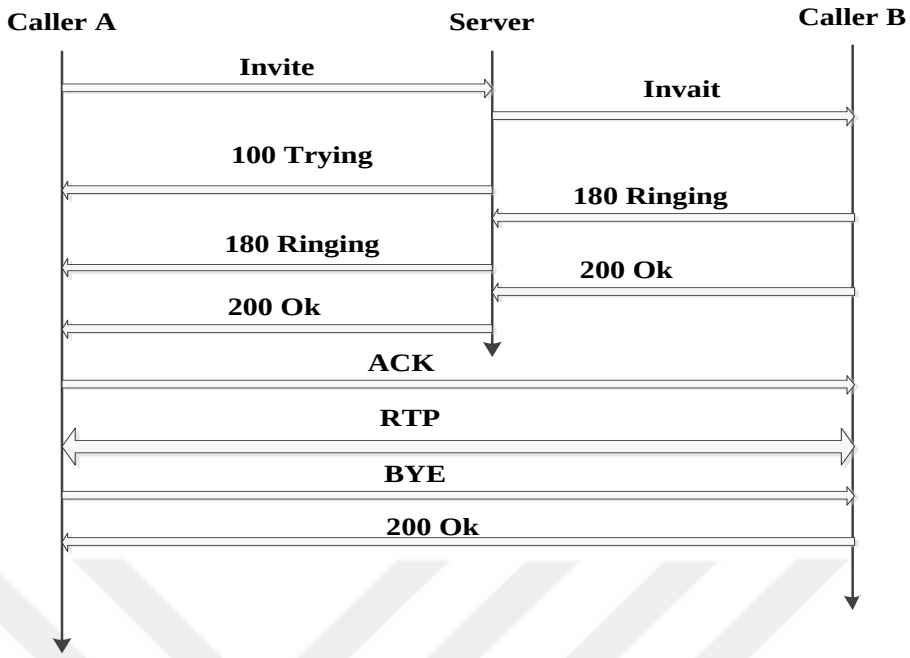

Figure 3.7. Basic SIP mechanism

3.6.8. Session Description Protocol

Session Description Protocol (SDP) is used for identifying the functions needed for the data in use. SDP sends the description of data in which the multimedia is requesting to be used through the network. SDP sends information messages to communicate with UDP. These messages contain information such as the name, session purpose, media type, session initiation time, etc. [34].

3.6.9. Media Gate Control Protocol

Media Gate Control Protocol (MGCP) is a supporting protocol that can be used as an alternative for H.323 functionalities [34].

3.6.10. Session Announcement Protocol

Session Announcement Protocol (SAP) is a multicast specialized protocol used for advertising the session by sending an announcing packet to the corresponding port and address [34].

Table 3.2. SIP Codes Response

Provisional 1xx

100	Trying
180	Ringing
181	Call Is Being Forwarded
182	Queued
183	Session Progress

Successful 2xx

200	OK

Redirection 3xx

300	Multiple Choices
301	Moved Permanently
302	Moved Temporarily
305	Use Proxy
380	Alternative Service

Request Failure 4xx

400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
410	Gone
413	Request Entity Too Large
414	Request-URI Too Long
415	Unsupported Media Type
416	Unsupported URI Scheme
420	Bad Extension
421	Extension Required
423	Interval Too Brief
480	Temporarily Unavailable
481	Call/Transaction Does Not Exist
482	Loop Detected
483	Too Many Hops
484	Address Incomplete
485	Ambiguous
486	Busy Here
487	Request Terminated
488	Not Acceptable Here
491	Request Pending
493	Undecipherable

3.6.11. Skinny Client Control Protocol

Skinny Client Control Protocol (SCCP), sometimes referred to as a skinny protocol, is an exclusive signaling protocol. SCCP is used as a signaling protocol for terminal control in VoIP. It has a very simplified composition which allows it to work with very little processing time and effort. This simplified nature is where the "skinny" name comes from (basically the essence of being lightweight). This protocol assists in reducing the cost of VoIP services by minimizing the processing cost [34].

3.6.12. Resource Reservation Protocol

Resource Reservation Protocol (RSVP) is a protocol used for creating a sort of circuit-switching network for IP network service to alleviate the issue of delay [34].

3.7. VoIP Advantages

- *Low Cost*: VoIP calls made through the computer to computer are free of charge. The only needed fee is the payment made for the Internet service which is not related to VoIP fees by any means. It is also possible to make very cheap calls from PC to phone via VoIP. The fee for international destinations would cost much less than the cellular calls or PSTN telephone calls. It is possible to find various free destinations in VoIP packages for landline and/or mobile phone destinations to some countries. In addition, VoIP service providers usually provide offers for certain packages with a monthly fee and unlimited free calls [40].
- *Low Taxes*: VoIP is generally not highly taxed as normal telephone services. In this regards, the consideration of Internet to operate VoIP plays a vital role in reducing the levied tax. This implies that using a proper VoIP package could significantly reduce the monthly calling bills [40].
- *Lower Infrastructure Cost*: VoIP service makes use of the available Internet service which does not need any special infrastructure for this purpose. Therefore, VoIP service maintains much lower implementation cost than PTSN or cellular [40].
- *Free Extra Features*: Telephone and cellular companies are charging a considerable amount of money for additional features such as call diversion, voicemail, multimedia, etc. However, most of these features are provided as free of charge in VoIP. In fact, VoIP has a special host for providing these features where a number of useful capabilities are provided totally for free [40].
- *Flexibility*: As mentioned earlier, VoIP service providers provide their users with a converter that enables PSTN telephone to use VoIP services. This is an excellent advantage as the original phone number will be maintained yet converted to a VoIP service. In addition, it is possible to use the same phone number with the provided converter even overseas as long as you are connected to a broadband or a high-speed Internet [40].
- *Video Conferencing*: Video conferencing is a special service that is considered relatively complicated and high cost. VoIP provides video conferencing at a much less cost as well as an acceptable quality of video calling [40].

3.8. Disadvantages of VoIP

The abovementioned VoIP advantages come at the cost of a few disadvantages which are listed in the following points [40]:

- *Service Interruption*: Unlike PSTN service, any interruption in the electric power causes an interruption in VoIP service. Meaning that backup power generators are needed to maintain VoIP services, especially for big organizations [40].
- *Emergency Calls*: Emergency calls in PSTN telephony systems are transferred to the nearest emergency call center based on the address. However, this is not the case in VoIP as it can be used anywhere with the same phone number. This feature is very important in emergency cases and it may create very problematic sequences [40].
- *Reliability*: VoIP service is Internet dependent; meaning that the quality of the call is directly affected by the speed and bandwidth of the available Internet connection. In addition, VoIP calls made from PC may also be much affected by the specifications of the computer and whether any other programs are being used or not. In many cases, these issues deteriorate the performance of VoIP service quality [40].
- *VoIP Voice Quality*: The quality of VoIP is also dependent and there is a number of factors affecting it. Some these factors the Internet speed, VoIP package, used devices, called destination, network traffic, calling time, etc. These factors may rapidly deteriorate the quality of VoIP calls and create serious issues in the conversation [40].
- *Security Issues*: VoIP service has a major concern regarding its security. The identity of the caller can be hidden, spamming and scamming may occur, call manipulation can be conducted, and the attackers may use their skills to deny the service of a legitimate user [40].
-

The risks of using VoIP applications are applicable to businesses, small companies, and individuals. Cyber-criminals may be looking for challenging and competitive achievements that generate several different types of risks. This includes the risk not only to VoIP but also to the data transmitted over the network.

3.9 VoIP Security

Ever since the development of VoIP in 1996, the progressive nature of VoIP applications and their usage have been growing. Within telecommunication technologies,

VoIP and its applications are regarded as relatively recent concept [45]. Before thinking about the necessity for VoIP system security, there are many problems to overcome. Various VoIP applications are threatened in their availability, integrity, and privacy. The followings are the most common security aspects that should be highly considered in VoIP applications:

- *Privacy*: Privacy is related to the type of information that cannot be used by unauthorized parties. Information privacy for network elements includes IP addresses, user information, operating systems, protocols used, etc. Getting to this information makes digital crimes easier.
- *Reliability*: The own user may possibly make a mistake or a change that allows unauthorized operations to damage or uncover information. However, the reliability of information means that the information is still unchanged by ordinary users.
- *Caller Identification Spoofing*: Caller identification is a service provided by most telephone companies. It enables the display of the caller's details such as the caller ID. A number of websites provide caller identification spoofing support the drop of the need for any special devices. However, recognizing caller identification spoofing by the incoming caller details may not be a straightforward task as the attacker may change the details around the outgoing calls. For VoIP, caller identification spoofing is easier than the traditional telephone as shown in Figure 3.8 [45].

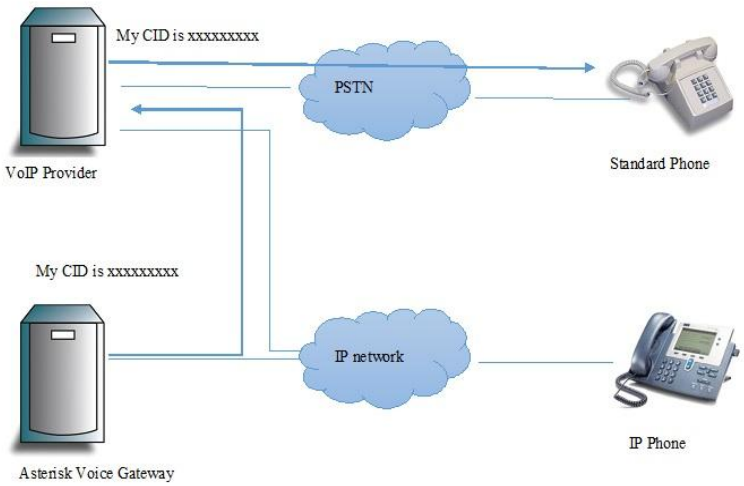

Figure 3.8. Caller ID spoofing

3.10. VoIP Threats

Cyber-criminals attempt to initiate their activities while considering the following: being invisible on the Internet, using different devices, diverting the original locations, using

several phone numbers, using hidden usernames and identities, and deploying several languages with different time zones. In addition, they usually use several accounts to communicate over the network using a composite of voice and other media. These provocative acts usually generate a condition that is similar to blackmail [34].

4. COMPUTER MEMORY FORENSIC

4.1. Memory Definition

Computer memory is a hardware part that is capable of storing data. It can be used for retrieving the stored data during the operational time or after starting up the machine. This variation in the mechanism depends on the type of the memory, namely volatile or non-volatile [46]. The technique used for data movement in memory is performed by electric signals including input and output information [47]. Regarding different types of memory, the research efforts have paid attention to improving the memory in terms of speed, capacity and physical size. Before 1994, scientists and researchers were looking for the proper development of memory such as audio cassette, floppy disk (8 and 5.25 inch), Compact Disc (CD), etc. In 1995, Digital Versatile Disc (DVD), which has the same physical dimension and shape of the CD but faster in speed and bigger in capacity, became commercially available. In 1997, the use of flash memory and Multimedia Card (MMC) became popular. Nowadays, massive storage types, like cloud computing, have become predominant [47].

4.2. Computer Memory Types

Usually, computer memory types are divided into two parts:

4.2.1. Non-volatile Memory

Non-volatile memory is the memory that keeps the information with or without electric power being on, such as memory cards as shown in Figure 4.1. This type of memory can be used for storing and retrieving information any time [39]. The followings are the main types of computer non-volatile memory:

- Hard Disk Drive (HDD): The concept of HDD includes read-write using magnetic mechanism and it offers a high capacity data storage. HDDs come in different sizes such as Giga-Byte (GB) or Tera-Byte (TB), etc. The design of HDD is consisting of a circular disk that spins a small needle to bring in and read data from the disk as shown in Figure 4.2 [48].

Figure 4.1. Non-volatile memory card

Figure 4.2. Hard Disk Drive

Figure 4.3. Solid State Drive

- Solid State Drive (SSD): is a new and modern technology of the HDD as shown in Figure 4.3. It has bigger capacities and smaller sizes than HDD [48]. One of the advantages of SSD is replacing the mechanical structure and operational mechanism by a solid-state technology.
- Read Only Memory (ROM): is a special type that is used only for reading. This type is mainly used for booting-up the computing's main information. ROM does not allow writing and that is the reason behind the name read-only [48].

- Flash Memory: is a relatively different type of memory which is classified as one of the secondary non-volatile storage types. However, it is popular, widely used and comes in different shapes and sizes as shown Figure 4.4. The flash memory can be used for read-write of digital data. The mechanism of this memory device needs a power supply of +5V received from the USB port of the computer [39].

Figure 4.4. Flash memories

4.2.2. Volatile Memory

All functions and activities of the computer use the volatile memory during the operational time. The idea of using volatile memory is employed for increasing activities speed and data processability. This type of memory is designed in a way that it loses the stored data after the power goes off [48].

4.3. Volatile Memory Architecture

Operations vary in speed while they are processed in the computer system. The processor deals with two memory types, as shown in Figure 4.5. The primary memory which stores data for short periods while the device is running such as RAM. The secondary memory, the storage that holds the information in memory for anytime use, where the information remains until it is deleted. Computer CPU is extremely fast compared to the secondary memory's access speed. As a result, the primary memory needs to offset this speed and make the access time close to the processor speed (a few nanoseconds) [49].

- Cache Memory: Cache memory is a small memory in the CPU that assists in filling the speed gap between the CPU and RAM [39].

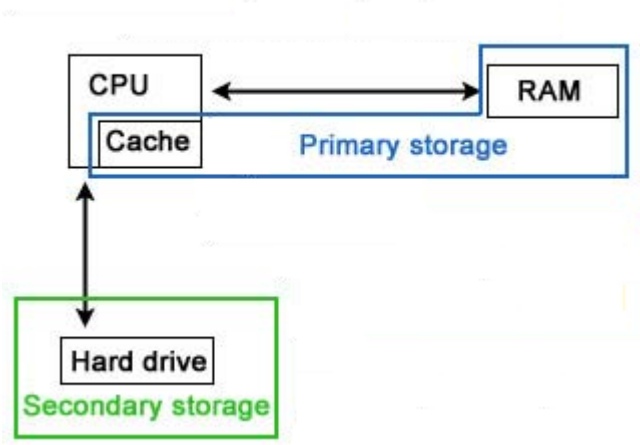

Figure 4.5. CPU architecture

- Random Access Memory (RAM): is a part of the computer data storage and it speeds up the movement of data during the processing operation. RAM loses the stored data once the power goes off. The computer needs enough RAM to run the operating system as quickly as possible. Every application loads its data into the RAM while running the machine in order to load the operating system and used applications [50]. The RAM has the following features:

  - The ability to read and write.
  - A faster speed than the ROM.
  - The ability to store temporary information at a high speed.
  - Data loss immediately once the power goes off.
  - The ability of upgrading by replacing the available RAM with a larger capacity one.

There are other types of volatile memory such as Dynamic Random Access Memory (DRAM), as shown in Figure 4.6, and Static Random Access Memory (SRAM), as shown in Figure 4.7 [50].

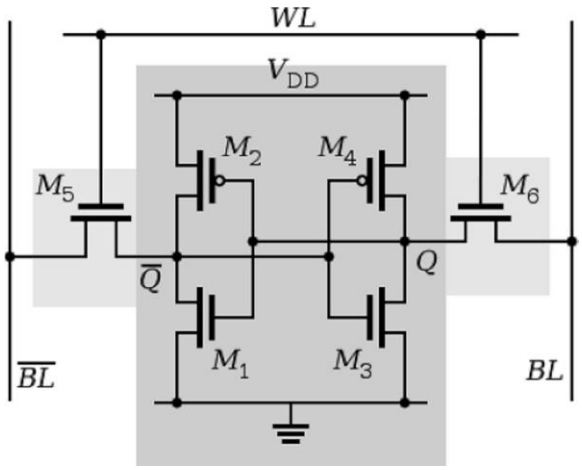

Figure 4.6. SRAM diagram transistors

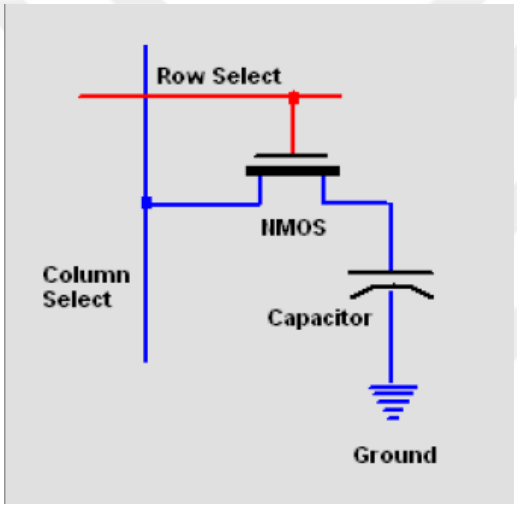

Figure 4.7. DRAM diagram

- Virtual memory: computer hardware supports the RAM to organize and manage the operating system algorithms. Virtual Memory (VM) is a type of software that has developed to extend RAM and improve the storage capacity [39]. Normally, users use many programs at the same time. For this reason, the mechanism of memory will require extending the capacity of the RAM. The limited RAM capacity may not be enough for satisfying the requirements of running operating system and applications. Therefore, the concept of VM supports the RAM in this regard. All these processes don't affect the operating system due to the reason that the system is already consistent through it is operations as shown in Figure 4.8 [39].

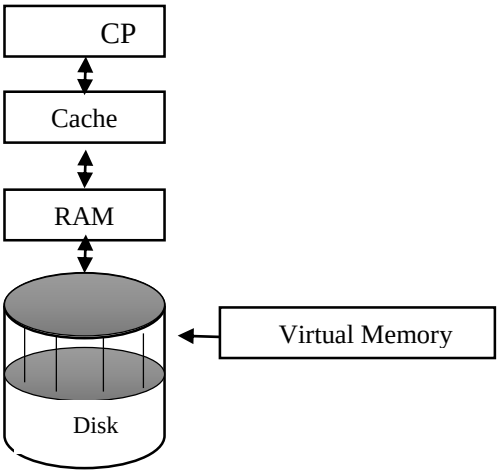

Figure 4.8. Virtual memory

All processes operating the computer keep a copy of their information in the RAM and DRAM. The DRAM saves data in capacitors as electric charges. unfortunately, DRAM loses the data even when the power is on as the capacitors need to be refreshed every 64ms. However, the RAM keeps its data as long as the machine is on. The RAM can be used for the digital investigation to collect meaningful artefacts by capturing and analyzing the contents of the RAM [29].

4.4. Digital Forensic

Digital forensic is state of the art of extracting and analyzing of digital information available in the computer memory, then converting the processed extracted information to a digital evidence in a reliable report form that can be used in the court of law [51].

4.4.1. Digital Forensic Concept

The concept of digital forensic is essentially based on determining, extracting, analyzing, presenting and reporting digital evidence in a way admissible in the court of law [52]. Digital forensic aims to analyze the gathered information through many techniques and to create as much useful information as possible to be able to identify the criminals. However, investigators can use special software and computing hardware devices with forensic tools to extract and analyze the data of interest [51]. Digital forensic is generally applied for all computing application cases. The difficulty is based on the orientation of

application and the available tools which are related to forensic issues. For example, in VoIP forensic cases, digital investigators need a deep knowledge in networking concept, VoIP protocols, and specific hardware parts such as memory. In addition, there is a number of digital forensic applications available for acquiring, analyzing, and reporting digital evidence.

4.5. Digital Evidence

Digital evidence is represented by the meaningful artefacts of digital information. These artefacts can be refined and presented as a readable report in legal cases. All data movements in the digital environment that include any type of data are considered as digital evidence [52]. Nowadays, all kind of online transactions such as social media activities, shopping, etc., present a traceable data that can be gathered and used for digital forensic purposes [34]. Likewise, VoIP applications can be also used for extracting digital evidence applicable for the digital investigation. These traces become artefacts stored in the computer memory or on a computing device's storage [53].

4.5.1. Digital Evidence Investigation

Digital evidence investigation is defined as detecting and providing effective digital artefacts from several parts of the computer and network. The investigation of digital evidence may be achieved from computer memory and storage capabilities over the network. To get engaged with the digital evidence investigation process, a starting point should be identified in order to recover a useful information for the legal case. This information may range based on the application, nature of evidence and the specific case. The general process of digital forensic investigation can be categorized into five phases as shown in Figure 4.9 [52]:

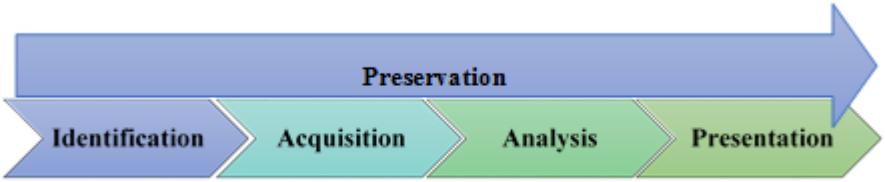

Figure 4.9. Digital Forensic Tenets

- *Identification*: This step is taken in order to determine which items (computing items) are considered as a part of the crime scene. Generally, any electronic device that has the ability to store digital data temporary or permanently is considered as a target for this step.
- *Preservation*: This step is taken to preserve the digital evidence. Essentially, ensuring correct images of the extracted data are made from the memory. This leads to presenting the digital evidence and properly saving it in a read-only format to prevent the manipulation of the acquired data [52], [53]. Preserving evidence starts first with a chain of investigation and continues over all digital forensic phases until handing the final report to the authority.
- *Acquisition*: This step needs various tools and methods to forensically acquire and collect digital evidence resides on the identified components. The examiners use software and hardware tools to copy hard disks or other memory types to avoid damaging the original copy and keep the evidence in a safe status [53]. It is important here to mention that it may be necessary, in some cases, to develop certain algorithms or filtering methods in order to extract the right data related to the needed forensic analysis.
- *Analysis*: This step is taken to regenerate the needed useful information that can be used as a legal evidence from an ambiguous acquired digital evidence. This step requires special tools and programs that vary according to the application. In some cases, it may be needed to use more than one tool to obtain the needed information. Here, understanding the background and the concept of the application under which the forensic is being conducted is essential [53].
- *Presentation*: The final step in digital forensic is generally creating a readable report that can be used in the court of law. The report includes affidavits of expert, experience and the history of the examiner. In general, the final report should include all methods operated and explain the tools and steps used for analysis as well as the original evidence copy. The produced report shall not be technical and hard to understand by non-specialists, rather, it should be in a sort of actual presentation of the followed methods, obtained evidence and the final conclusions and comments on the related legal case [52], [53].

