Disclaimer –

• This document is not a substitute for existing manuals available in the States/UTs. It is only a guide for awareness purpose. In case of any conflict, local manual/practice may prevail.

• BPR&D does not promote any tool/software of a particular vendor. All the tools and software mentioned in this manual are for illustration purpose only.

• Wherever any image/graphics/flowchart is taken from other sources, the same has been duly acknowledged.
संदेश

बहुत ही बात है कि पुलिस अनुसंधान एवं विकास ब्यूरो, ने साइबर उत्पीड़न के मामलों से नंपटने के लिए "साइबर उत्पीड़न जांच का््षप्रवाह नन्माविी" तैयार की है। ऐसे मामलों से नंपटने के लिए, वह मैनुअल जांच अधधकारर्ों का व्ापक मार्षदर्षन करेरा।

अंतरालिक सुरक्षाओं एवं विविध लक्ष्यों की बढ़ती उपवधाओं और लोकन नीतियों के उपयोग की लोकप्रियता से भी ही एक तरीक़े में, वर्तमान में, साइबर उत्पीड़न के मामलों में बहुत युग्द हुई है। साइबर अपराधियों के बढ़ते प्रयोग और स्थिति को अपने आप बना रहे हैं। यूनियन, नैतिक बने, धर्मांडों और अंतरालिक अंतरालिक सामाजिक किंकत्र के साथ-साथ उपवधाओं एवं आतंकी से भी प्रभाव पड़ता है, जिसका साह समाज को युक्तियां उठाने पर है। फिरस्त उपवधाओं से ही इस क्षेत्र में आंतरिक बनाम जम्मू नंपटने को लिये है।

शर्म सरकार ने, भारतीय साइबर अपराध लक्ष्य सर्वेक्षण (I4C) पटक और महहिाओं एवं बच्चों के खिलाफ साइबर अपराध दोषी (साइबरपीडा, पीडेी) प्रशासन, के माध्यम से महहिाओं और बच्चों के खिलाफ साइबर उत्पीड़न से नंपटने के लिए कब्जा किया है।

वह प्रशासनिक पुलिस अभीचार एवं विकास ब्यूरो द्वारा इस गढ़ गठन गठन प्रभावों का परिणाम है। इसके प्रकाश नंपटने के लिए समाज को महहिाओं और बच्चों की सुरक्षा और कल्याण मुखरबनाने के तत्काल संबंध में साक्षातक रूप से सामाजिक दोस्ती बढ़ाए।

अमित शाह
AMIT SHAH
Home Minister
India
I extend my appreciation to the Bureau of Police Research and Development for preparation of the ‘Investigative Workflow Manual on Cyber Harassment Cases’. The manual will prove to be a crucial step towards professionalisation of cyber investigation.

Life is becoming technology driven, be it entertainment, communication, transactions or any other dimension, dependence on IT has risen manifold.

While on one hand, platforms like Facebook, Instagram, Twitter etc. have democratized communication, they have brought to forefront a serious predicament of "cyber harassment". These platforms are widely used by cyber criminals to trap soft targets by using cyber techniques for financial gains and other forms of blackmail.

The need of the hour is to equip our first responders with a structured workflow to ensure speedy action and efficient redressal. The workflow manual will improve responsiveness, productivity and provide officers with a faster and more accurate way to approach cyber harassment cases.

The National Cyber Crime Research and Innovation Center under the Union Home Ministry has established the National Cyber Crime Research, Innovation & Capacity Building lab at the CDTI Hyderabad. The focus of the Center is to improve investigation & evidence collection skills of the officers.

I congratulate the BPR&D for this endeavour. A structured and professional approach will go a long way in curbing this menace.

(G. Kishan Reddy)
I am happy to note that the Bureau of Police Research and Development (BPR&D) is publishing an “Investigative Workflow Manual on Cyber Harassment Cases” for law enforcement agencies to effectively investigate and combat crimes involving cyber harassment.

2. States/UTs are primarily responsible for prevention, detection, investigation and prosecution of cyber crimes through their law enforcement machinery. However, cyber crime investigation, in a large number of cases, has inter-state and international ramifications and requires an enabling ecosystem for successful investigation. The Ministry of Home Affairs has launched the National Cyber Crime Reporting Portal which will help in reporting social media related crimes besides others.

3. To meet the challenges, the Union Home Ministry has also rolled out the ‘Indian Cyber Crime Coordination Centre (I4C)’, a scheme to combat cyber crime in a holistic manner. One of its components, the National Cyber Crime Research & Innovation Centre has been assigned to the BPR&D to identify emerging cyber threats and crimes and to proactively find R&D solutions by involving academia/institutions, start-ups and incubation centres.

4. I congratulate the BPR&D for the painstaking efforts in preparing the Investigative Manual which will go a long way in enabling investigation officers to play an effective role in cracking complex cyber harassment cases and, ultimately, curbing the menace.
The setting up of the National Cyber Crime Research & Innovation Centre (NCR&IC) at the BPR&D Hqrs. and its branch, the National Cyber Crime Research, Innovation and Capacity Building Centre, at the CDTI, Hyderabad, has been a major technological milestone in the cyber research and training capabilities of the BPR&D. The NCR&IC, as part of the umbrella scheme of the Indian Cyber Crime Coordination Centre (I4C), MHA, has been striving continuously to strengthen and augment the capacity of Law Enforcement Agencies (LEAs) in their efforts of cyber crime prevention and investigation.

To address the urgent need for protection of women and children from the scourge of cyber harassment, the ‘Investigative Workflow Manual on Cyber Harassment Cases’ has been brought out by the NCR&IC. It has been developed as a self-learning guide for hands-on training on the latest software tools, keeping in mind the skill set required by the concerned police officers. It deals with various facets of investigation, right from crime scene management to step-by-step detection methods and collection of evidence to prosecute the perpetrators.

This manual is a result of the sincere efforts of Sh. Karuna Sagar, IPS, IG/Director, Modernization, and his team comprising, Sh. B. Shanker Jaiswal, IPS, DIG (Modernization), and cyber security researchers at the NCR&IC, BPR&D. I record my deep appreciation for their hard work.

I believe this manual will be a useful guide to police officers in combating cyber harassment cases in a professional manner. Suggestions for further improvement in the content and presentation are welcome.

VSK Kaumudi,
Director General

The setting up of the National Cyber Crime Research & Innovation Centre (NCR&IC) at the BPR&D Hqrs. and its branch, the National Cyber Crime Research, Innovation and Capacity Building Centre, at the CDTI, Hyderabad, has been a major technological milestone in the cyber research and training capabilities of the BPR&D. The NCR&IC, as part of the umbrella scheme of the Indian Cyber Crime Coordination Centre (I4C), MHA, has been striving continuously to strengthen and augment the capacity of Law Enforcement Agencies (LEAs) in their efforts of cyber crime prevention and investigation.

To address the urgent need for protection of women and children from the scourge of cyber harassment, the ‘Investigative Workflow Manual on Cyber Harassment Cases’ has been brought out by the NCR&IC. It has been developed as a self-learning guide for hands-on training on the latest software tools, keeping in mind the skill set required by the concerned police officers. It deals with various facets of investigation, right from crime scene management to step-by-step detection methods and collection of evidence to prosecute the perpetrators.

This manual is a result of the sincere efforts of Sh. Karuna Sagar, IPS, IG/Director, Modernization, and his team comprising, Sh. B. Shanker Jaiswal, IPS, DIG (Modernization), and cyber security researchers at the NCR&IC, BPR&D. I record my deep appreciation for their hard work.

I believe this manual will be a useful guide to police officers in combating cyber harassment cases in a professional manner. Suggestions for further improvement in the content and presentation are welcome.

V.S.K. Kaumudi
The rapid technological developments in cyberspace have had a force multiplier effect on the speed of transactions, has enabled faster and cheaper communication and have overall greatly improved the quality of lives of people across the world. However, concomitant with it is the emergence of new age cybercrime, particularly with respect to cybercrime against women and children. Hence, prevention and detection of cybercrimes directed against women and children has become a huge challenge and also a major focus area for Law Enforcement Agencies across the world.

The investigation of such crimes has become more complex due to the sheer anonymity afforded to criminals in cyberspace, the transnational nature of such crimes and the newer and novel methods being employed by cyber-criminals. Hence, it is imperative upon the Investigating Officers to continually update their knowledge about the modus operandi of perpetrators, familiarize themselves with the statutory provisions & latest judicial pronouncements and also acquire necessary technical skills for investigation of such crimes.

In this context, it is heartening to note that the team of researchers at the NCR&IC, BPR&D under the able supervision of Sh. Karuna Sagar, IPS, IG/Director, Modernization, and Sh. B. Shanker Jaiswal, IPS, DIG (Modernization) have come up with ‘Investigative Workflow Manual on Cyber Harassment cases’. This Manual carries case studies on the investigation of cyber harassment cases, step by step methods of investigation, and a hands-on guide for using the latest cyber investigation tools.

I am sure that police officers will find this Manual useful in investigating cases of cybercrimes in a professional manner. I hope that they will gain new insights from the latest methods, software tools, and legal provisions described in the Manual.

Place: New Delhi
Date: 04.03.2021
Executive Summary

States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes through their law enforcement machinery. The Law Enforcement Agencies take legal action as per provisions of the law against reported cyber crimes.

As more and more users access internet and social media on a daily basis, social networks and media moderation policies have to evolve and respond to the growing amount of harmful content and behaviours online.

Government of India has rolled out an umbrella Scheme "Indian Cyber Crime Coordination Centre (I4C)" to combat cyber crime in the country, in a coordinated and effective manner. The scheme has seven components:

National Cyber Crime Research and Innovation Centre (NCR&IC) is one of the seven verticals under the Indian Cyber Crime Coordination Centre (I4C) which was allotted to the Bureau of Police Research and Development (BPR&D) with the aim of detecting various types of cyber crime and preventing them. The Central Government has initiated several measures for spreading awareness on cyber crimes, those include issuing cyber related alerts/advisories, capacity building/training of law enforcement officers/judges/prosecutors and to improve cyber forensics facilities etc. to prevent cyber crime and expedite investigations.

Technological tools and training modules to support the investigating officers on various cyber crimes are also being designed and developed at National Cyber Crime Research & Innovation Centre at the BPR&D.

The "Investigative Workflow Manual on Cyber Harassment Cases" is also one of the initiatives by the BPR&D undertaken in consultation with experts and other stakeholders.

I hope that this manual will assist all the Investigating officers across the country towards better preparedness in handling Cyber harassment cases.

