Digital Forensics Summary of Learning

Shasheen Bandodkar

Digital Forensics CSC 620-001

Spring 2020

TABLE OF CONTENTS

Introduction

The goal of this class was to learn by combining a theoretical foundation with practical use of commonly used techniques, methods and tools, about digital forensics. Topics include digital evidence collection, as well as evidence analysis and reporting. It also addresses legal and ethical implications of using forensic method. The learning goals of this class were:

• Master techniques to collect digital evidence using forensically sound practices.

• Be able to identify, acquire, and analyze evidence on storage media

• Be able to identify, acquire, and analyze network data.

• Be introduced to the legal and ethical ramifications of using forensics techniques.

The book that we used was Bill Nelson, Amelia Philips. Christopher Stuart: Guide to Computer Forensics Investigations 6th edition from Cengage. We had many practice sessions conducted on the Cengage website where we would connect to a virtual machine and perform many digital forensic steps of evidence gathering, documenting the case and sharing the outcome and quiz at the end of each lab activity

Chapter 1: Understanding the digital forensics profession and investigations.

Digital forensics: The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting and possible expert presentations.

The Federal rules of evidence was created to ensure consistency in federal proceedings which was signed into law in 1973 and many states rule maps to the FRE. The Fourth Amendment to the US constitution protects everyone's right to be secure and seizure. The US jurisdiction has case law related to the admissibility of evidence recovered from computers and other digital devices. Investigating digital devices include collecting data securely, examining suspects' data to determine details such as origin and content, presenting digital information to courts and applying laws to digital from data recovery. Digital forensics is different from data recovery which involves retrieving information that was deleted by mistake or lost during a power surge or server crash.

Vulnerability and threat assessment test and verify the integrity of stand along workstations and network servers. Network intrusion attacks by using automated tools and monitoring network firewall logs. Existing laws can't keep up with the rate of technology change. Examiners must be familiar with the recent court rulings on search and seizure in the electronic environment.

Digital Investigations are of two types Public sector and private sectors investigations. Public investigations involve government agencies responsible for the criminal investigations and prosecution. Private sector focuses more on policy violations. An affidavit is a sworn statement of support of facts about the or evidence of a crime. Line of authority states who has the legal right to initiate an investigation, who can take possession of evidence and who can have access to the evidence. For private investigations, you search for evidence to support allegations of the violations of the company's assets. A private sector you minimize the risk to the company. Professional conduct includes ethics, morals and standards of behavior.

Chain of custody - Route the evidence takes the time you find out until the case is closed or goes to court. An evidence custody form helps you document what has been done with the original evidence and its forensics copies. Securing your evidence - use evidence bags to secure and catalog the evidence, use antistatic bags and pads, use evidence tapes to seal all openings, write the initials on the tape to prove that evidence has not been tampered. According to attorney client privileges you must keep all findings confidential. Internet abuse investigations require examining server log data. A bit stream copy is a bit by bit duplicate of the original disk. Always maintain a journal to keep notes on exactly what you did. Always critique your own work.

Chapter 2: The investigator's office and laboratory.

A digital forensics lab is where you conduct investigations, store evidence and do most of your work. Seek to upgrade your skills through training. A lab facility must be physically secure so that evidence is not lost, corrupted or destroyed. It is harder to plan a computer forensics lab for a police department than for a private organization or corporation. A forensics workstation needs to have adequate memory, storage and ports to deal with common types of cases that come through the lab. Prepare a business case to enlist the support of your managers and the other team members when building a forensics lab.

An overview of a computer crime is to take a systematic approach and take steps for problem solving. Assessing the case such as assessing the situation, nature of the case and other specifics. The next stage is planning the investigation. Acquiring the evidence, prepare a forensics workstation, document what has been done with the original evidence and its copies. The next stage is securing the evidence. One should always maintain and critique your own work.

Chapter 3: Data Acquisition.

Forensics data acquisition are stored in three different formats:

Raw - makes it possible to write bit-stream data to files. The advantages are that it offers fast data transfers, ignores minor data reads and errors on the source drives and most tools can use the raw format. Disadvantages are that it requires more storage than the original drive and tools might not collect marginal sectors.