4.5.2. VoIP Forensic

The high implementation of communication technologies using computers, smartphones, and networks has become an important part of our life. This also has increased

the misuse and cyber-crime incidents. VoIP forensic has taken a major interest in the digital forensic field. VoIP is actually a technique created for voice communications over IP networks. Nowadays, it is easy to use VoIP services to create VoIP environment, as it needs only an e-mail address and/or a username in order to connect. This makes cyber-criminals interested in VoIP applications because a limited identity information and facts are needed for using VoIP applications over the network [37]. Moreover, usually, the standard technical wiretapping is unsuccessful for VoIP case. Ultimately, digital forensic detectives look for different ways for recovering evidence from VoIP applications. VoIP is affected by general threats that may affect other Internet services, especially voice and media communication service. However, some of the vulnerabilities can be generated due to the lack of a real physical connection with the caller or the true identity of the contacting party. This kind of threats is generally called social threats. There could be other types of attacks such as the Denial-of-Service (DoS), interception, service abuse, and eavesdropping [37]. Fortunately, digital forensic applications can be used for investigating and analyzing systems through software and hardware. This is equally applicable for recovering and extracting information from VoIP protocols and device memory such as volatile and/or non-volatile memory. This is conducted to provide enough evidence to let the offender be impeached by the respective judiciary system.

4.6. RAM Forensic

As a principle, investigating digital forensic depends on obtaining the necessary forensic details and reinstating the initial data to investigate and trace of cyber-criminals. In this context, all computer memory types provide information related to the digital forensic investigation. The information available in the physical memory could present a great deal about the system from the start-up until the shutdown [49]. Digital evidence types vary according to data movements. Generally, network packets produce a powerful source of evidence [49].

RAM is extremely useful in digital forensic as it holds information related to the used application from the start-up till shutting down the system. The commonly looked for information from the RAM is represented by [54]:

- Temporary files system
- Registry data: name, password, phone number, etc

- Operating system information
- Routing Tables
- The Address Resolution Protocol (ARP) Cache
- Kernel information
- Information related to media
- Data logged remotely
- Process Table

A detailed explanation about RAM forensic and its related tools and methods is given in Chapter 5.

4.7. Related RAM Forensics and VoIP

The thorough review of the topics related to the digital forensic field reveals that it is necessary to use more than one tool for analysis purposes. Also, one tool cannot solve all forensic issues [55]. Originally, the digital forensic of volatile memory deals with the recovery of data from memory. To keep up with the emerging science and the relationship between the RAM and VoIP forensic analysis, the investigator can take advantage of a “live" forensic and get more information about VoIP data which is very hard to get from basic forensic tools [25].

5. VoIP ARTEFACTS EXTRACTION FROM RAM

Since a decade ago, digital forensic researchers have been investigating VoIP forensic as well as volatile memory analysis. Besides, they have presented several methods that assist in recovering information and the success of the forensic investigation. In the modern technology of computing world, many forensic tools exist for assisting the investigators and simplifying VoIP forensic process [54]. The experimental work of this research is conducted using the following hardware and software tools:

- Enough capacity of the memory for saving the files created from RAM acquisition process. For this purpose, Maxtor HX-M500TC/GMR - 500GB external hard disk is used.
- Table 5.1 presents the used environments along with their hardware specifications of the used devices for VoIP calls.

Table 5.1. Experimental machines specifications – acquisition environments

Hardware Device	Operating System	Processor	System Type	RAM Size	RAM Type
Desktop	Windows10 Provisional	Intel	x64-based processor	4GB	DDR3
Laptop	Windows 10 Enterprise	Intel i5-3230	x64-based processor	8GB	DDR3

- Table 5.2 shows the details and specifications of the used examination and analysis devices.

Table 5.2. Experimental machines specifications – analysis environments

Hardware Device	Operating System	Processor	System Type	RAM Size	RAM Type
Desktop	Windows 10 Provisional	Intel i5	x64-based processor	4GB	DDR3
Laptop	Windows 10 Enterprise	Intel i5-3230	x64-based processor	8GB	DDR3
VM	Elastix Server	Intel i5-3230	x64-based processor	4GB	DDR3

- The used software tools are provided in Table 5.3.

Table 5.3. Experimental software tools

Software purpose	Type of software
VoIP server	Elastix VoIP server 2.5
RAM Acquisition Tools	FTK Imager v3.1, Magnet Capture V1.0, RAM capture.exe, and DumpIt
Forensic Analysis Tools	Forensic Explorer, FTK v6.0, X-Ways Forensics, Belkasoft, Magnet EIF6.8.

5.1. VoIP Data Extraction through RAM

VoIP forensic is a technique for identifying fraud calls over the network or from memory such as the remains of a call data in the RAM. Digital investigation is classified into two sections software and hardware. Understanding VoIP forensic methods, as presented in [6] leads us to suggest some ways for VoIP investigation based on two main categories. Each of these categories has its own two-way branches of investigation as shown in Figure 5.1.

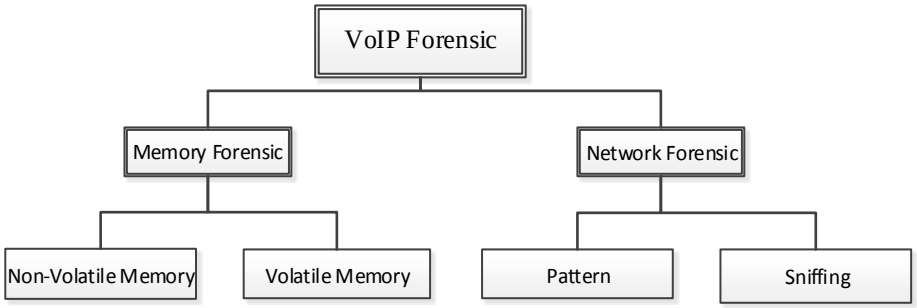

Figure 5.1. VoIP forensic categorization

The common way of digital forensic is essentially confined to scenarios [49]. Choosing the way of the investigation depends on the conditions of the cyber-crime or digital crime scene. For instance, if the system is off, the investigators should use non-volatile memory while if the system is still on, the investigators may use volatile memory. This operation is illustrated in Figure 5.2.

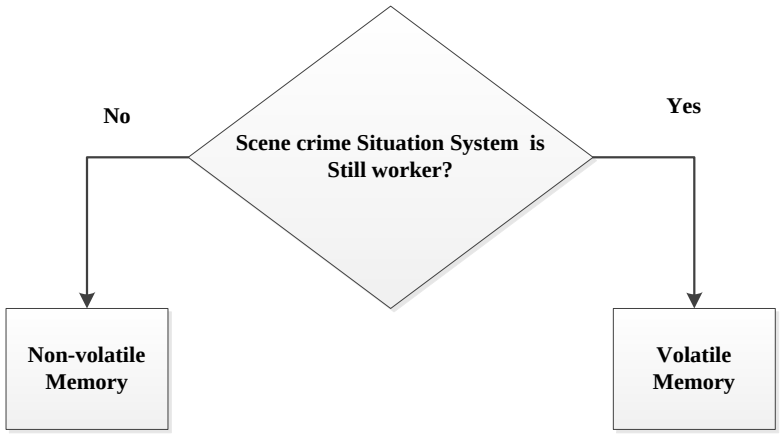

Figure 5.2. Cyber-crime condition and the applicable forensic technique

The common five phases of digital forensic are also applicable to VoIP forensic. These five steps have been used in this research work aiming to solve VoIP forensic issues and to detect the evidence related to VoIP from the RAM. This is clarified in a flowchart as presented in Figure 5.3.

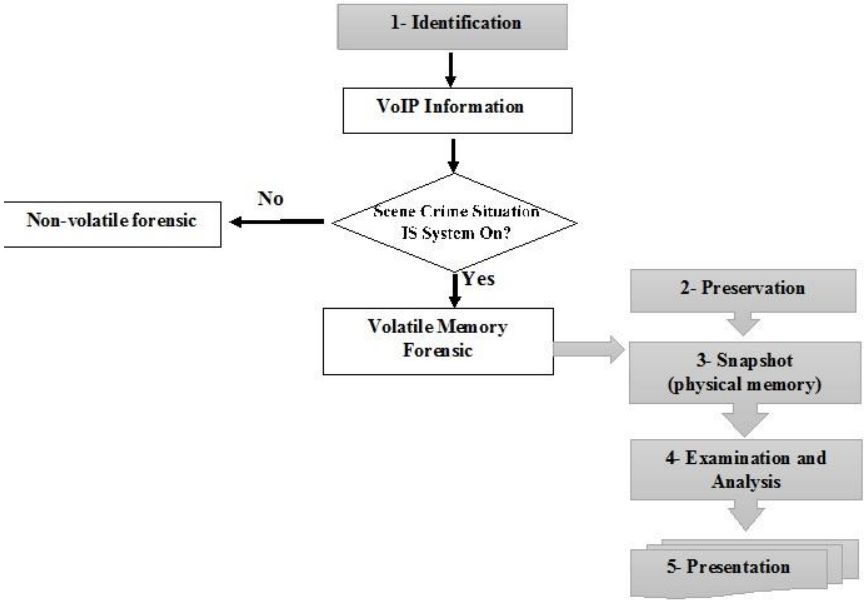

Figure 5.3. The use of volatile memory to investigate VoIP

5.1.1. Identification

In this study, the focus has been guided to the artefacts relevant to VoIP information remnants available in the RAM after the call is terminated. The main point is identifying the information of the VoIP user.

5.1.2. Preservation

VoIP forensic investigators usually try to obtain a protection for the crime scene without changing the environment, for more reliable and validated analysis. The success of investigation generally depends on the digital forensic preservation. Distorting the information relevant to the digital evidence may come from damaging the preserved contents. Here, this work is mainly based on volatile memory analysis. In order to conduct RAM forensic analysis, the system should be maintained "on" as the data will be lost in case of shutting down the system [49]. The seized systems should be kept un-tampered with so that RAM imaging would contain reliable data. The acquired RAM images are stored in and external hard disk and flash memory to back up and keep the original data without any change. Generally, the preservation starts from the first step and continues until the reporting.

5.1.3. Physical Memory Acquisition

Memory acquisition (i.e., dumping, snapshot, capturing, and imaging of memory) is collecting digital evidence via two methods, namely static acquisition, and live acquisition. The acquisition, in a basic sense, involves copying and saving the information from the memory [51]. Saving the original information for analysis is usually achieved by RAM and other memory imaging. It is important to understand how the tools work and the problems that may encounter as they have effects on the results and analysis capabilities [49]. In the standard of digital forensic science, memory imaging is used prior any analysis procedure. It is important to understand the snapshot of the current physical memory immediately after the event takes place. This is due to the fact that the memory processes may change in a short while as we deal with a volatile memory.

In this thesis, several memory capture tools such as Magnet Image, FTK Imager, RAM capture, and DumpIt are used for extracting and saving RAM information for further analysis.

5.1.4. Examination and Analysis

The main objective of examining and analyzing is to forensically provide enough information as a required by the legal case. Here, the focus is mainly guided towards the artefacts relevant to VoIP. This simplifies and speeds up the investigation process. The tools used in this study are FTK, X-Ways Forensics, Belkasoft, Magnet IEF and Forensic Explorer. All these tools apply different features and provide forensic analysis with advantages and disadvantages. The results of these tools are summarized to help examiners to choose the right tools. This study also implemented a filtering process to assist in finding special tags related to VoIP protocols.

5.1.5. Presentation

At the end, the presentation of electronic evidence must be reported in a formal readable document that is understandable by non-specialists. In this thesis, a comparison between the used VoIP server information with the analysis results is conducted. In general, this step is very important as the legal case will be built on the presented report created based on crime case analysis.

5.2. The Establishment of Call over Internet Environment

Individuals and companies nowadays find it much more useful to build a call over the Internet with the open source server PBX such as "Elastix server" software tool. The advantage of building a call over the Internet system is to present the information register. Elastix server is one of the common VoIP services that can be used for building the call communication through local and global networks, which deals with several protocols within this process [56]. This server utilizes the IP header of the packet to establish the communication.

Establishing the required communication scenario is done based on the following steps:

- Downloading the free Elastix software of VoIP server from (www.elastix.org/downloads). The deployed version in this research is Elastix 2.5.

- Creating a Virtual Machine (VM) to be used for the Elastix server operational process. The created VM in this work is named “Elastix 2.5” and it is based on Linux type. This step is shown in Figure 5.4.
- Bridging the created Elastix 2.5 VM with the available Internet connection. This is done from the settings of the created VM as shown in Figure 5.5. At this stage, the created VM should be ready to use for installing the Elastix server.
- Installing the Elastix server by booting up the created VM and filling the required information as shown in Figure 5.6.

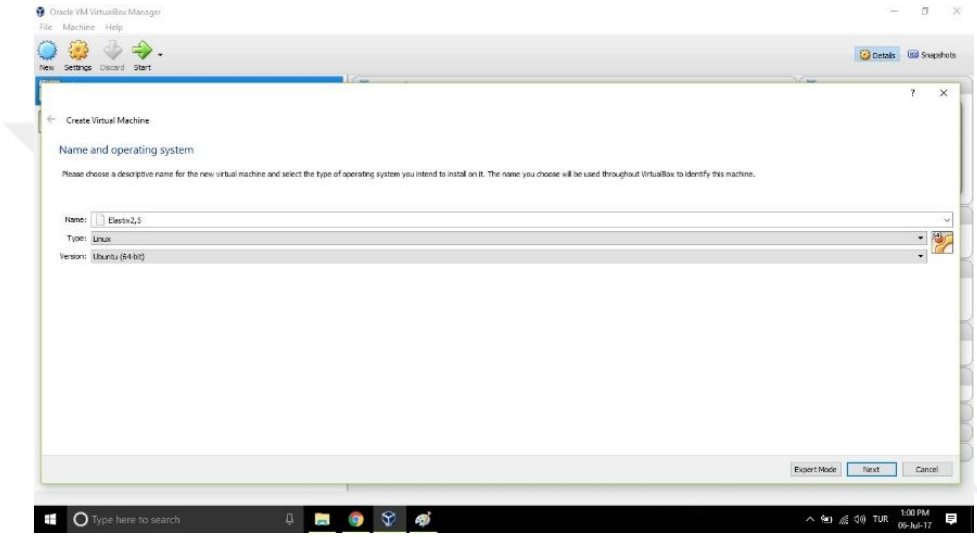

Figure 5.4. Creating a Virtual Machine (VM) to be used for the Elastix server

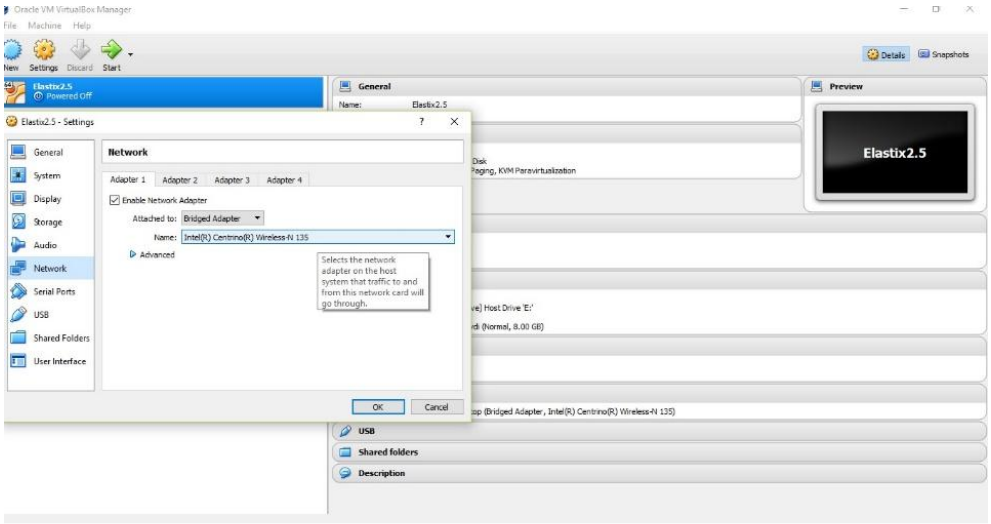

Figure 5.5. Bridging the created Elastix 2.5 with the available Internet connection.

Figure 5.6. Installing the Elastix server by booting up

- Setting up a dynamic IP address and Netmask for the created VM as shown in Figure 5.7. The used IP address and Netmask in this research are:

  IP : 192.168.56.1

  Netmask : 255.255.255.0
- Creating a root password and an admin password for the VM and rebooting the system.
- Logging in the created VM using the chosen root password as shown in Figure 5.7.
- An IP will be automatically generated from the VM as shown in Figure 5.8. This IP address will be used for accessing the Elastix sever as shown in Figure 5.9.

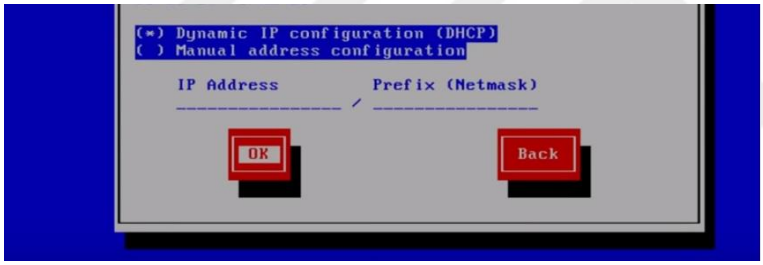

Figure 5.7. Creating a root password and an admin password

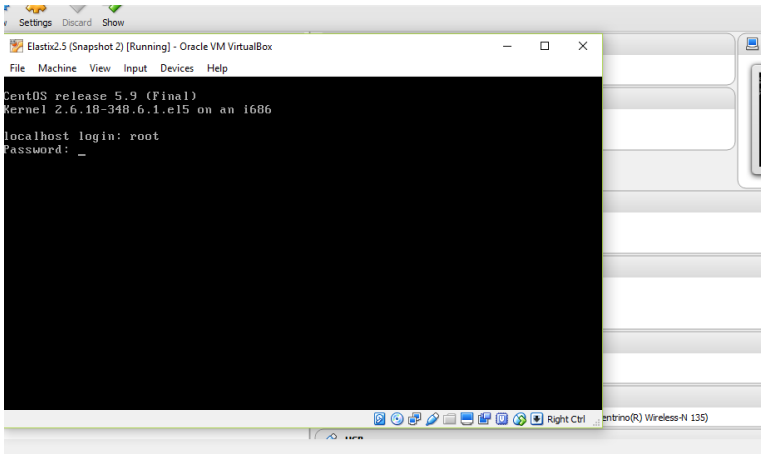

Figure 5.8. Automatically generated IP address from the created VM

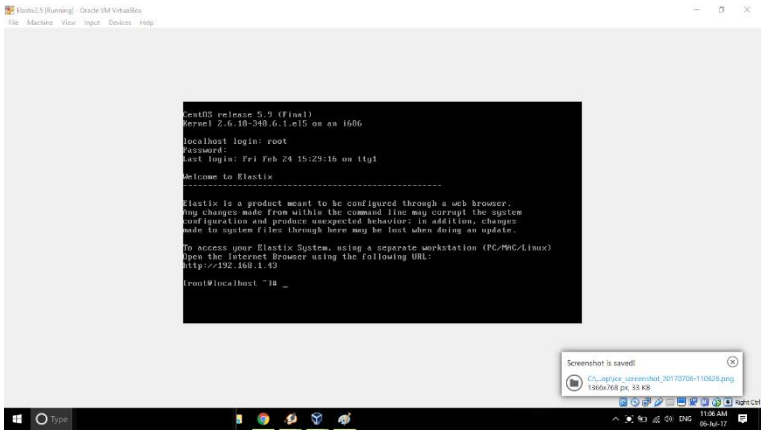

Figure 5.9. Accessing the Elastix server using the automatically created IP address

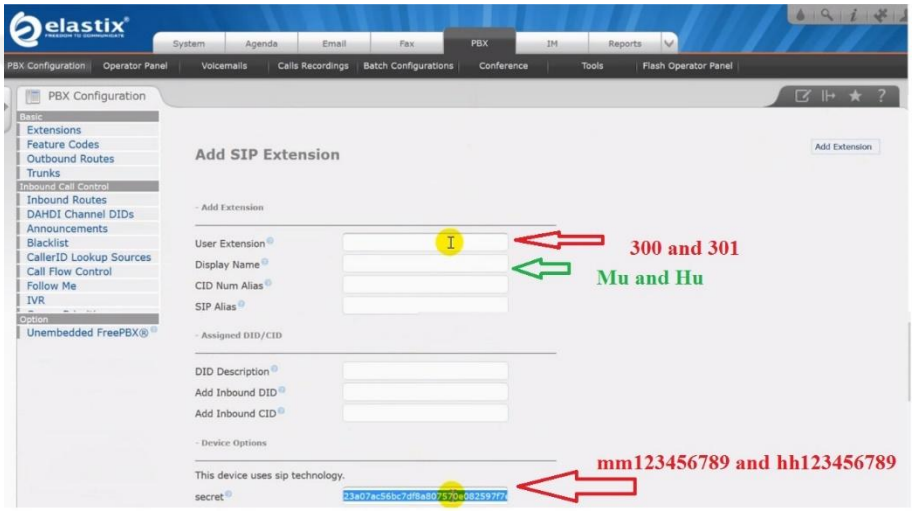

Figure 5.10. Elastix server configuration

- Adding SIP extension from the Elastix server options. Adding SIP extension option is found under PBX Configuration as shown in Figure 5.10. The required extension details are filled as provided in Tables 5.4 and 5.5 for both caller and receiver respectively.