(Karuna Sagar, I.P.S)  
IG/Director (Modernisation)
## Module I – Investigation of Cyber Harassment

### 1.0 Overview of Cyber Harassment cases

1.1 Categories of Cyber Harassment

<table>
<thead>
<tr>
<th>Category</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Bullying</td>
<td>27</td>
</tr>
<tr>
<td>Cyber Teasing</td>
<td>28</td>
</tr>
<tr>
<td>Cyber Stalking</td>
<td>29</td>
</tr>
<tr>
<td>Cyber Defamation</td>
<td>29</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>29</td>
</tr>
<tr>
<td>Catfishing</td>
<td>30</td>
</tr>
<tr>
<td>Doxing</td>
<td>30</td>
</tr>
<tr>
<td>Swatting</td>
<td>31</td>
</tr>
<tr>
<td>Cyber Trolling</td>
<td>31</td>
</tr>
<tr>
<td>Revenge porn</td>
<td>31</td>
</tr>
</tbody>
</table>

### 2.0 The Preliminary Investigation

Steps to be followed by IO

### 3.0 Handling Cyber Harassment Cases Using Cyber Investigation Procedures

3.1 E-mail Investigation:

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail Investigating Steps (known E-mail Services)</td>
<td>34</td>
</tr>
<tr>
<td>Investigation of E-mail (unknown e-mail services)</td>
<td>41</td>
</tr>
<tr>
<td>E-mail Intelligence</td>
<td>42</td>
</tr>
</tbody>
</table>

3.2 Website Investigation

3.3 Social Media/Networking Investigation

3.4 Instant Message Investigation Steps (WhatsApp, Facebook Messenger, Telegram and Imo, etc.)

3.5 Web based SMS Investigation

3.6 MMS Investigation

3.7 VoIP Call Investigations (WhatsApp, Viber, Messenger)

3.8 Suggested Websites for Investigation

3.9 References
### MODULE II - CRIME SCENE MANAGEMENT

#### 4.0 Handling Crime Scene Investigation on Cyber Harassment Cases

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Digital Forensics: Dealing with the scene of crime</td>
</tr>
<tr>
<td>4.1.1</td>
<td>Tools and Materials for Collecting Digital Evidence</td>
</tr>
<tr>
<td>4.2</td>
<td>Material to be used in packaging and transportation of evidence</td>
</tr>
<tr>
<td>4.3</td>
<td>Pre-requisites to handle mobile sets at the scene of crime</td>
</tr>
<tr>
<td>4.4</td>
<td>CSAM/obscene/explicit evidence extract triage tools</td>
</tr>
<tr>
<td>4.5</td>
<td>Crime Scene Management</td>
</tr>
<tr>
<td>4.6</td>
<td>Guidelines for Mobile Evidence Searching &amp; Seizure</td>
</tr>
<tr>
<td>4.7</td>
<td>Importance of Hashing</td>
</tr>
<tr>
<td>4.8</td>
<td>Imaging (Bit Stream Imaging)</td>
</tr>
<tr>
<td>4.8.1</td>
<td>Disk Imaging</td>
</tr>
<tr>
<td>4.8.2</td>
<td>Forensic Imaging</td>
</tr>
<tr>
<td>4.8.3</td>
<td>Stop Action of Imaging a Drive using FTK Imager 3.4.2.2</td>
</tr>
<tr>
<td>4.9</td>
<td>Digital Forensic Analysis</td>
</tr>
</tbody>
</table>

#### 4.1 Digital Forensics: Dealing with the scene of crime

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.1</td>
<td>Tools and Materials for Collecting Digital Evidence</td>
</tr>
</tbody>
</table>

#### 4.2 Material to be used in packaging and transportation of evidence

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 4.3 Pre-requisites to handle mobile sets at the scene of crime

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 4.4 CSAM/obscene/explicit evidence extract triage tools

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 4.5 Crime Scene Management

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 4.6 Guidelines for Mobile Evidence Searching & Seizure

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 4.7 Importance of Hashing

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 4.8 Imaging (Bit Stream Imaging)

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.8.1</td>
<td>Disk Imaging</td>
</tr>
<tr>
<td>4.8.2</td>
<td>Forensic Imaging</td>
</tr>
<tr>
<td>4.8.3</td>
<td>Stop Action of Imaging a Drive using FTK Imager 3.4.2.2</td>
</tr>
</tbody>
</table>

#### 4.9 Digital Forensic Analysis

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

### MODULE III - LEGAL NOTICES AND RESPONSES

#### 5.0 Notices & Responses

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Suggested Forensic/Investigative Tools for Combating CSAM Crimes</td>
</tr>
<tr>
<td>5.2</td>
<td>Suggested Forensic/Investigative Websites and Plugins related to Cyber Harassment Crimes</td>
</tr>
<tr>
<td>5.3</td>
<td>References</td>
</tr>
</tbody>
</table>

#### 5.1 Suggested Forensic/Investigative Tools for Combating CSAM Crimes

#### 5.2 Suggested Forensic/Investigative Websites and Plugins related to Cyber Harassment Crimes

#### 5.3 References

### MODULE IV - LEGAL INTERPRETATION

#### 6.0 Cyber Harassment Law Perspectives

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Cyber harassment cases at a rise</td>
</tr>
<tr>
<td>6.2</td>
<td>Legal provisions related to cyber crime</td>
</tr>
<tr>
<td>6.3</td>
<td>References</td>
</tr>
</tbody>
</table>

#### 6.1 Cyber harassment cases at a rise

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 6.2 Legal provisions related to cyber crime

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 6.3 References

### MODULE V - CYBER AWARENESS

#### 7.0 Cyber Safety & Awareness

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Stalker’s Strategies</td>
</tr>
<tr>
<td>7.2</td>
<td>Harassment Warning Signs</td>
</tr>
<tr>
<td>7.3</td>
<td>Online Monitoring</td>
</tr>
<tr>
<td>7.4</td>
<td>Cyber Harassment- Harmful Effects</td>
</tr>
<tr>
<td>7.5</td>
<td>Prevention Steps</td>
</tr>
<tr>
<td>7.6</td>
<td>Post Incident steps are to be taken in case any warning signs are observed</td>
</tr>
<tr>
<td>7.7</td>
<td>Reporting Procedure - Cyber Harassment Cases</td>
</tr>
<tr>
<td>7.8</td>
<td>Victim Counselling</td>
</tr>
<tr>
<td>7.9</td>
<td>Cyber Crime Categories, Symptoms and Actionable Steps (Victim Perspective)</td>
</tr>
<tr>
<td>7.10</td>
<td>Preventive Security Measures for Phishing Attacks</td>
</tr>
<tr>
<td>7.11</td>
<td>References</td>
</tr>
</tbody>
</table>

#### 7.1 Stalker’s Strategies

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 7.2 Harassment Warning Signs

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 7.3 Online Monitoring

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 7.4 Cyber Harassment- Harmful Effects

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 7.5 Prevention Steps

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 7.6 Post Incident steps are to be taken in case any warning signs are observed

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 7.7 Reporting Procedure - Cyber Harassment Cases

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1</td>
<td>National Cyber Crime Reporting Portal</td>
</tr>
<tr>
<td>7.7.2</td>
<td>Social Media Reporting</td>
</tr>
<tr>
<td>7.7.3</td>
<td>Local Police/ LEAs Reporting</td>
</tr>
<tr>
<td>7.7.4</td>
<td>School Administration</td>
</tr>
<tr>
<td>7.7.5</td>
<td>Online Service Providers</td>
</tr>
</tbody>
</table>

#### 7.8 Victim Counselling

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1</td>
<td>Student Counselling</td>
</tr>
<tr>
<td>7.8.2</td>
<td>Parent-Driven Counselling</td>
</tr>
<tr>
<td>7.8.3</td>
<td>School-Driven Counselling</td>
</tr>
</tbody>
</table>

#### 7.9 Cyber Crime Categories, Symptoms and Actionable Steps (Victim Perspective)

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 7.10 Preventive Security Measures for Phishing Attacks

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

#### 7.11 References

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Title</th>
</tr>
</thead>
</table>

### Annexure-A

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
</table>

### Annexure-B

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
</table>
Index of Tables

<table>
<thead>
<tr>
<th>S No</th>
<th>Topic</th>
<th>Page No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cyber Bullying (Means, Motives &amp; Targets)</td>
<td>27</td>
</tr>
<tr>
<td>2</td>
<td>Cyber Teasing (Means, Motives &amp; Targets)</td>
<td>28</td>
</tr>
<tr>
<td>3</td>
<td>Cyber Stalking (Means, Motives &amp; Targets)</td>
<td>29</td>
</tr>
<tr>
<td>4</td>
<td>Cyber Defamation (Means, Motives &amp; Targets)</td>
<td>29</td>
</tr>
<tr>
<td>5</td>
<td>Identity Theft (Means, Motives &amp; Targets)</td>
<td>30</td>
</tr>
<tr>
<td>6</td>
<td>Catfishing (Means, Motives &amp; Targets)</td>
<td>30</td>
</tr>
<tr>
<td>7</td>
<td>Doxing (Means, Motives &amp; Targets)</td>
<td>30</td>
</tr>
<tr>
<td>8</td>
<td>Swatting (Means, Motives &amp; Targets)</td>
<td>31</td>
</tr>
<tr>
<td>9</td>
<td>Trolling (Means, Motives &amp; Targets)</td>
<td>31</td>
</tr>
<tr>
<td>10</td>
<td>Revenge Porn (Means, Motives &amp; Targets)</td>
<td>32</td>
</tr>
<tr>
<td>11</td>
<td>Websites for Investigation</td>
<td>56</td>
</tr>
<tr>
<td>12</td>
<td>Table Of Differences Between Imaging &amp; Cloning Procedures</td>
<td>79</td>
</tr>
<tr>
<td>13</td>
<td>Sample Case Study Summary of Imaging Procedure Using Ftk Imager</td>
<td>86</td>
</tr>
<tr>
<td>14</td>
<td>Tools for Combating CSAM Crimes</td>
<td>102</td>
</tr>
<tr>
<td>15</td>
<td>Forensic/Investigative Websites and Plugins</td>
<td>102</td>
</tr>
<tr>
<td>16</td>
<td>Legal Provisions Related to Cyber Crimes</td>
<td>110</td>
</tr>
<tr>
<td>17</td>
<td>Cyber Crime Categories, Symptoms and Actionable Steps (User’s Perspective)</td>
<td>122</td>
</tr>
</tbody>
</table>

Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACPO</td>
<td>Association of Police Officers</td>
</tr>
<tr>
<td>CCTLD</td>
<td>Country Code - Top Level Domain Name</td>
</tr>
<tr>
<td>CFSL</td>
<td>Central Forensic Science Laboratory</td>
</tr>
<tr>
<td>CSAM</td>
<td>Child Sexual Abuse Material</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DOJ</td>
<td>Department Of Justice (In America)</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>FIR</td>
<td>First Information Report</td>
</tr>
<tr>
<td>FSL</td>
<td>Forensic Science Laboratory</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>IO</td>
<td>Investigating Officer</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>I4C</td>
<td>Indian Cyber Crime Co-Ordination Centre</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>LEA</td>
<td>Law Enforcement Agencies</td>
</tr>
<tr>
<td>LoR</td>
<td>Letter of Rogatory</td>
</tr>
<tr>
<td>MLAT</td>
<td>Mutual Legal Assistance Treaty</td>
</tr>
<tr>
<td>MSP</td>
<td>Mobile Service Provider</td>
</tr>
<tr>
<td>MX</td>
<td>Mail Exchanger</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>POS</td>
<td>Point of Sale</td>
</tr>
<tr>
<td>SFSL</td>
<td>State Forensic Science Laboratory</td>
</tr>
<tr>
<td>SWAT</td>
<td>Special Weapons And Tactics</td>
</tr>
<tr>
<td>TLD</td>
<td>Top Level Domain Name</td>
</tr>
<tr>
<td>TSP</td>
<td>Telecom Service Provider</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice Over Internet Protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WSP</td>
<td>Web Service Provider</td>
</tr>
<tr>
<td>NCR&amp;IC</td>
<td>National Cyber Crime Research and Innovation Center</td>
</tr>
</tbody>
</table>
Introduction

Dependence on the internet has increased manifold in the last decade and is increasing exponentially in the daily life of mankind. Though the use of the internet has eased access to several channels of information in the life of an individual, it has also invited many ill effects; many of those are reported as typical Cyber Crime cases. Social media is another domain where the usage of the internet poses a threat due to unresolved identities that have invited challenges to Law Enforcement Agencies (LEAs) to deal with them particularly in cases against Women and Children.