Proprietary - Offers options to compress or not to compress image files. Can split an image into smaller segmented files and can integrate into the image files. Disadvantages are the inability to share images between different tools and file size limitations for each segmented volume

AFF (Advanced forensics formats)- provides compressed or uncompressed image files. There are no size restrictions or disk to image files. Provides space in the image files for metadata. Simple design with extensibility. Open source for multiple platforms and internal consistency performs self-authentication.

Data acquisition methods:

Disk to image file - can make more than one copy. Copies are bit to bit replications of the original drive. Compatible with different tools.

Disk to disk copy - used when disk to image copy is not possible. Can adjust to the disk's geometric configuration.

Logical disk to disk or disk to data file - capture only specific files of interest to the case.

Sparse data copy- collects fragments of unallocated data.

Several tools are available and lossless compression is acceptable. Planning your digital evidence contingencies is important such as making a copy of each acquisition.

Write blocking devices or utilities must be used with the GUI acquisition tools for digital forensics acquisitions. Preferred Linux acquisition tool is dcfldd (not dd). It is important to use a physical write-blocker device for acquisitions. To acquire RAID disks, determine the type of RAID and then which acquisition tool which needs to be used. Remote network acquisition tools require installing a remote agent on the suspect's computer. The use of remote network acquisition tools can remotely connect to a suspect computer via a network connection and copy data from it. Disadvantages are that antivirus tools can be configured to ignore remote access programs. Commercial Acquisition tools are PassMark Software ImageUSB, ASRData Smart, Runtime Software, ILOOKIX Investigator IXimager, and SourceForge.

Lab: We did a lab in Cengage for data acquisition to understand the internet abuse investigation and examine the server log data, a bit-stream copy is a bit-by-bit duplicate of the original data, maintain journal to keep notes and critique your own work. In addition, we discussed about the attorney-client privilege cases.

Discussion:

Employee Termination

We had a discussion on terminating an employee of an organization who was a suspect in an internal harassment investigation. We discussed that the first step is to obtain an authorization to search and seize the computer of the terminated employee. If the system is on perform a live data acquisition (RAM dump), seize the computer and document the chain of custody. The next step was to acquire a disk image using write blocker, so it doesn't change the contents of the disk. Calculate the hash of acquired image. Document the chain of custody and seal the hard drive in the evidence bag. Create a report and submit to the HR team.

Chapter 4: Processing Crime and Incident Scenes.

Digital evidence is anything stored or transmitted on electronic or optical media. General tasks when working with digital evidence is to identify digital information, collect, preserve and document evidence. Analyze, identify and organize evidence. Rebuild evidence to verify the results can be reproduced. In the private sector, incident scenes are often in a contained and controlled area. Companies should publish the right to inspect computer assets policy. Private and public sectors follow the same computing investigations rules. Criminal cases require warrants. Dealing with digital records in a business through business record exemption, business records are authenticated by verifying that they were created. Business records are admissible. Computer records are usually divided into computer generated and computer stored records. Protect your safety and health as well as the integrity of the evidence. When processing an incident or a crime scene it is important to follow guidelines such as security perimeters and video recordings. Identifying potential hazards (HAZMAT) team. As you collect digital evidence, one needs to guard it against being physically destroyed or contaminating it. Forensic hash values verify that data or storage media have not been altered. To analyze computer forensics data, learn to use more than one vendor tool. Examples of not being able to use original evidence are

1. Investigations involving network servers.

2. Removing a server from the network to acquire evidence data could cause harm to the

business or an owner

Initial response field kit is lightweight and easy to transport. Create an extensive response field kit. One must handle all evidence the same way every time one handles it. After you determine that an incident scene has digital evidence, identify the digital information or artifacts that can be used as evidence. Maintain Two separate logs of collected evidence. Maintain constant control of the collected evidence and crime scene. Looks for passwords pins passphrases bank accounts. Collect as much personal data as possible. Collect documentation and media related to the investigation. The media one uses to store digital evidence usually depends on how long one needs to keep it: CDs DVDs, Solid-state USB drives, Magnetic tapes. Plan your investigations, Conduct the investigations, Complete the case report, Critique the case.

Lab: In this exercise we solved some flip card and crossword puzzle to discuss the crime processing and incident scene terminologies.

Discussion:

Investigating Picture sharing:

In the discussion section we responded to an investigation where he a roommate was accused of taking picture and sharing on social media. The first step is to get a search warrant to investigate this person's messages and verify the picture of the victim. In addition, the next step was to verify the roommate sent email since the pictures were sent to many people. I would share the evidence with the university public safety team who would further look into the investigation.