Table 5.4. Client A information

Name	Hu
Client Number	0090534
SIP	0090534
Mailbox	Hu534@firat
Password	hh123456789

Table 5.5. Client B information

Name	Mu
Client number	00964750
SIP	00964750
Mailbox	Mu750@firat
Password	mm123456789

A VoIP application softphone should be used in order to make a call using the created Elastix server. The used VoIP application here is Zoiper which is a free softphone source that supports Android and Windows operating systems. The following steps are followed to install and run Zoiper:

- Downloading Zoiper softphone application from (https://www.zoiper.com/en) [57].
- Installing Zoiper application.
- Creating a new account.
- Setting up the account type to SIP as shown in Figure 5.11.
- Providing the credentials of the created account as shown in Figure 5.12.

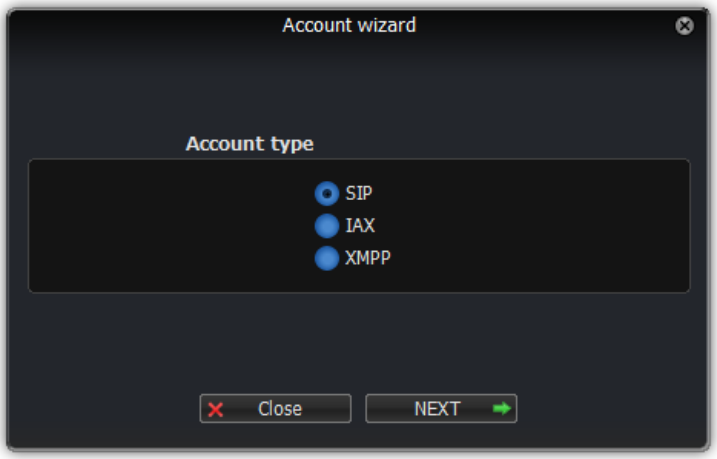

Figure 5.11. Setting up SIP account for Zoiper

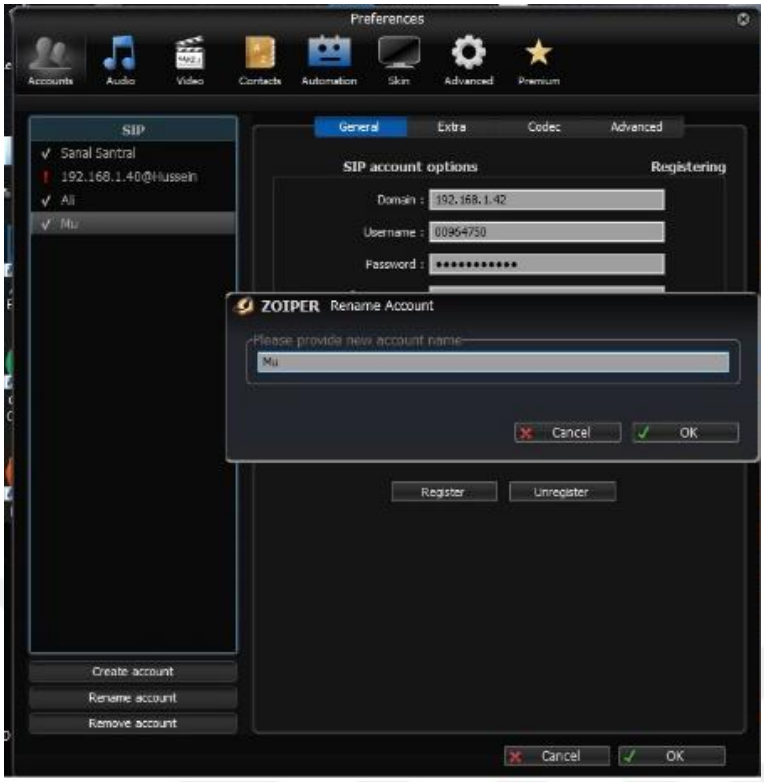

Figure 5.12. Setting up Zoiper account credentials.

Figure 5.13. Call history of Zoiper application

- Setting up the account name to the specific client, for example Mu and Hu. At this stage, the installation and setting up of Zoiper is done.
- Starting up Zoiper application and dialing any of the provided numbers in the adding extension step as shown in figure 5.13.

To ensure the applicability and reliability, two RAM sizes are used, namely 4 GB and 8 GB for acquisition and analysis purposes. The acquisition process of this research is done based on the following steps:

- Deleting the temporary files of the operating system for both used RAMs and restarting the system for each case.
- Starting up Zoiper application in the host system which is used as a host for receiving an unknown VoIP call.
- From another separate system, a VoIP call was made to the host system and the replay was given after around14 seconds from the beginning of the call.
- A real call was made over a period of 48 seconds and the call was terminated from the caller system.
- Zoiper application was logged out after the call termination and the RAM capturing process was then conducted.

To control and prove the communication, Wireshark, a network capturing software, is used for this purpose. Wireshark is an open source application tool used for analyzing network packets information. It can be downloaded from (https://www.wireshark.org/) [58]. Wireshark begins by sniffing packet information such as sender, destination, and the server computer device. It traces signaling information in the server as shown in Figure 5.14, it displays the information of sender as shown in Figure 5.15, and it displays the information of the destination as shown in Figure 5.16. From Musip: *00964750@10.6.0.27* To *<sip:0090534@10.93.198.151>*.

Figure 5.14. UDP of the Server Signal

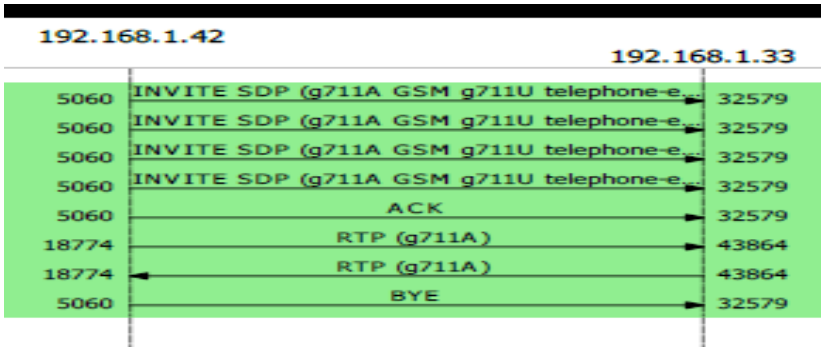

Figure 5.15. VoIP call tracing

```
INVITE
sip:0090534@10.6.0.27;transport=UDP SIP/2.0
Via:SIP/2.0/UDP0.6.153.154:58935;branch=z9hG4bK-524287-63b60c6db56534e9
Max-Forwards: 70
Contact: <sip:00964750@10.6.153.154:58935;transport=UDP>
To: <sip:0090534@10.6.0.27;transport=UDP>
From:<sip:00964750@10.6.0.27;transport=UDP>;tag=ba6edf35Call-ID:
026tel0ZcWUSJrzaX7EVfA..
CSeq: 1 INVITE
```

Figure 5.16. UDP of the destination signal

5.3. Physical Memory Acquisition

The endeavors direction of this research work is discovering the tools that may assist in VoIP investigation using the RAM. RAM is widely used in digital forensic where it may have artefacts of malicious codes, encryption Keys, full content codes of network packets, hidden processes, registry information (username and password), open Window registry keys, hold over remnants of VoIP calls, etc. [41].

In this work, RAM acquisition is obtained by four different tools. The used tools are FTK Image, Magnet RAM Capture and Belkasoft. Each tool has its own GUI or command line interface. In order to properly acquire the RAM information, the task starts after call termination according to the following steps:

- Determining the status of the device (off or on).
- Identifying acquisition type and log file (RAM Capture and analysis)
- Determining hardware and software specifications, including RAM capacity.
- Collecting possible information from the suspected device.
- Conducting these steps should be done as soon as possible as the important artefacts in the RAM can be lost.

5.3.1. FTK Image

FTK Image is developed by Access-Data and it is a GUI-based tool. FTK Image 3.1 is a free tool that can be downloaded from (www.accessdata.com/product-download). This tool can create a complete RAM imaging without affecting the original data. It can be used for RAM capturing with or without being installed on the computer. However, it supports files format types such as AD1 and RAW.

In this experimental work, FTK is used by running the imager to create a digital image of the RAM by clicking on the following icon ( ) . Setting the destination path of the output file is shown in Figure 5.17. All other details such as file name and extension can be set from the same properties.

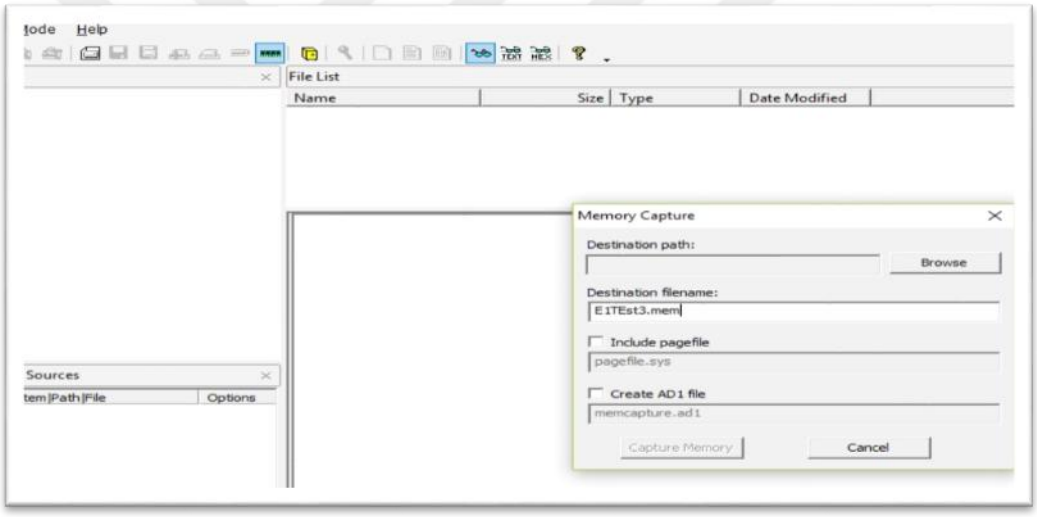

Figure 5.17. The interface of FTK RAM Capture

5.3.2. Magnet RAM Capture

Magnet memory Imaging is a free tool and can be used for RAM capturing with or without being installed on the device. The used version is downloaded from (www.magnetforensics.com/free-tool-magnet-ram-capture). It supports both Windows 32 and 64 systems and all Windows versions. The interface of RAM capture is very straightforward to apply. It is possible to run the capturing tool either from an external hard disk, a USB or from the local machine. In this work, the capturing tool is used from an

external hard disk. As shown in Figure 5.18, the default fragmentation setting “do not split” is kept the way it is. Before starting the capturing operation, it is necessary to specify the destination of the output file to be saved.

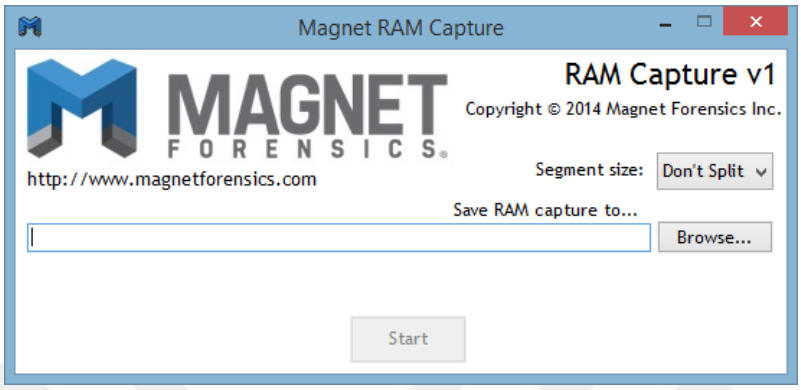

Figure 5.18. Magnet RAM Capture Tool

5.3.3. Belkasoft RAM Capture

Belkasoft RAM capture, as shown in Figure 5.19, is a proprietary software that offers a one-month trial version. It can be downloaded from (www.belkasoft.com). The tool is able to work with all Windows versions and system architecture (32-bits or 64-bits). The tool creates the file format .mem. This RAM capture tool does not require installation on the local device, rather it is possible to use it from a thumb drive or an external hard disk. The interface is simple to use and the capturing is applied by clicking the “Capture” button. The memory dump is saved on the same drive by default, and it does not give the option for changing the saving path.

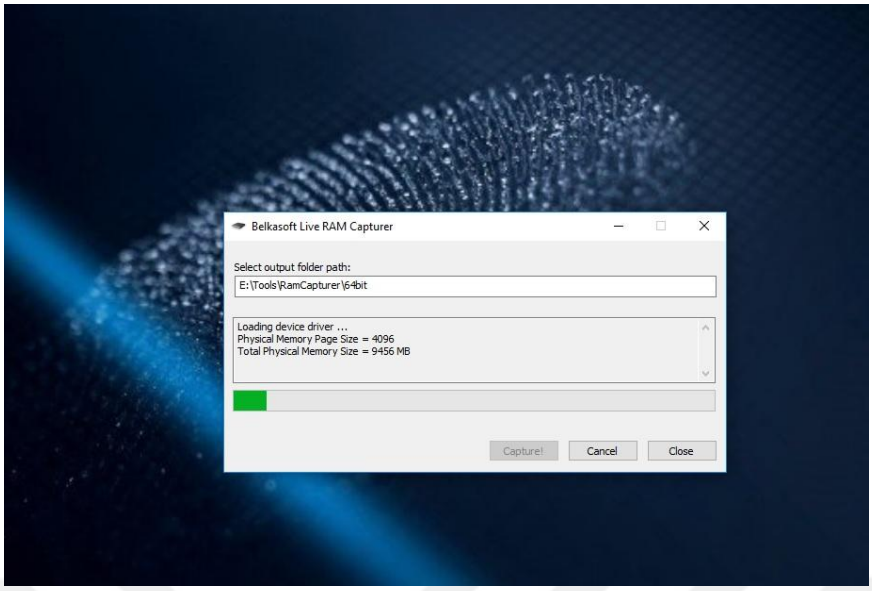

Figure 5.19. Belkasoft RAM Capture

5.3.4. DumpIt RAM Capture

This type of tool is an open source tool applicable for physical memory acquisition. This tool is a command-line forensic tool that is compatible with Windows 32-bits and 64-bits machines. The resulting format of the memory dump is .ram. This tool can be used with or without installation on the local machine. The process of memory acquisition using DumpIt.exe should be according to the following steps:

- Running the command-line prompt as administrator, as shown in Figure 5.20.

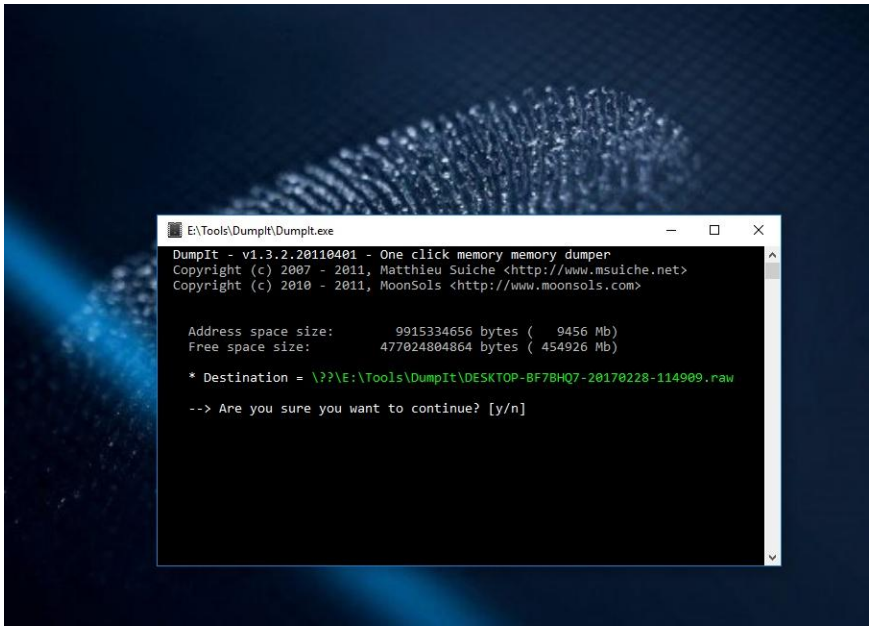

Figure 5.20. The command-line of DumpIt tool

- The interface, as a default option for output, shows choosing to accept answers 'yes' or ‘no’ to exit. Initially, this command-line shows the details of the computer’s memory with its total size.
- The generated output will be saved in the tool’s main folder and it is possible to change the destination of saving directory.

5.6. VoIP Forensics Analysis and Validation

Generally, the forensic analysis includes the recovery of artefacts and viewing Windows registry for any suspicious information. There are various forensic tools that can be applied in different cases. For this reason, the random selection of forensic tools to a specific VoIP case may lead to slowing down the investigation and even wasting the effort without any tangible results. Therefore, classifying forensic tools will assist investigators in selecting the suitable forensic tool according to the VoIP forensic case. There are many factors influence the investigators’ choice of the correct digital forensic tool. In this study, five types of forensic analysis tools are applied to recover artefacts relevant to VoIP from log files extracted from RAM imaging. This will be used for classification purpose in the next chapter.

5.6.1. Forensic Explorer

Forensic Explorer is a specialized digital forensic analysis and presentation tool. Forensic Explorer is developed by GetData Forensic (www.forensicexplorer.com). It is a GUI-based tool, and it develops along with investigators’ use and available information. This tool is able to recover system files, deleted files and it supports the acquisition of file formats (.raw, .e01, and .AFF). Forensic Explorer is compatible with Windows operating system environments, both 64-bits, and 32-bits.

To use Forensic Explorer tool, first it is needed to insert the USB dongle, as shown in Figure 5.21, that has the required key.

Figure 5.21. Hardware dongle of Forensic Explorer

Forensic Explorer uses log files to provide information on various areas assist in digital evidence analysis. The GUI of the tool provides validated files system section with comprehensive data views on the interface, including gallery disc, hex, and keyword search. In this experiment, evidence files were added by choosing the file (E1TEst3.raw) from an external hard disk. The configuration of the settings is shown in Figure 5.22 and Figure 5.23.

The analysis of an 8 GB RAM capture took around 6 seconds. The result is given in Figure 5.24. The output includes both hexadecimal and text data. In the same way, the second experiment was configured with the same setting and applied to a 4 GB RAM capture. The RAM capture file loaded from the external hard disk is named (E2Test3.raw). The analysis took approximately 9 seconds. The obtained results are shown in Figure 5.25.

