LAB MANUAL

MODERN EDUCATION SOCIETY'S WADIA COLLEGE OF ENGINEERING, PUNE

Fourth Year of Computer Engineering (2019 Course)

410247: Laboratory Practice IV
410244(C): Cyber Security and Digital Forensics

NAME OF STUDENT:	**CLASS: BE**
SEMESTER/YEAR: VII	**ROLL NO:**
DATE OF PERFORMANCE:	**DATE OF SUBMISSION:**
EXAMINED BY:	**EXPERIMENT NO:**

TITLE: Email Header Analyzer

AIM/PROBLEM STATEMENT: Write a program for Tracking Emails and Investigating Email Crimes. i.e. Write a program to analyze e–mail header

OBJECTIVES:

- To understand various vulnerabilities and use of various tools for assessment of vulnerabilities

OUTCOMES:

- Identify various vulnerabilities and demonstrate using various tools.

PRE-REQUISITES:

1. Knowledge of C, C++, python programming
2. Basic knowledge of computer, network and security information

THEORY:

The email header is a code snippet in an HTML email, that contains information about the sender, recipient, email's route to get to the inbox and various authentication details. The email header always precedes the email body.

What purpose do email headers serve

Providing information about the sender and recipient :
An email header tells who sent the email and where it arrived. Some markers indicate this information, like "From:" — sender's name and email address, "To:" — the recipient's name and email address, and "Date:" — the time and date of when the email was sent. All of these are mandatory indicators. Other parts of the email header are optional and differ among email service providers.

Preventing spam:
The information displayed in the email header helps email service providers troubleshoot potential spam issues. Encapsulating Security Payload (ESPs) analyzes the email header, the "Received:" tag, in particular, to decide whether to deliver an email or not.

Identifying the email route:
Identifying the email route. When an email is sent from one computer to another, it transfers through the Mail Transfer Agent which automatically “stamps” the email with information about the recipient, time and date in the email header.

How to Find an Email Header

Viewing an email header in Gmail:
Open an email. Find “More” (three vertical dots), choose “Show original.”

Viewing an email header in Outlook:

Open an email. Find “More actions” (three horizontal dots), choose “View message source.”

Viewing an email header in Yahoo:

Open an email. Find “More actions” (three horizontal dots), choose “View raw message.”

All ESPs allow curious users to see how the email looks from the inside, in HTML code. This function looks and works the same way with every ESP. Let’s take a closer look at it.

Analyzing an Email Header

The appearance of the email header differs between ESPs. To analyze it, you need to find the email header and examine the lines of interest to you. All the code from the beginning, until the <body> tag, represents the header. Here is the list of what you can find in the email header:

“Received:” lines. They show the address of the computer that received the email, as well as other computers’ addresses that an email may have been transferred through. Unlike other email header elements, “Received:” lines can’t be forged.

MIME-version. Multipurpose Internet Mail Extensions are an Internet standard that extends the format of email by supporting text and non-text attachments like audio, video, images, message bodies with multiple parts, etc.

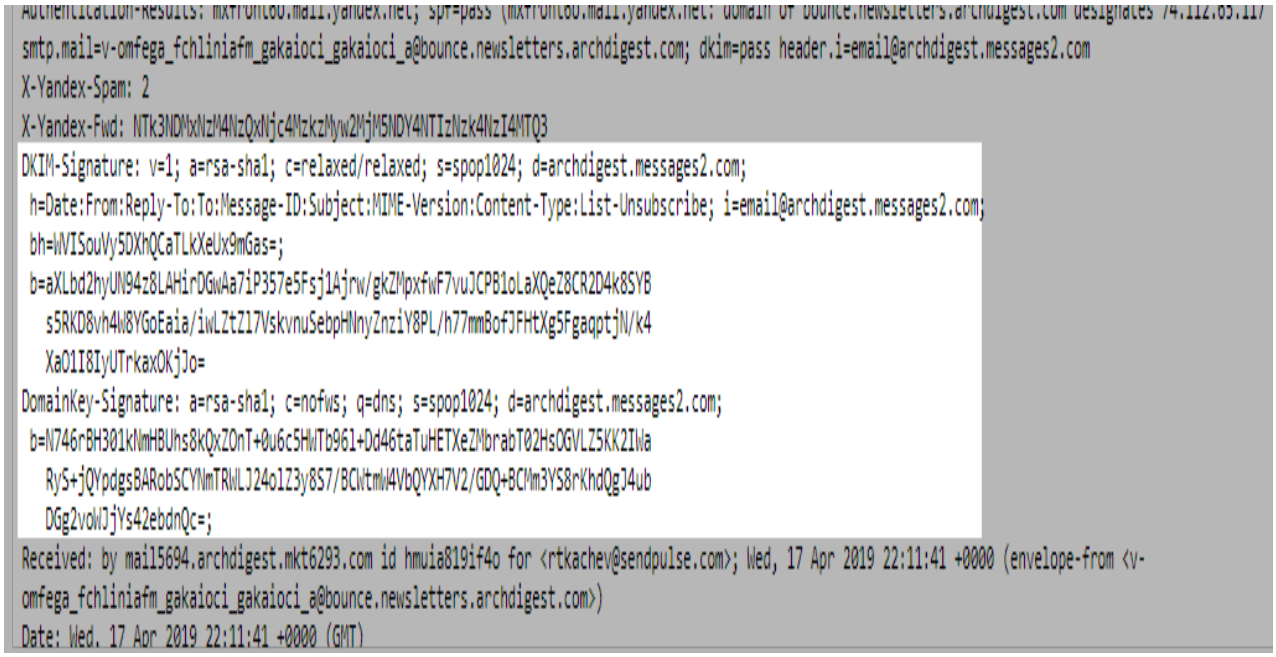
```
Date: Wed, 17 Apr 2019 22:11:41 +0000 (GMT)
From: Architectural Digest <email@archdigest.messages2.com>
Reply-To: email@archdigest.messages2.com
To: rtkachev@sendpulse.com
Message-ID: <763600385.13061421155553910l049.JavaMail.app@rbg23.atlis1>
Subject: Debate Over How Notre-Dame Will Be Rebuilt
MIME-Version: 1.0
Content-Type: multipart/alternative;
       boundary="----=_Part_35741_1805585129.1555539069133"
x-mid: 15488096
X-CSA-Complaints: whitelist-complaints@eco.de
x-rpcampaign: sp15488096
Feedback-ID: pod2_21948_15488096_1621134888:pod2_21948:ibmsilverpop
x-job: 15488096
x-orgId: 21948
List-Unsubscribe: <mailto:v-omfega_fchliniafm_gakaioci_gakaioci_a@bounce.newsletters.archdigest.com?subject=Unsubscribe>
X-Yandex-Forward: b01a1c6487a67e98038c94dff0bc5e09
```

Message-ID. The message-ID is a globally unique identifier used in email. Message-IDs have a specific format that is generated for a specific email address and message, thus, no two messages have the same Message-ID.

```
Received: by mail5694.archdigest.mkt6293.com id hmuia819if4o for <rtkachev@sendpulse.com>; Wed, 17 Apr 2019 22:11:41 +0000 (envelope-from <v-
omfega_fchliniafm_gakaioci_gakaioci_a@bounce.newsletters.archdigest.com>)
Date: Wed, 17 Apr 2019 22:11:41 +0000 (GMT)
From: Architectural Digest <email@archdigest.messages2.com>
Reply-To: email@archdigest.messages2.com
To: rtkachev@sendpulse.com
Message-ID: <763600385.13061421155553910l049.JavaMail.app@rbg23.atlis1>
Subject: Debate Over How Notre-Dame Will Be Rebuilt
MIME-Version: 1.0
Content-Type: multipart/alternative;
       boundary="----=_Part_35741_1805585129.1555539069133"
x-mid: 15488096
X-CSA-Complaints: whitelist-complaints@eco.de
x-rpcampaign: sp15488096
Feedback-ID: pod2_21948_15488096_1621134888:pod2_21948:ibmsilverpop
x-job: 15488096
x-orgId: 21948
List-Unsubscribe: <mailto:v-omfega_fchliniafm_gakaioci_gakaioci_a@bounce.newsletters.archdigest.com?subject=Unsubscribe>
X-Yandex-Forward: b01a1c6487a67e98038c94dff0bc5e09

------=_Part_35741_1805585129.1555539069133
```

DKIM Signatures. DomainKeys Identified Mail confirms the sender's authenticity by connecting the domain name with the email. DKIM is the technology that helps to reduce spam and phishing and allows companies to guarantee for their email messages.



CONCLUSION: Thus, implementation of email header program is performed successfully.