Chapter 5: Working with Windows and CLI Systems.

When starting a suspect's computer, using boot media such as forensic boot CD or USB drives, you must ensure that disk evidence isn't altered. A partition is a logical drive and a windows OS can have up to three primary partitions followed by an extended partition. The Master Boot Record (MBR) stores information about partitions on a disk. The FAT is structured in a way that each file and directory is allocated with a data structure which is called directory entry which consists of the filename, size, starting address of the file and other related metadata. Microsoft used a FAT12 and FAT16 on older systems.

To find a hard disk's capacity, we need to use the cylinders, heads and sectors (CHS) calculation. When files are deleted in a FAT file system, the hexadecimal value 0x05is inserted in the first character of the filename in the directory. NTFS is more versatile because it uses the Master File Table (MFT) to track file information. Records in the MFT contain attribute IDs that store metadata about files. To find a file or its references from the file system or directory we can use the file name searching, we can split the filename into chunks and perform an ASCII or Unicode keyword search for locating the filename. When we recover the data from a file system, we can use various techniques or tools to recover the data, we can read the data from all clusters from the starting cluster or read only the unallocated clusters, where the hidden data can also be found. To conclude, the FAT file system is designed for its simplicity and using simple data structures. For analyzing the file system in an automated manner, the boot sector and FAT are vital. By analyzing the directory entries, we can recover the deleted files and data without using other application-level techniques.

In NTFS, an alternate data stream or streams can obscure information that might be of evidentiary value. File slack, RAM slack and drive slack are areas in which valuable information can reside on a drive. NTFS can encrypt data with EFS and Bitlocker. NTFS can compress files, folders or volumes. Windows registry keeps a record of attached hardware, user preferences, network connections and installed software. Virtualization software enables you to run the other operating systems on a host computer.

Lab:

In addition, we created a disk image and verify the work. We used dd command for byte to byte copy from source to destination, bs to give the block size, count = amount of data to copy, If= Original file location, of = detitanation file to copy the data

dd if=/dev/zero bs=1024 count=$((20*1024*1024)) of=assignment7.dd

Discussion:

We verify the primary partition that exist in a disk image using the dd with xxd command and check the largest primary partition in the disk image and the OS type. Below is a command to find the primary partition.

Chapter 6: Current Digital Forensics Tools

Two types of forensic tools: hardware forensic tools which range from simple, single-purpose components to complete computer systems and servers and software forensics tools. Such as cmd and GUI applications. Computer forensics tools functions are

Acquisition: Making a copy of the original drive

Validation and verification: A way to confirm that a tool is functioning as intended is validation and verification is that two sets of data are identical by calculating the hash values or a similar method.

Extraction: Recovery of data

Reconstruction: Re-create a suspect drive to show what happened during a crime or an incident.

Reporting: To perform a forensics disk analysis and examination and would need to create a report.

It is important to maintain a software library. Forensics hardware are customized equipment, commercial options and includes workstations and write-blockers. Advantages- customized to your records and you save money. disadvantages - hard to find support for problems and can become expensive if careless. Tools that run in Windows and other GUI environments don't require the same level of computing expertise as command-line tools. Always run a validation test when upgrading your forensics tools. Freeware tools include Sleuth Kit and its Web browser interface, Autopsy Forensic Browser, maintained by Brian Carrier. Foremost is a carving tool that can read many image files formats, such as raw and Expert Witness. A tar ball is a highly compressed data file containing one or more files or directories and their contents. It's like Windows zip utilities and typically has a .tar or .gz extension.

Lab and Discussion:

A procurement error caused your forensics analysis software to be unavailable, an urgent analysis needs to be conducted by hand, so we analyse the disk image in /srv/images/fat-analysis.raw on the compsci-server. We verify the first file in the root directory. In addition, we were able to extract the contents of a compressed file, file name and its size.

Chapter 7: Linux and Macintosh File Systems

Unix was created to be a multiuser, multithreaded and secure OS. The Linux kernel is usually packaged with other software components such as GUI and applications. Linux supports a wide range of file systems. Unix and Linux have four components defining the file system

Boot block: Contains bootstrap code and has only one boot block

Superblock: Specifies disk geometry available space and tracks all nodes, manages the FS

I node block: first data after super block, assigned every file allocation unit

Data Block: where directories and files are stored.