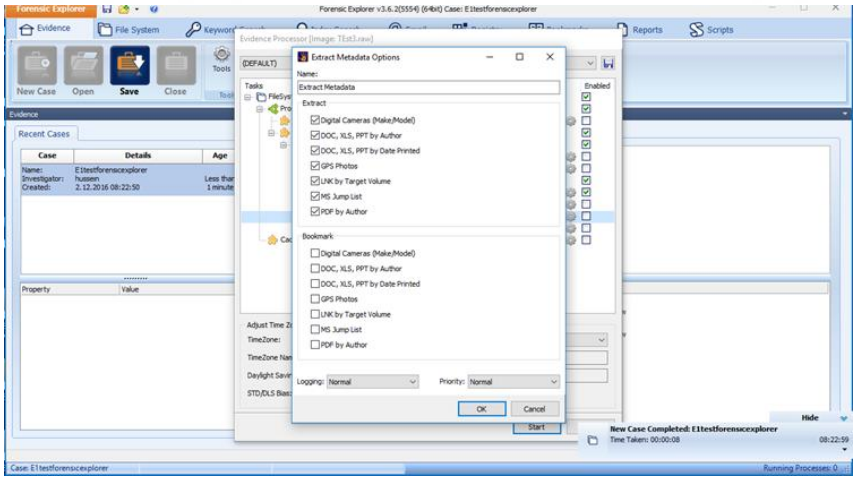

Figure 5.22. Configuration setting of system tool – extract metadata options

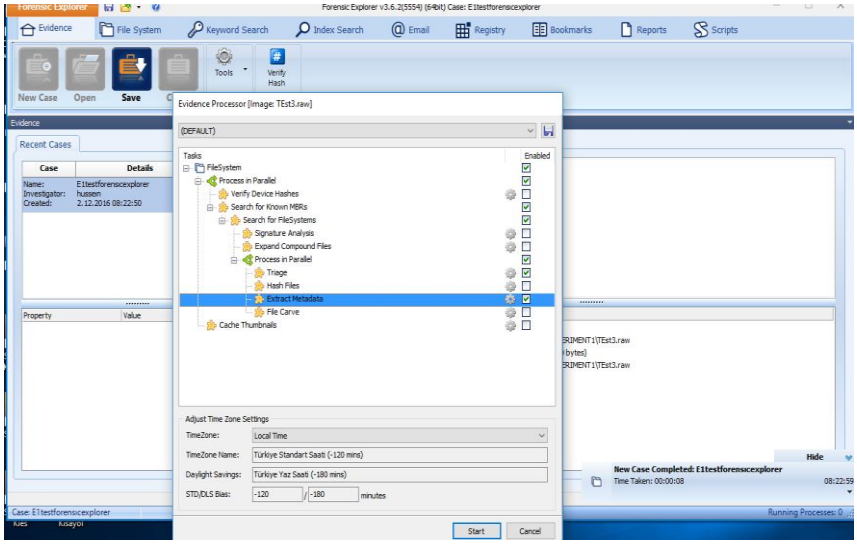

Figure 5.23. Configuration setting of system tool – evidence processor

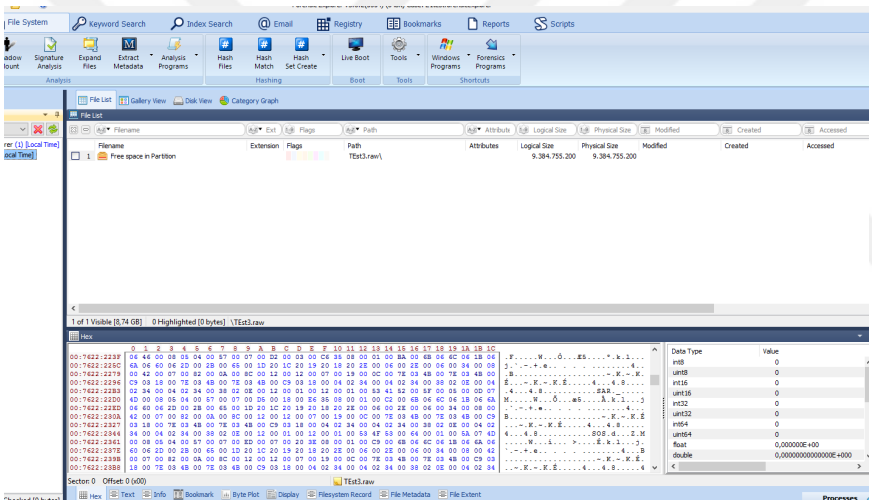

Figure 5.24. Forensic Explorer analysis results for 8 GB RAM capture

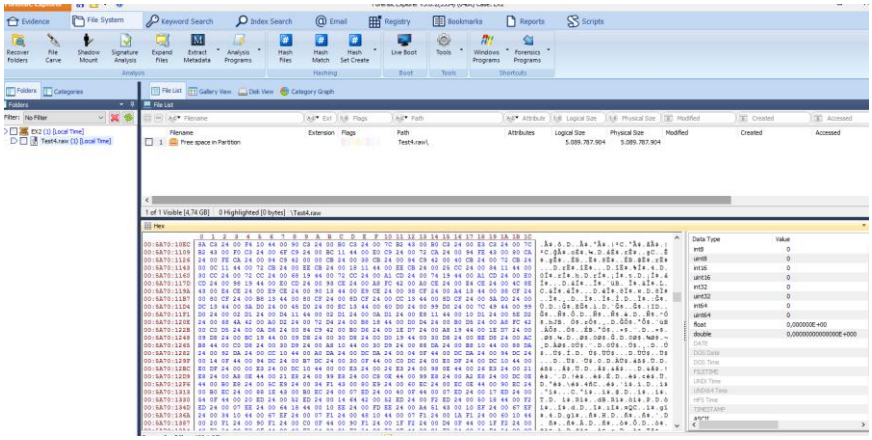

Figure 5.25. Forensic Explorer analysis results for 4 GB RAM capture

5.6.2. FTK v6

The Forensic Toolkit (FTK 6.0) is developed by AccessData. It is a GUI-based tool that allows discovering and searching for different pieces of evidence or data that investigators are looking for. As shown in Figure 5.26, the interface of FTK tool is divided into two sides: left side (marked as 1) which displays the cases under investigation, and the right side (marked as 2) which provides some information about the cases.

In this experiment, to create a new case, it is needed to fill some information about the name of the case as shown in Figure 5.27. To make the analysis easier for the investigators, the "detailed" option can be checked. This makes the results of evidence more detailed. However, for this specific case, the setting is left as default as shown Figure 5.28.

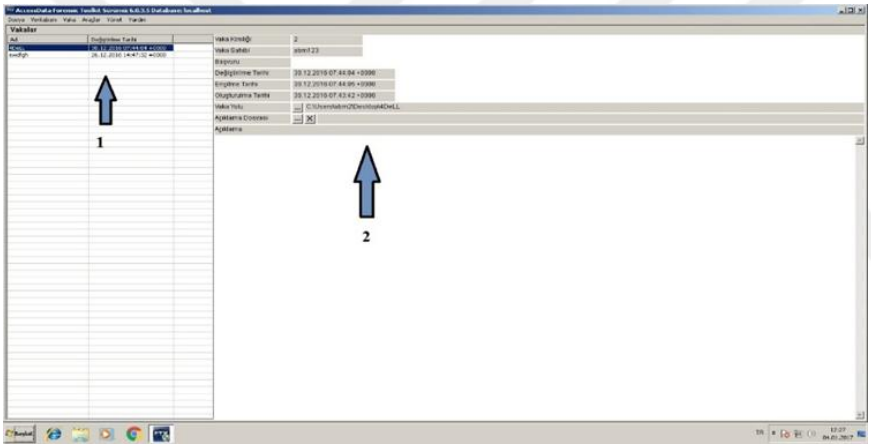

Figure 5.26. The interface FTK Tool

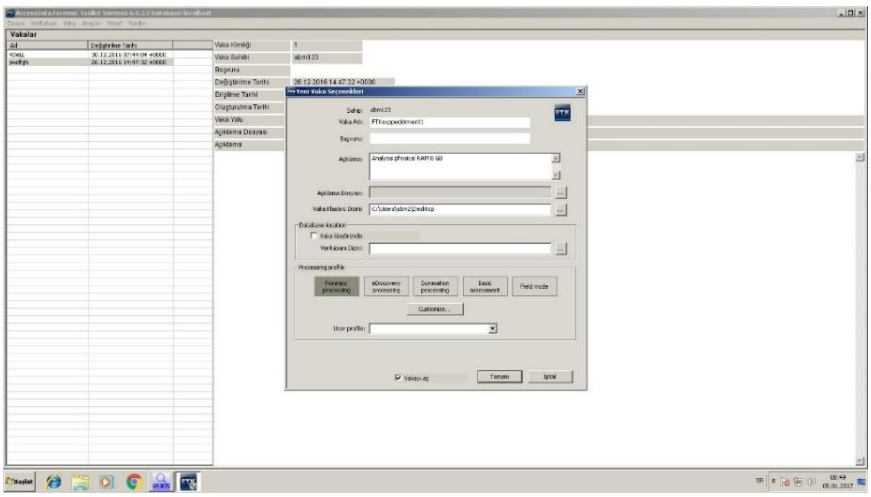

Figure 5.27. Building a new case in FTK 6.0

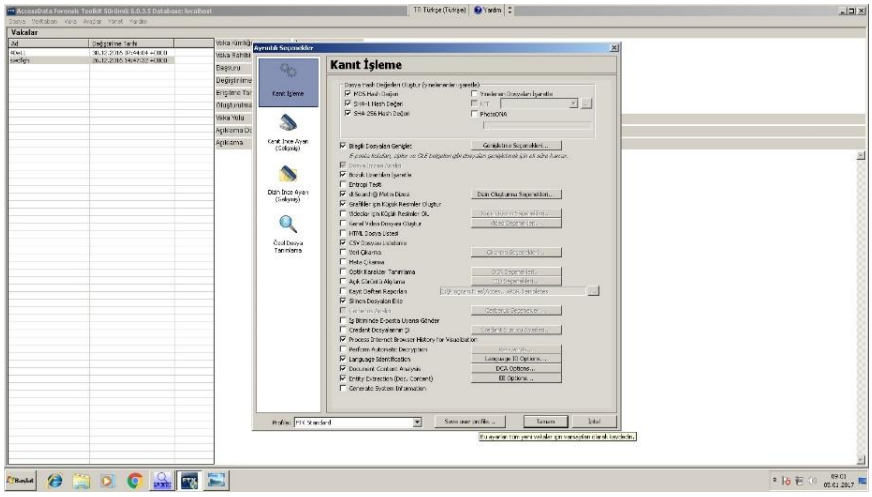

Figure 5.28. Default settings for FTK 6.0

After building a new case, the evidence file should be selected to be investigated. Similar to the previous experiment, the 8 GB RAM capture file here is named "FTKexpermient1" as shown in Figure 5.29. The correct time zone should be set. Since the experiment was conducted in Turkey, the time zone option is set to "Istanbul" time zone. Finally, some information about this case such as the name and description had also to be filled. The analysis process took around 7 minutes to produce the final output.

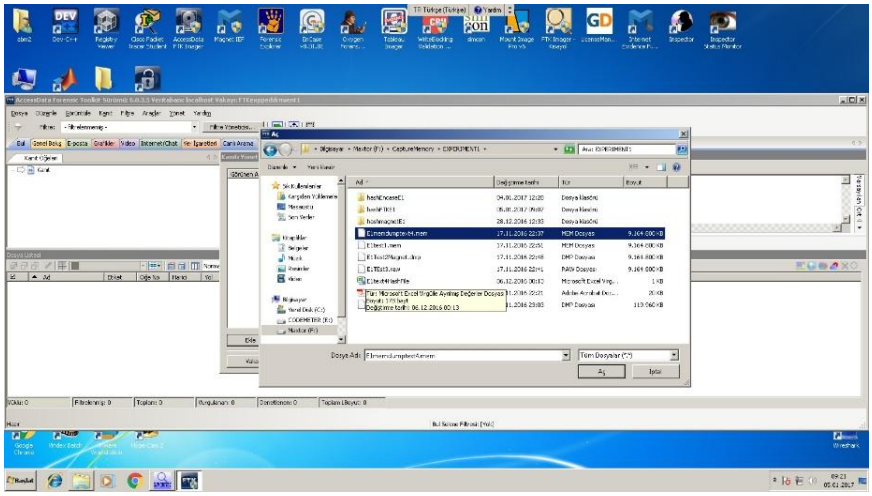

Figure 5.29. Evidence file Selection

In the second experiment, the file captured from a 4 GB RAM was used and the same steps were applied for the analysis process. The analysis time needed around 4 minutes for completing the process. The analysis results are shown in Figure 5.30.

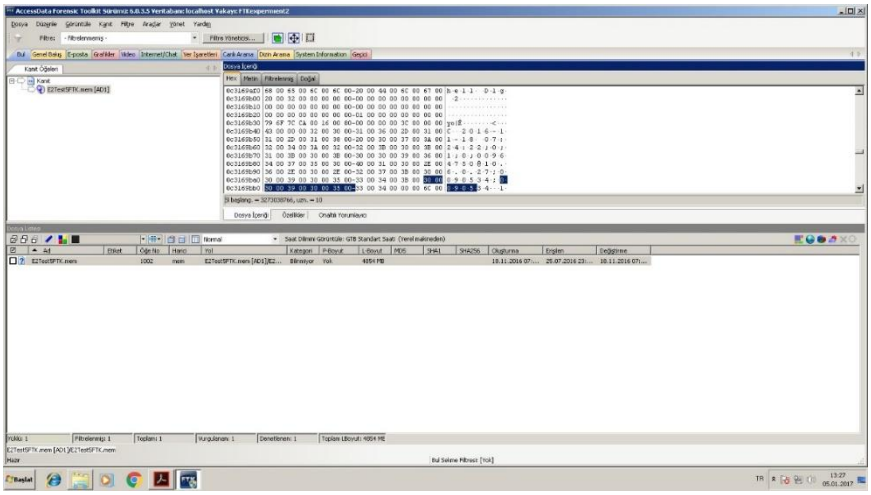

Figure 5.30. The results of the 4 GB RAM capture file analysis using FTK 6.0

5.6.3. Magnet IEF v6.8

Magnet Internet Evidence Finder (IEF), is a commercial software, development by Deloitte. It is a GUI-based software that assists investigators to analyze many types of forensic cases, such as computers, smartphones, and tablets. In addition, Magnet forensic tool is able to examine the Internet and communications activities. With a focus on recovering the deleted network data, such as chat logs of call application software, temp file, and user browser history. To get started with IEF, the USB dongle key must be plugged in to unlock the software. Then, the driver of interest can be selected as shown in Figure 5.31.

To analyze a RAM capture file with Magnet IEF, the image file icon should be clicked as shown in Figure 5.32. Next, the capture file created during the acquisition should be specified from the external hard disk to be analyzed as shown in Figure 5.33. A list of the software settings displays various options to be chosen by the examiner as shown in Figure 5.34. A large list of supported VoIP applications, such as WeChat, Viber, QQ chat, Skype, WhatsApp, Facebook, etc is found within the analysis option of this tool. It is possible to disable or enable any of these icons based on the orientation of the analysis. The next step is to fill the required information for the new case as shown in Figure 5.35.

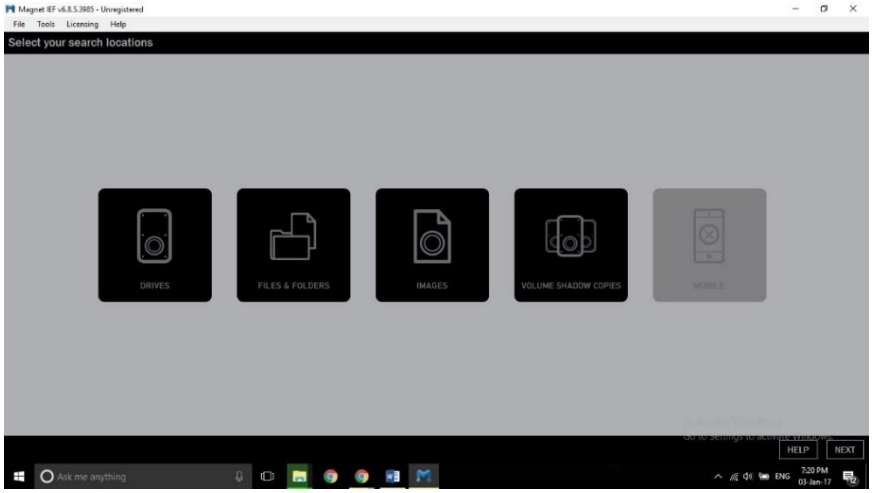

Figure 5.31. Interface of Magnet IEF

Figure 5.32. Image file selection icon

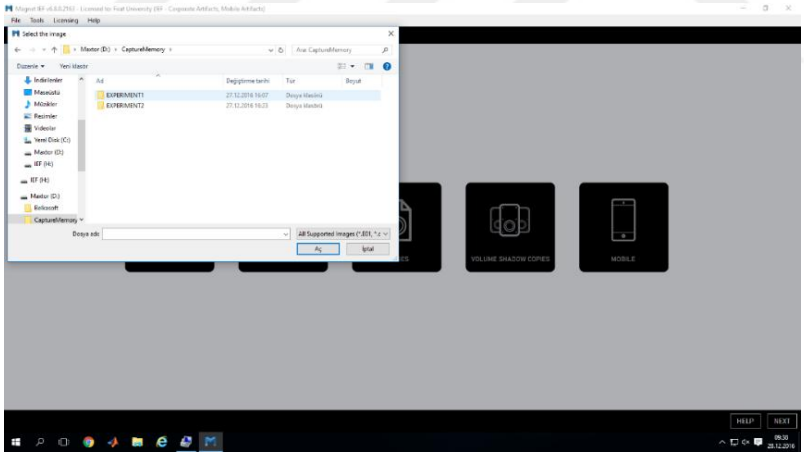

Figure 5.33. Specifying capture file path from the external hard disk

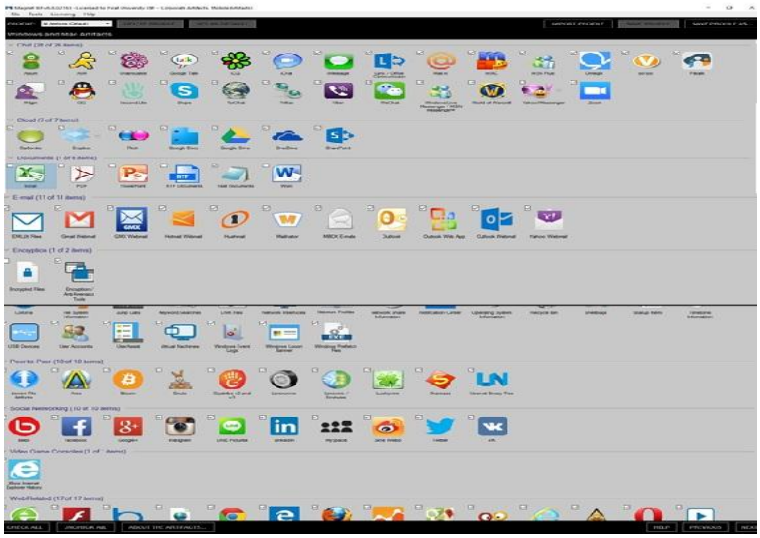

Figure 5.34. Supported applications and software by Magnet IEF

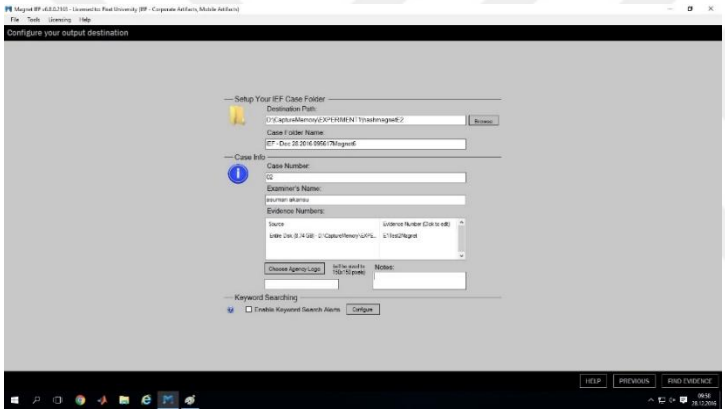

Figure 5.35. New case information form

Eventually, to run the analysis, the start button should be clicked as shown in Figure 5.36. The elapsed time for evidence extraction and analysis is around 27 minutes. The extracted artefacts are presented in Figure 5.37.

These results are related to meaningful data relevant to VoIP and other applications or system information. Magnet IEF is essentially presenting the results in hexadecimal format as shown in Figure 5.38.

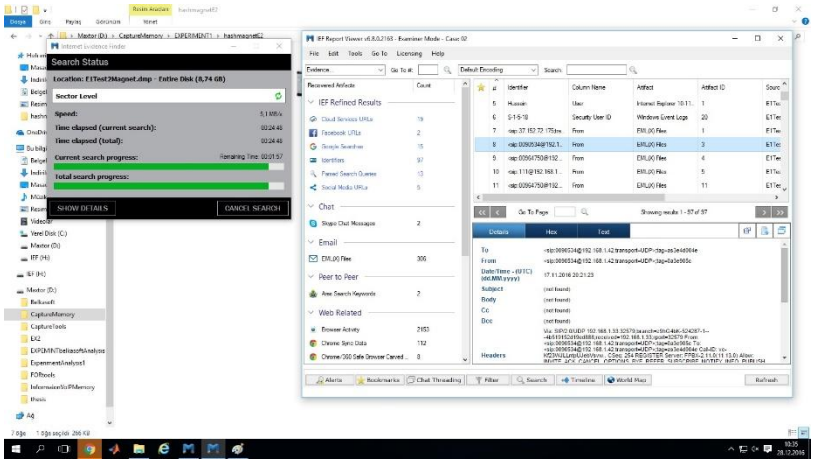

Figure 5.36. Magnet start up interface

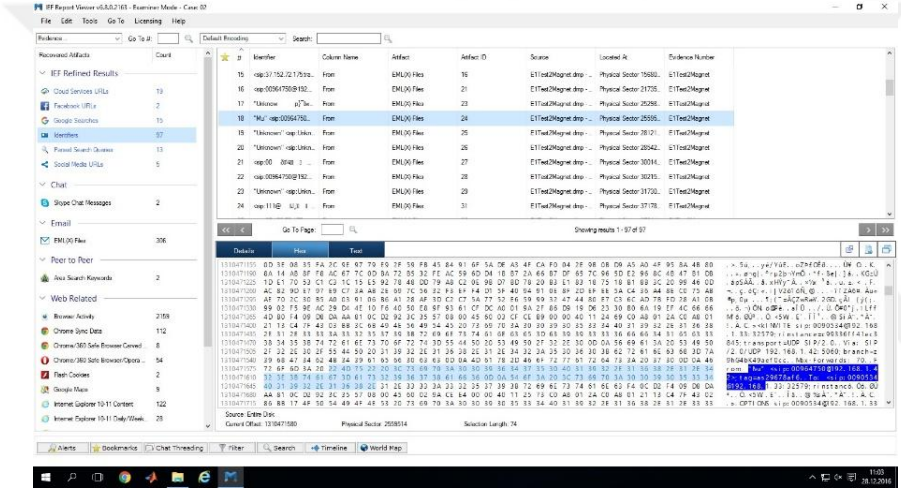

Figure 5.37. Analysis results of Magnet IEF

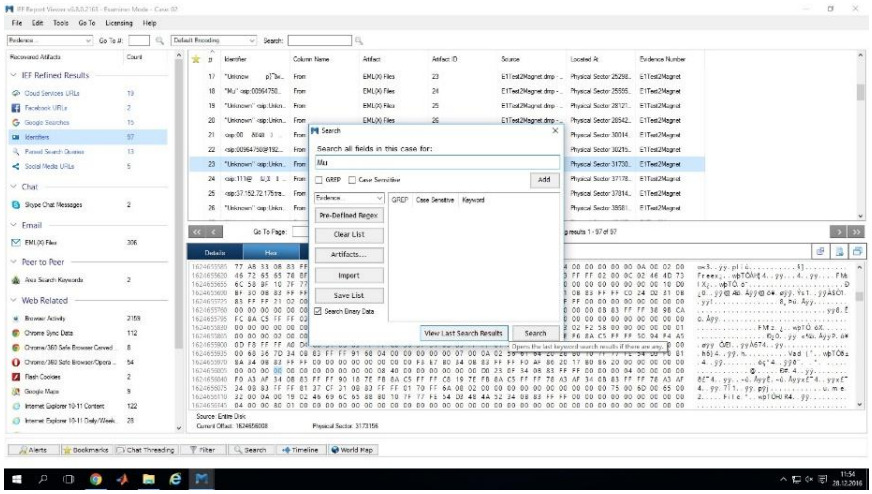

Figure 5.38. Manual search for a special text case

The second experiment was applied to the capture file of a 4 GB RAM. The used file name is E2TestMagnet as shown in Figure 5.39. The setup configurations for the second experiment was set to the same option as the first experiment. The analysis process spent around 14 minutes to get the results as shown in Figure 5.40.