QUESTIONS:

1. Why are email headers so important in computer forensics ?

2. How can an email header analysis be used in the legal process ?

3. How the use of email header information could be used by a digital forensic professional in an investigation ?

MODERN EDUCATION SOCIETY'S WADIA COLLEGE OF ENGINEERING, PUNE

Fourth Year of Computer Engineering (2019 Course)

410247: Laboratory Practice IV
410244(C): Cyber Security and Digital Forensics

NAME OF STUDENT:	**CLASS: BE**
SEMESTER/YEAR: VII	**ROLL NO:**
DATE OF PERFORMANCE:	**DATE OF SUBMISSION:**
EXAMINED BY:	**EXPERIMENT NO:**

TITLE: CAPTCHA image

AIM/PROBLEM STATEMENT: Implement a program to generate and verify CAPTCHA image

OBJECTIVES:

- To understand various vulnerabilities and use of various tools for assessment of vulnerabilities

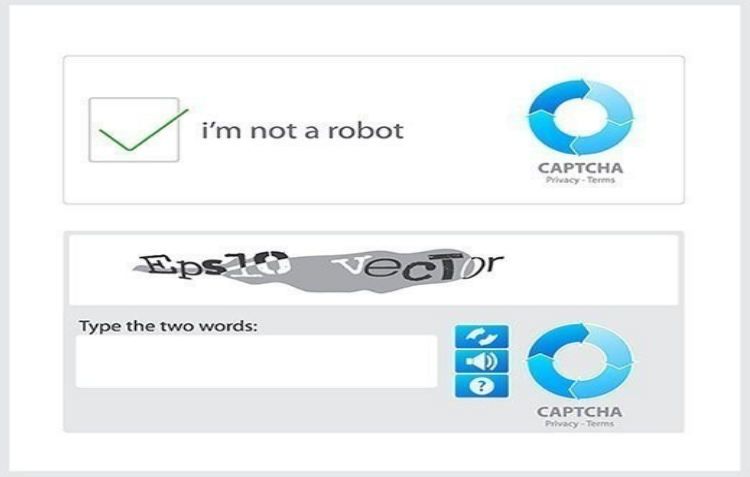
OUTCOMES:

- Identify various vulnerabilities and demonstrate using various tools.

THEORY:

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of security measure known as challenge-response authentication. It is a test to determine whether the user is human or not.

CAPTCHA helps protect you from spam and password decryption by asking you to complete a simple test that proves you are human and not a computer trying to break into a password protected account.



History of CAPTCHA

The need for CAPTCHAs began as far back as 1997. At that time, the internet search engine AltaVista was looking for a way to block automated URL submissions to the platform that were skewing the search engine's ranking algorithms.

To solve the problem, Andrei Broder, formerly AltaVista's chief scientist, developed an algorithm that randomly generated an image of printed text.Although computers could not

recognize the image, humans could read the message the image contained and respond appropriately. Broder and his team were issued a patent for the technology in April 2001.

In 2003, Nicholas Hopper, Manuel Blum, Luis von Ahn of Carnegie Mellon University, and John Langford of IBM perfected the algorithm and coined the term CAPTCHA for Completely Automated Public Turing Test to Tell Computers and Humans Apart.

A Turing test uses artificial intelligence (AI) to determine whether a computer is capable of thinking like a human being or not. It is named after its founder, Alan Turing, a computer scientist, cryptanalyst, mathematician and theoretical biologist.
Jason Polakis, a professor in computer science, took credit for an increase in CAPTCHA difficulty in 2016 when he published a paper where he used image recognition tools to solve Google image CAPTCHAs with an accuracy of 70%.Polakis believes we are at a point at which making CAPTCHAs harder for software to solve will now simultaneously make it more difficult for humans to solve.

Different types of CAPTCHAs

The most common type of CAPTCHA is the text CAPTCHA, which requires the user to view distorted letters or distorted text, usually containing a string of alphanumeric characters in an image, and enter the characters in an attached form.

This throws off bots that are typically trained in pattern recognition and are simply unable to react independently as a human would.Text CAPTCHAS are also rendered as MP3 audio CAPTCHAs to meet the needs of the visually impaired. Just as with images, bots can detect the presence of an audio file, but only a human can listen and know the information the file contains.

Another common CAPTCHA uses picture recognition by asking users to identify a subset of images within a larger set of images. For instance, the user may be given a set of images and asked to click on all the ones that have cars, buses or street signs in them.
Arkose Labs ML models for 3D questions used for fraud prevention purposes
Cybersecurity vendor Arkose Labs implements ML models to generate 3D questions for fraud prevention purposes.

Other forms of CAPTCHAs include:

- **Math CAPTCHA**. Requires the user to solve a basic math problem, such as adding or subtracting two numbers.
- **3D Super CAPTCHA**. Requires the user to identify an image rendered in 3D.
- **I am not a robot CAPTCHA**. Requires the user to check a box.
- **Marketing CAPTCHA**. Requires the user to type a particular word or phrase related to the sponsor's brand.

How does the CAPTCH WORK ?

A CAPTCHA test is made up of two simple parts: a randomly generated sequence of letters and/or numbers that appear as a distorted image, and a text box. To pass a the test and prove your human identity, simply type the characters you see in the image into the text box.

Quite simply, CAPTCHA works by asking end users to perform some task that a software bot cannot do. If the user can do the task correctly, it provides authentication to the service that the user is a human being and not a spambot and allows the user to continue. Tests often involve JPEG or GIF images because while bots can identify the existence of an image by reading source code, they cannot tell what the image depicts.

Because some CAPTCHA images are difficult to interpret, human users are usually given the option to request a new CAPTCHA test.CAPTCHA helps protect you from spam and password decryption by asking you to complete a simple test that proves you are human and not a computer trying to break into a password protected account

Algorithm:

The set of characters to generate CAPTCHA are stored in a character array chrs[] which contains (a-z, A-Z, 0-9), therefore size of chrs[] is 62.

To generate a unique CAPTCHA every time, a random number is generated using rand() function (rand()%62) which generates a random number between 0 to 61 and the generated random number is taken as index to the character array chrs[] thus generates a new character of captcha[] and this loop runs n (length of CAPTCHA) times to generate CAPTCHA of given length.

Advantages and disadvantages of CAPTCHAs

Advantages of CAPTCHAs include:

- They prevent spam from automated programs that could send emails, comments or advertisements.
- They prevent fake registrations or sign-ups for websites.
- CAPTCHAs are familiar, so website visitors automatically understand what they are tasked to do.
- CAPTCHAs are also easy to implement in building a website.

Disadvantages of CAPTCHAs include:

- CAPTCHAs are not fool proof and can only limit spam.
- They can be time consuming or annoying to end users.
- To some people, CAPTCHAs may be challenging to read.
- Websites using CAPTCHAs may notice traffic decreases because users find the tasks difficult.

CONCLUSION: Thus, we have implemented image captcha successfully.

QUESTIONS:

1. What's the purpose of CAPTCHA technology and how does it work ?
2. How attackers defeat CAPTCHAs ?

MODERN EDUCATION SOCIETY'S WADIA COLLEGE OF ENGINEERING, PUNE

Fourth Year of Computer Engineering (2019 Course)

410247: Laboratory Practice IV
410244(C): Cyber Security and Digital Forensics

NAME OF STUDENT:	**CLASS: BE**
SEMESTER/YEAR: VII	**ROLL NO:**
DATE OF PERFORMANCE:	**DATE OF SUBMISSION:**
EXAMINED BY:	**EXPERIMENT NO:**

TITLE: WIRESHARK

AIM/PROBLEM STATEMENT: Configure and demonstrate use of vulnerability assessment tool like Wireshark or SNORT

OBJECTIVES:

- To understand various vulnerabilities and use of various tools for assessment of vulnerabilities

OUTCOMES:

- Identify various vulnerabilities and demonstrate using various tools.
- To apply the scientific method for security assessment

PRE-REQUISITES:

1. Knowledge of C, C++, python programming
2. Basic knowledge of authentication, access control, intrusion detection and prevention.

THEORY:

Wireshark is an open-source network protocol analysis software program started by Gerald Combs in 1998. A global organization of network specialists and software developers support Wireshark and continue to make updates for new network technologies and encryption methods. Wireshark is absolutely safe to use. Government agencies, corporations, non-profits, and educational institutions use Wireshark for troubleshooting and teaching purposes. There isn't a better way to learn networking than to look at the traffic under the Wireshark microscope.

There are questions about the legality of Wireshark since it is a powerful packet sniffer. The Light side of the Force says that you should only use Wireshark on networks where you have permission to inspect network packets. Using Wireshark to look at packets without permission is a path to the Dark Side.

How does Wireshark work?

Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis. Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE.802.11), Token Ring, Frame Relay connections, and more.

Ed. Note: A "packet" is a single message from any network protocol (i.e., TCP, DNS, etc.)
Ed. Note 2: LAN traffic is in broadcast mode, meaning a single computer with Wireshark can see traffic between two other computers. If you want to see traffic to an external site, you need to capture the packets on the local computer.

Wireshark allows you to filter the log either before the capture starts or during analysis, so you can narrow down and zero into what you are looking for in the network trace. For example, you can set a filter to see TCP traffic between two IP addresses. You can set it only to show you the packets sent from one computer. The filters in Wireshark are one of the primary reasons it became the standard tool for packet analysis.

How to Download Wireshark
Downloading and installing Wireshark is easy. Step one is to check the official Wireshark Download page for the operating system you need. The basic version of Wireshark is free.
Wireshark for Windows
Wireshark comes in two flavors for Windows, 32 bit and 64 bit. Pick the correct version for your OS. The current release is 3.0.3 as of this writing. The installation is simple and shouldn't cause any issues.

Wireshark for Mac
Wireshark is available on Mac as a Homebrew install.
To install Homebrew, you need to run this command at your Terminal prompt:
/usr/bin/ruby -e "$(curl -
fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
Once you have the Homebrew system in place, you can access several open-source projects for your Mac. To install Wireshark run this command from the Terminal:
brew install Wireshark

Homebrew will download and install Wireshark and any dependencies so it will run correctly.

Wireshark for Linux

Installing Wireshark on Linux can be a little different depending on the Linux distribution. If you aren't running one of the following distros, please double-check the commands. Ubuntu

From a terminal prompt, run these commands:

1. sudo apt-get install wireshark
2. sudo dpkg-reconfigure wireshark-common
3. sudo adduser $USER wireshark

Those commands download the package, update the package, and add user privileges to run Wireshark.

