Steps in Email Investigation/Analysis

- Examine the email
- Copy the email
- Print the email
- View the email headers
- Examine the headers
- Examine attachments
- Trace the email

Laws against Email

- The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, also known as the CAN-SPAM Act, was set up to protect consumers from unsolicited emails, regardless of bulk spam emails or commercial emails, from brands and businesses
- Seven requirements

Messenger Forensics

Yahoo messenger

- Similar like window registry
- Yahoo messenger registry
- Investigator try to find out the yahoo user ID
- Version of ym
- Save password
- Windows vista as P2P
- User\software\yahoo\pager\profiles\profile_name\chat ---→location of chat room

Yahoo messenger

Yahoo! Registry at a Glance for Windows Vista and 7

File	Location	Description	XP[1]	Vista	Windows 7
HKEY_CURRENT_USER	\Software\Yahoo\Pager\	Gives User ID	Yahoo! User ID	Yahoo! User ID	Yahoo! User ID
		Gives the installed version	N/A	Version	Version
		Gives the version revisions	N/A	VersionRev	VersionRev
		Shows if the password is saved	Save Password	Save Password	Save Password
		Shows if auto sign in is turned on or off	N/A	Auto Login	Auto Login
		Number of P2P users	N/A	P2P count	N/A
HKEY_CURRENT_USER	\Software\Yahoo\pager\profiles\screenname\Chat	Gives the last selected chat room category	Chat (Rooms visited or created)	Chat	Chat
HKEY_CURRENT_USER	\Software\Yahoo\pager\profiles\screenname\Chat\Favorite Rooms	Gives the list of saved favorite rooms for the user	N/A	Favorite Rooms	Favorite Rooms
HKEY_CURRENT_USER	\Software\Yahoo\Pager\profiles\screenname\FT	Location of last received file and last sent transferred file	File Transfer	FT	FT
HKEY_CURRENT_USER	Software\Yahoo\Pager\profiles\screenname\FriendIcons	Location of user icon displayed to friends	N/A	FriendIcons	FriendIcons

YM

- User\software\yahoo\pager\profiles\profile_name\chat\favorite_rooms
- User\software\yahoo\pager\profiles\profile_name\FT
- Photo sharing -creation of S folder
- 2 ways of sharing photo
- 1. yahoo photo sharing
- 2.file transfer option

Social Media Forensics

- Collect evidences
- Built cases
- Use pics
- Personal information ascertains character
- 80% people
- FB
- LI
- TW

Social media Forensics

- YT
- IG
- Reddit
- Gathering Evidence for court

Relevant statements

Metadata from post

Past illegal activity

Photos

Content

association

SMF

- Employment Checks

  to assess your character, work experience & education
- Credit reporting

<u>Types of evidences</u>

Posts and photos –drug use

Posts relating to objectionable content(eg:-racist)

Education & employment

SMF

- Person Location

  from metadata posts

  from images

Statement and laims

Photo analysis

Interviews and social connections

Tool----for SMF-----Screencast-O-Matic