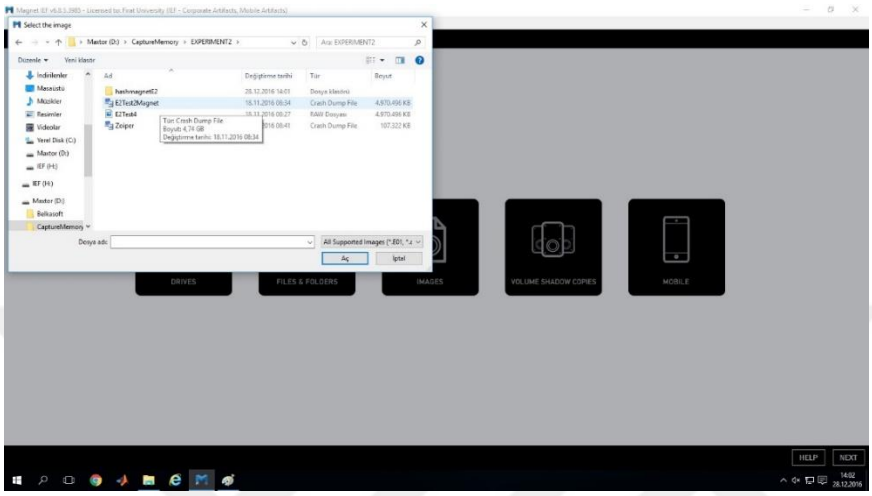

Figure 5.39. Second case file path specification

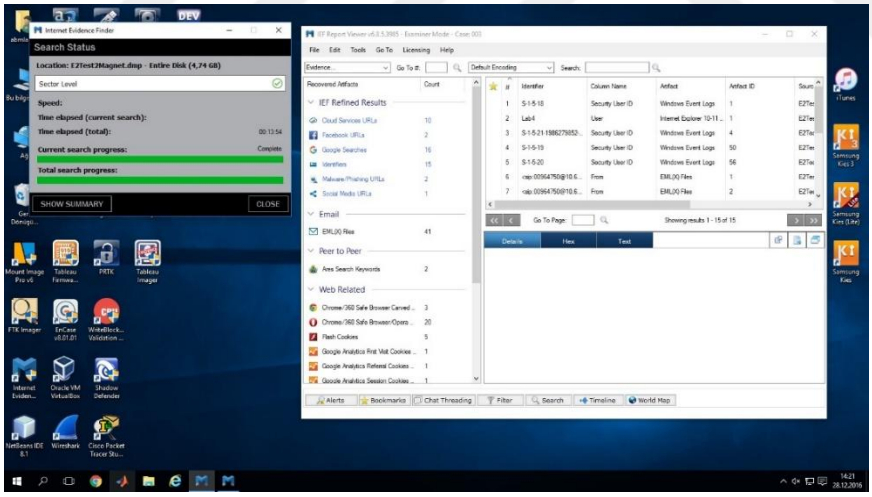

Figure 5.40. (4 GB) RAM capture analysis using Magnet IEF

5.6.4. Belkasoft Tool

Belkasoft is a GUI-based proprietary software tool that can be downloaded from http://belkasoft.com/. Belkasoft is useful for memory images analysis. It supports file formats .e01, .ex01 and .DD images and it is compatible with Windows 64-bits and 32-bits, Mac, Linux, and Android operating systems. The first step in using Belkasoft for analysis is

choosing the RAM capture file. This experiment deployed the 8 GB RAM capture file named E1Test1. The next step should be dedicated to filling the required new case details and configuring the settings of the tool for the analysis as shown in Figure 5.41. These settings assist the investigators to analyze the operations and make the process easier and faster. In this case, image and video formats are not required, thus, they were unchecked. The analysis took around 40 minutes. The obtained results are shown in Figure 5.42.

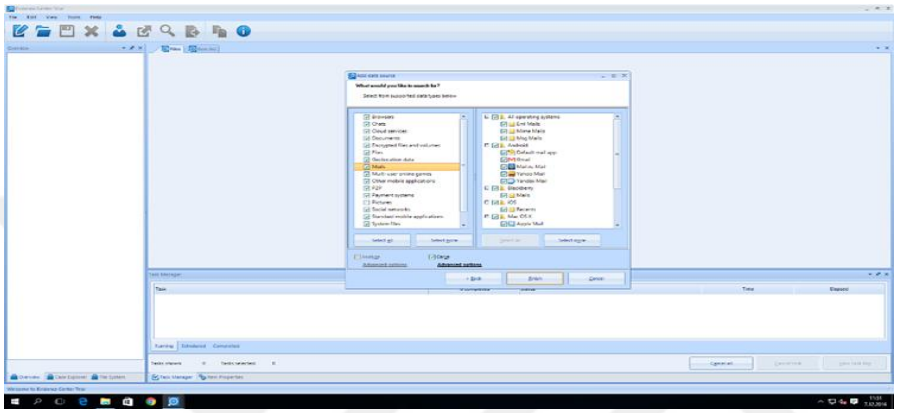

Figure 5.41. Belkasoft analysis

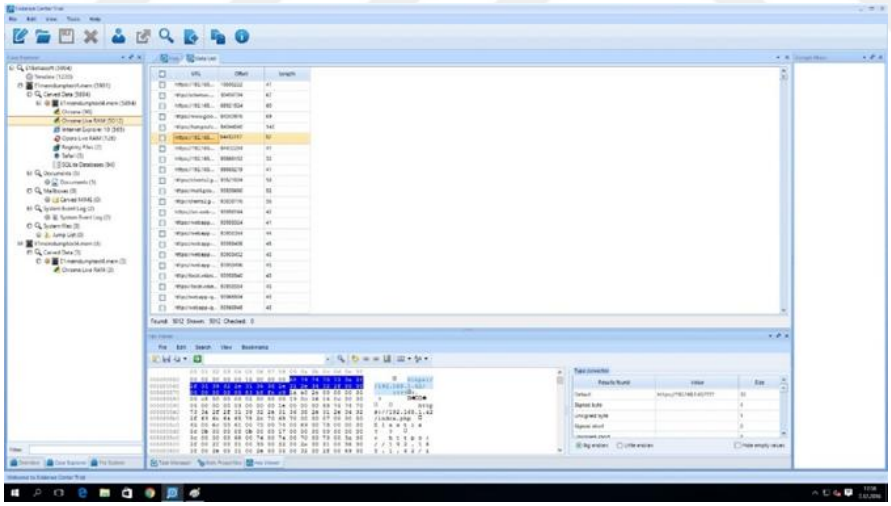

Figure 5.42. Analysis output of 8 GB capture file analysis

The Belkasoft offers the ability to search through the obtained results using special words related to VoIP applications. The output result of the Hex editor is shown in Figure 5.43. The second experiment deployed the 4GB RAM capture file and it was done in the same way and with the same configurations. The analysis needed approximately 23 minutes to complete. The results are shown in Figure 5.44.

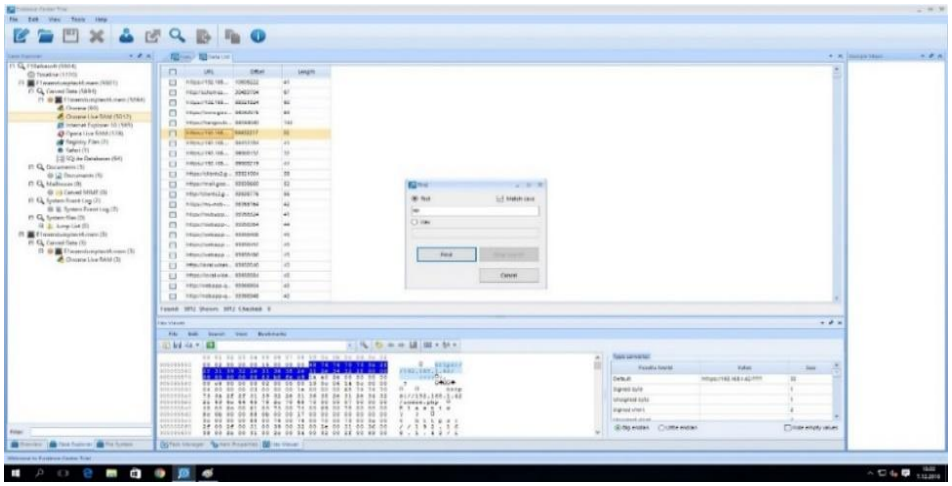

Figure 5.43. Output filtering results

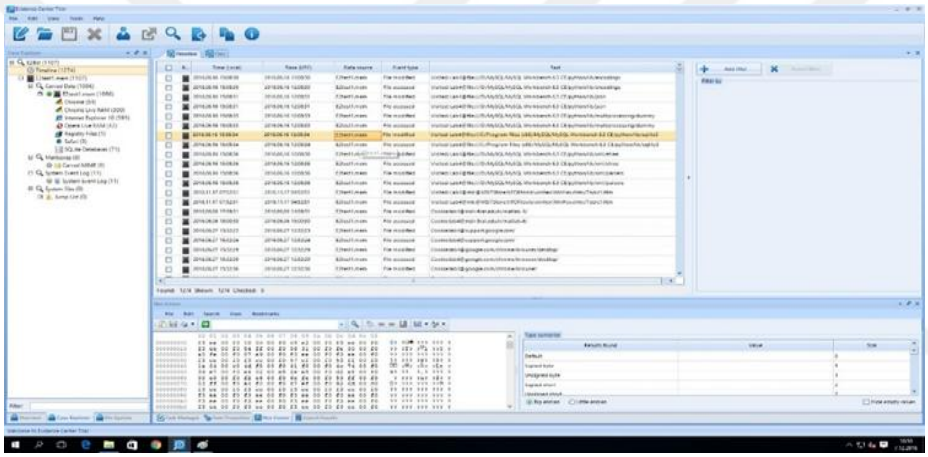

Figure 5.44. (4 GB) RAM capture analysis using Belkasoft

5.6.5. X-Ways Forensic Tool

X-Ways Forensic was developed by Aktieng Gesellschaft (AG) in 2002 and it is available for the download from (www.x-ways.net). X-Ways tool is compatible with Windows operating systems. It presents its analysis output in Hexadecimal editor. In order to analyze a file content, specifying a memory image file should be done first. The used file in this experiment is named E1Test1 and it is loaded from an external hard disk. The analysis of an 8 GB RAM capture had taken around 2 seconds While the analysis of the 4 GB RAM capture file had taken approximately 0.65 seconds.

The analysis result of the used 8 GB file is shown in Figure 5.45. The results present artefacts and its related information. However, the data related to VoIP is not clear, yet it is still possible to find some useful data through the hexadecimal and text editor.

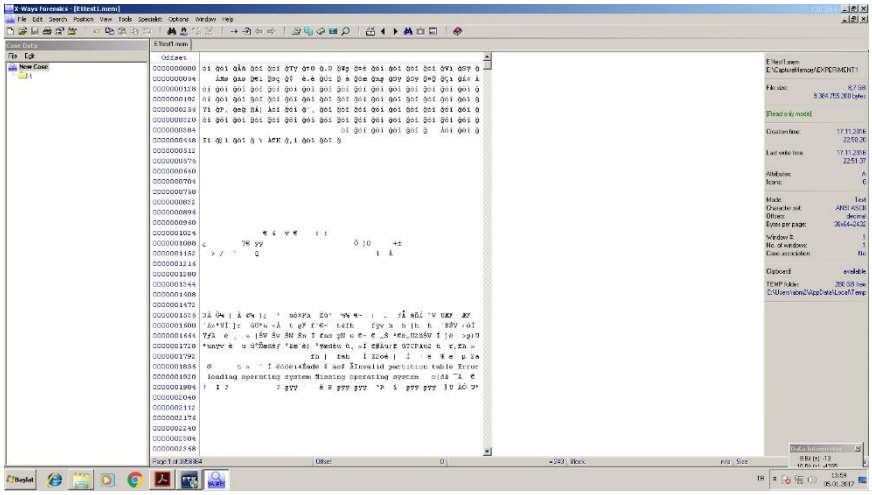

Figure 5.45. Analysis output of 8 GB RAM capture file using X-Ways tool

6. EXPERIMENTAL RESULTS AND DISCUSSION

6.1. Simulated VoIP Server

The idea of creating the server of VoIP comes from the use of unknown VoIP applications to discover the tools that best enable the investigators to produce reliable results. Identifying and recording the caller ID information assist in classifying the performance of the forensic tools. The basic details of the created VoIP server are provided in Table 6.1. The results of packets movements tracing between the caller and the receiver using Wireshark application are provided in Table 6.2. As shown in Table 6.2, the UDP information resulted from packet capturing prove that there is an ordinary communication that can be traced for forensic purposes. In addition, the information provided can be used for special word search in forensic investigation. Here, in order to find the artefacts related to VoIP calls, some special words can be used such as Hu, Mu, 00964750, 009050, and IP domain server.

Table 6.1. Server user information

Type of Information	**First user**	**Second user**
Name	Hu	Mu
Client Number	0090534	00964750
SIP	0090534	00964750
Mailbox	Hu534@firat	Mu750@firat
Password	hh123456789	mm123456789

Table 6.2. UDP packets information

UDP Server signal	From “Mu”<sip:00964750@10.6.0.27>
	To<sip:0090534@10.93.198.151>
UDP Destination signal	To: sip: 0090534@10.6.0.27; transport=UDP
	From sip: 00964750@10.6.0.27; -transport =UDP

6.2. RAM Capture

In this study, applying physical memory acquisition tools is the key element for VoIP forensic investigation procedure. In this research work, four different tools were used for RAM capturing process. The capturing metrics of the results of the used tools are provided in Tables 6.3 and 6.4 for RAM of two sizes, namely 8 GB and 4 GB respectively.

Various factors are considered here such as capturing time, output file format, output file size, tool license type, interface type and portability. The used tools here are generally used in forensic investigation process as well.

Table 6.3. General capturing tools comparison – 8GB

Tool	Capturing time	File format	Capture size	License	Interface
RAM capture.exe	00:01:28.51	.mem	8.74GB	Free	GUI
Magnet Capture	00:02:24.63	.dmp	8.74GB	Free	GUI
Dumplt	00:03:08.23	.raw	8.74GB	Free	Command line
FTK Imager V3.1	00:01:29.91	.mem	8.74GB	Free	GUI

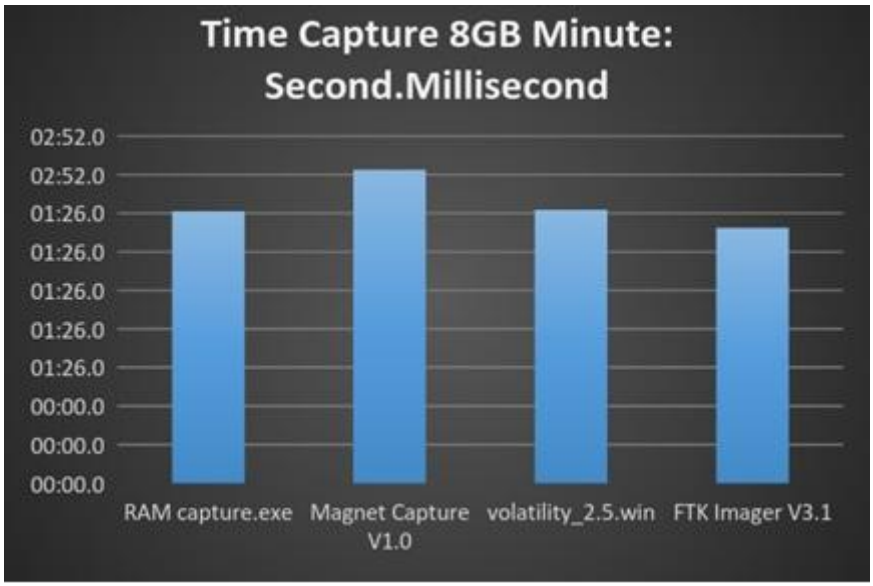

Figure 6.1. RAM capturer processing time comparison – 8GB

Table 6.4. General capturing tools comparison – 4GB

Tool	Capturing time	File format	Capture size	License	Interface
RAM capture.exe	00:02:01.81	. mem	4.74GB	Free	GUI
Magnet Capture	00:02:20.44	. dmp	4.74GB	Free	GUI
Dumplt	00:02:02.46	. raw	4.74GB	Free	Command line
FTK Imager	00:01:54.38	. mem	4.74GB	Free	GUI

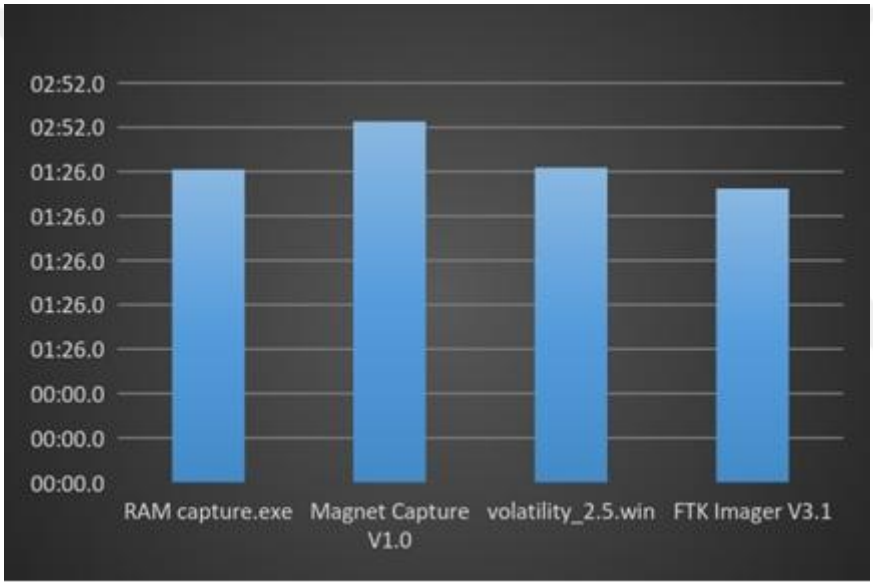

Figure 6.2. RAM capturer processing time comparison – 4GB

The captured sizes of the used memories appear to be more than the sizes of the original memories. This is due to the fact that the logical memory is also included while capturing the RAM which provides and extra size to the total captured RAM size. Moreover, the physical memory and virtual memory work together to improve and build a complete view of the system memory [54].

6.2.1. Belkasoft Live RAM Capture

In this research, Belkasoft was operated using the 64-bit file, as shown in Figure 6.3. This software is a GUI-based interface and it is simple to use. The produced output capture file format is .mem. Capturing an 8 GB RAM had taken 1 minute while capturing a 4 GB RAM had taken 2 minutes. The advantages and disadvantages are listed as follows:

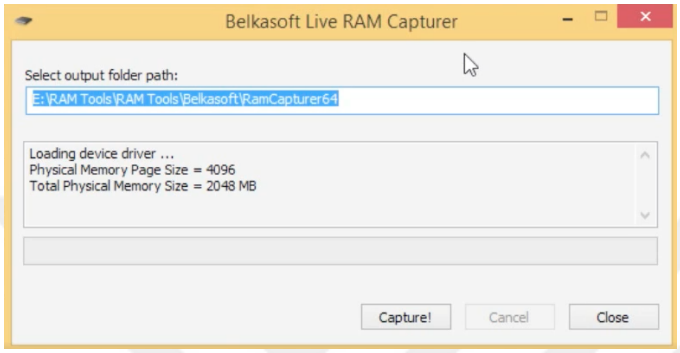

Figure 6.3. The interface of RAM Capture

Advantage:

- Easy to apply the tool; not only for experienced personnel but also non-technical investigators.
- Can be used from USB as a portable tool without being installed on the system.
- Convenient GUI.

Disadvantage:

- The RAM capture splitting option is not available.
- Captured file path setting is not possible; only default path is used by the tool.