In the Linux file system, a hard link is a pointer that allows accessing the same file by different filenames. File content is stored in blocks which are a group of consecutive sectors. Meta data for each file and directory are stored in a data structure called an I node. The name of the file is stored in a directory entry structure which has a pointer to the I nodes. Each I node can store the addresses of the first 12 blocks that a file has allocated. If a file needs more than 12 blocks, a block is allocated to store the remaining addresses. File Name Category stores the data structures that store the name of each file and directory. ExtX uses blocks as its data unit and a block is a group of consecutive sectors. It is similar to a cluster in FAT or NTFS. It ranges from 1024, 2048 to 4096. I node consists of the metadata in a data structure format. All ExtX I node are the same size, which can be defined in the superblock. I node 1 to 10 are reserved and should be in an allocated state.

Before macOS, the file systems HFS and HFS+ were used. In older versions of macOS, a file consists of two parts: a data fork and a resource fork. A volume is any storage medium used to store files. Plist files are preference files for installed applications on a macOS system. In macOS, unified logging has been added for recording log files and includes new utilities and to help the forensics examiners. The biggest challenge in acquiring images from the mac OS systems is often physical access to the drive. Linux forensics tools are often freeware.

Lab:

We analyse a raw disk image using a simple command line tool. We were able to find the superblock data structure, number of I nodes and number of blocks, size of the block group, we were able to find the root directory’s data block. In addition, we were able to find the I node of a file called findme.txt

Chapter 8: Recovering Graphics Files

There are three types of graphics files: Bitmap, vector and metafile. Image quality depends on various factors such as screen resolutions, software contributions and color bits per pixel. Standard graphics file formats include gif, jpeg, bmp and tif whereas Nonstandard file formats include tga, rtl, psd and svg. Some image formats compress their data and such compressions are either called lossless or lossy compressions. Digital camera photos are typically in raw and EXIF-JPEG formats. Methods of recovering image files are the carving file fragments and rebuilding image headers. The internet is the best platform for learning more about the file formats and their extensions. There are different software's for image editors and image viewers.

Steganography hides information inside image files. Has methods just as insertion and substitution inside forms. Steganalysis finds whether image files hide information. Fair use allows using copyrighted material for noncommercial or educational purposes without having to compensate the material's originator or owner.

Chapter 9: Digital Forensics Analysis and Investigation.

Examining and analyzing digital evidence depends on the nature of the investigation and the amount of data to process. There are times when the investigation expands beyond the original description which is scope of the process. Evidence collection process differs from case to case.

To start with the investigation, we do the following steps which are wiping and preparing target drives, document all hardware components on the suspect's computer, check data and time values in suspect's CMOS, list of all files and folders etc. These all steps must be documented thoroughly and should keep in mind the evidence preservation procedures.

To do this it is important to wipe and prepare target drives, document all hardware components on the suspect's computer's CMOS, acquire data and document steps, list all folder and files, attempt to open password - protected files, determine functions of executable function of executable files and document steps. Advanced digital forensics tools have features such as indexing text data, making keyword searches faster. Bit shifting changes data from readable code to data that looks like binary executable code. A critical aspect of digital forensics is validating digital evidence which is ensuring the integrity of data you collect is essential for presenting evidence in court. Data hiding involves changing or manipulating a file to conceal information. Three ways to recover passwords: dictionary attacks, brute-force attacks and rainbow attacks.

Lab:

We worked on Pro-Discover to search and extract possible evidence of JPEG files to uncover hidden data from a USB drive.

Chapter 10: Virtual Machine Forensics, Live Acquisitions and Network Forensics.

Virtual machines are used extensively in organizations and are a common part of forensics investigations. There are two types of hypervisors for running virtual machines: Type 1 which loads on the physical hardware and does not require a separate OS and Type 2 which rests on top of an existing OS and is normally loaded on a suspect's machine. Virtualization Technology is Intel's CPU design for security and performance enhancements that enables the BIOS to support virtualization. Forensics procedures for VMs start by creating an image of the host machine, and then exporting files associated with a VM. Order of volatility is how long the piece of information will last on the system.

Live acquisitions are necessary to retrieve volatile items such as RAM and running processes.