Red Hat Fedora

From a terminal prompt, run these commands:

1. sudo dnf install wireshark-qt
2. sudo usermod -a -G wireshark username

The first command installs the GUI and CLI version of Wireshark, and the second adds permissions to use Wireshark.

Kali Linux

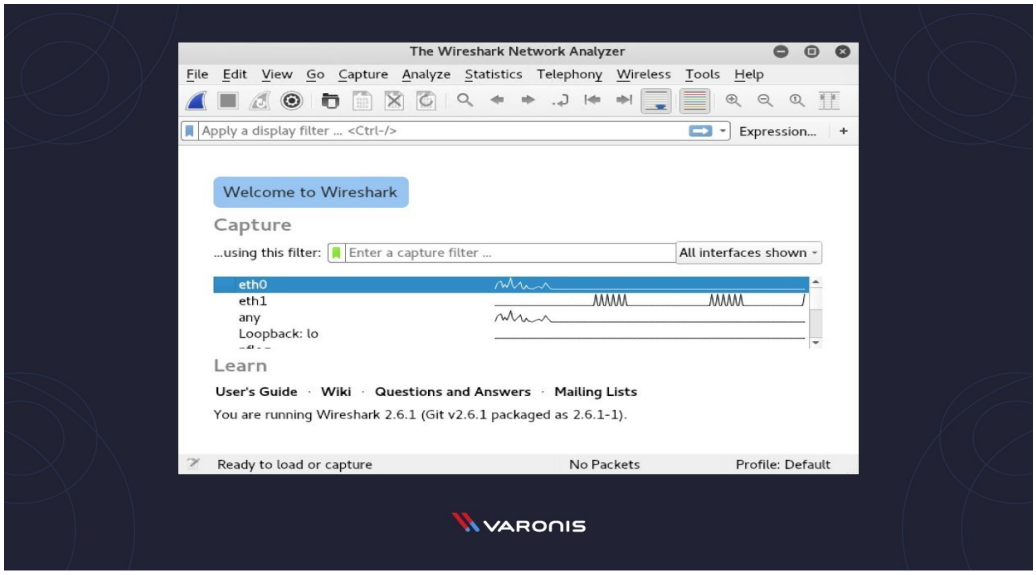
Wireshark is probably already installed! It's part of the basic package. Check your menu to verify. It's under the menu option "Sniffing & Spoofing."

Data Packets on Wireshark

Now that we have Wireshark installed let's go over how to enable the Wireshark packet sniffer and then analyze the network traffic.

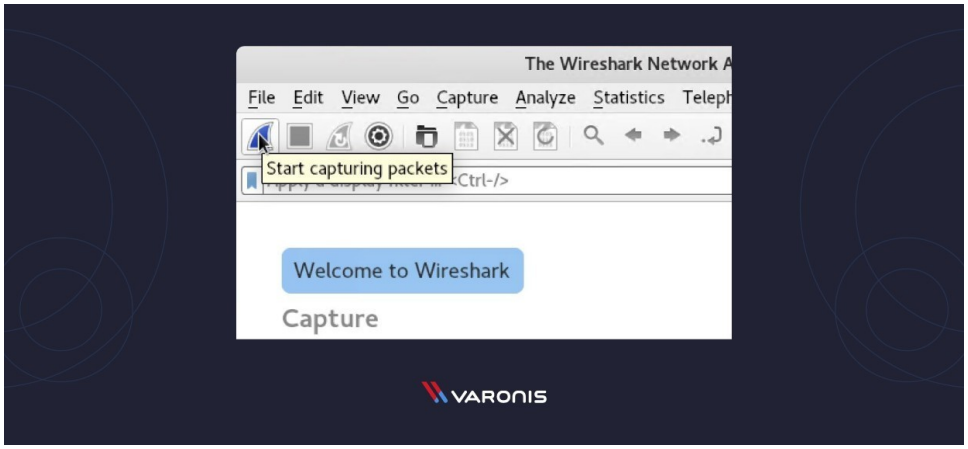
Capturing Data Packets on Wireshark

When you open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor. You also have a capture filter field, so you only capture the network traffic you want to see.

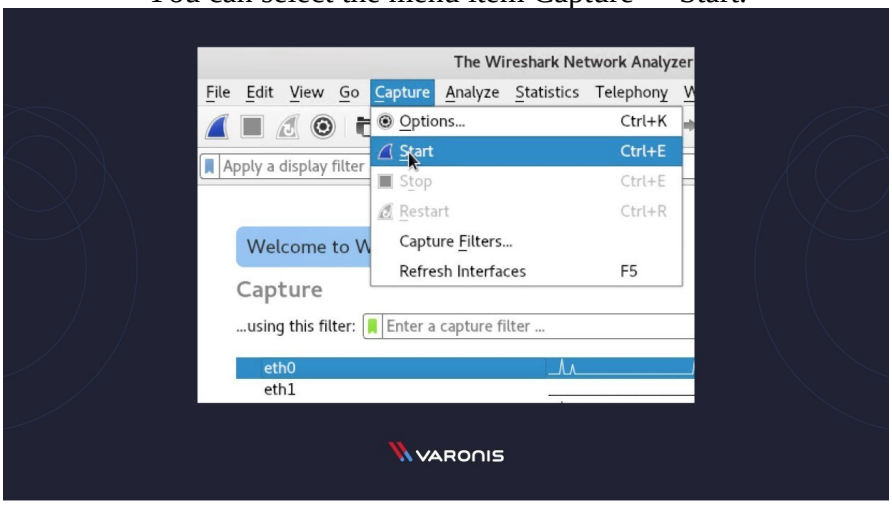


You can select one or more of the network interfaces using “shift left-click.” Once you have the network interface selected, you can start the capture, and there are several ways to do that.

Click the first button on the toolbar, titled “Start Capturing Packets.”

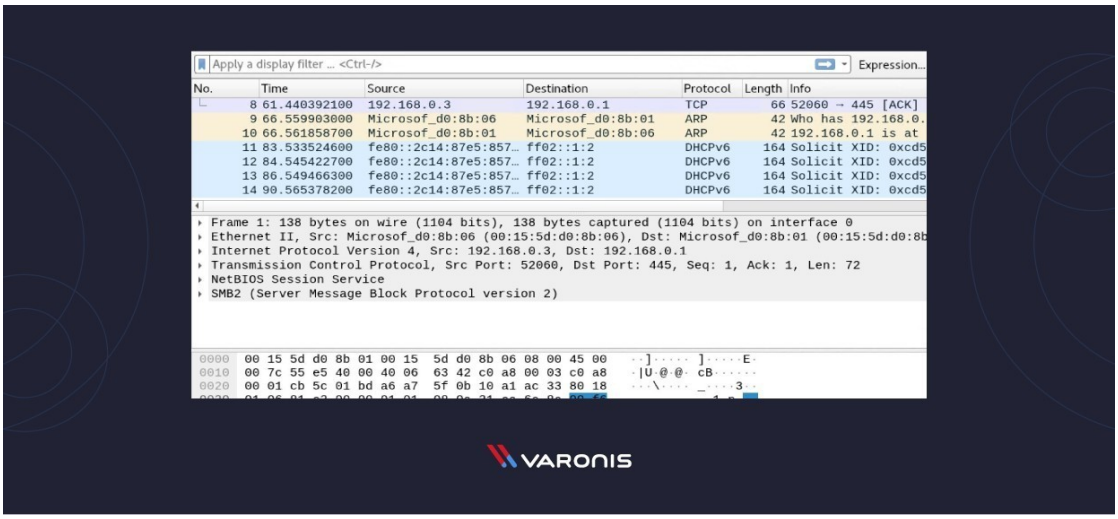


You can select the menu item Capture -> Start.



Or you could use the keystroke Control – E.

During the capture, Wireshark will show you the packets that it captures in real-time.



Once you have captured all the packets you need, you use the same buttons or menu options to stop the capture.

Best practice says that you should stop Wireshark packet capture before you do analysis.

Analyzing Data Packets on Wireshark

Wireshark shows you three different panes for inspecting packet data. The Packet List, the top pane, is a list of all the packets in the capture. When you click on a packet, the other two panes change to show you the details about the selected packet. You can also tell if the packet is part of a conversation. Here are some details about each column in the top pane:

- **No.**: This is the number order of the packet that got captured. The bracket indicates that this packet is part of a conversation.
- **Time**: This column shows you how long after you started the capture that this packet got captured. You can change this value in the Settings menu if you need something different displayed.
- **Source**: This is the address of the system that sent the packet.
- **Destination**: This is the address of the destination of that packet.
- **Protocol**: This is the type of packet, for example, TCP, DNS, DHCPv6, or ARP.
- **Length**: This column shows you the length of the packet in bytes.
- **Info**: This column shows you more information about the packet contents, and will vary depending on what kind of packet it is.

Packet Details, the middle pane, shows you as much readable information about the packet as possible, depending on what kind of packet it is. You can right-click and create filters based on the highlighted text in this field. The bottom pane, Packet Bytes, displays the packet exactly as it got captured in hexadecimal. When you are looking at a packet that is part of a conversation, you can right-click the packet and select Follow to see only the packets that are part of that conversation.

Wireshark Filters

One of the best features of Wireshark is the Wireshark Capture Filters and Wireshark Display Filters. Filters allow you to view the capture the way you need to see it so you can troubleshoot the issues at hand. Here are several filters to get you started.