6.2.2. Magnet RAM Capture

Magnet RAM Capture is a GUI-based tool used for memory acquisition as well as forensic analysis. This tool offers the investigators some useful options such as size segmentation and capture file saving path setting as shown in Figure 6.4. The default output of the capture file format is .dmp. The time needed for capturing an 8 GB RAM is 2 minutes while the time needed for capturing a 4 GB RAM is around 2 minutes. The advantage and disadvantage of this tool are listed as follows:

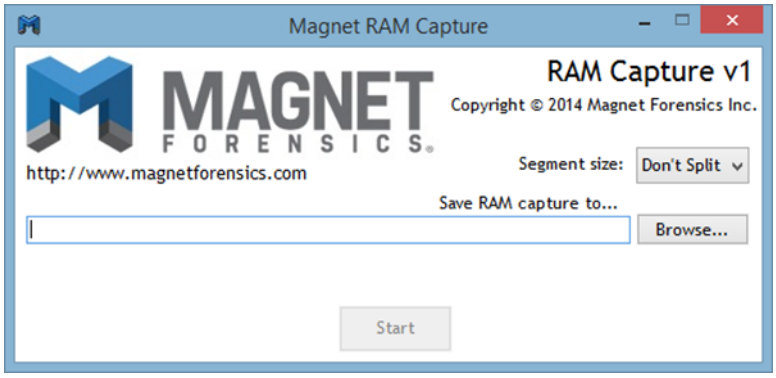

Figure 6.4. Magnet RAM Capture interface

Advantages:

- Easy to apply the tool; not only specialists but also non-technical investigators can run it.
- Can be used from USB as a portable tool without being installed on the system.
- Convenient GUI.
- Optional setting and modifying of the saving file path.
- Optional file name setting.
- The ability to split the captured file.

Disadvantages:

- Capturing duration is generally the slowest among all used tools.

6.2.3. Dumplt

DumpIt is a command-line tool used for memory capturing and digital forensic investigation. The captured file format is .raw as shown in Figure 6.5. This tool was used for capturing both used RAM sizes deployed in this work. The time elapsed for capturing an 8 GB RAM is 3 minutes while the elapsed time for capturing a 4 GB RAM is around 2 minutes. The advantages and disadvantages of the tool are listed as follows:

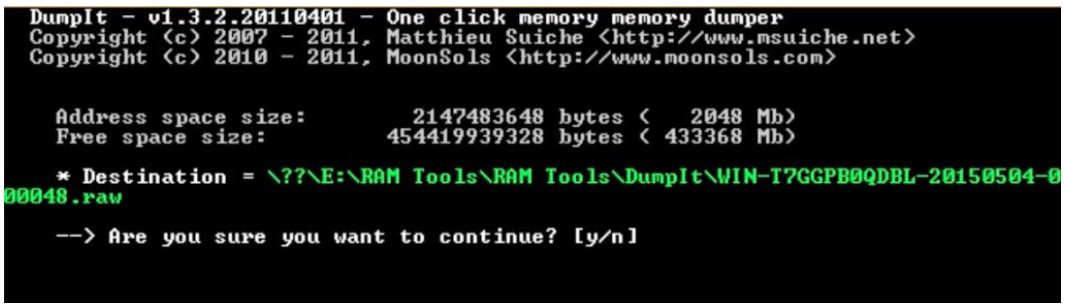

Figure 6.5. The command-Line of Dumplt

Advantages:

- Portable operational process; the tool can be applied from an external memory without being installed.
- Convenient operational process; not only for experienced personnel but also for non-technical investigators.

Disadvantages:

- The output file is saved based on the default path which cannot be changed.
- There is no option for splitting the output file.

6.2.4. FTK Imager

The design of FTK Imager interface merges both analysis and capturing capabilities together as shown in Figure 6.6. The properties assist the investigator to choose the path to save the output file path. The possible RAM capture file formats are .mem and .AD1. The capturing operation needed 1 minute for an 8 GB RAM capture and 2 minutes for a 4 GB RAM capture. The advantages and disadvantages of this tool are listed as follows:

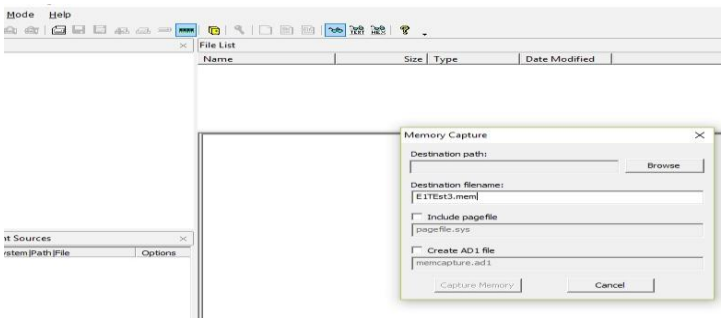

Figure 6.6. Interface of FTK Imager v3.1

Advantages:

- Multiple output file formats are available such as .mem and .AD1.
- It is possible to choose the output file path.
- The capturing process is faster than other tools.
- It is possible to modify the output file name.

Disadvantages:

- Only experienced and specialists can run the tool.
- .AD1 file needs a long period to be created.

- It is applied in user mode.

6.3. VoIP Forensic Analysis Results

The forensic analysis tools' performance depends not only on the analysis time but also on the ability to produce artefacts relevant to VoIP applications. It is clear that most of the experimental results are close in terms of the performance. The classification results of VoIP forensic analysis tools are provided in Tables 6.5 and 6.6 for the used 8 GB and 4 GB RAM sizes respectively. These tables consider useful comparison criteria such as analysis time, interface type, and output file format and size. The details of the analysis results produced by the tools are provided in the following sub-sections.

Table 6.5. Analysis processing details of 8GB RAM

Forensic Tool	Captured file extension	Processing time	License	Interface
Forensic Explorer	.raw	00:00:06.15	Proprietary	GUI
FTK V6.0	.mem	00:06:54.58	Proprietary	GUI
X-Way Forensics	.raw	00:00:01.95	Proprietary	GUI
Belkasoft	.mem	00:39:56.26	Proprietary	GUI
Magnet 6.8	.dmp	00:00:26:58	Proprietary	GUI

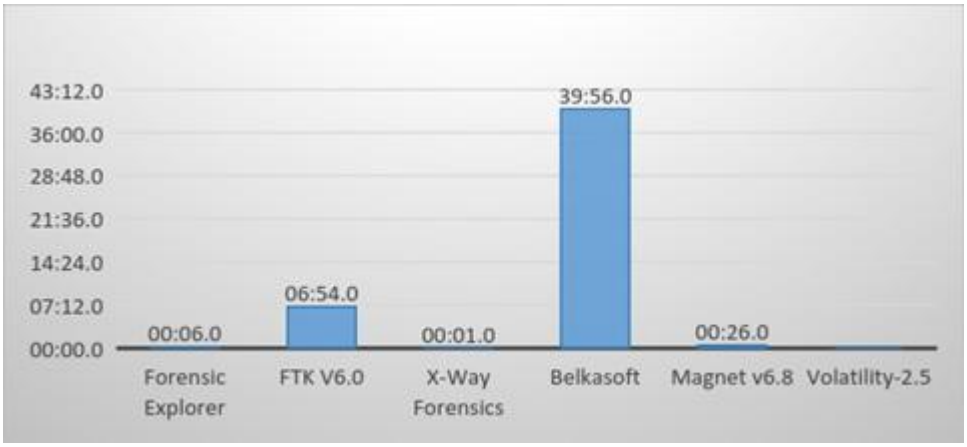

Figure 6.7. Distribution analysis processing details of 4GB RAM

Table 6.6. Analysis processing details of 4GB RAM

Forensic Tool	Captured file extension	Processing time	License	Interface
Forensic Explorer	.raw	00:00:08.94	Proprietary	GUI
FTK V6.0	.mem	00:03:48.76	Proprietary	GUI
X-Way Forensics	.raw	00:00:00.65	Proprietary	GUI
Belkasoft	.mem	00:23:22.01	Proprietary	GUI
Magnet V6.8	.dmp	00:00:13.54	Proprietary	GUI

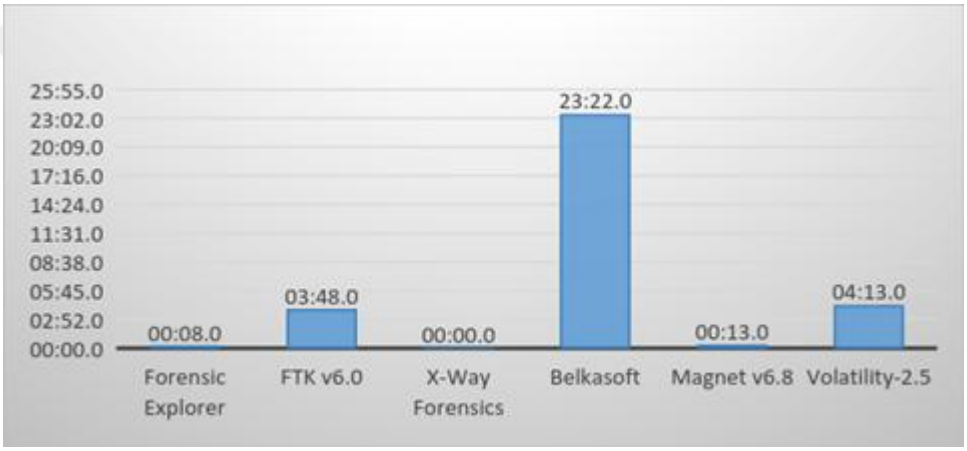

Figure 6.8. Distribution analysis processing details of 4GB RAM

Simplifying and speeding up the analysis process often involve determining what Tools to be used and which data to be investigated. There are some forensic investigation tools that cannot capture the RAM, but they can analyze the (. raw) format. RAM capture files are based on (.raw) image files, which can be analyzed by almost all forensic analysis tools. Thus, using this type of capture file format is advisable. The tool which is dealing just with Hexadecimal may also be viewing commands. In this regard, X-Ways tool gives a view of the Hexadecimal editor and how it is applied to VoIP forensic artefacts. Using tools such as Belkasoft, Forensic Toolkit, and Magnet Forensic IEF for extracting VoIP artefacts is useful as they are able to achieve RAM acquisition as well as analysis.

All processor actions and processes must leave artefacts that remain in the RAM. Generally, forensic analysis tools make use of these artefacts in order to extract valuable information on the legal case. However, in the case of unknown VoIP applications, the artefacts left behind can be also used for analysis purposes, yet the results will not be well-

categorized and presented compared to their known applications counterpart. Therefore, extracting evidence from unknown VoIP applications needs a special search for the information provided in the hexadecimal editor of the tool. Here, searching through evidence presented in hexadecimal needs time and knowledge in order to link the evidence to the used VoIP applications. This prompts the use of special word search to quickly reach to the attacker's information. In this work, the use of special words for searching all experiments analysis results have been conducted. Special words in this study refer to Hu, Mu, 009053, and 00964750.

6.3.1. Forensic Explorer RAM Capture Results

Forensic Explorer does not capture the RAM contents but it can analyze the captured files with (.raw) format. The analysis result of the first experiment using Forensic Explorer analysis for the 8 GB RAM capture took around 6 seconds. Generally, it does not provide any mechanism related to VoIP forensic analysis as shown in Figure 6.9. The output interface includes file list, a hexadecimal editor, and text. Also, the data related to VoIP is not categorized but it can still be used to inspect evidence through the hexadecimal editor and text editor for specific purposes.

The second experiment of the 4 GB RAM capture analysis using Forensic Explorer had been conducted in around 9 seconds. The produced output is shown in Figure 6.10. Generally, the results are presented in the hexadecimal editor. The data relevant to VoIP is not clear, yet some relevant VoIP data can be found from the hexadecimal editor.

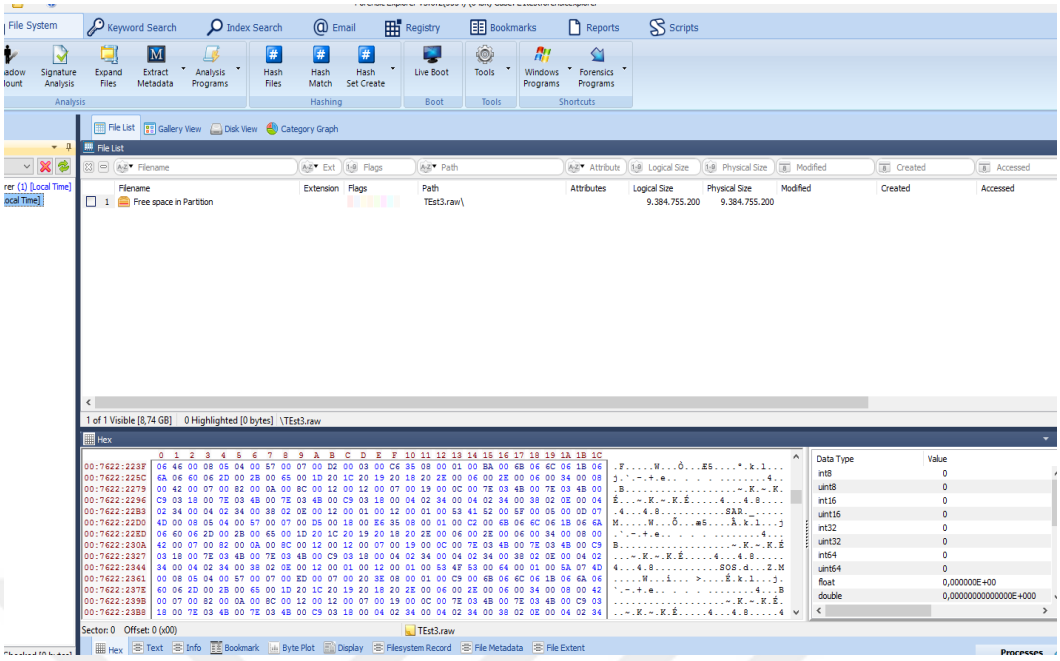

Figure 6.9. Analysis results of 8GB RAM using Forensic Explorer

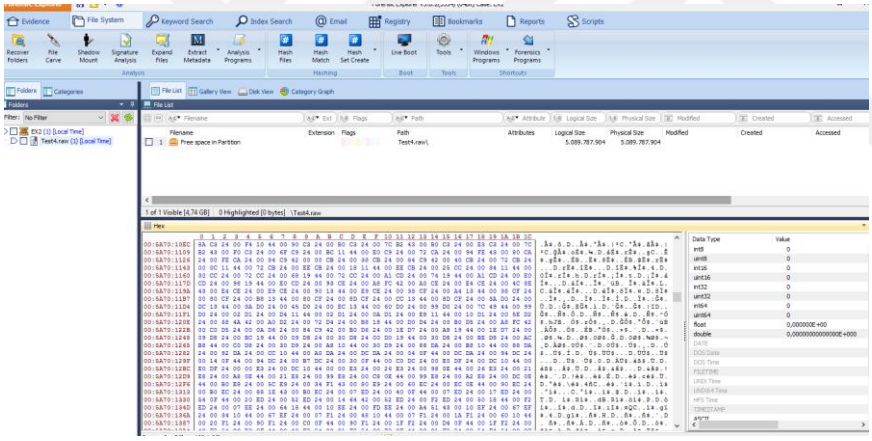

Figure 6.10. Analysis results of 4GB RAM using Forensic Explorer

Forensic Explorer tool has limited interface options that can assist in identifying artefacts relevant to VoIP. Essentially, searching for special words from the hexadecimal editor, as shown in Figure 6.11, can be concluded from this result. The search here needs an adequate level of proficiency to obtain evidence related to VoIP.

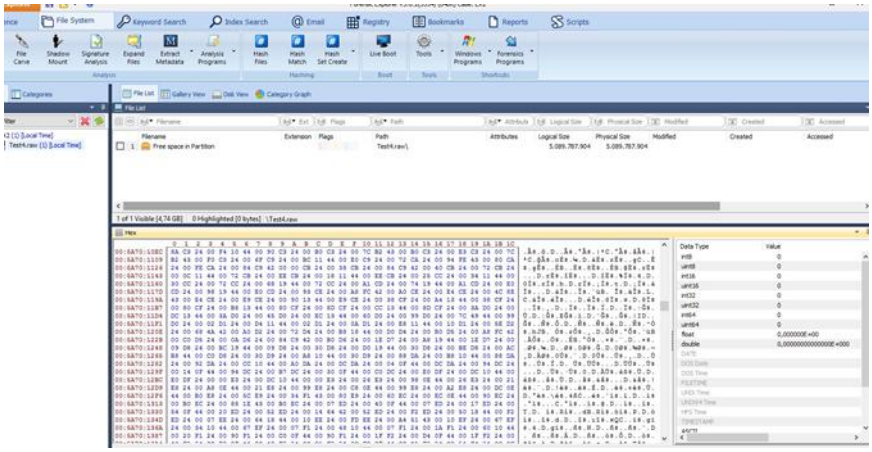

Figure 6.11. Forensic Explorer hexadecimal editor special word search

6.3.2. FTK RAM Capture Analysis Results

The first experimental result using the 8 GB RAM capture has presented many pieces of evidence. Unfortunately, the artefacts are not properly categorized by their relevance to VoIP. The interface of the tool is divided into three sections, as shown in Figure 6.12, which are:

1. Data view: Presents pieces of evidence that are found from the analysis of the RAM capture file.

2. Detail list view: hexadecimal information view.

3. Detail information view.

Generally, the evidence related to VoIP applications can be found from the hexadecimal editor of the tool. Apart from the first experiment, the second experiment which deployed the 4 GB RAM capture file for the analysis purposes has produced similar results to the first experiment; yet less extracted information could be found due to the used RAM size. The output of the obtained results is shown in Figure 6.13.

The search results of FTK 6.0 forensic tool in both FTKexpermient1 and FTKexpermient2 led to similar analysis processing time. The analysis operation presented important evidence via various useful tool options that assist the investigation process. However, none of these are solely specialized for VoIP applications. The examiners should have a good experience to deal with this tool in order obtain the needed relevant VoIP evidence. Applying special words for searching and sorting of the artefacts can be done using the hexadecimal editor as shown in Figure 6.14.

