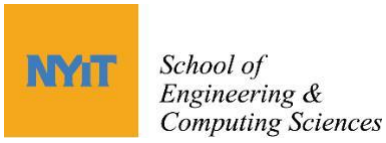
New York Institute of Technology



School of Engineering and Computing Sciences

Computer Forensics

Project Final report

Submitted by,

Avinash Muppavarapu

Your Incident Scenario

SBS is a Canada wide leader in providing exquisite datacenters for small scale industries in Vancouver, Canada. Established in the year 2005 comprising 500 employees. The company deals with multiple domains like website designing.

It took one of the projects for a NashInfo Pvt.Ltd to design a website. Company decided to handle that project to a team of 10 members. The tasks were divided into three main areas- Architecture & design, Developing & coding, and Testing. They have assigned 4 people for architecture & design, 4 people for Developing & Coding and two people for Testing. One day IT security guy found that there is fraud alert from the Testing workstation notified that an email has been sent from testing department workstation to a strange email address which is not link to the company's email address. IT security guy was reported this situation to the HR Manager and IT Manager immediately. They get to know the suspected employee was on leave from past three days and the data which was leaked from the system related to the present project i.e, design of a website for the NashInfo pvt.ltd.

In this scenario, we are going to investigate on the following tasks.

a. Who are involved in this data theft and Cybercrime.

b. To whom they sent the email.

c. What information they emailed and deleted.

Detailed Forensic techniques and tools

For the recovery of the data which was deleted. We use the EaseUS Data Recovery Tool to recover the deleted file.

Email information and to whom the email was sent for these findings we use the MBOX File Viewer tool.

In our investigation process we found that intruder send the file in different format that is not in the scenario we submitted previously. The Intruder changed the file from one format to another and send to outside. To find that data file we use Autopsy tool.

Your findings by forensic analysis

According to our Project initial report. We need to perform the following tasks.

In this scenario, we are going to investigate on the following tasks.

a. Who are involved in this data theft and Cybercrime.

b. To whom they sent the email.

c. What information they emailed and deleted.

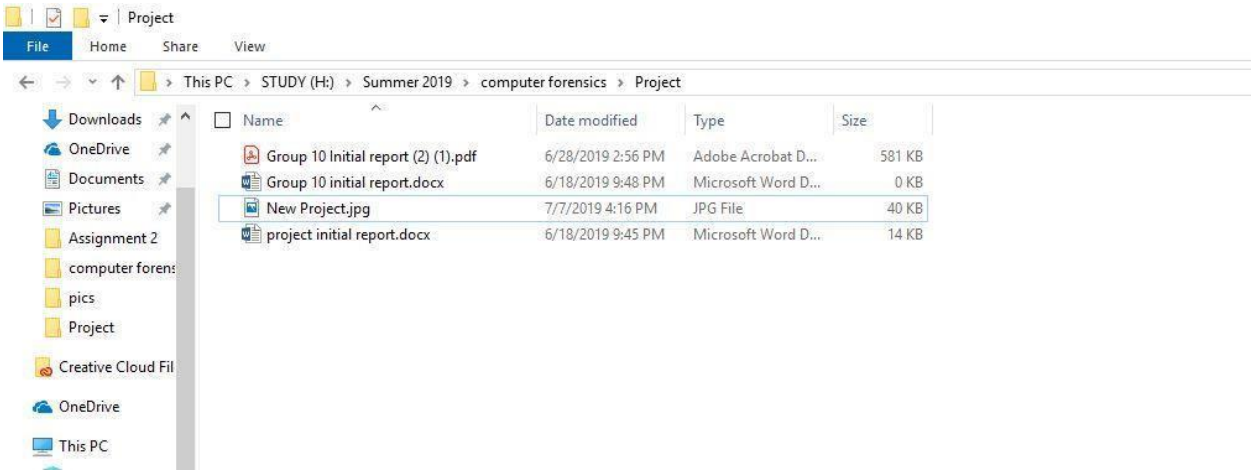
In our investigation process of the data theft and deletion of the project data in SBS company we find the Intruder who sent the data from the company to outside. The person name is ‘Nash’ he misused his responsibilities and sent company’s information to outside. He sent an email to outside which contains the confidential information of Nashinfo Pvt ltd web page which is the present project going for the SBS company. After he sent the data, he deleted the project file which was in the final stage of testing. He is the junior test engineer in SBS Company. When senior testing engineer was not at the site. He took the project for few days till the senior engineer take over that project. He got full access to the project. In the mean while he took this as an advantage and send the project file to outside.

He also changed the format of project file and send it to outside of the company.