Network forensics is the process of collecting and analyzing raw network data and systematically tracking network traffic to ascertain how an attack took place. As the cost of hardware and software is increasing, organizations need to pay close attention to make best investments for IT infrastructure. Here, use of virtual machines is benefited for the company as one server can easily support the entire department or company. Well-equipped workstations can fully handle the functioning of a small business and its needs. Steps must be taken to harden networks before a security breach happens. Testing is an important part of testing servers and securing a network.

The most important procedure defined when investigating a Virtual Machine is given below:

-Create an image of the host machine.

-Locate virtualization software and VMs and using this information you can further get more

information on file extensions and network adapters.

- Export all the files that are associated with VM including the log files, virtual adapters, and

snapshots.

- Record hash values of these files.

- Finally, you can create an image of the VM in forensic software or mount VM as a drive and

then create an image or perform live search.

Performing live acquisition is often considered to be crucial as they include all snapshots, as snapshot is the current state captured, and must be incorporated when performing live acquisition. Network administrators also depend on snapshots as they are useful in case of failure of update or software installation. If you are

a law enforcement officer or working for any outside company maintaining good relationships with network administrators and technicians can be very beneficial.

Conducting investigation with Type 2 Hypervisor - Investigating on a virtual machine involves the same procedure as standard investigation, no other specific steps are being involved. Initially, we begin by acquiring images of the host computer as well as network logs. To determine the data accessed by VM, we can link VM's IP address to log files. Detecting virtual machines, whether on host computers, is a challenging task for digital investigators. On different operating systems VM's can be stored at different locations. To find relevant information from a suspect's computer and other information such as websites and network files, all the files associated with VM's must be extracted and examined.

Being able to spot variations in network traffic can help track intrusions. Several tools are available for monitoring network traffic such as packet analyzers and honeypots. Network ogs record ingoing and outgoing traffic. The honeynet Project is designed to help people learn the latest intrusion techniques that attackers are using. Examples are zero-day attacks, honeypot and honeywalls.

Lab:

We learned how to perform an image acquisition on a virtual machine by mounting a VM as a drive in OS Forensics.

Chapter 11: Email and Social Media Investigations.

Email fraudsters use phishing, pharming and spoofing scam techniques. In both internet and intranet email environments, email messages are distributed from one central server to connected client computers. Email investigations are similar to other kinds of investigations. Forensics linguistics in a field where language and the law intersect to determine the author of emails, text messages and other online communications.

Communicating via email can be done in two environments i.e. via internet or intranet. To communicate via emails messages client/server architecture is configured. Email programs are run by the server to provide email services such as Microsoft Exchange Servers and the client uses email programs such as Outlook for communication with the server. While investigating email crimes the main aim is to find who attempted the crime or who violated the policies, preserve and collect the evidence and build a complete report investigating the case. While collecting evidence you must also have prior knowledge of rules and regulations, as the laws differ for each country and every state. Laws of some states do not consider a crime if any spam email is sent, but some states consider it as a crime.

While investigating email you also need to trace its path and domain from where it came. There are tools available to trace the emails and from where it has originated. You can also use registry sites to find additional information. Use of American registry for Internet Numbers, arin.net or google.com can help you trace the IP addresses and point of contact for further investigation. You can also obtain the log information from network administrators as they manage the router supply and supply log files. They also maintain logs for firewalls and these logs can also be useful for investigation. To obtain the information you must take quick steps as most administrators do not maintain the data for more than 30 days, some of them do create a backup and it can benefit you to recover information. Configuration files are also beneficial to find the log information. Unix consists of various email servers and the syslog.conf file lets you know where different logs are saved and mail log file which is crucial for investigation lets you to the IP address, timestamp, Post Office Protocol Version and Internet Message Access Protocol event information.

In UNIX you can also use the find or locate command to find the email-logs. Access the victim's computer to recover evidence. Copy and print the email message involved in the crime or policy violation. Use the emails programs that created the message to find the email header, which provides supporting evidence and can help you track the suspect to the originating location. When investigating email abuse, the investigator must be familiar with the email servers and client operations. For many email investigations you can rely on email message files, headers and server log files. For email applications that use the mbox format, a hexadecimal editor can be used to carve messages manually.