Cyber Harassment cases are one of the major challenges LEAs face currently where Cyber Predators/Harassers make use of digital technology as a medium for committing the crime. Various types of Cyber Crime include cyberbullying, stalking, trolling etc. While committing the crimes, stalkers use fake profiles, identity theft, proxies, VPN services and masquerading methods. Due to these techniques which provide anonymity, investigating officers encounter significant problems in tracking the culprits. As per the National Crime Records Bureau Report (NCRB 2019), cybercrimes in India have increased dramatically in the year 2019 as compared to previous years. It is anticipated that such crimes will become epidemic unless they are effectively and promptly dealt with and the perpetrators are convicted and punished.

The National Cyber Crime Research and Innovation Center (NCR&IC) under the I4C scheme of the MHA set up at the Bureau of Police Research and Development (BPR&D) has compiled this manual, viz. “Investigative Workflow Manual on Cyber Harassment Cases” to provide a comprehensive guideline to Investigating Officers (IOs) to deal more effectively with the cyber-harassment cases. The step-by-step approach towards such cases would help LEAs build effective and foolproof cases against culprits leading to the conviction. Simultaneously, the manual will help IOs in extending a helping hand to victims by better counselling which would help them recover from the after-effects of such incidents.

This Manual has been categorized into five modules:

- Cyber Harassment Investigation
- Crime Scene Management
- Legal Notices and Responses
- Legal Interpretation
- Cyber Awareness

Cyber Harassment Investigation
This module deals with the understanding of cyber harassment cases and their various aspects, including Case Registration Procedure and Evidence Collection as per the adopted modus operandi. This manual also highlights preliminary and detailed investigation procedure for tackling cyber harassment cases using crime inputs such as Websites, E-mails, Calls/VoIP calls, SMS/MMS, Instant chats and other services.

Crime Scene Management
This module highlights details on crime scene investigation, computer evidence collection and preservation procedure, Imaging/Cloning of digital evidence at the crime scene, mobile device seizure procedure, understanding the importance of hashing digital evidence, the practical procedure for generating Hash Value and verification of evidence authentication.

Legal Notices and Responses
This module provides sample forms for generating notices with respect to section 91 Cr. P.C 65(B) I.E Act and template for search & seizure memo, evidence packaging procedure, chain of custody template for computer systems, mobile and other electronic evidence, FSL forwarding notes, etc.

Legal Interpretation
This module highlights the interpretation of the law related to cyber harassment. It also focuses on IPC/Cl.P.C/IEA/IT Act sections, Court Judgments, Government Orders (GOs), Gazette notifications, etc. to understand each case in the light of legal perspective.

Digital Awareness
This module draws the spotlight on safety, security.
and awareness guidelines for the society on cyber harassment cases. It further explains the steps and best practices for effective victim counselling, DOs and DONTs on the internet, online and offline complaint reporting procedure. This segment also emphasizes the awareness of parents and educational institutions and highlights the need for combating Cyber Harassment cases in a collaborative environment with civil society.

In general, this manual would be an effective and comprehensive guide to an Investigating Officer for handling and systematically investigating Cyber Harassment cases. It would also provide detailed guidelines for documentation, including the procedure for collection and preservation of potential evidence, so that relevant cases can withstand judicial scrutiny.
1.0 OVERVIEW OF CYBER HARASSMENT CASES

The use of digital technology has become an integral part of our lives. Any technology can be used for constructive or destructive purposes. Misuse of information and communication technology is an important ingredient of Cyber Crime. Among many offensive acts in cyberspace, online abuse/harassment is a common phenomenon that directly or indirectly affects cyberspace users of diverse age groups.

Cyber Harassment is defined as a repeated, unsolicited, hostile behaviour by a person through cyberspace with an intent to terrify, intimidate, humiliate, threaten, harass or stalk someone. Any harassment caused through electronic media is considered to have a similar impact as traditional offence of harassment. It can be done through various means of ICT as depicted in Figure 1.

1.1 CATEGORIES OF CYBER HARASSMENT

Based on the severity of Online Harassment and the modus operandi, the Department of Justice (DOJ) of USA and ACPO (Association of Chief Police Officers) in the UK and other international agencies have broadly classified Cyber Harassment into 10 categories, as shown in Figure 2.

1.1.1 Cyber Bullying

Cyberbullying is an act of sending, posting or sharing negative, harmful, false or demeaning content regarding others. Sharing personal or private information which could cause embarrassment or humiliation to others too falls under the ambit of Cyberbullying. It takes place through digital devices such as cell phones, computers, and tablets via services such as SMS, texts, Apps, social media platforms, online forums and gaming where people can view, participate or share content.

Modus operandi used:
- Posting nasty or humiliating content or comments about an individual online
- Publishing an embarrassing or demeaning photo or video
- Creating a fake profile of another individual
- Online threats provoking an individual to harm/kill himself or hurt someone else
- Triggering religious, racial, regional, ethnic or political vitriol online by posting hate comments or content
- Using other’s identity online to ask for or post personal or fake, embarrassing information about someone
- Repeatedly harming a player’s character, asking for monetary exchange, ganging up on a player or using personal information to make direct threats
- Posting online stories, pictures, jokes, or cartoons that are intended to embarrass or humiliate others.

Hacking someone’s e-mail, other social media accounts and/or sending/posting embarrassing content whilst pretending to be the victim whose account has been hacked. Table 1 below shows the various means, motives and targets of Cyberbullying.

<table>
<thead>
<tr>
<th>Type</th>
<th>Means of ICT used in the crime</th>
<th>Motive behind the commission of crime</th>
<th>General Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Bullying</td>
<td>• E-mail; Social Media/Networking (Facebook, Instagram, WhatsApp, Twitter, YouTube etc.) • Website • Instant Messages • Web-based SMS • MMS • Online Games</td>
<td>• To gain popularity and influence within the dominant social circle</td>
<td>• School kids</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sometimes bullies do it to take revenge</td>
<td>• Teenagers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Many cyberbullies perform their actions for pure entertainment</td>
<td>• Women</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To isolate the victim</td>
<td>• Colleagues</td>
</tr>
</tbody>
</table>

Table 1: Cyber Bullying (Means, Motives & Targets)
1.1.2 Cyber Teasing

Cyber teasing is an attitude, a mindset, a pattern of behaviour and/or actions that are construed as an insult and an act of humiliation to the target. Generally, it is the harassment of women by strangers in public places, streets and public transport but when a similar crime occurs using means of ICT then it is called Cyber Teasing.

Modus operandi used:
- Sending, sharing, posting vulgar/defamatory/messages to a victim's website, profile, or blog.
- Publishing/posting derogatory remarks against the victim's name. These often involve subscriptions to magazines in the victim's name, or subscribe to magazines in the victim's name.
- Creating websites, profiles, or other accounts that contain messages to threaten or harass the victim or creating circumstances as if the victim created a particular website that contains provocative or pornographic photographs
- Hate speech, i.e., the language that denigrates, insults, threatens or targets an individual based on their identity and other traits (such as sexual orientation or disability or religion, etc.)
- Impersonating the victim's online identity to harm reputation or relationships.
- Monitoring the victim's movements using GPS, tracking apps or spyware.
- Ordering goods or services: Ordering items or subscribe to magazines in the victim's name. These often involve subscriptions to pornography or ordering sex toys and having them delivered to the victim's workplace.

<table>
<thead>
<tr>
<th>Type</th>
<th>Means of ICT used in the crime</th>
<th>Motive behind the commission of crime</th>
<th>General Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Teasing</td>
<td>- E-mail</td>
<td>- For gaining sexual attention</td>
<td>Women</td>
</tr>
<tr>
<td></td>
<td>- Social Media/Networking (Facebook, Instagram, WhatsApp, Twitter, YouTube etc.)</td>
<td>- Exacerbate feeling of shame and humiliation</td>
<td>Teenage Girls</td>
</tr>
<tr>
<td></td>
<td>- Website</td>
<td>- Out of revenge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Instant Messages</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Web-based SMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- MMS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Cyber Teasing (Means, Motives & Targets)

1.1.3 Cyber Stalking

Cyberstalking is the usage of Information and Communications Technology (ICT) to stalk, control, manipulate or habitually threaten a minor, an adult or a business group. Cyberstalking is both an online assiduous tactic and typology of psychopathological ICT users. Cyberstalking includes direct or implied threats of physical harm, habitual surveillance and gathering information to manipulate and control a target. Table 3 describes the various means of ICT, motives behind their usage and the various targets.

Modus operandi used:
- Leaving harassing or threatening messages in the guestbook, on the victim’s website, social media profile, or blog.
- Sending inappropriate electronic greeting cards to the victim.
- Posting personal advertisements in the victim’s name.
- Creating websites, profiles, or other accounts that contain messages to threaten or harass the victim. Table 3 describes the various means of ICT, motives behind their usage and the various targets.

<table>
<thead>
<tr>
<th>Type</th>
<th>Means of ICT used in the crime</th>
<th>Motive behind the commission of crime</th>
<th>General Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Stalking</td>
<td>- E-mail</td>
<td>- Jealousy</td>
<td>Young women</td>
</tr>
<tr>
<td></td>
<td>- Social Media/Networking (Facebook, Instagram, WhatsApp, Twitter, YouTube etc.)</td>
<td>- Obsession and attraction</td>
<td>Teenagers</td>
</tr>
<tr>
<td></td>
<td>- Website</td>
<td>- Erotomania</td>
<td>Ex-girlfriend or boyfriend</td>
</tr>
<tr>
<td></td>
<td>- Messages (SMS)</td>
<td>- Sexual Harassment</td>
<td>Colleagues</td>
</tr>
<tr>
<td></td>
<td>- Postal letters</td>
<td>- Revenge and hatred</td>
<td>Unknown victims</td>
</tr>
<tr>
<td></td>
<td>- Telephone/cell phone conversations</td>
<td></td>
<td>Celebrities or famous personalities</td>
</tr>
</tbody>
</table>

Table 3: Cyber Stalking (Means, Motives & Targets)

1.1.4 Cyber Defamation

Cyber defamation is the act of publishing defamatory content using electronic devices and the internet. If someone publishes some defamatory statement and/or sends e-mails containing defamatory content to other people to defame the victim then this would be considered as an act of cyber defamation. Table 4 describes the various means of ICT, motives behind their usage and the various targets.

Modus operandi used:
- Publishing/posting derogatory remarks against individual(s)/organization(s) on websites.
- Publishing/posting derogatory remarks against individual/organization on social media/networking.
- Spreading false information against individual/organization through e-mails.