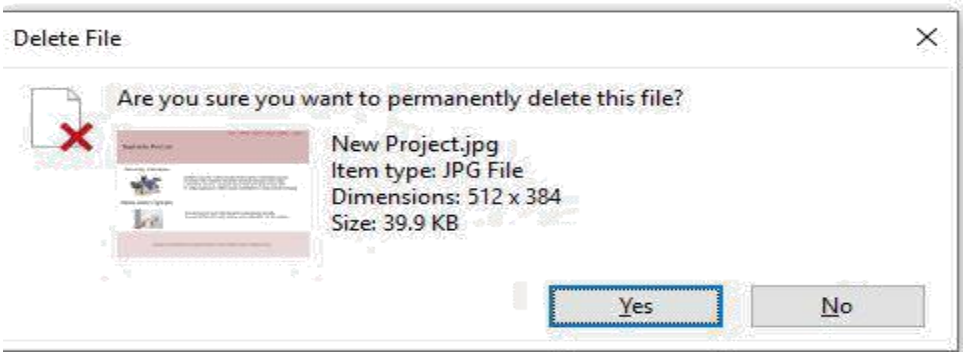
Here we attach the findings we came through in our investigation process.

a. Data Recovery

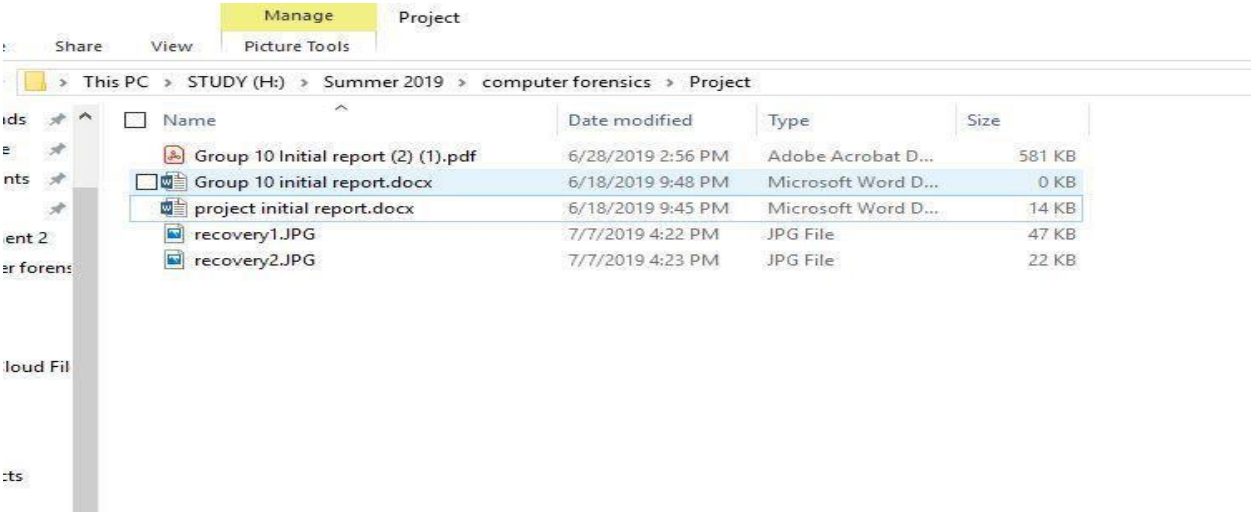
New project is the file which was deleted by the person who involved in the crime.



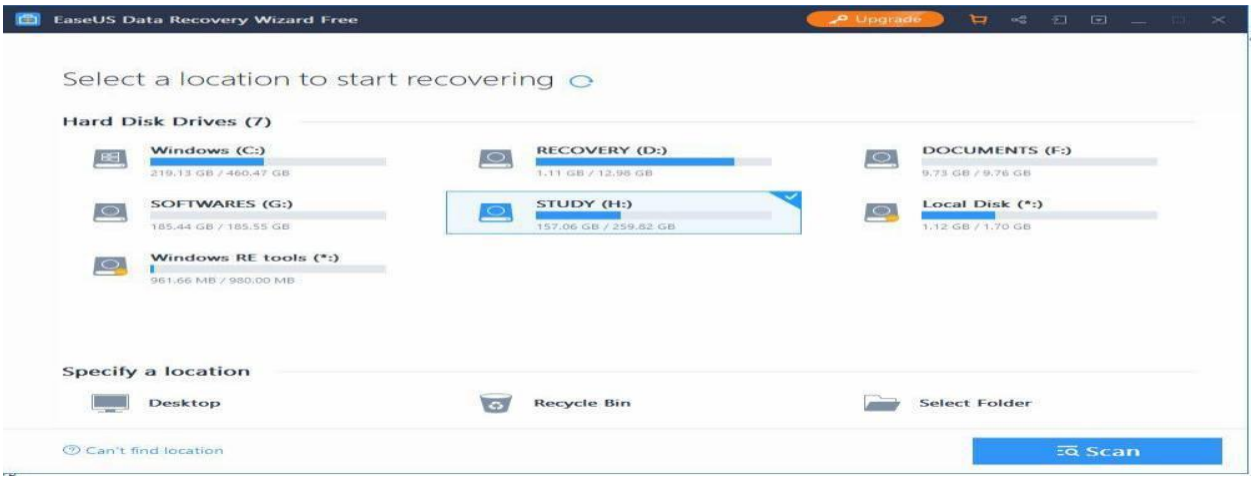
He permanently deleted the file from the system.