Wireshark Capture Filters

Capture filters limit the captured packets by the filter. Meaning if the packets don't match the filter, Wireshark won't save them. Here are some examples of capture filters:

host IP-*address*: this filter limits the capture to traffic to and from the IP address

net 192.168.0.0/24: this filter captures all traffic on the subnet.

dst host IP-*address*: capture packets sent to the specified host.

port 53: capture traffic on port 53 only.

port not 53 and not arp: capture all traffic except DNS and ARP traffic

Wireshark Display Filters

Wireshark Display Filters change the view of the capture during analysis. After you have stopped the packet capture, you use display filters to narrow down the packets in the Packet List so you can troubleshoot your issue.

The most useful (in my experience) display filter is:

ip.src==*IP-address* and ip.dst==*IP-address*

This filter shows you packets from one computer (ip.src) to another (ip.dst). You can also use ip.addr to show you packets to and from that IP. Here are some others:

tcp.port eq 25: This filter will show you all traffic on port 25, which is usually SMTP traffic.

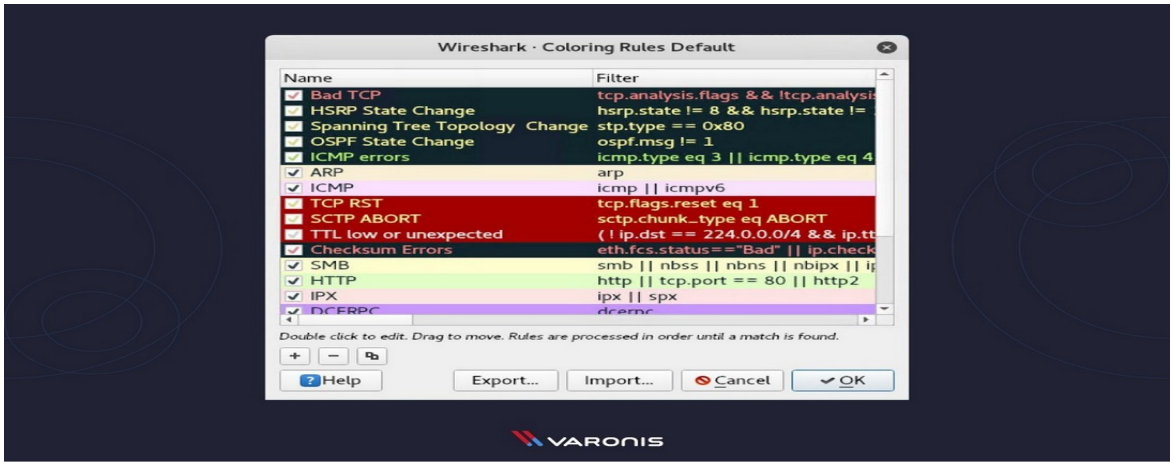
icmp: This filter will show you only ICMP traffic in the capture, most likely they are pings.

ip.addr != *IP_address*: This filter shows you all traffic except the traffic to or from the

specified computer.
Analysts even build filters to detect specific attacks, like this filter to detect the Sasser worm:
ls_ads.opnum==0x09

Additional Wireshark Features

Beyond the capture and filtering, there are several other features in Wireshark that can make your life better.
Wireshark Colorization Options
You can setup Wireshark so it colors your packets in the Packet List according to the display filter, which allows you to emphasize the packets you want to highlight. Check out some examples here.



Wireshark Promiscuous Mode

By default, Wireshark only captures packets going to and from the computer where it runs. By checking the box to run Wireshark in Promiscuous Mode in the Capture Settings, you can capture most of the traffic on the LAN.

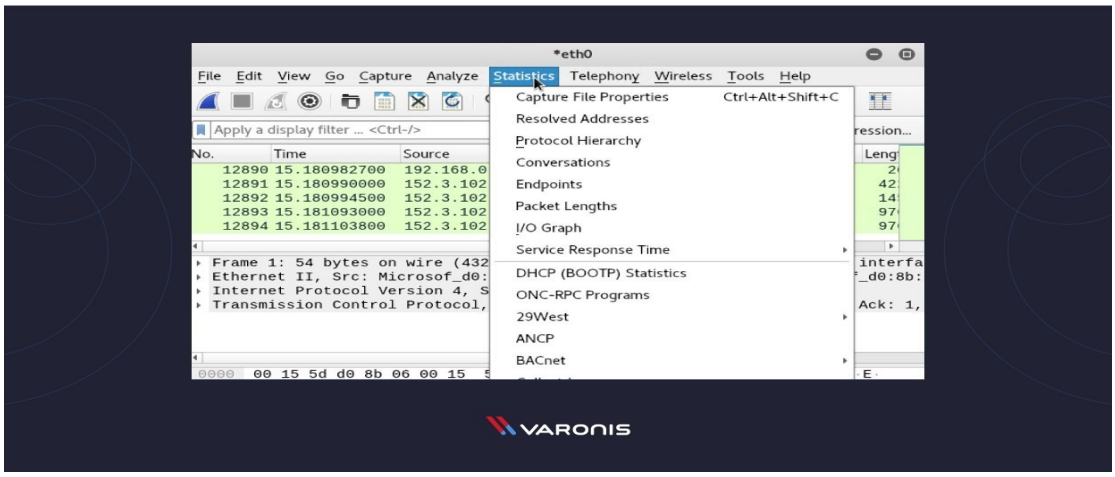
Wireshark Command Line

Wireshark does provide a Command Line Interface (CLI) if you operate a system without a GUI. Best practice would be to use the CLI to capture and save a log so you can review the log with the GUI. Wireshark Commands

- wireshark : run Wireshark in GUI mode
- wireshark –h : show available command line parameters for Wireshark
- wireshark –a duration:300 –i eth1 –w wireshark. : capture traffic on the Ethernet interface 1 for 5 minutes. –a means automatically stop the capture, -i specifics which interface to capture

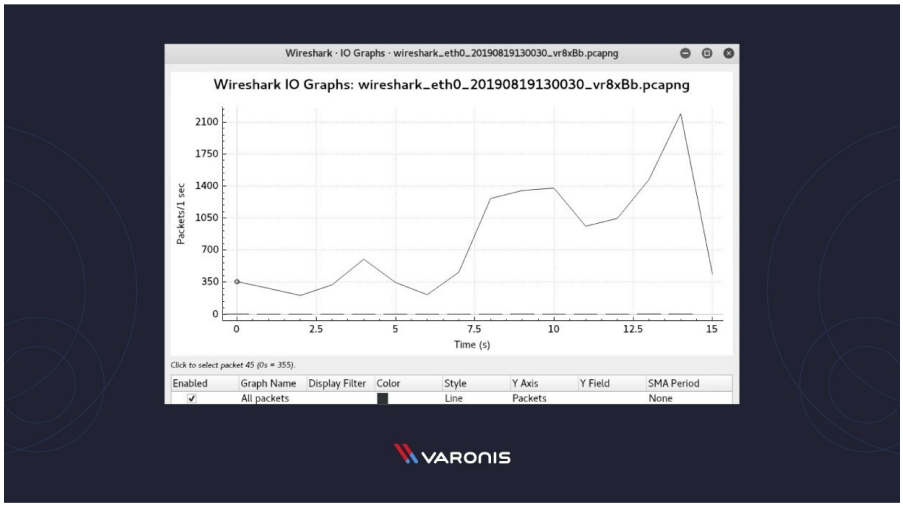
Metrics and Statistics

Under the Statistics menu item, you will find a plethora of options to show details about your capture.



Capture File Properties:

Wireshark I/O Graph:



WIRESHARK/SNORT LINKS FOR CODE

https://github.com/sujay-mahadik/CL7/blob/master/ICS/Assignment4/README.md

CONCLUSION: Thus, we have implemented wireshark successfully.

QUESTIONS:

1. What should I look for in Wireshark capture?

2. How do you analyze packet captures?

MODERN EDUCATION SOCIETY'S WADIA COLLEGE OF ENGINEERING, PUNE

Fourth Year of Computer Engineering (2019 Course)

410247: Laboratory Practice IV
410244(C): Cyber Security and Digital Forensics

NAME OF STUDENT:	**CLASS: BE**
SEMESTER/YEAR: VII	**ROLL NO:**
DATE OF PERFORMANCE:	**DATE OF SUBMISSION:**
EXAMINED BY:	**EXPERIMENT NO:**

TITLE: Configure a Wi-Fi adapter and Access Point.

AIM: To prohibit the unauthorized access to Wi-Fi network (wired/wireless), Deny unethical access to different IP resources connected to the network using router and its features.

OBJECTIVES: To understand various vulnerabilities and use of various tools for assessment of vulnerabilities

OUTCOMES: Identify various vulnerabilities and demonstrate using various tools.**PRE-**

REQUISITES: Knowledge of Networking, Access Point, ARP - Binding, IP Address, MAC Address. Basic knowledge of computer, routers, network and security information.