Impact of Cyber Defamation:
- Loss of reputation of individual/organization
- Loss of business in case organization is defamed

<table>
<thead>
<tr>
<th>Type</th>
<th>Means of ICT used in the crime</th>
<th>Motive behind the commission of crime</th>
<th>General Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Defamation</td>
<td>- E-mail</td>
<td>- To defame an individual/organization</td>
<td>Individuals</td>
</tr>
<tr>
<td></td>
<td>- Social Media/Networking (Facebook, Instagram, WhatsApp, Twitter, YouTube etc.)</td>
<td>- To take revenge from an individual/organization</td>
<td>Organizations</td>
</tr>
<tr>
<td></td>
<td>- Website/Blogs</td>
<td>- Political motivation can be the reason to defame public figure/organization</td>
<td>Public/Political figures</td>
</tr>
</tbody>
</table>

Table 4: Cyber Defamation (Means, Motives & Targets)

1.1.5 Identity Theft

Identity theft is the act of using other’s Personal Identity Information such as name, identification number, or credit card number, without their permission, to commit fraud. Table 5 lists the means of ICT, motives and general targets.

Modus operandi used:
- Phishing
- Skimming
- Data Breach
- Phone scams
Module I – Investigation of Cyber Harassment

**1.1.6 Catfishing**
Catfishing is a type of deceptive activity where a person creates a fake identity on a social network account, usually targeting a specific victim for abuse, deception, fraud and various other gains. Table 6 lists the means of ICT, motives and general targets.

<table>
<thead>
<tr>
<th>Type</th>
<th>Means of ICT used in the crime</th>
<th>Motive behind the commission of crime</th>
<th>General Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catfishing</td>
<td>• E-mail</td>
<td>• Low self-esteem and build a fictitious online persona to interact with people</td>
<td>• Young women</td>
</tr>
<tr>
<td></td>
<td>• Social Media/networking (Facebook, Instagram, WhatsApp, Twitter, YouTube etc.)</td>
<td>• Seek money, and build a fake relationship with their victims to get it</td>
<td>• Ex-girlfriends/boyfriends</td>
</tr>
<tr>
<td></td>
<td>• Website/blogs/forums</td>
<td>• Revenge from others</td>
<td>• Celebrities or famous personalities</td>
</tr>
</tbody>
</table>

**1.1.7 Doxing**
Doxing is the process of retrieving, hacking and publishing other people’s information such as names, addresses or phone numbers and/or credit/debit card details. Doxing may be targeted toward a specific person or an organization. Table 7 lists the means of ICT, motives and general targets.

<table>
<thead>
<tr>
<th>Type</th>
<th>Means of ICT used in the crime</th>
<th>Motive behind the commission of crime</th>
<th>General Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doxing</td>
<td>• E-mail</td>
<td>• Harassment of individuals/Public figure/Organization</td>
<td>• Individuals</td>
</tr>
<tr>
<td></td>
<td>• Social Media/Networking (Facebook, Instagram, WhatsApp, Twitter, YouTube etc.)</td>
<td>• To extort individual for financial gains</td>
<td>• Public/Political figures</td>
</tr>
<tr>
<td></td>
<td>• Website/blogs/forums</td>
<td>• To make others feel low self-esteem or disgraced</td>
<td>• Celebrities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To take revenge</td>
<td>• Specific communities</td>
</tr>
</tbody>
</table>

**1.1.8 Swatting**
Swatting refers to a harassment technique most often perpetrated by members of the online gaming community. Online gamers make a hoax call, wherein they dial authorities and give them some false information diverting the police and emergency service response team to another person’s address. Table 8 lists the means of ICT, motives and general targets.

<table>
<thead>
<tr>
<th>Type</th>
<th>Means of ICT used in the crime</th>
<th>Motive behind the commission of crime</th>
<th>General Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swatting</td>
<td>• E-mail</td>
<td>• Harassment</td>
<td>• Teens</td>
</tr>
<tr>
<td></td>
<td>• Phone call</td>
<td>• To take revenge</td>
<td>• Kids</td>
</tr>
<tr>
<td></td>
<td>• Social media</td>
<td>• To extort individual for financial gains</td>
<td>• Online gamers</td>
</tr>
</tbody>
</table>

**1.1.9 Cyber Trolling**
Cyber trolling is a deliberate act of making random unsolicited and/or controversial comments on various internet forums with the intent to provoke an emotional response from the readers to engage them in a fight or argument which may be just for amusement or for other specific gains. Now that almost anyone can comment on a status update, reply to a tweet, converse in a community thread or send an anonymous question, trolling is everywhere that people interact. Table 9 lists the means of ICT, motives and general targets.

<table>
<thead>
<tr>
<th>Type</th>
<th>Means of ICT used in the crime</th>
<th>Motive behind the commission of crime</th>
<th>General Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trolling</td>
<td>• E-mail</td>
<td>• To make others feel low self-esteem or disgraced</td>
<td>• Individuals</td>
</tr>
<tr>
<td></td>
<td>• Social Media/Networking (Facebook, Instagram, WhatsApp, Twitter, YouTube etc.)</td>
<td>• To take revenge</td>
<td>• Public/Political figures</td>
</tr>
<tr>
<td></td>
<td>• Website/blogs/forums</td>
<td>• Ideological differences</td>
<td>• Celebrities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Religious discontentment</td>
<td>• Specific communities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Gender biases</td>
<td></td>
</tr>
</tbody>
</table>

**1.1.10 Revenge Porn**
Revenge porn or revenge pornography is the distribution of sexually explicit images or videos of individuals to bring disgrace and damage their reputation. The sexually explicit images or videos may be made by a partner of an intimate relationship with or without the knowledge and consent of the subject. Table 10 lists the means of ICT, motives and general targets.

<table>
<thead>
<tr>
<th>Type</th>
<th>Means of ICT used in the crime</th>
<th>Motive behind the commission of crime</th>
<th>General Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenge Porn</td>
<td>• E-mail</td>
<td>• To bring disgrace and damage</td>
<td>• Individuals</td>
</tr>
<tr>
<td></td>
<td>• Social Media/Networking (Facebook, Instagram, WhatsApp, Twitter, YouTube etc.)</td>
<td>• To bring disgrace and damage</td>
<td>• Public/Political figures</td>
</tr>
<tr>
<td></td>
<td>• Website/blogs/forums</td>
<td>• To bring disgrace and damage</td>
<td>• Organizations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To bring disgrace and damage</td>
<td></td>
</tr>
</tbody>
</table>
Modus operandi used: The possession of the material may be used by the perpetrators to blackmail the subjects into performing other sex acts or to coerce them into continuing a relationship or to punish them for ending the relationship or to threaten them.

<table>
<thead>
<tr>
<th>Type</th>
<th>Means of ICT used in the Crime</th>
<th>Motive behind the Commission of Crime</th>
<th>General Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenge Porn</td>
<td>• E-mail</td>
<td>• To take revenge</td>
<td>• Young Women</td>
</tr>
<tr>
<td></td>
<td>• Website</td>
<td>• To humiliate and intimidate</td>
<td>• Children</td>
</tr>
<tr>
<td></td>
<td>• Social Media</td>
<td>• To blackmail</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MMS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 10: Revenge Porn (Means, Motives & Targets)

### 2.0 THE PRELIMINARY INVESTIGATION

After the Investigation Officer and his team determine that this is indeed a cyber harassment case, he or she should initiate a preliminary criminal investigation.

#### STEPS TO BE FOLLOWED DURING THE INVESTIGATION

The steps for initiating a preliminary inquiry are shown in Figure 3:

1. Obtain a detailed description of the incident as well as the time of occurrence of incident from the complainant.

2. Ask the complainant if he or she knows who is sending the harassing messages. If he/she knows the suspect then IO may ask for information about the suspect: name, age, address, telephone number, vehicle information, and relationship to victim.

3. Ask the complainant, if he or she knows why he or she is being harassed. If so, record the complainant’s explanation in as much detail in the narrative portion of the report. Knowledge of the reason can help in the identification of the harasser.

4. What communication has the complainant had with the harasser? Did the complainant respond to the messages? Copies of the responses are necessary for the investigation.

5. Ascertain when and how the harassment began. Find out if it has happened only via the Internet (e-mail messages, chat rooms, mailing lists, instant messages, Web site) or through telephone calls, cell phone calls or texts, postal letters as well.

6. Determine whether the complainant has been threatened with violence, rape, and even death. The investigating officer needs to establish the details of how these threats were communicated.

7. Obtain a copy (hard/soft) of the messages for the case file showing the e-mail address, Website URL and the content(s) of the message(s). Hard copies of the screenshot taken should be signed by the victim.

8. Secure any physical evidence available and start the chain of custody to protect the evidence from getting tampered. The evidence should be recorded in both paper printouts and electronic files or on an electronic media such as a disk or CD/DVD-ROM. Ask the complainant, if he or she has any material evidence. Items to request include:

   - Web page images
   - Chat room messages
   - Instant messages
   - E-mail messages and e-mail headers
   - Social network messages/wall posts
   - Mailing list messages
   - Message Board messages
   - Phone conversation recordings
   - Text Messages

**Figure 3: Steps followed for Preliminary Enquiry**

*Note: Copy of the Incident Reporting Form (Annexure-B) can be provided to the victim.*
Module I – Investigation of Cyber Harassment

3.0 Handling Cyber Harassment Cases Using Cyber Investigation Procedures

Cyber Harassment cases are observed to be committed through various means such as Websites, E-mails, Calls, VoIP Calls, and Instant Chats/Messages etc. Analyse the cyber-harassment incident based on the modus operandi used.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail</td>
<td>It can be launched using e-mails</td>
</tr>
<tr>
<td>Website</td>
<td>Content can be posted on websites</td>
</tr>
<tr>
<td>Social Media</td>
<td>Harassment can be done using social media platforms</td>
</tr>
<tr>
<td>Instant Chat</td>
<td>Instant chat services can be used for harassment purposes</td>
</tr>
<tr>
<td>Web Based SMS</td>
<td>Free web based sms services can be used for online harassment</td>
</tr>
<tr>
<td>MMS</td>
<td>Online harassment can be committed through MMS</td>
</tr>
<tr>
<td>VoIP Call</td>
<td>VOIP calls usages for cyber crime are on the rise</td>
</tr>
</tbody>
</table>

![Figure 4: Modus Operandi - Technology used in Cyber Harassment](image)

3.1 E-mail Investigation

Cyber Harassment Crimes can be committed using e-mail services. Generally, the suspect/accused may use the below-mentioned e-mail services for committing the crime.

- a) E-mail using known e-mail services
- b) E-mail using anonymous e-mail services

3.1.1 E-mail Investigating Steps (known E-mail Services)

Popular e-mail services are defined as known E-mail Services e.g. Gmail, Yahoo, Rediff, Outlook etc. and have their user interfaces to extract e-mail header details.

**Step 1:** Collect the e-mail header of the original e-mail from the victim. The header is a section of code that contains information about the source of the e-mail and how the message reached its destination. Headers contain the e-mail address of the originator and/or the device the perpetrator/sender was using. Always preserve a screenshot of the harassment message in a soft/hard copy. Follow the below-mentioned steps to collect the e-mail header of different e-mails:

**Extracting E-mail Header in Google (Gmail) Webmail:**

Login to the Gmail account and open the mail. Click “Down-Arrow/Dash line/More option” on the top-right of the message and select “Show Original”. Now one can see the complete source details of the message in Figure 5.