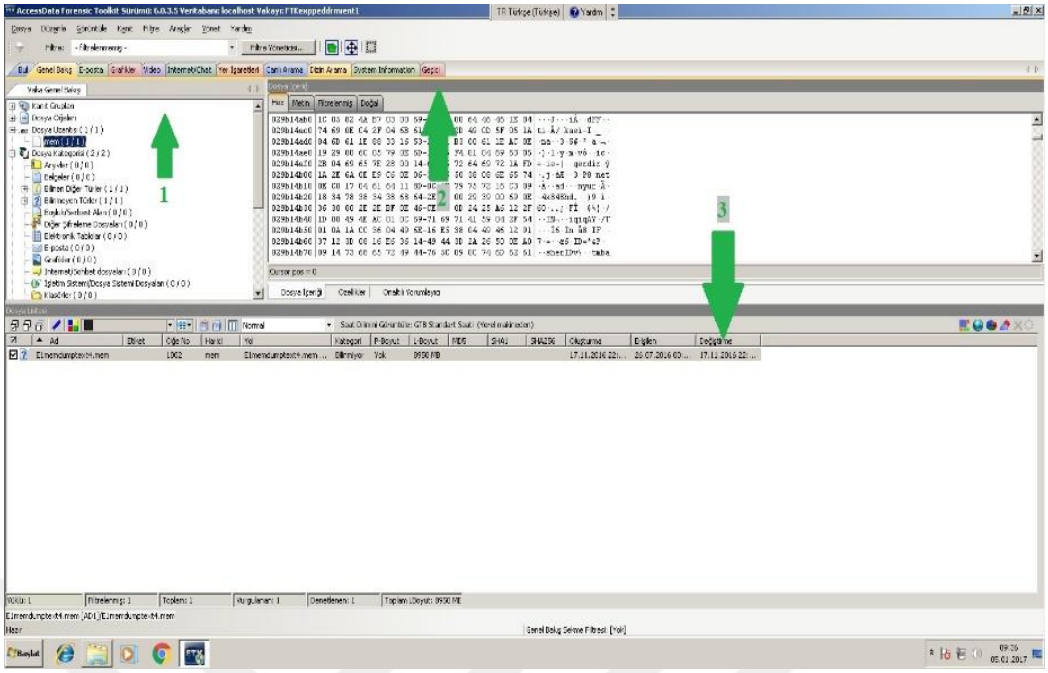

Figure 6.12. 8 GB RAM capture analysis using FTK 6.0

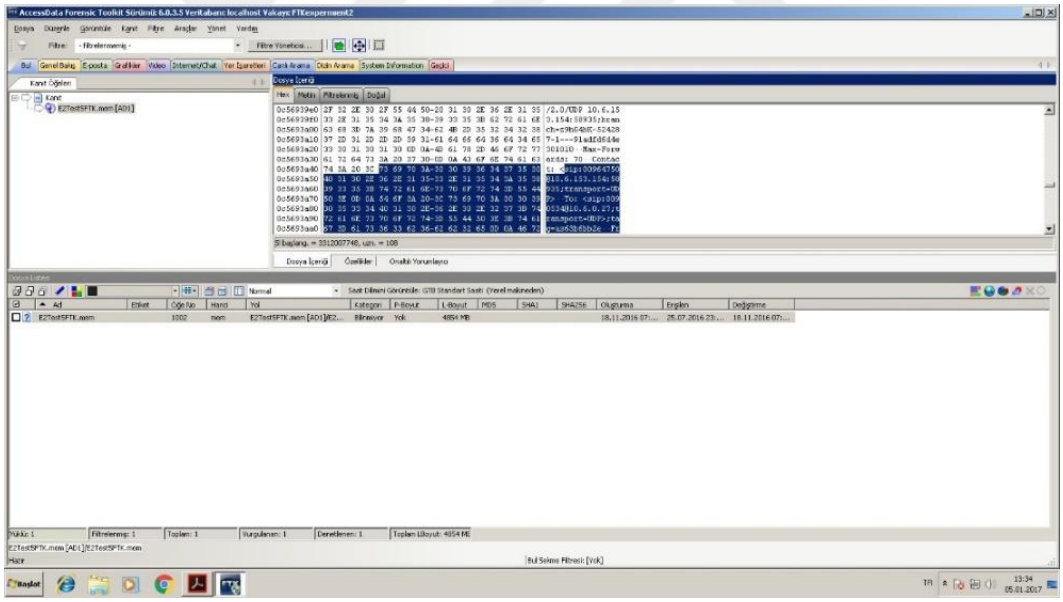

Figure 6.13. 4 GB RAM capture analysis using FTK 6.0

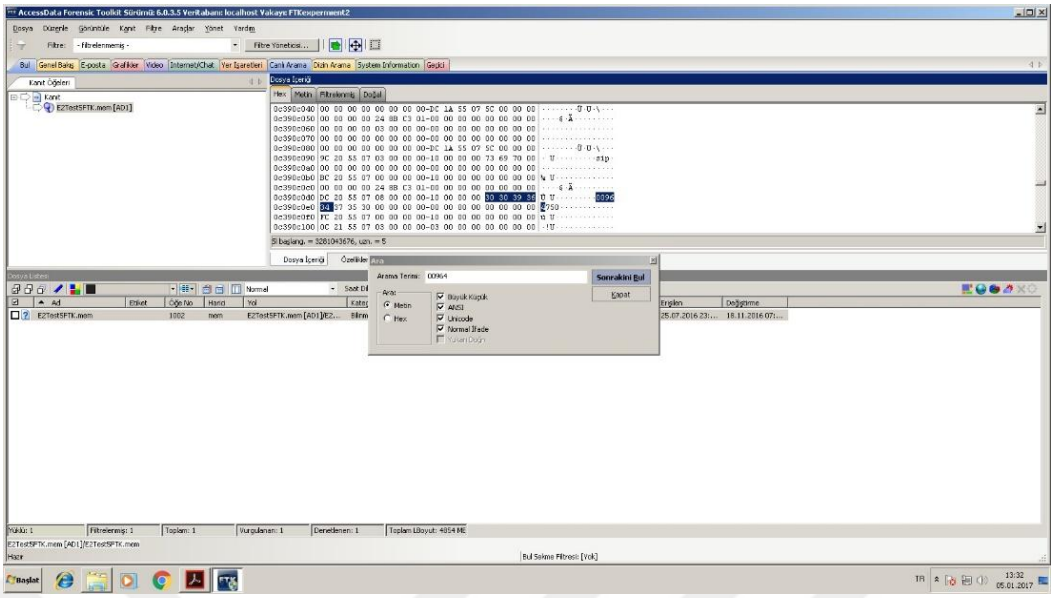

Figure 6.14. FTK 6.0 Search Result

6.3.3. X-Ways RAM Capture Analysis Results

X-Ways forensic tool is convenient and fast for analysis purposes but it only produces the results using the hexadecimal editor. X-Ways took approximately 2 seconds to analyze the 8 GB RAM capture file. The results of the analysis are presented in Figure 6.15. On the other hand, analyzing the 4 GB RAM capture file took around 0.65 seconds to obtain the results shown in Figure 6.16. X-Ways analysis results present the artefacts in a list view relevant to VoIP and other applications processes. Essentially, the evidence related to VoIP can be extracted from the hexadecimal editor.

X-Ways forensic tool lacks the specialized options that assist the investigation process. Specific evidence can be extracted and displayed using special words search as shown in Figure 6.17.

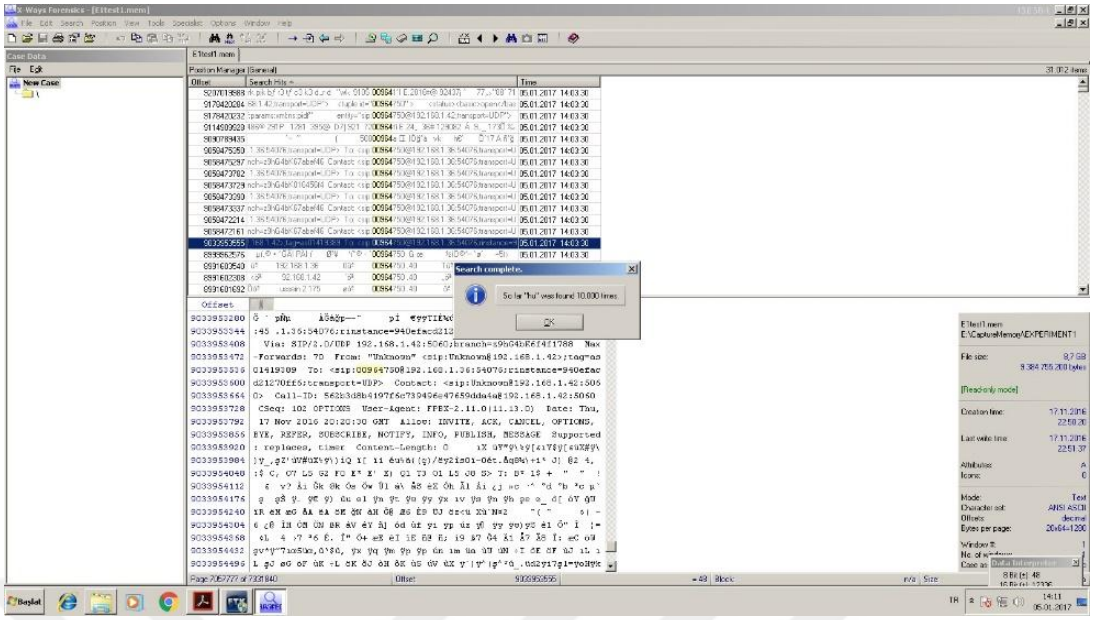

Figure 6.15. 8GB RAM capture analysis using X-Ways

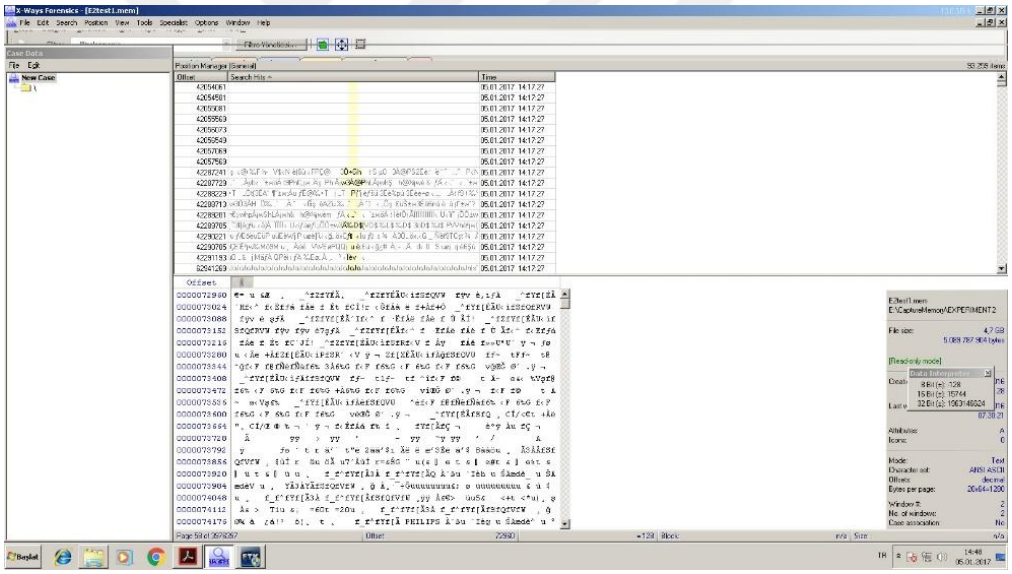

Figure 6.16. 4GB RAM capture analysis using X-Ways

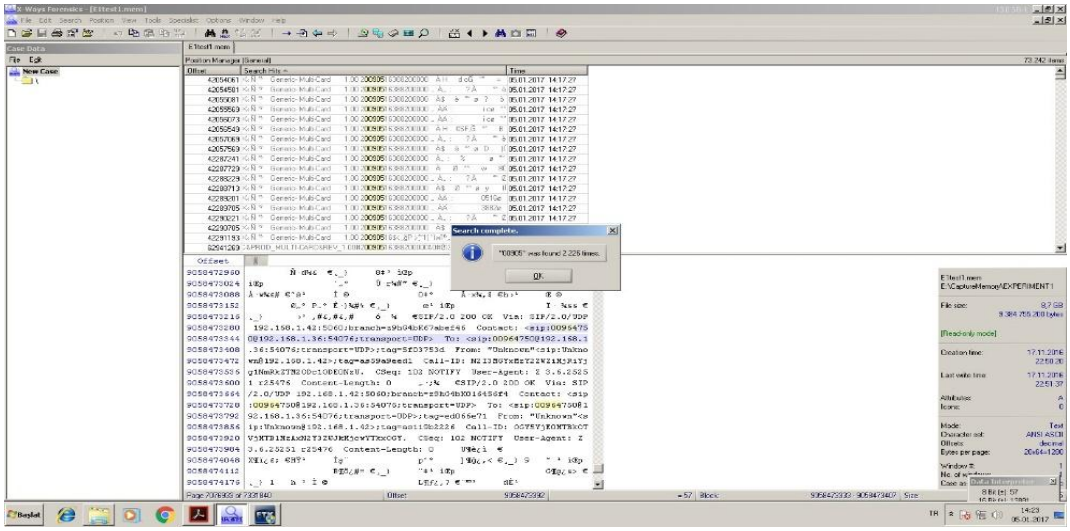

Figure 6.17. Searching for a special word in X-Ways

6.3.4. Belkasoft RAM Capture Analysis Results

Belkasoft has produced a thorough view of the used RAM artefacts, yet it needed a very long time compared to other tools. The elapsed analysis time of the 8 GB RAM capture using Belkasoft is approximately 40 minutes. The obtained results are shown in Figure 6.18. This tool has many options assist the investigators compared to previously used tools. However, the presented artefacts relevant to VoIP can be viewed from the hexadecimal editor. In addition, the time needed for analyzing the 4 GB RAM capture took around 23 minutes and 22 seconds to be conducted. The result of the 4 GB RAM capture analysis is shown in Figure 6.19. The Belkasoft forensic tool is classified as one of the easiest tools and it does not require a high proficiency level in order to be used. It has various options available for recovering meaningful evidence with multi-properties for file categorizing within the front interface. The result of special words search is shown in Figure 6.20.

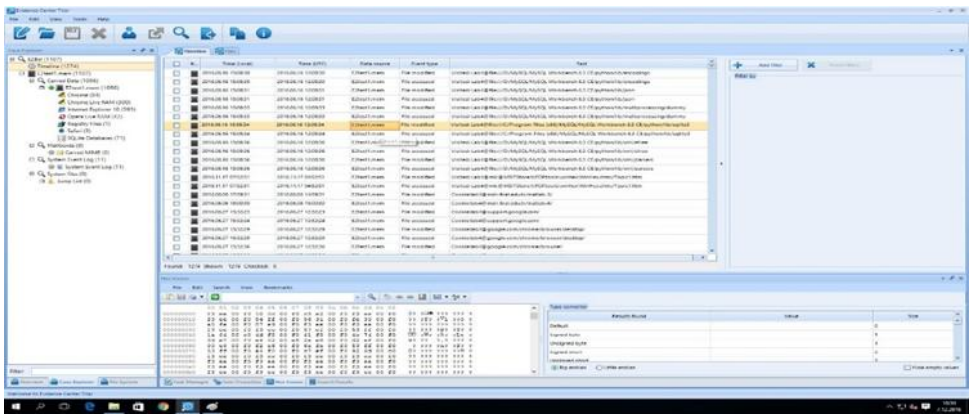

Figure 6.18. 8 GB RAM capture analysis using Belkasoft

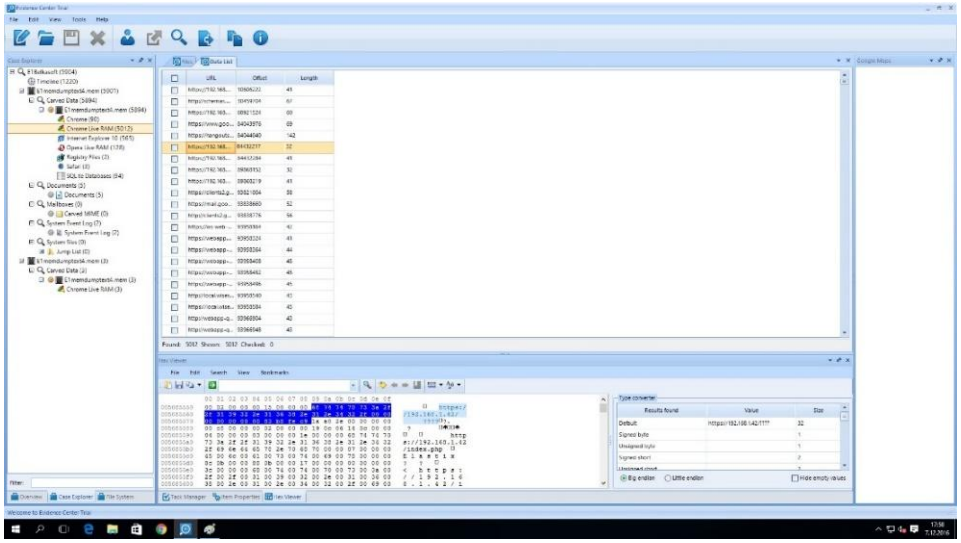

Figure 6.19. 4 GB RAM capture analysis using Belkasoft

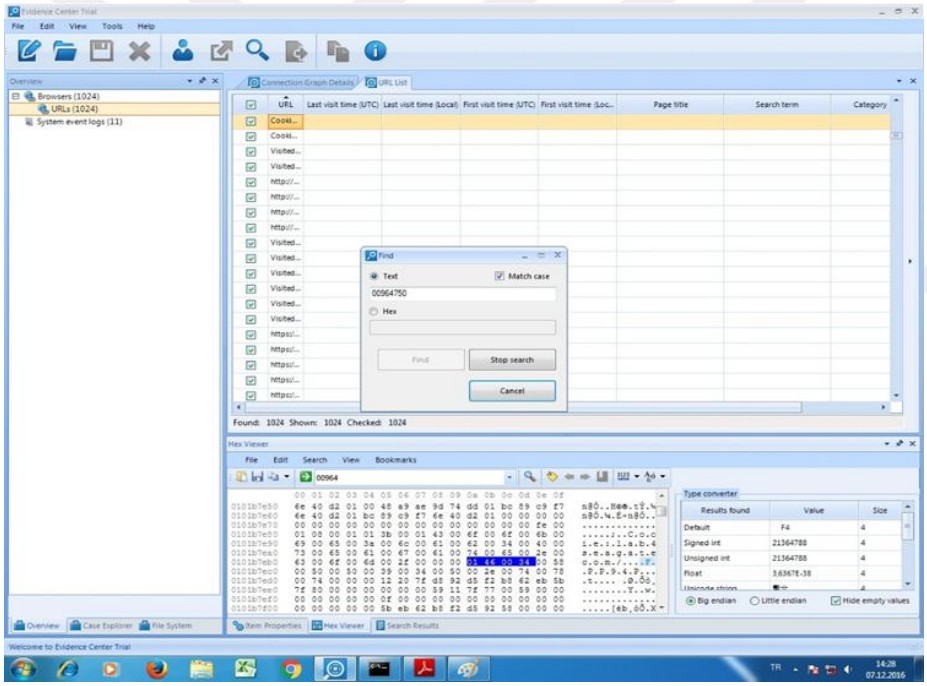

Figure 6.20. Searching for a special word using Belkasoft

6.3.5. Magnet IEF RAM Capture Analysis Results

Magnet IEF tool is used in this study for analyzing the capture files of both 8 and 4 GB RAM. Analyzing the used 8 GB RAM capture had taken around 27 seconds. The obtained output results are shown in Figure 6.21. Further, analyzing the used 4 GB RAM capture had taken around 14 seconds to be achieved. The obtained analysis results, in this case, are shown in Figure 6.22.

This tool offers a number of useful options that assist the VoIP forensic investigation. The analysis results are categorized in different forms and they do present artefacts relevant to VoIP. The categorization of the analysis here covers the hexadecimal editor, the text editor, refined IEF results, e-mail and peer-to-peer.

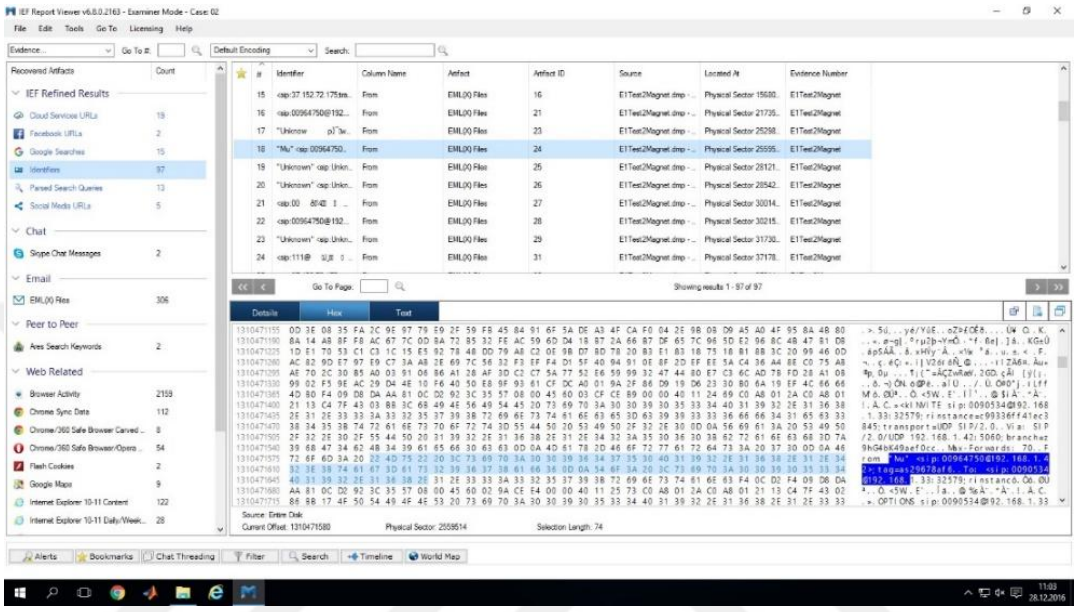

Figure 6.21. 8 GB RAM capture analysis using Magnet IEF

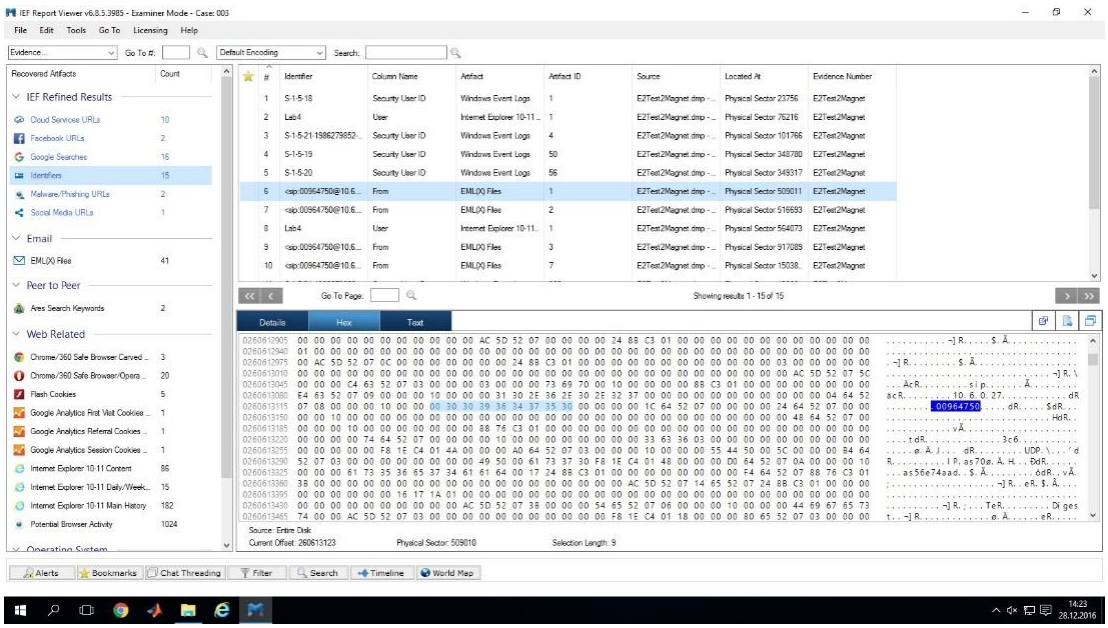

Figure 6.22. 4 GB RAM capture analysis using Magnet IEF

Figure 6.23. VoIP relevant evidence presented in Hex and List

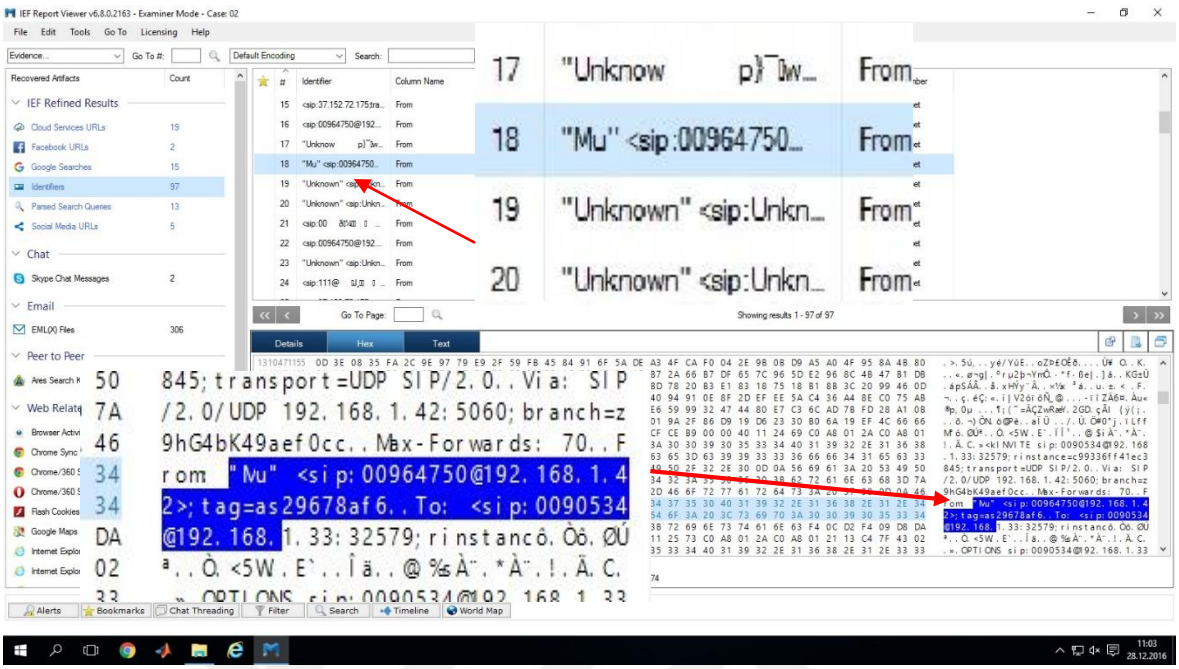

Figure 6.24. Unknown VoIP caller IP address extraction using Magnet IEF

It is important to mention that Magnet IEF tool is useful for tracking the caller login information. This is represented by the extraction of the client user name “Mu”, as shown in Figure 6.23, used for conducting a call over the simulated unknown VoIP server. In addition, the tool is able to extract the caller IP address, as shown in Figure 6.24, which can be used for discovering the origin of the caller area and location.