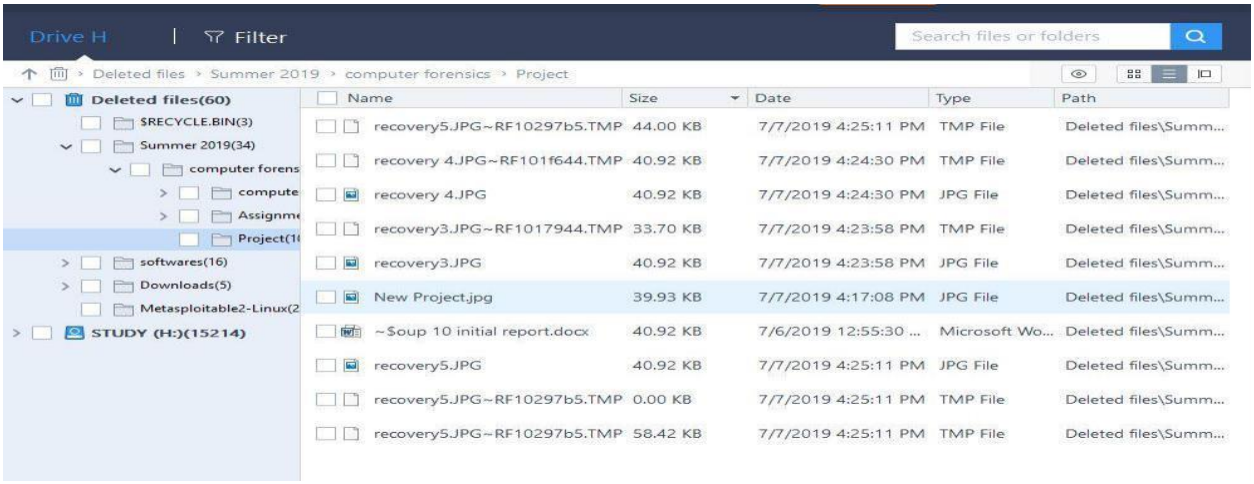
The file was deleted from the drive.



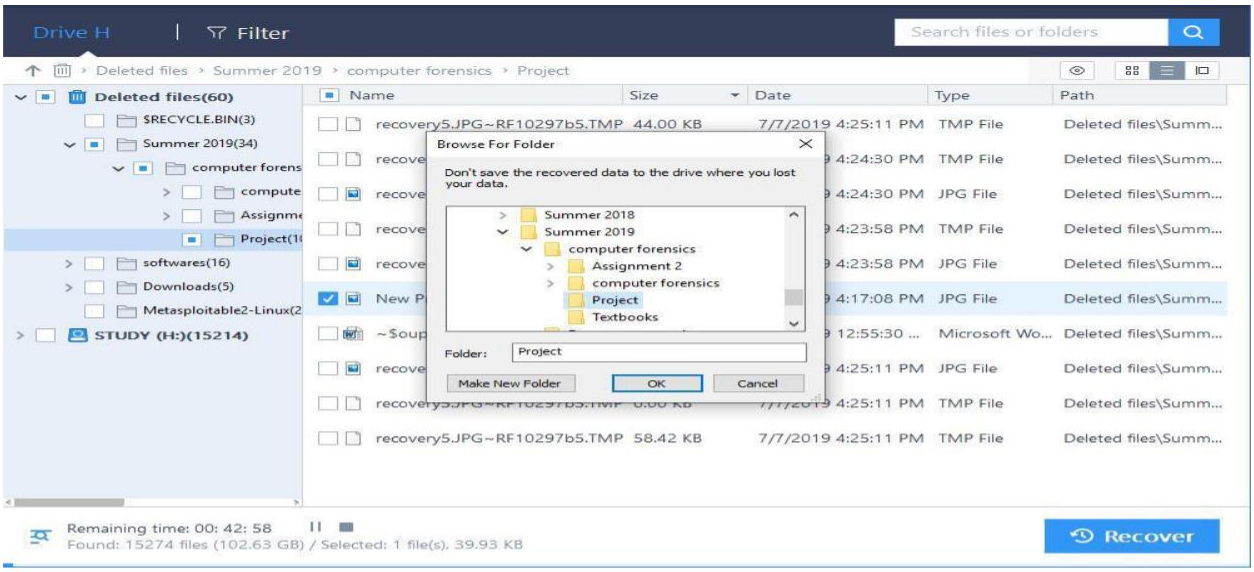
According to forensics, the file doesn't delete permanently. It will store as a pointer in unallocated space. So we scan the drive to recover the deleted file.