![Figure 5: Gmail E-mail Header](image)

**Extracting E-mail Header in Yahoo! Webmail:**

Login to the yahoo account on the webpage. Open the message and click on “More” and select “View raw message” as shown in Figure 6.

![Figure 6: Yahoo E-mail Header](image)

**Extracting E-mail Header in Hotmail Webmail:**

Login to the account on the webpage and go to the Inbox list of messages. Right-click on the suspect message and then select the icon “View Source” as in Figure 7.
Figure 7: Hotmail E-mail Header

Extract the Message Header in MS Outlook:
Open the message in MS Outlook. Now go to “View” and select the icon- “Message” or “File” ->“Info” ->“Properties”. Look at “Internet Headers” as shown in Figures 8-10.

Open Outlook application and click on “File” as shown in Figure 8:

Click on Properties as shown in Figure 9:

Click on “Internet Header” as shown in Figure 10:

Extract the Message Header in Thunderbird:
Open the message, and then click on “View” and select “Message Source”. View the Message Header in MS Windows Mail (or MS Outlook Express). Select the message in the list, right-click on it and select “Properties” and go to “Details” as shown in Figure 11.
Step 2: If images, audio, video or any other file attachments about the harassment are found in the e-mail then download the file in a safe environment and keep it as evidence. It is recommended to take the hash value of the downloaded file. Also, the system on which e-mail was received can be seized.

Sample Message Header

![Sample Message Header](image)

The "From" line, which contains information (mail ID) of the message sender, can be easily altered. Hence one should not rely on this information.

The lines in green (refer to the sample message header in Figure 12 above) contain the routing information, from the sender’s computer to the recipient’s mail server. The following are construed from the header and are to be seen in reverse order of IPs depicted in the sample message header:

(1) The message was finally received by the recipient mail server from the recipient’s mail exchanger 192.168.1.2.
(2) The message was transferred from the sender’s mail server with the IP address 192.168.1.3 to the recipient’s mail exchanger. The mail exchanger is the mail server, which accepts incoming messages for a particular domain.
(3) The message was sent from the sender’s computer with the IP address 104.100.10.5 to the mail server of the sender. In many cases the sender IP 104.100.10.5 is a dynamic IP address, e.g. IPs allocated by DSL. The IP address gives much information about the sender, the location of the sender and the service provider. Refer to the screenshot in Figure 13.

Step 3: Analyze the complete e-mail header. Specifically, look for the originating e-mail IP and MX (mail exchanger) domain as shown in Figure 12.

Meaning of each field

![Meaning of each field](image)

Return-Path: The e-mail address which should be used for bounces i.e. the mail server will send a message to the specified e-mail address if the message cannot be delivered.

Delivery-date: The date on which the message was delivered.

Subject: The message subject.

Step 4: Open the ‘Whois’ website which can be used to derive information on whether an IP address belongs to India or not. A sample screenshot is shown in Figure 15. If it is from India, check which Internet service provider (ISP) organization it belongs to. Below mentioned are some of the utility URLs for accessing the ‘Whois’ record.

- https://lookup.icann.org/
- https://whois.net/
- http://whois.domaintools.com/
- https://manytools.org/network/online-whois-query/
**Module I – Investigation of Cyber Harassment**

Note: WHOIS (pronounced as the phrase “who is”) is a query and response protocol that is widely used for querying databases that not only store the registered users or assignee on an Internet resource, such as a domain name, an IP address block or an autonomous system but also store a wider range of other information as shown in Figure 15.

**IP Information**

<table>
<thead>
<tr>
<th>IP Location</th>
<th>Australia Sydney Akami Technologies Inc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN</td>
<td>AP9443 INTERNETPRIMUS-AS-AP Primus Telecommunications, AU (registered Nov 12, 1998)</td>
</tr>
<tr>
<td>Resolve Host</td>
<td>4104-100-10-5.deploy.static.akamitechnologies.com</td>
</tr>
<tr>
<td>Whois Server</td>
<td>whois.arin.net</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.100.10.5</td>
</tr>
</tbody>
</table>

**Figure 15: Visualization of ‘Whois’ lookup Data**

Step 5: If required, IP details (found in the e-mail header) can be obtained from the ISP. The timestamp mentioned in the e-mail header is very important. While requesting IP details from ISP we need to mention the exact time (with proper time zone). Summons under u/s 91 of Cr. P.C (Summon to produce documents) submitted to the e-mail service provider to furnish the account registration details along with log details in respect of the e-mail account.

Step 6: If IP does not belong to India, then we can use the MLAT process to obtain information.

Step 7: If originating IP does not exist in the e-mail header then notice should be issued u/s 91 of Cr.P.C. (Summon to produce documents) to the e-mail service provider of the sender e-mail such as Google, Yahoo, Microsoft etc. for registration and to access logs details. A sample registration access log is shown in Figure 16.

**Figure 16: Sample Registration access log detail from Google**

Step 9: Based on the details provided by the E-mail service provider in Step 8 above, the following additional user details can be further obtained.

i. IP address details from ISP
ii. Mobile number details from mobile service Provider

**Step 10:** If the e-mail service provider replies that the user details cannot be provided because of a jurisdiction issue then follow the MLAT/LoR process to obtain log information.

### 3.1.2 Investigation of E-mail (unknown e-mail services)

**Step 1:** If the harasser uses an anonymous e-mail service then request for user registration and access log details from the anonymous e-mail service provider. Agencies such as CERT (Computer Emergency Response Team), Interpol etc. can also be involved to obtain specific details or to identify the culprit.

**Step 2:** In most cases, anonymous service providers are from countries other than India. In such scenarios, information can be obtained using the MLAT/LoR process. Protonmail is one of the examples of an anonymous e-mail service, a screenshot of which is shown in Figure 17.
3.1.3 E-mail Intelligence

Email is most commonly used in internet communication. Email addresses are linked to various social media accounts, mobile phones and other personal/confidential information. This makes email too good target for investigators to dig the internet to get a substantial amount of information about the target and also to get some crucial leads in the investigation. There are various tools and methods to gather the information from the email address as follows:

**Verify Email:**
(http://www.verify-email.org) identifies if a given email address is presently valid or not as seen in the below figure:

![Verify Email](image1.png)

**Steps 1:** Open the https://quickemailverification.com/

**Step 2:** Then click on Get started free button (100 free trials per day)

**Step 3:** Create a free account and in a few minutes “quick email verification” will send an email verification mail in the given email id, then click on the highlighted button as shown in the figure.

![Quick Email Verification Link](image2.png)

**Step 4:** After that, another window will appear. Put the email address for validation and click on the Verify Email address as shown in the figure.

![Email Address for Validation](image3.png)

**Verification result dialogue box is shown in the figure**

**Pipl:** (https://pipl.com)
The Pipl website takes an email address as input and presents all the available related information for further investigation.

![The Pipl Interface](image4.png)

Here a search for mobile no. “9755141800”
Here another email search “a*****.g******@gmail.com”
As result, the link of Facebook, LinkedIn, and profile is provided. In addition to this also obtain the full name.

Note: PiPL search is a paid tool.

Whoxy: (https://www.whoxy.com/whois-lookup/) allow searches via the email address, owner name, company name and domain name.
Eg: In this case we searched enifachub.com and as a result got domain registration details of the domain.

Note: Annexure-A may be referred for contact details of the service providers

3.2 WEBSITE INVESTIGATION
If online abuse has been done through websites then the following steps should be taken.

Step 1: Obtain the screenshot of the abusive (derogatory, obscene, bullying etc.) content from the victim. Soft copy, as well as the hard copy of the screenshots, can be kept for evidence purpose. Make sure the exact URL is visible while taking screenshots along with the date and time. Also, the URL shall be securely recorded in the case file. By using Website Preservation Tools (Camtasia, Snagit, FAH, Httrack, OSINT etc.) may preserve the evidence for forensic
examination purpose.

Step 2: If uploaded content is an image, video or audio etc., download the content from the target website and calculate the hash value and keep it as evidence for admissibility purpose.

Note: The contents of a file are processed through a cryptographic algorithm, and a unique numerical value – i.e. the Hash Value is generated that identifies the contents of the file. If the contents are modified in any way, the value of the hash also changes significantly hence indicating that the file has been altered.

Step 3: Extract the name of the website on which offence has taken place and shall use websites such as www.who.is, www.domaintools.com, www.centralops.net etc. to get details of the defined domain such as "ebay.in". Specifically, look for Domain Registrar and Registrant and web hosting details as shown in Figure 27.

Figure 27: Whois Details

Registry: A domain name registry is an organization that manages top-level domain names. They create domain name extensions, set the rules for that domain name, and work with registrars to sell domain names to the public. For example, VeriSign manages the registration of .(dot)com domain names and their domain name system (DNS).

Domain Registrar: The registrar is an accredited organization, like GoDaddy, that sell domain names to the public. Some have the ability to sell top-level domain names (TLDs) like .com, .net, and .org or country-code Top-level domain names (ccTLDs) such as in, .ca, and us.

Registrant: A registrant is a person or company who registers the domain name. Registrants can manage their domain name’s settings through their registrar. When changes are made to the domain, their registrar will send the information to the registry to be updated and saved in the registry database.

Step 4: Verify from Whois record whether the domain registrar is from India or outside India.

Step 5: If the domain registrar belongs to India then a notice can be issued to the registrar to get details such as:
   a) The uploader of the content (IP address of the uploader)
   b) Date and timestamp of the uploaded content (along with the time zone)
   c) User details if any (such as e-mail address, mobile number while creating account)

Make sure that the URLs hosting abusive content are mentioned properly in the notice.

Step 6: The notice to block/remove the content can also be issued to the registrar. Specify the exact URL of the content

Step 7: If required court notice can also be obtained and sent to ISP to block/remove the content from the website.

Step 8: If the domain registrar is not from India then the MLAT process can be followed to obtain information mentioned in step 5 (a to c).

Step 9: If the suspect has been identified then his/her mobile device/computer system can also be seized for further investigation.

Note 1: A mutual legal assistance treaty (MLAT) is an agreement between two or more countries to gather and exchange information to enforce public or criminal laws.

Note 2: Annexure-A may be referred for the contact details of the service providers

3.3 SOCIAL MEDIA/NETWORKING INVESTIGATION

Step 1: Obtain the screenshot of the abusive content on Facebook, WhatsApp, Twitter, Snapchat, TikTok, etc. from the victim. Soft copy, as well as hard copy of the screenshots, can be kept for evidence purpose. Make sure the exact URL/message/user ID/WhatsApp number/Twitter ID etc. is visible while taking screenshots along with date and time.

Step 2: The victim can be asked to save the messages or to take the backup in case of WhatsApp chat.

Step 3: If uploaded content is video, audio etc., download the content. Calculate the hash value and keep it as evidence. Hash values are fingerprints for files that help to identify any alteration in files.

Step 4: A notice (refer Figures 21-23) can be issued to social media/networking organization u/s 91 of Cr. P.C (Summon to produce documents) to obtain the following details:

Step 6: The notice to block/remove the content can also be issued to the registrar. Specify the exact URL of the content

Step 7: If required court notice can also be obtained and sent to ISP to block/remove the content from the website.

Step 8: If the domain registrar is not from India then the MLAT process can be followed to obtain information mentioned in step 5 (a to c).