Social media or OSN can provide evidence in criminal and civil cases and the software for collecting the OSN information is currently being developed. The majority of the people engaging in social media communications are mobile users. Social media forensics tools have evolved with the technology and many forensics suites have built-in social media tools. Accessing social media via mobile phones have become common and studies have also revealed that most of the data was stored in databases as the contacts from mobile phones as they were synced and all information from mobiles was extracted. Many tools have been developed to extract information from mobile devices as the synchronization allows every information to be accessed. Therefore, we studied email investigations in detail and got to know the crimes that take place through social media. We also study various tools to extract information whenever investigating for a crime.

Lab:

We used Aid4mail and Autopsy tool to investigate e-mail. We also learned how to recover deleted emails using OS Forensics tool. Also, we perform an investigation on FB account by using the software Facebook Forensic though which we were able to extract many information.

Chapter 12: Mobile Device Forensics and the Internet of Anything.

People store a wealth of information on smartphones, including calls, text messages, picture and music files, address books and more. Mobile devices have gone through four generation:

Analog, Digital personal communications service (PCS), Third generation (3G), Fourth generation (4G).

5G standards are being negotiated and developed by the IMT 2020 working group of the International Telecommunications Union. Mobile devices range from the basic, inexpensive phones used primarily for phone calls to smartphones. Global System for Mobile Communications (GSM) uses the time division multiple access (TDMA) that multiple phones take turns sharing a channel. Phones store system data in electronically erasable programmable read-only memory that enables service providers to reprogram phones without having to physically access memory chips. Data can be retrieved from several different places in phones. Use of personal digital assistants (PDAs) have declined due to the popularity of smartphones. All mobile devices have volatile memory, so it is important to retrieve RAM data which is critical. It's better to get a warrant or subpoena and make a note of the time of seizure. A phone that is seized should be isolated from incoming signals and broadcasting. It needs to be handled with care and protect them from environmental factors and sources of electromagnetic interference. The data can be retrieved by logical or physical acquisition as per the case. The service provider can help to track the location and time of the call. Also, most of the data are stored on the cloud server by the service provider which is again a complicated process. As with computers, proper search and seizure procedures must be followed for mobile devices. To isolate a mobile device from incoming messages, you can put it in airplane mode, turn the device off, or place it in a special treated paint can or evidence bag. SIM cards store data in a hierarchical file structure. Mobile device forensics is becoming more important as these devices grow in popularity. Many software tools are available for reading data stored in mobile devices. The Internet of Things (IOT) has resulted in yet another challenge for digital forensics investigators. Collecting information from wearable computers will pose many new challenges for investigators.

Chapter 13: Cloud Forensics

Three services levels are available for the cloud: software as a service, platform as a service and infrastructure as a service. CSPs use servers on distributive networks or mainframes that allow elasticity of resources for customers. With multinational clouds, you should seek legal counsel before proceedings with an investigation. Cloud investigations are necessary in cases involving cyberattacks, policy violations, data recovery and fraud complaints.

Before initiating a cloud investigation, review the CSA to identify any restrictions that might limit collecting and analyzing data.

Technical challenges in cloud forensics involve cloud architecture, data collection, analysis of cloud forensic data, anti-forensics, incident first responders, role management, legal issues and standards and training. Anti-forensics is an effort to alter log records as well as date and time values of important system files and install malware to hide hacker's activities. CSPs should have an incident response team ready to respond to network intrusions. Role management defines the duties of CSP staff and customers. The cloud security alliance has developed resources that guide CSPs in privacy agreements and security measures. Procedures for acquiring cloud evidence include examining network and firewall logs, performing disk acquisitions of a cloud system's OS and examining data storage devices

When investigating a cloud incident, apply a systematic approach to planning and processing the case. The three cloud services which are Dropbox, Google Drive and Microsoft OneDrive contain data on a user's computer or mobile device that can reveal what files were copied or accessed. Vendors offer tools that can be combined for cloud forensics.

Cloud forensic is widely used by many small and large organizations for their daily business. It has many critical data uploaded on the cloud. Once the cloud system is compromised the investigator needs to determine the type of crime whether it's civil or criminal. Once this is known the investigator's next step is to perform steps to retrieve evidence with the help of cloud forensics tools and CSPs network admin team.

Lab**:** We learned to investigate mobile phones by using the tool called SIM Con. SIM Con is a program that allows the user to securely image all files on a GSM/3G SIM card.