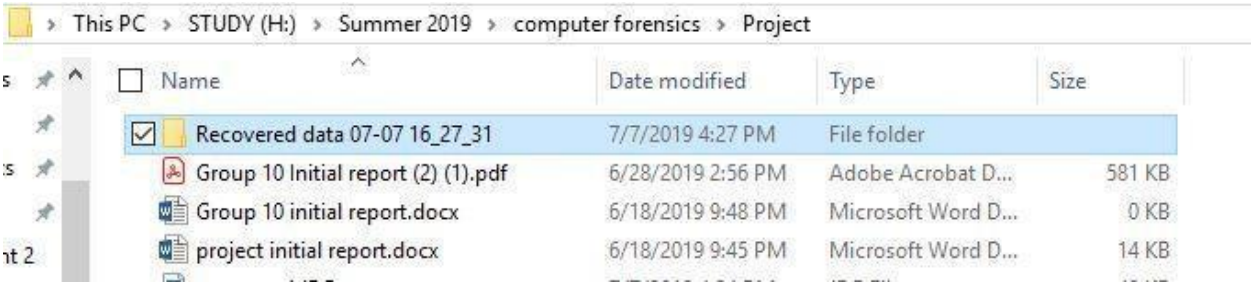
We found the New project image file was deleted as shown in the below fig.



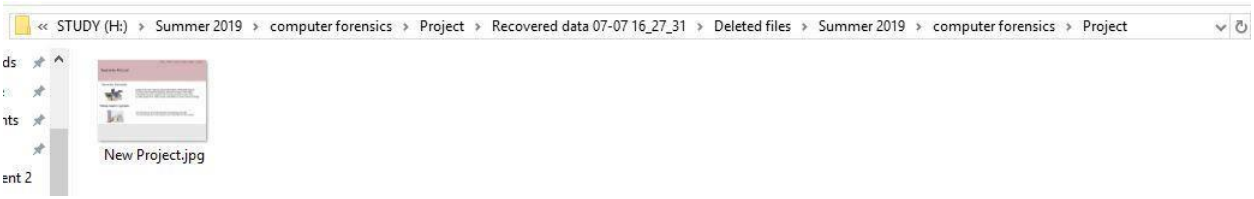
We recover the file to the destination.



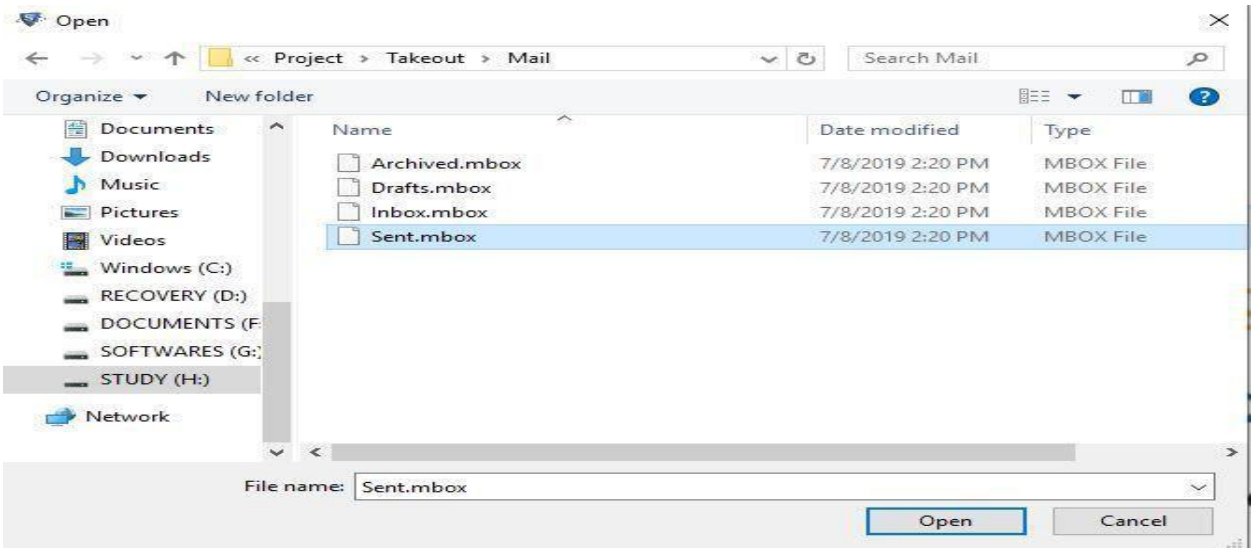
This below fig shows the recovered data file.