Step 9: If the suspect has been identified then his/her mobile device/computer system can also be seized for further investigation.

Note 1: A mutual legal assistance treaty (MLAT) is an agreement between two or more countries to gather and exchange information to enforce public or criminal laws.

Note 2: Annexure-A may be referred for the contact details of the service providers

Also, the URL of the objectionable message can be copied and kept in the case file.

Step 3: If uploaded content is video, audio etc., download the content. Calculate the hash value and keep it as evidence. Hash values are fingerprints for files that help to identify any alteration in files.

Step 4: A notice (refer Figures 21-23) can be issued to social media/networking organization u/s 91 of Cr. P.C (Summon to produce documents) to obtain the following details:

\(^{1}\)FAW as of November 2020 can capture WhatsApp and facebook however facebookId is required for more information please check the following link :https://en.fawproject.com/use-of-the-faw-facebook-tool/
a) The uploader of the content (IP address of the uploader)
b) Date and timestamp of the uploaded content (along with the time zone)
c) User details if any (such as e-mail address, mobile number and alternate e-mail id while creating account)

---

In inviting reference to the case on the subject cited above, this is to intimate that someone has created a fake Facebook account having user name K Kumar impersonating the identity of complainant K Kumar, with an intention to defame, denigrate and demoralize the image of the Complainant in the society. The accused person has morphed the photograph of complainant having pornographic content and has posted published several obscene nude photos containing vulgarity and sexual explicit act and conduct in the said fake account. The URL of the fake Facebook account is:


---

Figure 28: Sample Letter to Facebook for Obtaining Registration access logs details

Note: Annexure-A may be referred for the contact details of the service providers.

Figure 29 is the reference of the law enforcement portal created by Facebook for requesting the user details of the suspect:

URL as follow - https://www.facebook.com/records

---

Figure 29: Sample law enforcement Online Request (FACEBOOK)

---

Figure 30 shows the “Online Portal” of Twitter for Law Enforcement Request:

URL as follow - https://help.twitter.com/forms/lawenforcement

---

Figure 30: Sample Law enforcement Online Request (Twitter)

---

Step 5: A notice can be issued to the social media/networking organization to block the objectionable content. A proper URL for the content should be mentioned in the notice.
INVESTIGATIVE WORKFLOW MANUAL ON CYBER HARASSMENT CASES

Module I – Investigation of Cyber Harassment

5. Email service provider can also be approached.

Step 8: Registration access logs detail obtained from Step 4, can further be analyzed to get hold of the culprit.

Step 9: If the suspect has been identified, then his/her mobile device/computer system can be seized for further investigation.

5.1.3 Fake Social Media profile Investigation

While registering FIR for any cybercrime, (whether it is social media or job fraud or email threatening or any other digital crime), precautions should be taken for the collection of information from complainant and service provider. Let’s take a typical example of the fake profile created in the name of the complainant and understand the investigation procedure.

1. Any case investigation will be started with information gathering from the complainant. For cases like fake profiles, self-attested printout copies of the fake profile need to be printed (where profile ID needs to be clearly mentioned). Soft copies of offensive chat or messages along with the date and time stamps need to be collected.

2. Investigation officer (IO) can request registration details of the fake profile created by the accused. Details may include:
   a. Name
   b. Date of Birth
   c. IP Address
   d. Date and time the profile was created
   e. Email ID if any when the profile was created

3. The above details can be requested using one of the following methods:
   • Issue a code of criminal procedure (Cr P.C.) notice under section 91 to the service provider details of that particular IP.
   • Upon collecting the information about the IP address from the internet service provider or based on local investigations about the relevant scene of the offence, the IO has to plan his actions for search/ seizure as per the appropriate legal provisions under Cr PC.
   • The digital evidence needs to be seized by the accused and also reveal the usage of any other software used by the accused.

4. Upon collecting the information about the related details like name, IP address, date of creation etc. from the service provider, IO should plan for requesting physical location details of the IP address obtained from the above report as per the appropriate legal provisions under Cr P.C.

5. Email service provider can also be approached.

Step 10: The IO has to brief the jurisdictional court and obtain a search warrant to perform search & seizure of the premises where the IP address is traced.

9. To determine whether seized digital evidence from the accused contained evidence regarding usage of the system for creating the fake profile and uploading the offensive photographs of the complainant using any tools or morphing software. Ensure that all the details relevant are furnished along with the expert opinion request.

10. The IO has to brief the jurisdictional court and obtain a search warrant to perform search & seizure of the premises where the IP address is traced.

11. The accused must be arrested and remanded to the court, based on the investigations and evidence collected. The IO has diligently worked along with technical experts to map the information from the social networking site company, ISP and other service providers.

12. It is very important that all the evidence are collected with timestamps and converted into Indian Standard Time (IST). A majority of the service providers are international companies and record the time in their time standards (UTC/GMT, PST etc.)

13. The IO will send the seized articles for forensic examination by preparing a questionnaire related to the case.

3.3.2 Obtain potential evidence/Footprint from Social media platforms

3.3.2.1 Illustration for Facebook

The FAW FACEBOOK tool allows you to acquire the entire profile of a Facebook user quickly and easily.

When the tool is started, the following window is shown in the Figure 31.

The acquisition of the Facebook profile is based on the user ID, therefore it is necessary to retrieve this identification code before starting the acquisition of the profile pages.

If you do not know the user’s Facebook ID, you can retrieve it with the tool made available by FAW – at the end of this guide, you will find the procedure to follow. The Facebook ID must be entered in the text box called “Facebook ID”, after which all the pages of the user profile that can be acquired are visible in the lower part of the window; by default all are selected, but the user can also select only those that interest him.
At this point, you must click on the [F11 – Save] button, in this way an XML file is generated in the acquisition folder of the case called ResultsFACEBOOK001.xml. If the operation is repeated several times (even with different Facebook IDs), other XML files will be created with progressive numbering: ResultsFACEBOOK002.xml
ResultsFACEBOOK003.xml
ResultsFACEBOOK004.xml

The generated XML file must then be opened with the FAW MULTI tool to perform page acquisitions automatically.

By clicking the [Go to FAW Multi] button it is possible to go directly to the FAW MULTI tool with the list of URLs already preloaded and ready to be acquired.

Retrieve the Facebook ID of a user whose login credentials are known

Open FAW and log in to Facebook with the user’s credentials, go to the user profile page by clicking on the thumbnail of your photo. Normally the user profile is visible at an address such as https://www.facebook.com/name.surname.

By pressing the [F11 – Save] button, FAW will start scrolling the chat up to the maximum allowed. The XML file will then be displayed in a new window.

The FAW WHATSAPP tool allows you to acquire WhatsApp Web chats including all the multimedia elements contained in them.

When the tool is started, the FAW window opens with the URL https://web.whatsapp.com already loaded (Fig. 32).

If the FAW FACEBOOK tool is opened and no value appears in the “Facebook ID” text box, it means that the tool was not able to acquire the Facebook ID; in this case, you can try to search for the ID starting from another Facebook page.

Attention: recovering the Facebook ID is currently only possible from the classic version of Facebook, from the new graphic version of Facebook it does not work. However, if you are using the new version of Facebook it is possible to return to the classic view and then recover the Facebook ID.

At this point in the upper FAW menu choose Tools and click on Search Facebook ID, a procedure will start that searches for the Facebook ID within the open page and the recovered ID will be shown in the “Facebook ID” text box of the FAW FACEBOOK tool.

3.3.2.2 Illustration for WhatsApp

The FAW WHATSAPP tool allows you to acquire WhatsApp Web chats including all the multimedia elements contained in them.

At this point, in the FAW top menu choose Tools and click on Search Facebook ID, a procedure will start that searches for the Facebook ID within the open page; once the Facebook ID has been found it will be shown in the “Facebook ID” text box of the FAW FACEBOOK tool.

On the WhatsApp Web home page, the QR Code is shown that the user must frame with their phone to authorize the connection with their phone to retrieve the chat contents.

A few seconds after recognition, the WhatsApp interface appears on the PC screen with all the chats from which you can select the one to acquire (Fig. 33).

At this point, you can decide how to proceed; whether to acquire the chat from a specific date until today or to acquire the whole chat from start to finish.

NOTE: The FAW WHATSAPP tool automatically sets the acquisition mode to “Page Scroll Mode”.

Acquire chat from a specific date to today - Select the chat to capture.

The chat opens in the right area of the page, slide the chat down until you reach the date from which the acquisition must begin.

Run the script to calculate the height of the chat. Open the Tools> Run Script menu and click on wa-chatheight.txt; a pop-up will open indicating the height of the chat in pixels.

Open the FAW configuration by going to Configuration> Preferences> Acquisition and set the “Maximum Scroll Height” value equal to or slightly higher than the height of the chat indicated in the previous pop-up.

Start the acquisition and click on the [Acquire] button, FAW will start scrolling the chat up to the most recent date, the screenshot of the entire chat will be acquired and then it will begin to acquire the objects contained on the page; wait for the operations to finish until the window showing the acquisition files opens.

Capture all chat from start to finish

To acquire all the chat from start to finish, you can use the previous method by scrolling the chat down until you reach the beginning, but if the chat is particularly long you can avoid scrolling all manually using the following procedure.

In the FAW> Acquisition configuration, enable the “WhatsApp Automatic Reverse Scroll” option.

This option causes FAW to automatically scroll the chat to the beginning; once the start is reached, the acquisition is automatically started.

Select the chat to capture.

The chat opens in the right area of the page, scroll the chat down until you reach the date from which the acquisition must begin.

Start the acquisition and click on the [Acquire] button, wait for the end of the acquisition.

FAW as of November 2020 can capture WhatsApp and Facebook however FacebookId is required for more information please check the following link https://en.fawproject.com/use-of-the-faw-facebook-tool/
3.4 INSTANT MESSAGE INVESTIGATION STEPS
(WhatsApp, Facebook Messenger, Telegram and Imo, etc.)

Step 1: Obtain the screenshot of the abusive, derogatory, obscene, bullying etc. content from the victim. Soft copy as well as hard copy of the screenshots can be kept for evidence purpose. Make sure that screenshot includes User ID/Messenger ID.

Step 2: Date and time of the received objectionable message are noted down.

Step 3: Notice can be issued u/s 91 of Cr.P.C. (Summon to produce documents) to Messenger service provider for registration and access logs details. Make sure to clearly mention the User ID/ Messenger ID/Phone number along with the message screenshot (with date and time) while sending notice to the messenger service provider.

Step 4: User access details obtained from the messenger service provider can be analyzed and details obtained can be used for further investigation. There may be a IP address in the details provided, in such case notice can be issued to ISP to provide the details of IP address.

Step 5: MLAT/LoR process needs to be initiated if the source IP is outside the Indian jurisdiction.

Step 6: If suspect is identified then his/her mobile device/computer system can be seized for further investigation.

Figure 34: Procedure for Instant chat investigation

Note: Annexure-A may be referred to for the contact details of the service providers.

3.5 WEB BASED SMS INVESTIGATION

Step 1: Obtain the screenshot of the abusive, derogatory, obscene, bullying etc. message from the victim. Soft copy as well as hard copy of the screenshots can be kept for evidence purpose. Make sure that screenshot should include User ID/Phone Number.

Step 2: Date and time of the received objectionable message should be noted down.