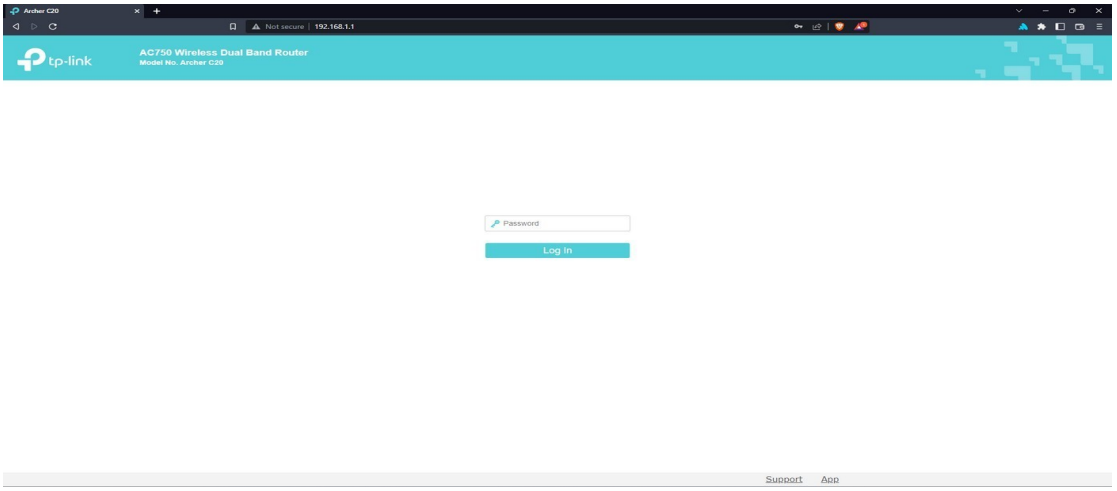
THEORY:

A **wireless router** is a device that performs the functions of a router and also includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network. Depending on the manufacturer and model, it can function in a wired local area network, in a wireless-only LAN, or in a mixed wired and wireless network.Wireless routers typically feature one or more network interface controllers supporting Fast Ethernet or Gigabit Ethernet ports integrated into the main system on a chip (SoC) around which the router is built. An Ethernet switch as described in IEEE 802.1Q may interconnect multiple ports. Some routers implement link aggregation through which two or more ports may be used together improving throughput and redundancy.All wireless routers feature one or more wireless network interface controllers.

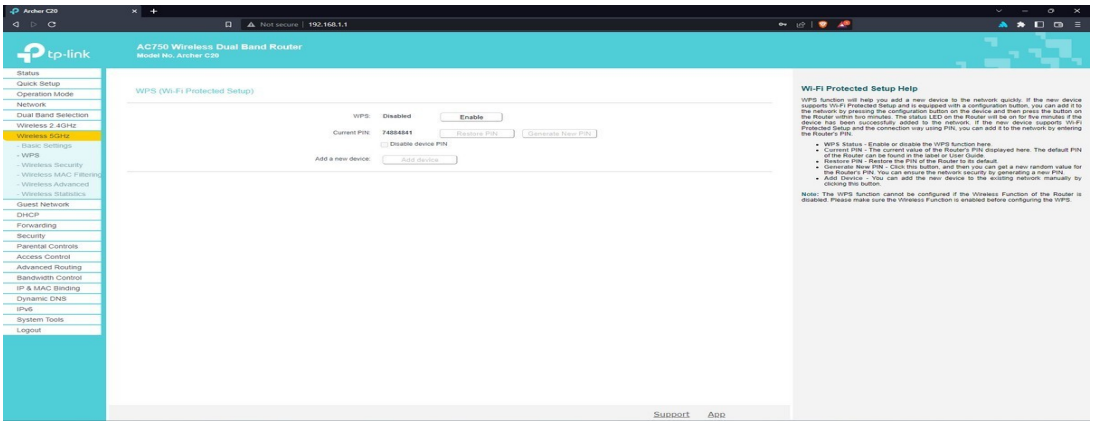
These are also integrated into the main SoC or may be separate chips on the printed circuit board. It also can be a distinct card connected over a MiniPCI or MiniPCIe interface. Some dual-band wireless routers operate the 2.4 GHz and 5 GHz bands simultaneously. Wireless controllers support a part of the IEEE 802.11-standard family and many dual-band wireless routers have data transfer rates exceeding 300 Mbit/s (For 2.4 GHz band) and 450 Mbit/s (For 5 GHz band). Some wireless routers provide multiple streams allowing multiples of data transfer rates (e.g. a three-stream wireless router allows transfers of up to 1.3 Gbit/s on the 5 GHz bands). Some wireless routers have one or two USB ports. These can be used to connect printer or desktop or mobile external hard disk drive to be used as a shared resource on the network.

A USB port may also be used for connecting mobile broadband modem, aside from connecting the wireless router to an Ethernet with xDSL or cable modem. A mobile broadband USB adapter can be connected to the router to share the mobile broadband Internet connection through the wirelessnetwork. Some wireless routers come with either xDSL modem, DOCSIS modem, LTE modem, or fiber optic modem integrated.

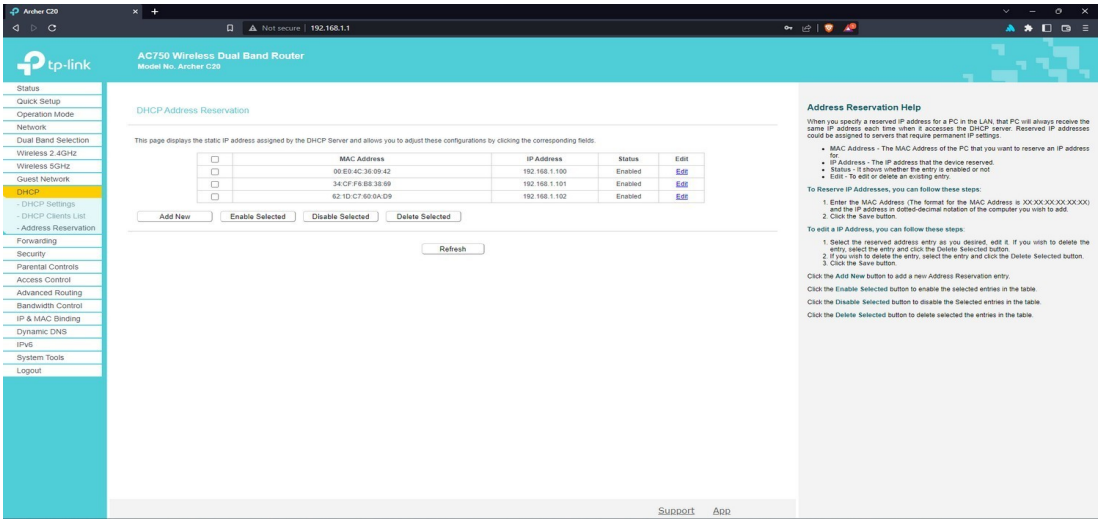
Local Login Page For Wifi Configuration



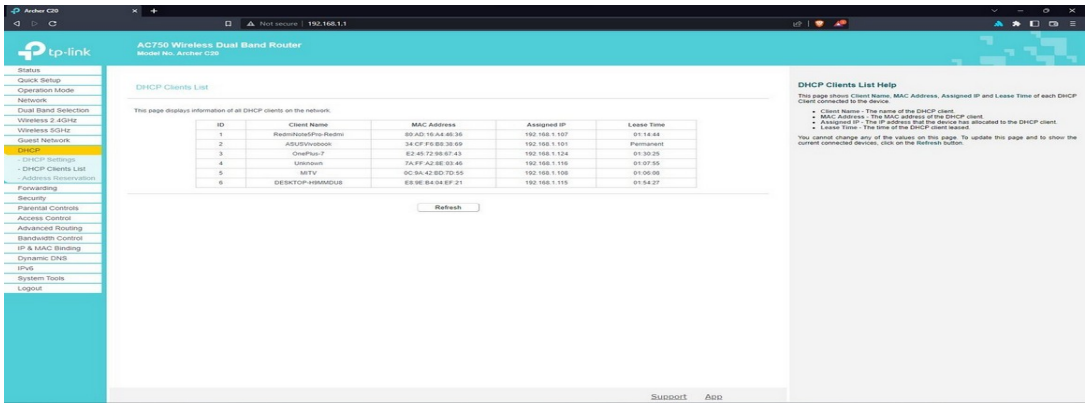
Disable WPS mode, No-one can brute-force on the SSID



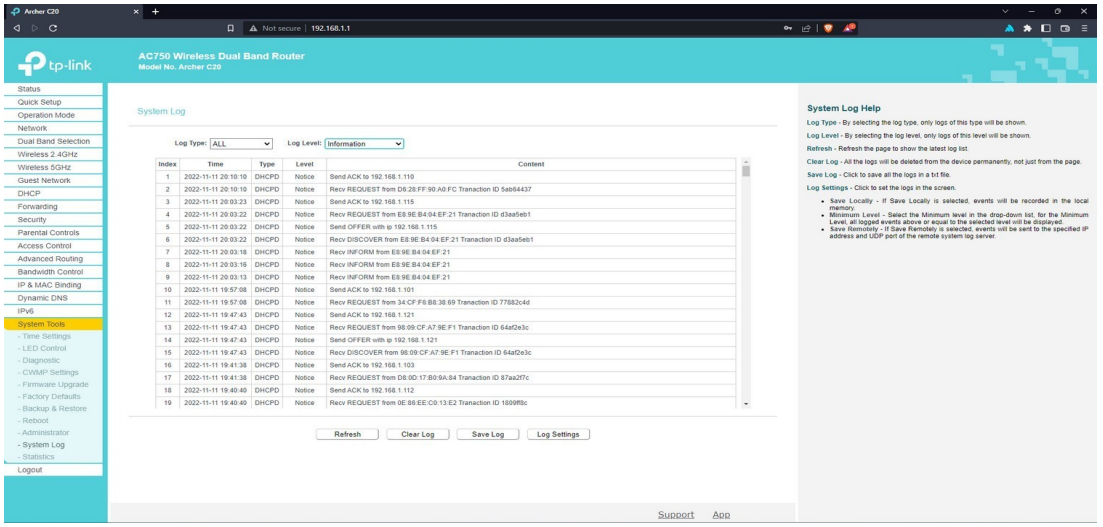
Displaying all devices connected to the network



Performing Address Reservation via MAC address



Making Check at System Log Files



CONCLUSION:

- Hence, by doing the basic configuration's in local Wi-Fi console we can prohibit the unauthorized and unethical use of network.