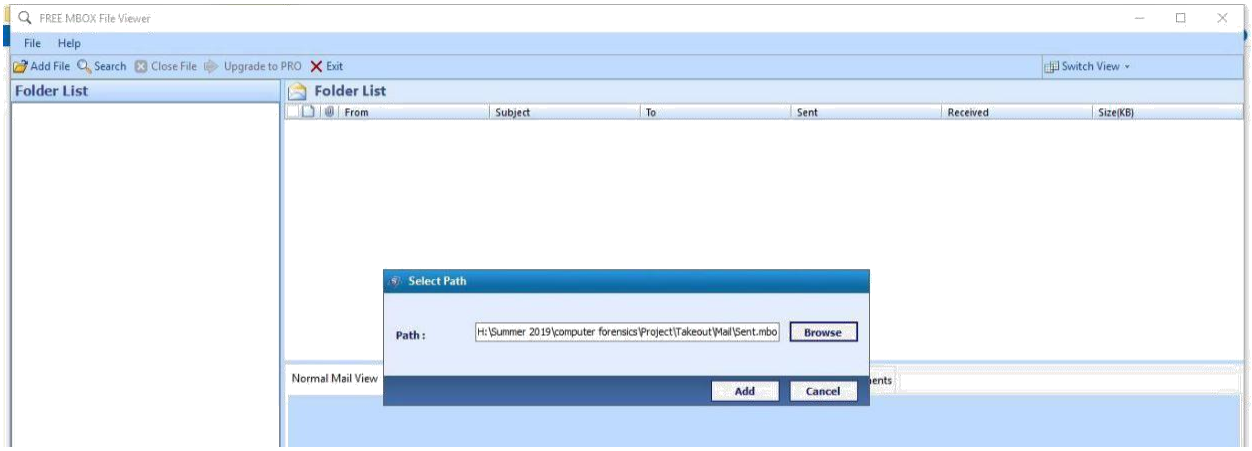


The below fig shows the deleted file New Project.jpg



b. To whom the email was sent





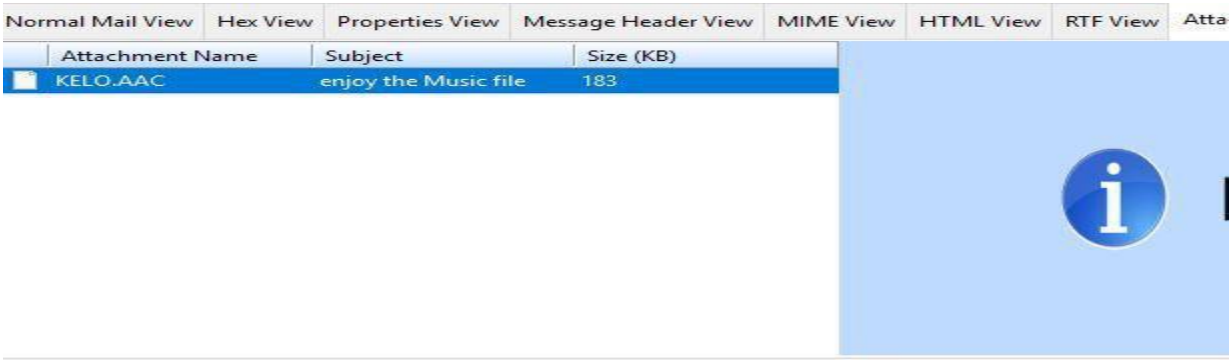
By using Mbox viewer we saw the person who sent the mail to whom