Step 3: Notice can be issued u/s 91 of Cr.P.C. (Summon to produce documents) to web based sms service provider for registration and access log details. Make sure to clearly mention the User ID/Phone number along with the message screenshot (with date and time) while sending notice to the web based sms service provider.

Step 4: User access details obtained from the web based sms service provider can be analyzed and details obtained can be used for further investigation. There may be a IP address in the details provided, in such case notice can be issued to ISP to provide the details of IP address.

Step 5: MLAT process needs to be initiated if source IP is outside the Indian jurisdiction.

Step 6: If suspect is identified then his/her mobile device/computer system can be seized for further investigation.

Figure 35: Procedure for Web based SMS Investigation

Note: Annexure-A may be referred to for the contact details of the service providers.

3.6 MMS INVESTIGATION
Figure 36 shows the detailed steps for MMS Investigation:

Step 1: Obtain the screenshot of the abusive, derogatory, obscene, bullying etc. message from the victim. Soft copy as well as hard copy of the screenshots can be kept for evidence purpose. Make sure that screenshot should include User ID/Phone Number.

Step 2: Date and time of the received objectionable message should be noted down.

Step 3: Notice can be issued to mobile service provider for registration and access log details. Make sure to clearly mention the user ID/Phone number along with the message screenshot (with date and time) while sending notice to the mobile service provider.

Step 4: User access details obtained from the mobile service provider can be analyzed and details obtained can be used for further investigation.

Step 5: MLAT process needs to be initiated if source IP is outside the Indian jurisdiction.

Step 6: If suspect is identified then his/her mobile device/computer system can be seized for further investigation.

Figure 36: MMS Investigation

Note: Annexure-A may be referred to for the contact details of the service providers.

3.7 VoIP CALL INVESTIGATIONS
(WhatsApp, Viber, Messenger)

Voice over Internet Protocol (VoIP) is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. VoIP can be used for fraud purpose as it is difficult to detect frauds committed using VoIP calls. Figure 37 shows the steps for investigating VoIP calls.

Obtain the details of VoIP call (such as calling number) from the victim.

Obtain IPDR details of the victim from the mobile service provider.

Obtain Trunk Gateway (TG) details of the call from the service provider.
After getting details from trunk gateway identify the gateway from where such VoIP calls were originated e.g. Reliance, Airtel etc.

The gateway will furnish further details of VOIP carrier used to route the call which can be like Skype, Nymgo, etc.

VoIP carrier can be further contacted for registration and access logs details of user. These details can be correlated and the culprit can be identified based on the details provided.

MLAT process needs to be initiated if source IP is outside the Indian jurisdiction.

Figure 37: VoIP Call Investigation

Note: Annexure-A may be referred to for the contact details of the service providers.

### 3.8 SUGGESTED WEBSITES FOR INVESTIGATION

<table>
<thead>
<tr>
<th>Modus Operandi</th>
<th>Suggestive Investigative Websites Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website Related Crimes</td>
<td><a href="https://ca.godaddy.com/whois">https://ca.godaddy.com/whois</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://domainbigdata.com/">https://domainbigdata.com/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://centralasps.net/co">https://centralasps.net/co</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://whoisology.com/">http://whoisology.com/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://viewdns.info/">https://viewdns.info/</a></td>
</tr>
<tr>
<td>E-mail Related Crimes</td>
<td><a href="https://mxtoolbox.com/">https://mxtoolbox.com/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://www.whatsmyip.com/email-header-analyzer/">https://www.whatsmyip.com/email-header-analyzer/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://www.iptrackeronline.com/email-header-analysis.php">https://www.iptrackeronline.com/email-header-analysis.php</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://mha.azurewebsites.net/">https://mha.azurewebsites.net/</a></td>
</tr>
<tr>
<td>Social Media Related Crimes</td>
<td><a href="https://lookup-id.com/">https://lookup-id.com/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://youtube.github.io/geo-search-tool/search.html">https://youtube.github.io/geo-search-tool/search.html</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://twitter.com/search-advanced">https://twitter.com/search-advanced</a></td>
</tr>
</tbody>
</table>

Table 11: Websites for investigation

### 3.9 REFERENCES

3. https://www.ipredator.co/cyberstalking/
7. https://www.techopedia.com/definition/29025/doxing
9. https://www.citipostmail.co.uk/blog/how-technology-is-tackling-the-trolls/
4.0 HANDLING CRIME SCENE INVESTIGATION ON CYBER HARASSMENT CASES

4.1 DIGITAL FORENSICS: DEALING WITH THE SCENE OF CRIME

In this module, we will discuss the general guidelines, best practices and the techniques that are to be followed in dealing with the scene of crime related to cyber harassment cases and CSAM crimes, particularly cyberstalking, identity theft, obscenity, bullying, cyber trolling, revenge porn-related digital evidence. This module also explains the procedure for search and seizure, acquisition of digital devices, chain of custody document and CFSL/SFSL questionnaire procedures of electronic evidence.

Follow these steps before starting the Crime Scene Examination:

- To begin with, receive a complaint of the cybercrime/cyber harassment given by the victim or complainant.
- Based on the complaint inputs, perform investigative analysis and enquiry for getting more details.

Note – In case of preliminary forensic examination of the digital evidence, a proper examination report may be prepared by the Cyber Forensic Professional (Cyber unit) in detail in presence of the witness and accused both, as the Investigator officer is not able to technically ponder the testimony of the case during trial.

1. Analyze the Complaint
   - Analyze the complaint using modus operandi and investigation module procedure steps to trace the location of the scene of crime/suspect location

2. Triage Preparedness
   - Prepare the digital forensics toolkit/Evidence triage toolkit (computer disk imaging tools, mobile extraction tools, hashing tools, live evidence extraction tools) for extraction of evidences at the scene of crime

3. Evidence preparedness
   - Prepare the investigation team along with Cyber Forensic Professional to collect the evidences at the scene of crime to avoid breach in chain of custody.
   - Preserving the crime scene by photography & videography
   - Collecting the digital evidences, labelling and packaging
   - Documentation of findings – Filling seizure memo, chain of custody form, producing 65B certificate if required
   - Enquiry at the scene of crime

Figure 38: Steps before start of investigation

4.1.1 Tools and Materials for Collecting Digital Evidence

Crime scene management is an extremely sensitive task where the best practices and relevant toolkits must be used. In addition to tools for processing crime scenes in general, first responders should have the following items as shown in Figure 39 in their digital evidence collection toolkit:

- Fingerprint ink pad and pint cards for elimination prints
- Pocket knife
- Volatile Data Collection Kit – New/Sterilized CDs, DVDs, USB drives and hard disk etc.
- Digital Evidence Storage Containers – anti-static bags, faraday bags, plastic bubble wrap etc.
- Cables – R45, Cross over, USB cables, mobile charging/sync cables etc.
- Physical Acquisition Units/Imaging Tools – UFED Touch / Tableau / Solo 4 etc. for disk duplication
- Hardware Write Blockers & Cables (USB / SCSI / SATA / Firewire etc.)
- Digital Workstation – Laptop with at least i7 processor, 32 GB RAM, 2 TB Hard drives, 2 GB Graphics Processor etc.
- Forms (seizure memo, the chain of custody, forwarding letter, 65-B certificate)
- IQ & Police station seal & stamp & wax
- Magnifier
- Staplers, pin and paper clips
- A Laptop of good configuration, installed with all software tools (For hashing, imaging& analyzing disk, mobile, network & live system data)
- CDs/DVDs/pen drives with portable software tools can be used for hashing, imaging& analysis of data
- Hardware / Software write blocker to protect the suspect media from tampering with the data while doing the hashing, imaging and analysis (if needed)

Figure 39: Indicative Tools & Material Used at Scene of Crime

List of things to be carried by the Investigation officer/team at the Crime Scene
- Cameras (photo and video)
- Cardboard boxes
- Notepads
- Gloves
- Evidence tape
- Paper evidence bags
- Evidence stickers, labels, or tags
- Crime scene tape
- Antistatic bags
- Permanent markers
- Nonmagnetic tools
- First responding officers
- Crime scene personnel
- Consent/search forms
- Crime scene barricade tape
- First-aid kit
- Flashlight and extra batteries
- Markers
- Notebook
- Paper bags
- Personal protective equipment (e.g. gloves)
- Camera (plus memory cards, back up battery, remote flash, tripod and remote cord)
- Evidence seals/tape
- Blank papers, pen & pencils
- Labels / Scales for Photography
- Physical Evidence collection containers
- Evidence Identifiers
- Extension cords

Module II – Crime Scene Management

INVESTIGATIVE WORKFLOW MANUAL ON CYBER HARASSMENT CASES

National Cyber Crime Research & Innovation Centre

Bureau of Police Research & Development
Figure 40: Evidence Duplicators & Extractors

- Disk imaging hardware or software tools for taking a copy of original storage media (suspect media)
- External Sterile Media to store the image (file) of a suspect media

4.2 MATERIAL TO BE USED IN PACKAGING AND TRANSPORTATION OF EVIDENCE

- Anti-static bags for storing the seized electronic media which are prone to damage caused by electrostatic discharge
- Bubble wraps for packaging the seized electronic media to prevent physical damages or scratches
- Tapes (e.g.: transparent or brown) for sealing or packaging
- Anti-static faraday bag for packaging

4.3 PRE-REQUISITES TO HANDLE MOBILE SETS AT THE SCENE OF THE CRIME

- SIM Card Data Extractor/Analyzer
- SD Card/Memory Card Reader
- Cables, power cords for various mobiles
- Forensically sound boot disks like Helix, Palladin, DeFT, porn detection sticks etc. can also be used for the collection and analysis of digital evidence.

Note:

- Portable scanner and portable printers can also be carried to the scene of the crime
- Software or hardware-based tools can be used for the collection and analysis of digital evidence.

The above-mentioned list is not exhaustive. It is an indicative list that has no limit and the kit size depends on the scene of the crime.

4.4 CSAM/OBSCENE/EXPLICIT EVIDENCE EXTRACT TRIAGE TOOLS

The Investigation team shall adopt the following tools and procedures to extract the evidence of CSAM related offences from the suspect’s electronic devices by using live evidence capturing devices some of which are shown in Figure 42.

Figure 42: Forensically Live Evidence Capturing Devices

i. Porn content data recovery USB tools would help to recover the live and deleted obscenity/pornographic content from the culprit’s systems for speedy investigation.

ii. Porn detection and evidence recovery USB tool-kits are designed for scanning a computer system for traces of pornographic material from a suspect’s system.

iii. These triage tools are generally integrated software that forensically scans and provide a detailed report of porn content.

iv. The Porn Detection/Chat Recovery/Voice Recovery Forensic Sticks have recovery functionalities along with a user-friendly operation.

v. The Porn/Chat/Voice USB Sticks effectively scan for deleted images, chat history, voice logs and internet cache files even if the cache files have been deleted. Securely store objectionable images and other evidence.

Note – Cyber Forensic professional will seize the digital device and along with the Seizure memo and handed over to the Investigation officer.

4.5 CRIME SCENE MANAGEMENT

Steps, as shown in Figure 43, are to be followed for properly collecting the evidence or preserving the same based on the scenarios at the digital crime scene.