QUESTIONS:

1. Describe the process of building a wireless network.
2. How to ensure that Wi-Fi is Blocking Hackers?
3. Explain the modes of wireless security in brief.

MODERN EDUCATION SOCIETY'S WADIA COLLEGE OF ENGINEERING, PUNE

Fourth Year of Computer Engineering (2019 Course)

410247: Laboratory Practice IV
410244(C): Cyber Security and Digital Forensics

NAME OF STUDENT:	**CLASS: BE**
SEMESTER/YEAR: VII	**ROLL NO:**
DATE OF PERFORMANCE:	**DATE OF SUBMISSION:**
EXAMINED BY:	**EXPERIMENT NO:**

TITLE: Permanent Deleted Files

AIM/PROBLEM STATEMENT: Computer forensic application program for Recovering permanent Deleted Files and Deleted Partitions

OBJECTIVES:

- To understand various vulnerabilities and use of various tools for assessment of vulnerabilities

OUTCOMES:

- Identify various vulnerabilities and demonstrate using various tools.

PRE-REQUISITES:

1. Knowledge of C, C++, python programming
2. Basic knowledge of computer, network and security information

THEORY:

1. COMPUTER FORENSICS TOOLS

This section introduces a series of tools which can be used to restore a file and is used during the process of acquiring evidence.

1.1 Deleted Digital Data Restoration Tools

Restoration Tools are used to recover data that have been accidentally or intentionally deleted or corrupted. Depending on the software used, different features are available to perform the recovery of the data. However recovery of the data can only be performed if the file has not been overwritten on the disk space.

1.1.1 Data Recovery Pro

Data Recovery Pro software (Data Recovery Pro, 2018) is a free evaluation software which can be used to recover deleted files. To use the Advance features, the users need to make a purchase. For example, to recover a file, the user needs to register for this feature. The software provides the following features:

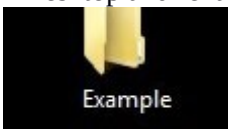
- Restoration of deleted email and deleted email attachments
- Recovery of files from a recently formatted or partitioned disk

● Restoration of a large variety of file types (Binary files or compressed files) Restoration of files from peripheral storage devices (such as USB) Recovery of Windows system files.

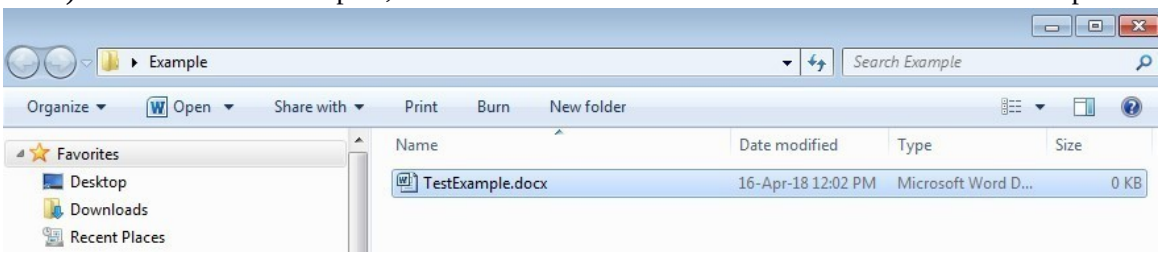
Below are screen shots of searching and recovering a deleted file.

2) Download and install the software from http://www.datarecoverydownload.com/download/

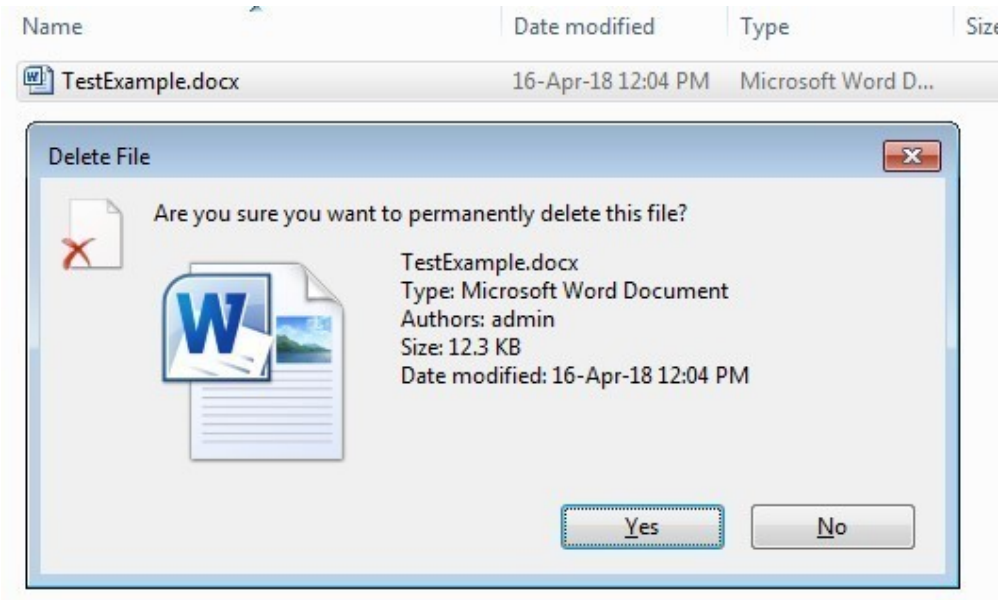
3) As an example, create a folder on your Desktop and rename it as “Example”.



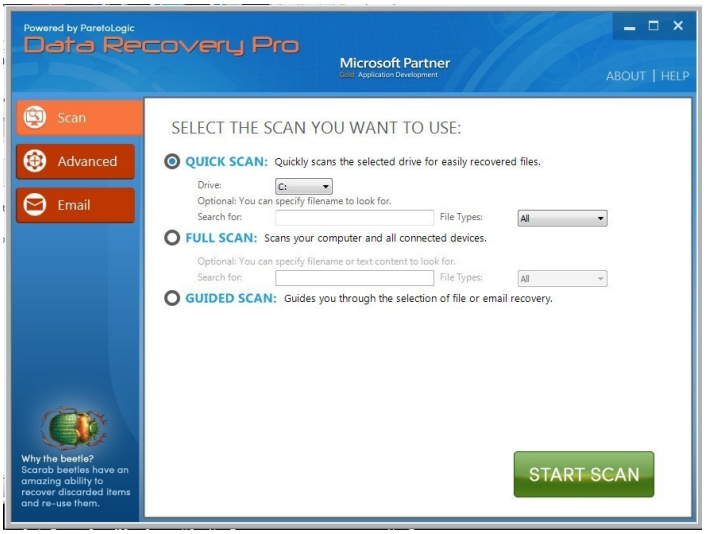
4) In the folder “Example”, create a Word Document file and name it as “TestExample.doc”.



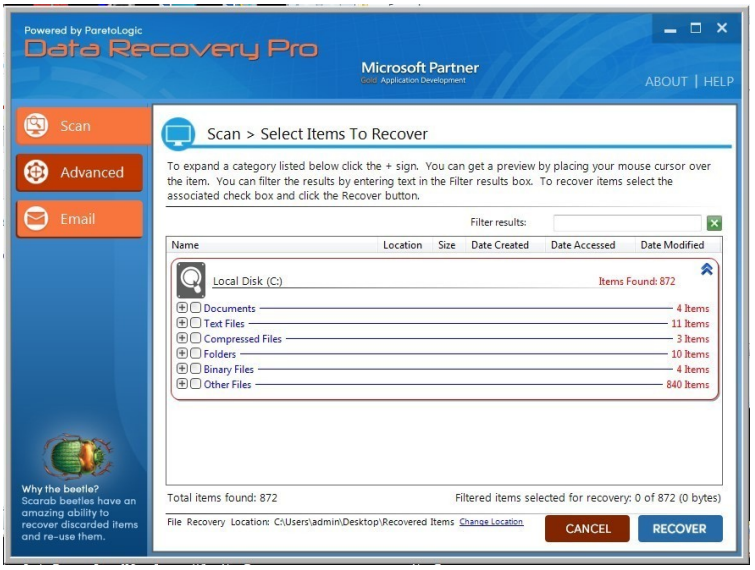
5) On the TestExample.doc, click on the file and press “Shift+Delete”



6) Press “Yes**”**. The file will not be sent to the Recycle Bin, and the folder Example will be empty. At this moment, we may think that we have “permanently” lost the file. However, at this stage we can still restore the file using the tool Data Recovery Pro. As mentioned, the file has an entry removed from the file allocation table and is still on the disk space unless the file is overwritten. To recover the file, run the program Data Recovery Pro.