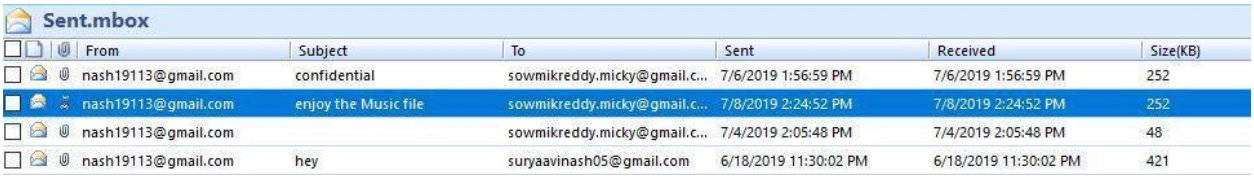
From: Nash
To: Sowmik.
Date and Time: 7/8/2019 2:24 PM

C. Email Header

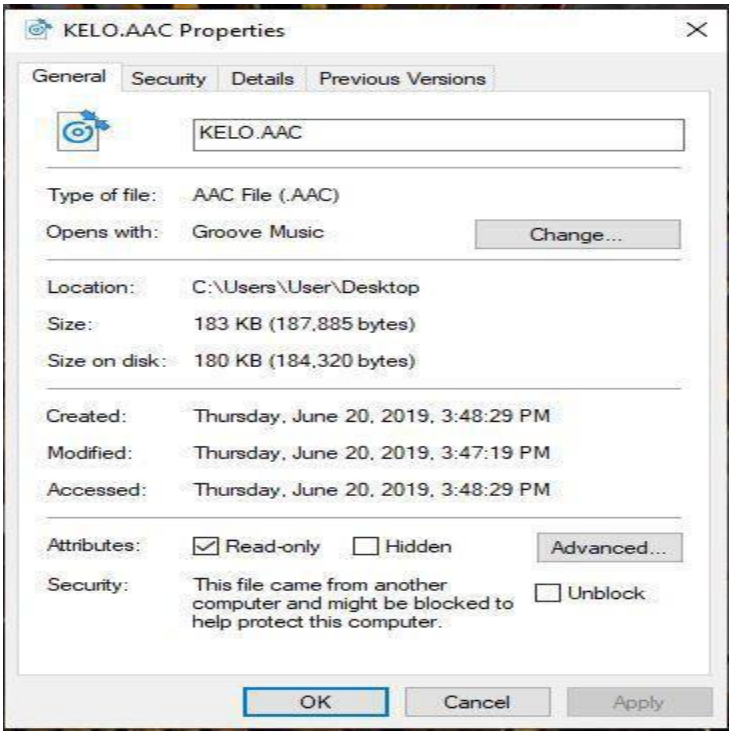
D. What information they emailed and deleted.

Kelo.AAC is the file sent to the outsider.