Magnet forensic tool has a straightforward interface that combines different useful options in the same tool. In addition, it provides the features of Internet applications as evidence which can be used in general digital forensic as well as VoIP forensic investigation. For this reason, it is more distinguished over other forensic tools applicable to VoIP forensic as shown in Figure 6.25.

In order to throw light on VoIP artefacts remained in the RAM, the search should be conducted manually by special words such as (Hu and Mu) which were used during the simulation of the server. The ultimate outcomes are shown in Figure 6.26. Furthermore, it is possible to search using the area code of the used phone number.

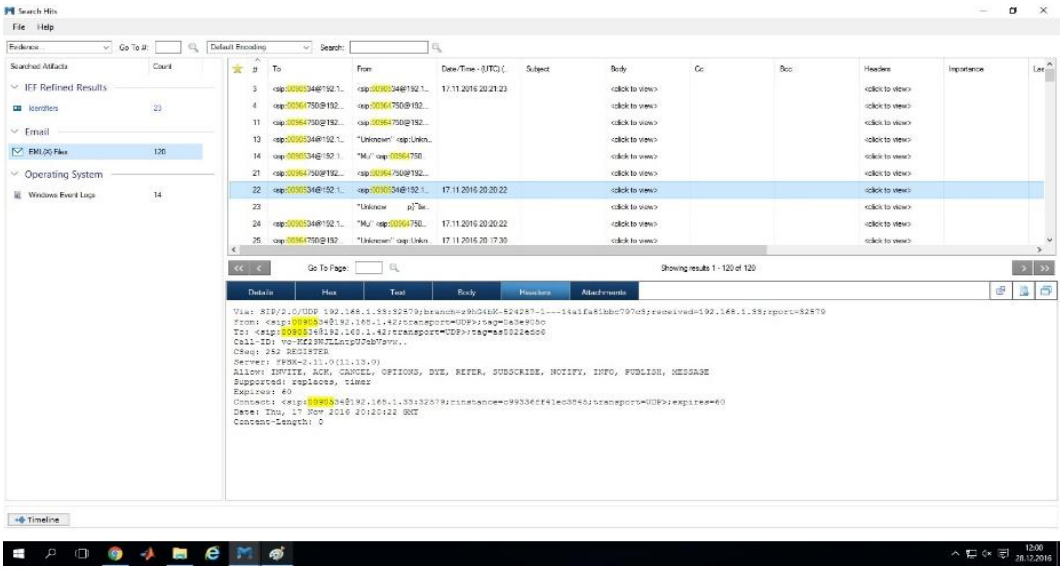

Figure 6.25. Output search results of the admin server IP number

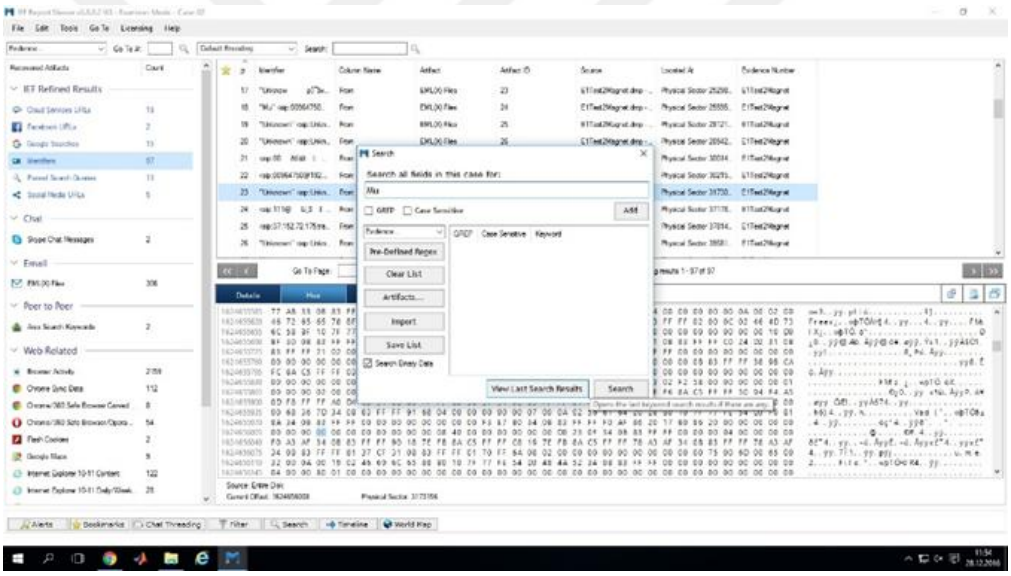

Figure 6.26. Manual search using special word

7. CONCLUSIONS AND FUTURE WORK

7.1. Conclusions

This thesis has presented a classification study for digital forensic analysis tools with respect to their performance considering VoIP forensic investigation as the main target. The essential disciplines needed for conducting a VoIP forensic investigation were given within the chapters of this thesis to ensure the best understanding. Among the classification goals tackled in this research is the inspection of forensic analysis tools' performance in extracting evidence relevant to unknown VoIP applications. This was achieved by simulating a client-server unknown VoIP connection. The simulated client-server connection was used for conducting a thorough forensic investigation aiming to discover artefacts related to the users. Despite the fact that the forensic analysis can be conducted using the information residing on any memory type. In this work, only RAM artefacts were analyzed and considered. Even though there are various forensic tools that can be used for digital forensic cases including live memory acquisition tools, choosing the right tool is not a straightforward task. Investigators may have their own worries and troubles while choosing the right tool which suits the analysis of unknown VoIP applications. Classifying the operational behavior and results of VoIP forensic tools can assist in achieving faster and more accurate digital forensic results. It is essential for the investigators to understand the basic mechanism of different digital forensic tools as well as their applicable scope and limitations. This simply facilitates the proper choice of the possible investigation technique.

The deployment of two sizes of RAM (4 and 8 GB) was used throughout the classification process. Four tools were used for RAM capturing, namely Belkasoft, Magnet RAM Capture, DumpIt and FTK imager; while five analysis tools were used for discovering VoIP relevant evidence, namely Forensic Explorer, FTK, X-Ways, Belkasoft and Magnet IEF. Some of these tools are capable of capturing and producing live RAM analysis while others are only specialized only in analysis purposes. The classification process considered different factors including tool features, analysis time, output view, analysis capabilities, VoIP forensic relevance and evidence categorization. In general, the obtained results vary based on the used tool and RAM size, yet the optimal choice is generally case-dependent. This is basically due to the fact that there is no an exact best tool; however, some tools perform better in specific cases. In addition, all used tools presented minimal information

about unknown VoIP call from their GUI. However, the result of the analysis presented in the hexadecimal editor could still provide vital evidence collections. This implies the need for special word search for the artefacts available in the hexadecimal editor related to VoIP. Therefore, the investigators' technical proficiency should be able to work around these challenges. Moreover, many VoIP artefacts need manual search depending on the application being investigated. So, if an unknown VoIP application is used, it would be more difficult in the investigation process. This suggests that the initial step should start by checking the system for any VoIP services installed or any history of previous installations. A random looking for VoIP artefacts in the memory could be time-consuming and very tedious. Thus, VoIP utilized SIP protocols and authentications can be searched for any similarities across services installed or the history of previous installations. Fully grasping the dimensions of all protocols used for VoIP is extremely important. This is very necessary for establishing the needed interface filter for unknown VoIP applications forensic.

7.2. Future Work

The future research direction will focus on improving the whole cyber forensic investigation process by introducing the mechanism of VoIP forensic for tunneled traffic. This will be applied for special cases that use virtual private networks or proxy servers to hide the real identity and the origin of the traffic. Apart from that, it is difficult to fully grasp the dimensions of all VoIP protocols by a manual tracing. Therefore, another direction for further research could be establishing a specialized interface filter for unknown VoIP applications forensic. This can be done by developing a filter for special words that can be updated both manually and automatically.

REFERENCES

[1] "VoIP History," VoIP Insight, [Online]. Available: http://www.voipinsights.com/voip_history.html. [Accessed 25 Dec 2016].

[2] K. Deyermenjian., "PSTN vs. VoIP: What's best for your business," 2016. [Online]. Available: http://searchunifiedcommunications.techtarget.com/feature/PSTN-vs-VoIP-Whats-best-for-your-business. [Accessed 25 Dec 2016].

[3] R. River, "Why VoIP's Popularity is Rapidly Growing," 2013. [Online]. Available: http://www.redriver.com/collaboration-technology/why-voips-popularity-is-rapidly-growing. [Accessed 26 Dec 2016].

[4] N. Sapiens, "As VoIP gains popularity in the enterprise, changes are sure to follow," 2015. [Online]. Available: http://www.netsapiens.com/as-voip-gains-popularity-in-the-enterprise-changes-are-sure-to-follow/. [Accessed 26 Dec 2016].

[5] D. Kuhn, T. Walsh and T. Fries, "Recommendations of the National Institute of Standards and Technology," Security Considerations for Voice Over IP Systems, U.S. Department of Commerce, 2005.

[6] H. AL-saadawi and A. Varol, "Voice over IP Forensic Approaches: A Review," in *5th International Symposium on Digital Forensics and Security*, Romania, 2017.

[7] M. Simon and S. Jill, "Recovery of Skype Application Activity Data from Physical Memory," in *ARES'10 International Conference*, 2010.

[8] N. Petroni, A. W. F. Timothy and A. William, "FATKit: A framework for the extraction and analysis of digital forensic data from volatile system memory," *Digital Investigation*, vol. 3, pp. 197-210., 2006.

[9] D. Manson, C. Anna, R. Steve, G. Alain and K. Matthew, "Is the Open Way a Better Way? Digital Forensics Using Open Source Tools," in *System Sciences, 2007. HICSS*, Hawaii, 2007.

[10] C.-M. Leung and C. Yuen-Yan, "Network forensic on encrypted peer-to-peer voip traffics and the detection, blocking, and prioritization of skype traffics," in *16th IEEE International Workshops on*, 2007.

[11] C. Juan and B. Eduardo, "VoIP Network Forensic Patterns," in *Fourth International Multi-Conference on Computing in the Global Information Technol*, 2009.

[12] E. Fernandez, P. Juan and L.-P. Maria, "Attack patterns: A new forensic and design tool," in *IFIP International Conference on Digital Forensics*, Springer New York, 2007.

[13] L. A. Khan and S. A. Y. Muhammad, "Speaker recognition from encrypted VoIP communications," *digital investigation*, vol. 7.1, pp. 65-73, 2010.

[14] J. François, S. Radu, E. Thomas and F. Olivier, "Digital forensics in VoIP networks," *IEEE International Workshop on*, pp. 1-6, 2010.

[15] D. Irwin and S. Jill, "Extracting evidence related to VoIP calls," in *FIP International Conference on Digital Forensics*, Berlin, 2011.

[16] I. David, S. J and D. A, "Extraction of Electronic Evidence from VoIP: Forensic Analysis of a Virtual Hard Disk vs RAM," *Digital Forensics, Security and Law*, vol. 6, pp. 15-36, 2011.

[17] H.-M. Hsu, S. Yeali, M. Sun and C. Chang, "Collaborative scheme for VoIP traceback," *digital investigation*, vol. 7, pp. 185-195, 2011.

[18] G. Hongtao, "Forensic Method Analysis Involving VoIP Crime," in *Knowledge Acquisition and Modeling (KAM)*, 2011.

[19] S. Vömel and F. Felix, "A survey of main memory acquisition and analysis techniques for the windows operating system," *Digital Investigation*, vol. 8, pp. 3-22, 2011.

[20] Z. Su and H. Lian, "Evaluating the Effect of Loading Forensic Tools on the Volatile Memory for Digital Evidences," in *In Computational Intelligence and Security (CIS)*, 2011.

[21] M. Ibrahim, T. Mohd and A. D. Abdullah, "VoIP Evidence Model: A New Forensic Method for Investigating VoIP Malicious Attacks," in *Cyber Warfare and Digital Forensic (CyberSec)*, 2012.

[22] C. Leonardo, C. Varol and L. Chen, "Tools for collecting volatile data: A survey study," in *Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE)*, Konya, 2013.

[23] R. Dave, R. Nilay and M. Mistry, "Volatile Memory Based Forensic Artifacts & Analysis," *Science and Engineering Technology (IJRASET)*, vol. 2, 2014.

[24] K. Le, S. C. Nhien-An and T. Kechadi, "Forensic Acquisition and Analysis of Tango VoIP," in *In International Conference on Challenges in IT, Engineering and Technology (ICCIET 2014),* Phuket, Thailand, 2014.

[25] Psaroudakis and e. Ioannis, "A method for forensic artefact collection, analysis and incident response in environments running session initiation protocol and session description protocol," *International Journal of Electronic Security and Digital Forensics,* vol. 6, pp. 241-267, 2014.

[26] X. Zhang, L. Hu, S. Song and Z. Xie, "Windows Volatile Memory Forensics Based on Correlation Analysis," *JNW,* vol. 9, pp. 645-652, 2014.

[27] T. Manesh, M. Saied, M. Abd El-atty, S. Muhammed and B. B, "Forensic investigation framework for VoIP protocol," in *IEEE First International Conference on Anti-Cybercrime (ICACC),* 2015..

[28] M. M., M. T. and S. M., "VoIP Forensic Analyzer," *International Journal of Advanced Computer Science & Applications,* vol. 7, pp. 109-116, 2016.

[29] L. Carvajal, C. Lei, V. Cihan and R. Danda, "Detecting Unprotected SIP-based Voice over IP Traffic," in *Digital Forensic and Security (ISDFS), 2016 4th International Symposium on. IEEE,* 2016.

[30] R. McDown, V. Cihan, C. Leonardo and C. Lei, "In-Depth Analysis of Computer Memory Acquisition Software for Forensic Purposes," *Journal of forensic sciences,* vol. 61, 2015.

[31] N. Kumari and A. Mohapatra, "An Insight into Digital Forensics Branches and," in *In Computational Techniques in Information and Communication Technologies (ICCTICT),* 2016.

[32] A. Joseph and K. John, "Review of Digital Forensic Models and A Proposal For Operating System Level Enhancements," *International Journal of Computer Science and Information Security,* vol. 14, p. 797, 2016.

[33] J. Regis, Securing VoIP: Keeping Your VoIP Network Safe, Elsevier, 2014.

[34] T. Porter and M. Gough, How to cheat at VoIP security, Syngress, 2011.

[35] H. Joe, A brief history of VoIP, Evolution, 2004.

[36] "Understanding VoIP," 207. [Online]. Available: www.packetizer.com/ipmc/papers/understanding_voip/how_voip_works.html. [Accessed 9 Feb 2017].

[37] I. Androulidakis, BX security." In VoIP and PBX Security and Forensics, Springer International Publishing, 2016.

[38] J. Radecki, Z. Zeljko and R. Katarzyna, "Echo cancellation in IP networks," in *MWSCAS-2002. The 2002 45th Midwest Symposium on*, 2002.

[39] S. Wang and R. S, Computer Architecture and Security Fundamentals of Designing, Singapore: John Wiley & Sons, 2013.

[40] "ProgrammerWorld.NET," May 2016. [Online]. Available: http://faq.programmerworld.net/voip/voip-advantages-disadvantages.htm.. [Accessed 27 Feb 2017].

[41] M. F. Finneran, Voice over WLANS: The complete guide, Newnes, 2011.

[42] "Voice protocols –VoIP protocols," May 2016. [Online]. Available: http://howdoesinternetwork.com/2012/voip-protocols. [Accessed 28 Feb 2017].

[43] A. Rakesh and R. Jain, "Voice over IP: Protocols and standards," in *Network Magazine*, 1999.

[44] "Components of SIP," 15 Aprl 2015. [Online]. Available: http://www.siptutorial.net/SIP/component.html. [Accessed 12 May 2017].

[45] "Memory," computer hop: free computer help and information, 2017. [Online]. Available: www.computerhope.com/jargon/m/memory.htm. [Accessed 24 Feb 2017].

[46] W. C. D. f. NPTEL, Interviewee, *Computer Organization and Architecture*. [Interview]. 2011.

[47] Z. Staff, "Zetta," History of Data Storage Technology, 5 May 2016. [Online]. Available: www.zetta.net/about/blog/history-data-storage-technology. [Accessed 8 Feb 2017].

[48] P.-C. Lacaze and L. Jean-Claude, Non-volatile memories, John Wiley & Sons, 2014.

[49] H. Michael, C. Andrew, L. Jamie and W. Aaron, the art of memory forensics: detecting malware and threats in windows, linux, and Mac memory, John Wiley & Sons, 2014.

[50] S. Banerji, Architectural Design of a RAM Arbiter, rXiv preprint arXiv:1405.4232, 2014.

[51] B. Nelson, P. Amelia and S. Christopher, Guide to computer forensics and investigations, Cengage Learning, 2014.

[52] M. Harbawi and V. Asaf, "The role of digital forensics in combating cybercrimes," in *In Digital Forensic and Security (ISDFS), 2016 4th International Symposium on*, 2016.

[53] L. Daniel, Digital forensics for legal professionals: understanding digital evidence from the warrant to the courtroom, Elsevier, 2012.

[54] B. Anderson and A. Barbara, "Seven deadliest USB attacks," in *RAM Dump*, Syngress, 2010, pp. 117-151.

[55] B. Shavers and E. Zimmerman, X-Ways Forensics, Elsevier, 2014.

[56] "elastixbook," [Online]. Available: www.elastixbook.com. [Accessed 26 Oct 2016].

[57] "Zoiper VoIP softphone," Download Zoiper, [Online]. Available: https://www.zoiper.com/en. [Accessed 16 Sep 2016].

[58] "wireshark," Download Wireshark, [Online]. Available: https://www.wireshark.org/#download. [Accessed 22 Nov 2016].

CURRICULUM VITAE

Hussein Farooq Tayeb AL-saadawi

husseintaeyb@gmail.com

Telephone: +905349333083

+9647503238046

Nationality : Iraq

Place of birth : Basra

Date of birth : 07 / 04 / 1981

Marital status : Married

EDUCATION

2015 – 2017 MCE (Master of Software Engineering), Firat University, Elazig, Turkey.

2007 – 2011 Bachelor of Computer Science, Cihan University Erbil-Iraq

2000 – 2002 Technician Diploma in ELECTRONIC Erbil Technical Institute-Iraq

1994 – 1999 High School, Miqdam High School Baghdad-Iraq

1988 – 1993 Primary School, Moroj Primary School, Mosul-Iraq

WORK EXPERIENCES

- Programmer Chief Assistant, Kurdistan Parliament - IRAQ
- Electronic and Electric maintenance, Ministry of Reconstruction & Development Erbil - Iraq
- Electronic and Electric maintenance Haiman Trading Company, Erbil – Iraq

PUBLICATIONS

Al-Saadawi, H., & Varol, A. (2017, April). Voice over IP forensic approaches: A review. In *Digital Forensic and Security (ISDFS), 2017 5th International Symposium on* (pp. 1-6). IEEE.