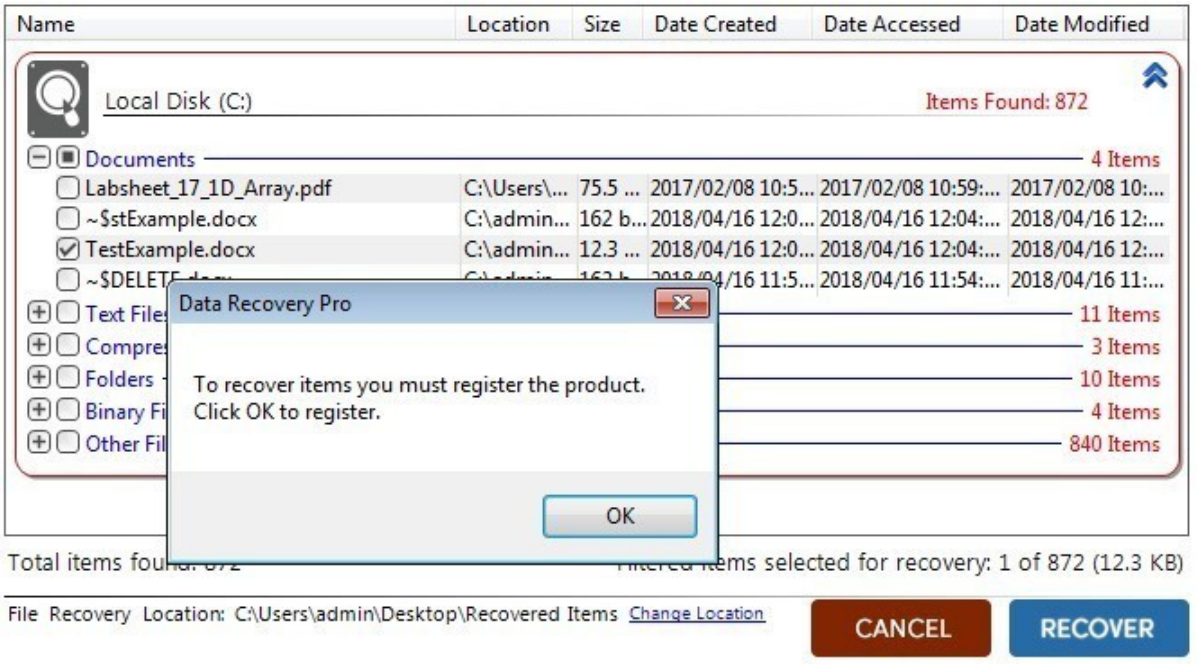


7) Press “Start Scan”. After the software has scanned the disks, the following screen will be presented:



8) Expand the “Documents” and the TestExample.docx will be available.

9) Click on TestExample.docx and press the button “Recover”. Since we are using a free version, this feature will not be available until we register the product. But we have illustrated how tools can recover deleted files.



2. DELETED PARTITIONS RECOVERY

Dividing a hard disk into different volumes is known as partitioning. Each partition is labelled as a drive letter by the operating system and becomes a logical drive as shown in Figure 3.8. Each logical drive can be formatted to support different operating systems as well

as to use different file systems (either FAT16, FAT32, NTFS). Partitioning is performed for increased performance and management of data. For each partition created, an entry is performed in the partition table. Therefore when a partition is deleted, the entry is removed from the partition table (and the space becomes unallocated). To restore the partition, forensic software tools can be employed. Those tools usually search for the boot sector in order to restore the partition. This section introduces some of the tools used to restore a partition.

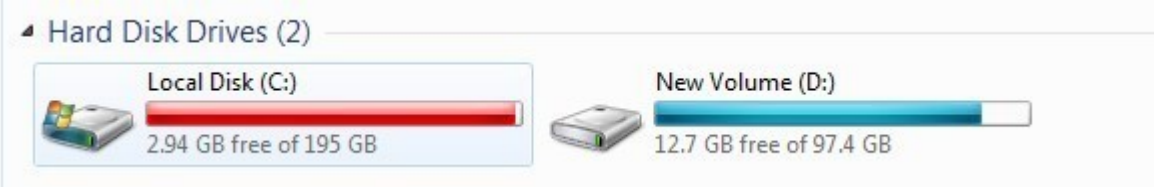
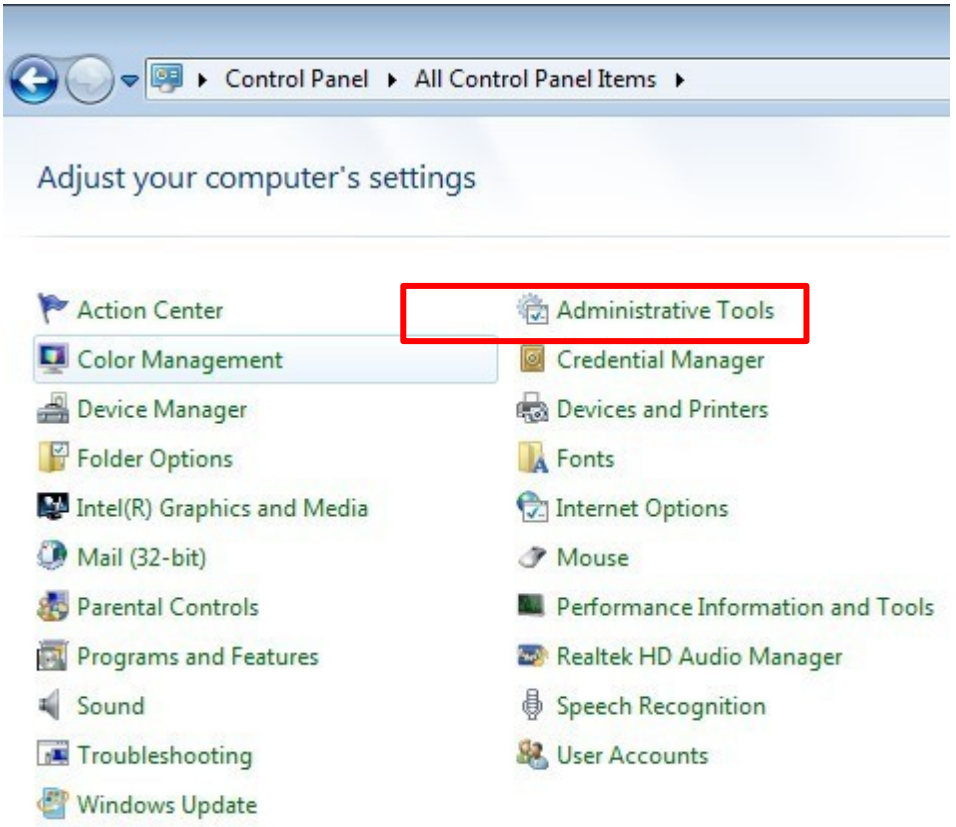


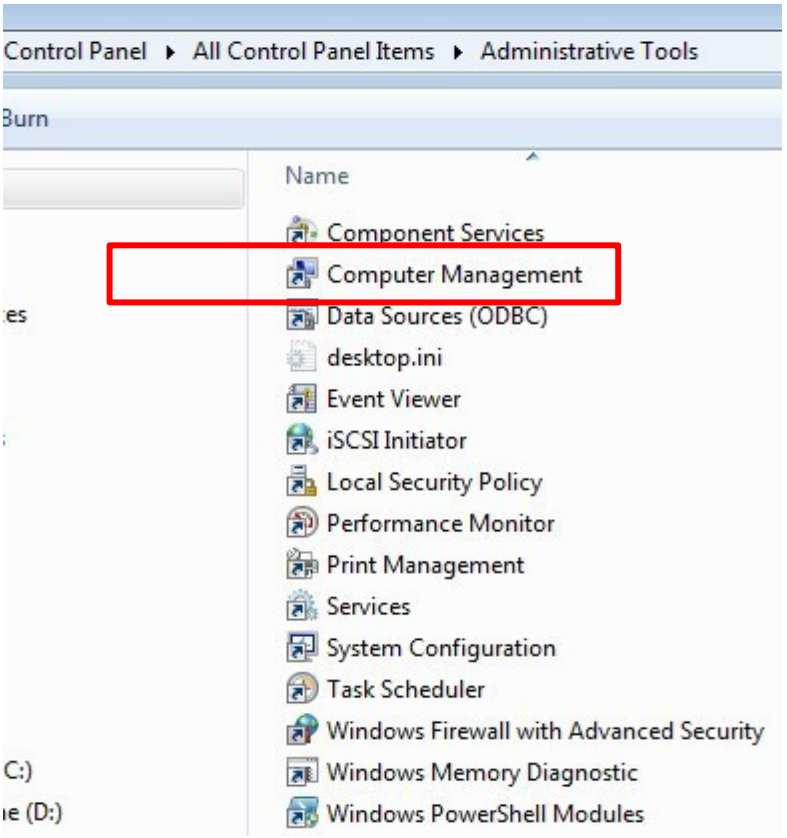
Figure 3.8

To manage and view the partitions on a hard disk in Windows, follow the steps below:

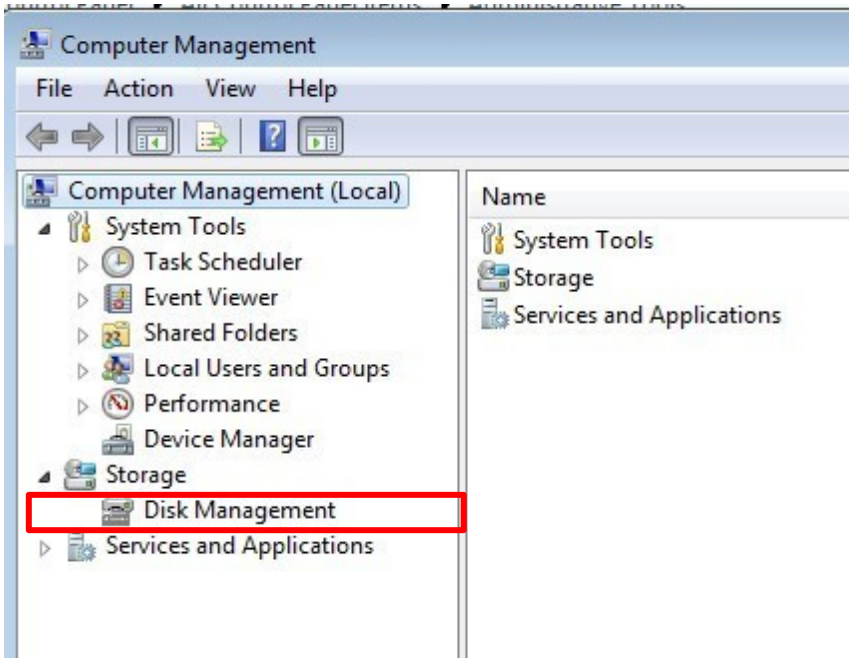
- Go to Control Panel
- Select Administrative tools



□ Click on“Computer Managem”.ent

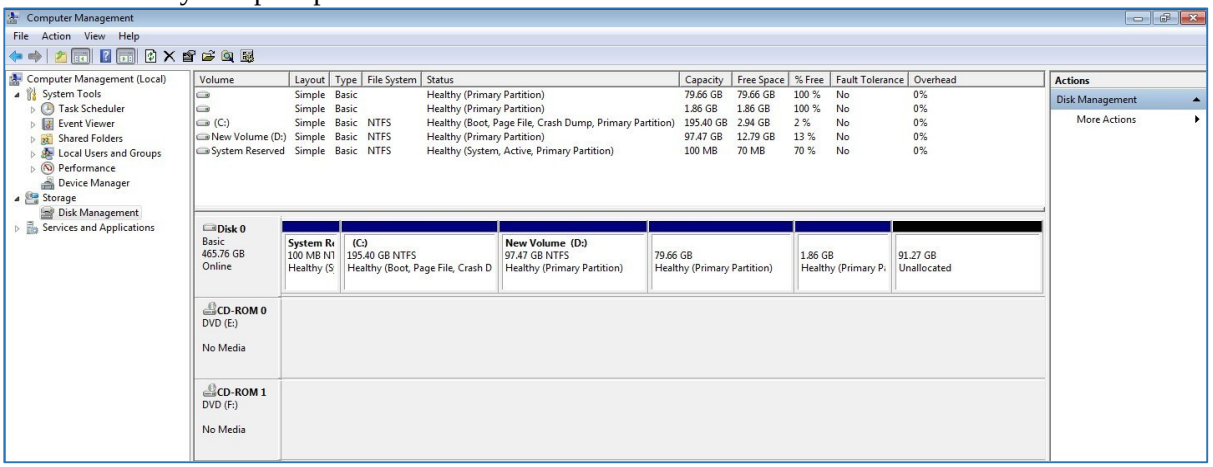


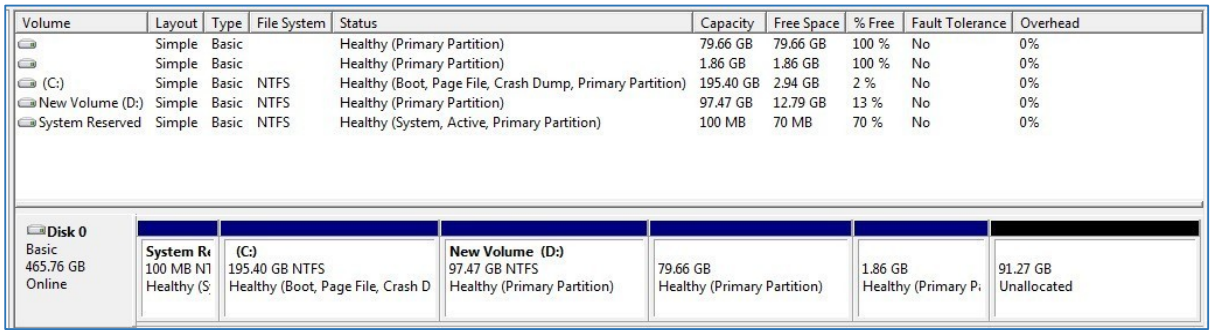
- Select “Disk Management”.



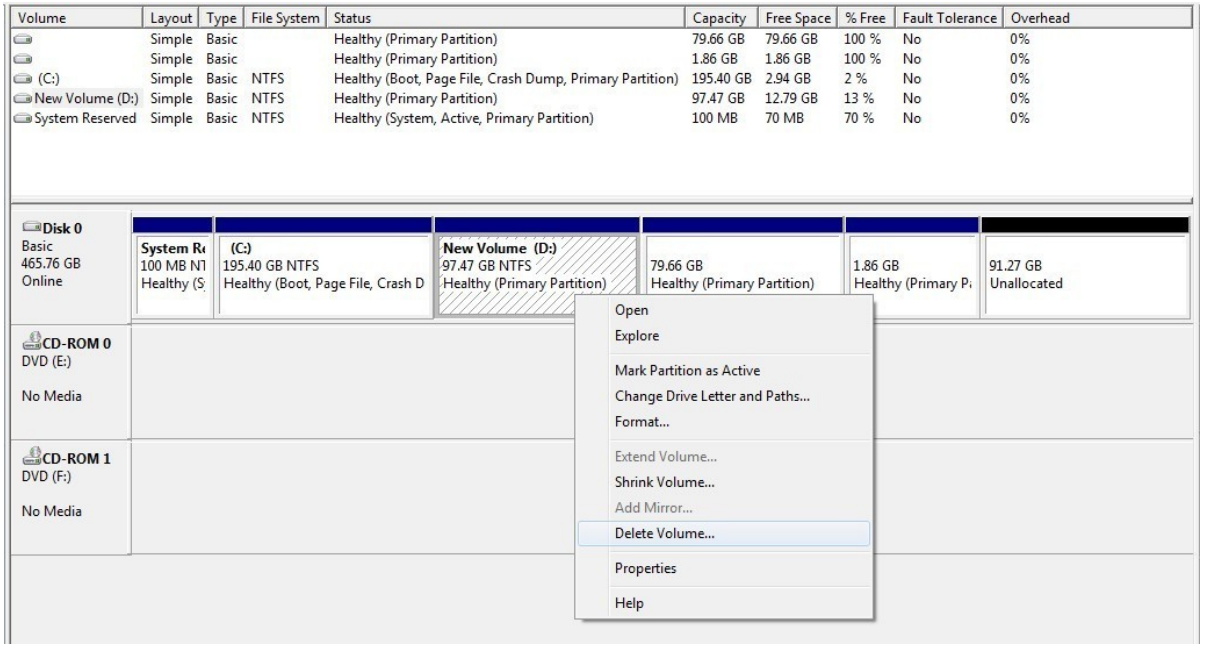
- Upon clicking on “Disk Management”, the utility will show all the logical drives available and their properties. In this example, there are five partitions (System Reserved, C:, D:, two healthy partitions and an unallocated partitions). The C: logical drive is the Boot volume, that is, it contains the files to start up the computer. The C:

logical drive is also the Page File and Crash Dump volume, meaning that it contains all the memory dump output.





- To delete a partition, Right-Click on the “volume” and select “**Delete”**. As stated earlier, deleting a partition or volume, does not necessary mean that the partition has been permanently removed. It can still be recovered through the use of computer forensics recovery software.



2.1 Deleted Partitions Restoration Tools

When a partition or volume is erased/deleted, the entry in the partition table is removed. Removing an entry from the partition table does not mean that the partition has been purged permanently. The partition may still be available on the disk. The partition can be recovered through the use of partition recovery software tools as long as the partition has not been overwritten on the disk space. The main thrust of the partition recovery software tool is to find the boot sector of the deleted partition and restore the partition by making an entry in the partition table. This section will highlight some of the partition recovery tools by computer forensic analyst to recovery deleted partitions.

2.1.1. EaseUS Partition Recovery Wizard

EaseUS (EaseUS, 2018) is a partition recovery tool used to restore deleted partitions. This tool scans several areas in the disk to search the location of the deleted partition. The software recovers deleted, lost and damaged FAT, NTFS, HFS, HFS+, HFSX, Ext2, Ext3 partitions under Windows.

Conclusion: Thus we have coded computer forensic application for Recovering permanent Deleted Files and Deleted Partitions

Questions:

1. List some of the softwares for recovering deleted files?
2. List some examples of file systems

MODERN EDUCATION SOCIETY'S WADIA COLLEGE OF ENGINEERING, PUNE

Fourth Year of Computer Engineering (2019 Course)

410247: Laboratory Practice IV
410244(C): Cyber Security and Digital Forensics

NAME OF STUDENT:	**CLASS: BE**
SEMESTER/YEAR: VII	**ROLL NO:**
DATE OF PERFORMANCE:	**DATE OF SUBMISSION:**
EXAMINED BY:	**EXPERIMENT NO:**

TITLE: Honeypot

AIM: Study of Honeypot.

OBJECTIVES:

- To understand various vulnerabilities and use of various tools for assessment of vulnerabilities

OUTCOMES:

- Identify various vulnerabilities and demonstrate using various tools.

PRE-REQUISITES:

1. Knowledge of C, C++, python programming.
2. Basic knowledge of computer, network and security information.