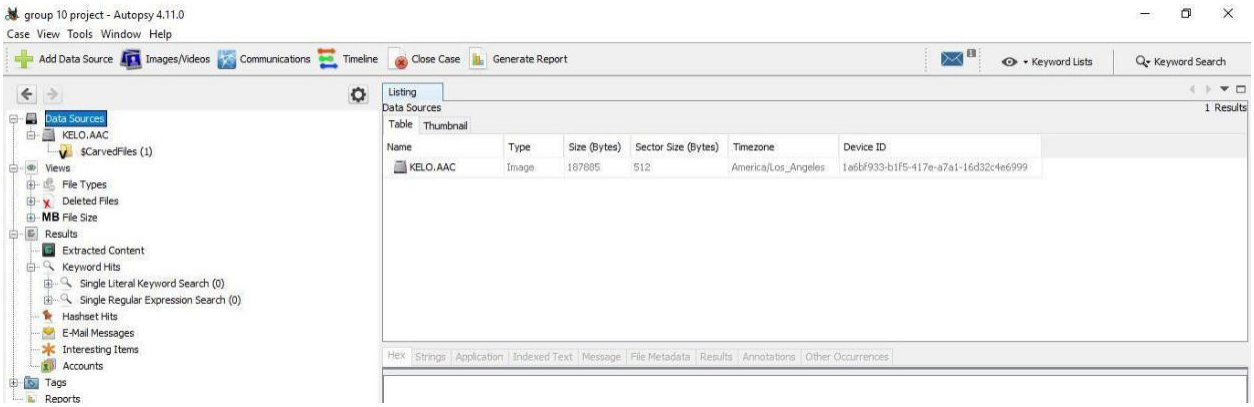




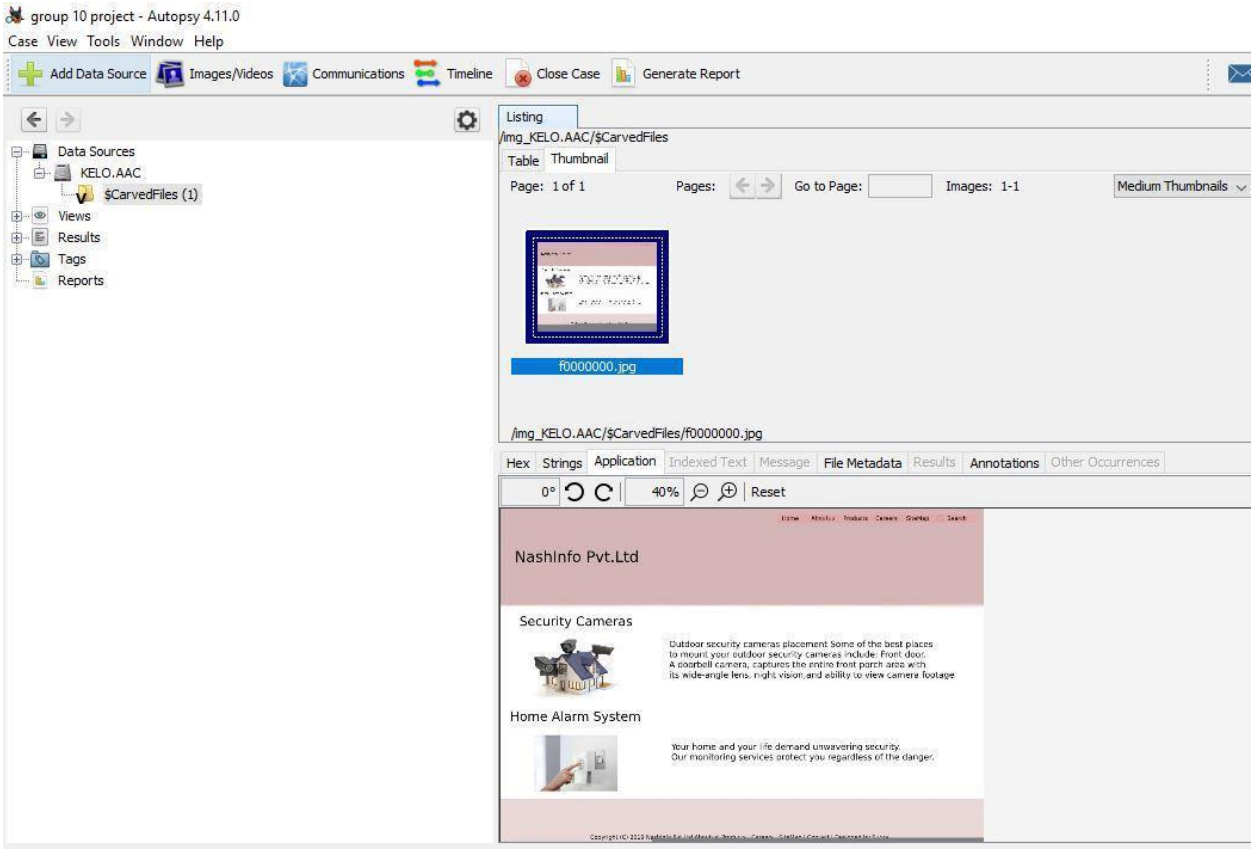
By using Autopsy tool, we find the attachment he sent to outside.



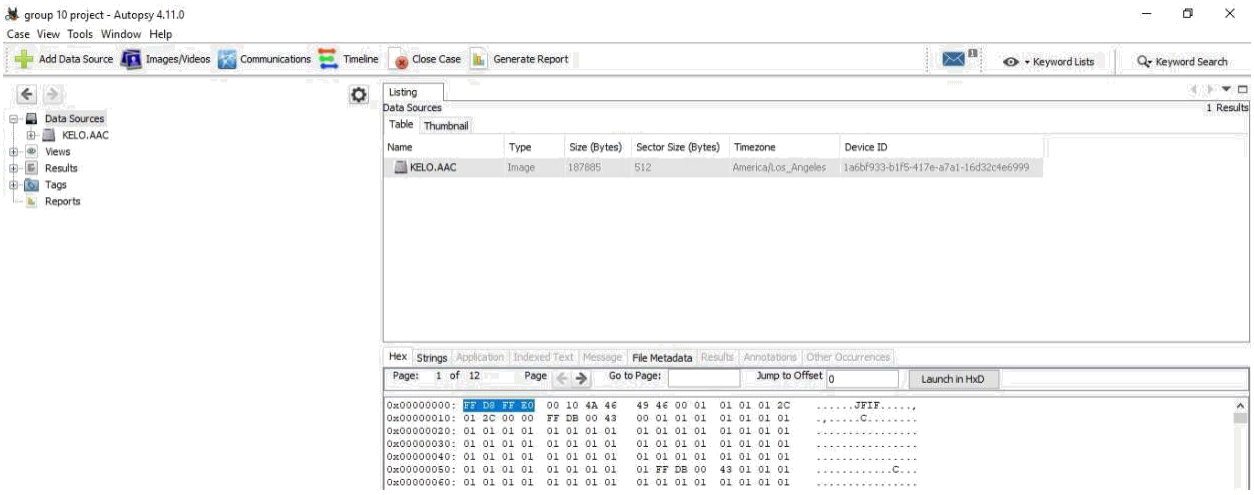
We attached the Kelo.aac to data source in autopsy to find the original data.



In the carved files it shows the file that was New project.jpg

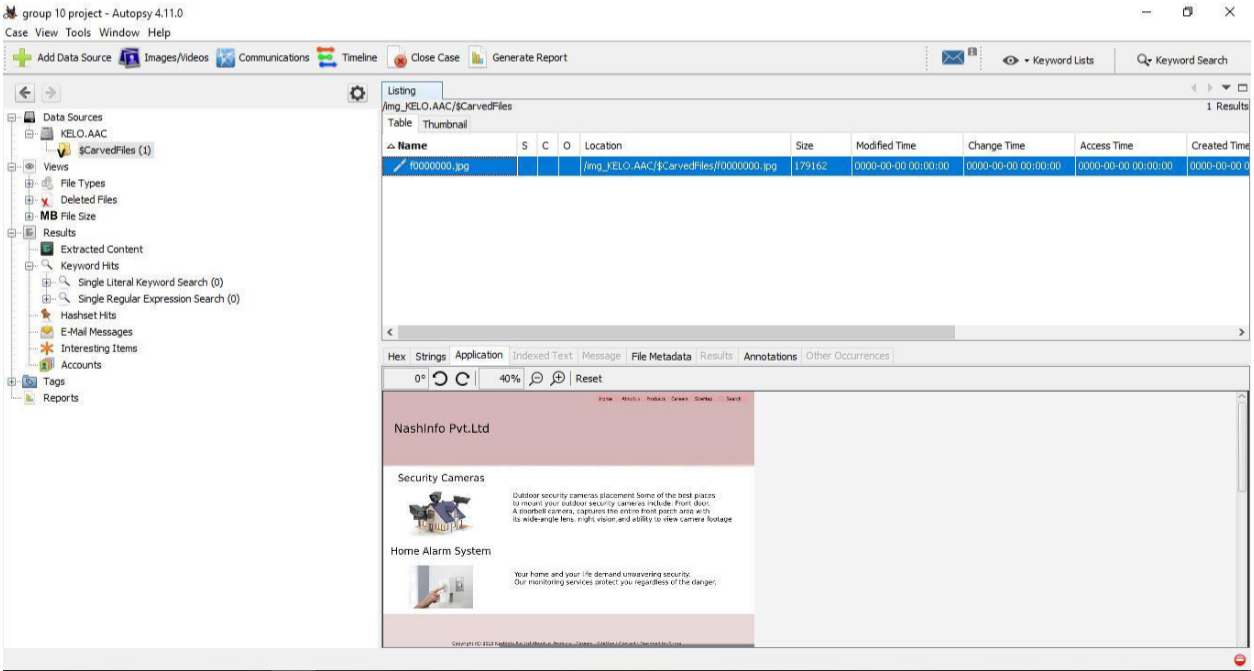


The below fig shows the hex value of the file FF D8 FF E0



According to file signatures the hex value shown in the above fig is the JPEG file.

FF D8 FF DB	ÿØÿÛ	0	jpg jpeg	JPEG raw or in the JFIF or Exif file format
FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿà..JFIF..			
FF D8 FF EE	ÿØÿî			
FF D8 FF E1 ?? ?? 45 78 69 66 00 00	ÿØÿá..Exif..			



Description of how your findings could solve the challenge or issue.

From the above findings of our investigation process we solve the issue faced by the SBS company. We found the person who sent the email to whom and we found the file which was sent to the outsider and recovered the deleted file. We gave the report to the SBS company that ‘Nash’ is the person who convicted the crime and we found the person who is on the other side of the crime. We solved the case by finding two people who were involved in this crime.