Figure 43: Evidence Collection & Preservation Procedure
Figure 44 shows the procedure for packaging Digital evidence:

### Packaging Procedure of Digital Evidence

- Case Registration Number (F.I.R. No. / N.C.R. No./C.R. No./A.D.R. No./L.A.C. No. etc.) should be labelled and then the following should be followed:
  - Make sure CD/DVD ROM drives are empty
  - Remove all connections
  - Use gem clip or pin to open ROM drive
  - In the case of multiple computer systems, label each CPU system along with their keyboard, mouse and attached peripherals in order to reconstruct the scene as found
  - Magnetic storage media devices like CDs/DVDs etc. should be packed in an antistatic packaging plastic bag with bubble wraps.
  - Containers used to hold the collected evidences including connecting wires should be properly labelled.

![Figure 44: Packaging Procedure of Digital Evidence](image)

Figure 45 shows a sample Proforma to be labelled on the packaged evidence:

### PROFORMA OF A LABEL ON PACKED EVIDENCE:

- a) Case Registration Number (F.I.R. No. / N.C.R. No./C.R. No./A.D.R. No./L.A.C. No. etc.)
- b) Sections of IPC Act, IT Act and others if any
- c) Date of Seizure
- d) Signatures of Investigating Officer (IO) and two witnesses
- e) Description of the exhibit inside the sealed parcel. E.g. In case of
  - Mobile Phones - Do mention the Make, Model No., Type, IMEI No. etc.
  - SIM Cards - Do mention Make, Card No., SIM serial Number, Colour etc.
  - Memory Cards - Do mention make, type, capacity, any other printed number etc.
  - Hard Disk Drives - Do mention Make, Model No., Serial

![Figure 45: Proforma of a Label on Packed Evidence](image)

Handling of Crime Scene Based on Different Scenarios:

Figure 46: Indicative Crime Scene labelling & numbering procedure

After approaching the crime scene, the system/laptop may be in any of the following modes as shown in Figure 47.

![Figure 47: Crime scene scenarios related to computer system](image)

Broad Crime Scene Scenarios are shown in Figure 48.

![Figure 48: Flow graph of Crime Scene](image)
Photography and Videography Coverage
Take photographs of the Front Panel and Back Panel of the CPU and in case it is a laptop, take photos from different angles to identify the devices connected to the system such as keyboard, mouse, USB devices, external Hard Disk, NIC cards, WiFi or Bluetooth devices etc.

Removing the Power Cable
Remove the power plug from the the CPU and cpu case and take photographs of the "Internal Connectivity of the Devices to the Motherboard" and then remove the Hard Disk Connectivity (Power & Data Cables) from the Motherboard.

Removing the Hard Disk
Remove the Hard Disk and take photographs of the Hard Disk with the Hard Disk Make, Model and Capacity clearly visible. Note down all the details in the Seizure memo like Date & Time of seizure, location, Applicable IT Act section, Jurisdiction of Police station, name of the IO, condition of the system (ON/OFF), seized Digital Storage Devices (Ex: Hard Disk, PenDrive, SD Card etc.), their Make, Model and Capacity.

Calculating the Hash Value
Connect the seized device to Forensic Laptop via WriteBlocker and calculate the hash value of the entire seized storage media using the hashing tools. Fill the details in the seizure memo like software or hardware tool (including the version number) used for hashing and also mention the hash value and the hashing algorithm (SHA-2/SHA-1 etc.) used.

Imaging the Drive
After calculating the hash value, take the Bit Stream Image of the entire storage media using the imaging tools and fill the details in the seizure memo like software or hardware tool (including the version number) used for imaging and store the extracted image file in the external sterile media.

Flowchart 1: If Computer System is OFF-State may follow preservation steps as shown in Figure 49.

Flowchart 2: If Computer System is ON and in Unlocked State, may follow preservation steps as shown in Figure 50.

Photography and Videography Coverage
• Take photographs of the Front Panel and Back Panel of the CPU. In case of a laptop, take photographs from different angles capturing devices connected to the system such as keyboard, mouse, USB devices, external hard disk, NIC cards, WiFi or Bluetooth devices.
• Take the photograph of the screen to have a clear view of data visible on the screen (e.g. opened documents or browsing data) and the date and time of the system.

Isolation of the user from using the System
• Isolate the person (if any) working on the system and interrogate the person for details such as 1) Who had been using the system. 2) How many user accounts are available on the system. What are the general activities for which the system was used Password of the system. 4) BIOS password, if any.

Collection of Live Data
• Check whether there is any Disk/Drive Encryption software installed in culprit's system by using Encrypted Disk Detector (EDD) tool.
• Collect the RAM Dump using FTK Imager/Magnet RAM Capture/Belkasoft acquisition tool/ Volatility/Encase/Helix/OsTriage. Recon can be used for Macintosh.
• Collect the system details like RAM Size, Hard Disk details, System Hardware and installed software details using WinAudit tool.
• Collect the System details, Date & Time using Systeminfo Date & Time Commands.
• Live network traffic acquisition using tools such as wireshark/networkminer/suricata/ ettercap/cain and abel/netsniff-ng.

Isolation of the System from Network Connection
• Isolate the system from the Internet connectivity. If it is connected via NIC cable - remove the cable or if connected via Wi-Fi - switch off the WiFi connection or if connected to Bluetooth - turn off the Bluetooth connection.

Collection of more data relevant to case
• Collect any other information relevant to case like browser history, USB connection details, Registry Dump, Running Process Details etc.
• Note: Any suitable tools for the above purpose can be used.

Capture the live data (RAM Capture):
1. Require blank storage media drive to store the RAMdump.
2. Magnet RAM Capture is a portable tool.
3. The destination drive should be double the capacity of the RAM (if the RAM is 8 GB then the destination drive should be at least 16 GB capacity).
Figure 51: Magnet RAM Capture

Now choose the destination, where the RAM dump file is to be stored then click on start.

Figure 52: Magnet RAM Capture – Saving RAM Capture

RAM Capture: Belkasoft Live RAM Capture is a portable tool. The same steps will be followed as previous steps.

Figure 53: Magnet RAM Capture Processing

Figure 54: Magnet RAM Capture – Capturing Completed

Figure 55: Belkasoft Live RAM Capture

Figure 56: Belkasoft Live RAM Capture - Processing
Photography and Videography Coverage
Take photographs from different angles to identify the devices connected to the system e.g. keyboard, mouse, USB devices, external harddisk, NIC cards, wi-fi or Bluetooth devices.

If the system is Hibernated
Use password cracking tools to login such as Hirensboot.iso/John the ripper/ THC Hydra/medusa/windows password recovery software/Elcomsoft system recovery/passware etc to remove windows operating system password. If successful collect relevant data, else carry on with next step
Hibernate the system to move RAM data (live data) files to hiberfil.sys file, which is available at c:\hyberfil.sys.

Photography and Videography Coverage
Take photographs of Front panel and Back panel of the CPU. In case it is a laptop take photographs from different angles to identify the devices connected to the system e.g. keyboard, mouse, USB devices, external harddisk, NIC cards, wi-fi or Bluetooth devices.

4.6 GUIDELINES FOR MOBILE EVIDENCE SEARCHING & SEIZURE
It is important to understand the best practices stated by the Association of Police Officers (ACPO) of the UK for handling mobile devices and digital evidence along with seizure. The details are shown in Figure 61.

1. Secure and take control of the area containing the equipment. Do not allow others to interact with the device.
2. Photograph the device in situ, or note where it was found and record the status of the device along with on-screen information.
3. If the device is switched on, turn it off. It is important to isolate the device from receiving signals from a network to avoid changes being made to the data it contains.
   Note: It is possible to wipe/factory reset certain devices remotely hence powering off the device would prevent this and must put the mobile device in the flight mode/Airplane mode also switching off the Wi-Fi option in the mobile device.
4. Seize cables, chargers, packaging manuals, phone bills etc. as these may assist the enquiry and minimize the delay in any examination.
5. Packaging materials and associated paperwork may be a good source of PIN/PUK details.
6. Be aware that some mobile phone handsets may have automatic housekeeping functions which clear data after several days. For example, some Symbian phones start clearing call/event logs after 30 days or any other user-defined period. Submit items for examination as soon as possible.
4.7 IMPORTANCE OF HASHING

What is a Hash Function?
A hash function is any well-defined procedure or mathematical function for turning some kind of data into a relatively small integer. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes.

What is Hashing?
In authentication, hashing is used to create a set of numbers that represent a drive or set of files. Hashes in the Digital world are analogous to fingerprints in humans in terms of their uniqueness. Hashing generates a fingerprint from the evidence. No details about the evidence can be determined from the hash value, but if the evidence is altered in any way, the hash value also changes hence alarming about the evidence being tampered.

Note: Hashing is done on the data itself, and not on the names of files.

Important hashing algorithms are:
- SHA1
- SHA2

SHA1 (Secure Hash Algorithm 1)
SHA1 is a 160-bit hash function that is similar to the MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. Cryptographic flaws were discovered in SHA-1 after which it is no longer approved for most cryptographic uses after 2010.

SHA2 (Secure Hash Algorithm 2)
A family of two similar hash functions with different block sizes namely the SHA-256 and SHA-512. They are computed with 32-bit and 64-bit words. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds.

Uses of Hashing
- Verification: This can be used to show that data object (file, partition, disk drive, and media device) has not changed
- Hashing is a way to identify and eliminate all files that contain no potential evidence e.g. Software files
- Identify the "needle in the haystack" – If known, the hash value may help the investigator to find one file out of thousands of other files.
- Hash value match for file exclusion such as operating system files. This is known as Negative Hashing.
- Hash Value Match for File Flagging: A list of hash values for known and sought out files are compiled and can be used to search and identify files of interest to the Investigator as shown in Figure 64 using the file compare utility.

Figure 62: Advisory flowchart for handling procedure of mobile device at crime scene

Figure 63: Flow graph of generating the hash value using hashing algorithms

SHA1 (Secure Hash Algorithm 1)
SHA1 is a 160-bit hash function that is similar to the MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. Cryptographic flaws were discovered in SHA-1 after which it is no longer approved for most cryptographic uses after 2010.

SHA2 (Secure Hash Algorithm 2)
A family of two similar hash functions with different block sizes namely the SHA-256 and SHA-512. They are computed with 32-bit and 64-bit words. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds.

Figure 64: Exemplary Source and Duplication files comparison using hashing tools (Hash Calculator)

Step Action Using FTK Imager (Hashing)

http://csmdf.blogspot.com/2012/10/first-responder flow-chart-for-mobile.html
How to verify the MD5 SHA1 hash value of an image Using FTK Imager:

1. Launch FTK Imager as shown in Figure 65.

2. Select File > Add Evidence Item as shown in Figure 66.

3. Select "Image File" and proceed to add the image shown in Figure 67. The interface confirms the upload of the required file shown in Figure 68.
4. Under the "Evidence Tree", right-click your image and select Verify Drive/Image.
5. Compare the hash value calculated with the known hash value as shown in Figure 69.

How to collect the potential evidence such as multimedia images and documents with FTK Lite version 3.1.1.8
1. Launch FTK Imager and click on the create disk image as shown in Figure 70.

2. Select Evidence > as shown in Figure 71.

Figure 69: FTK Imager – Verifying Image File

Figure 70: Create disk image

Figure 71: Select Evidence
3. Select the evidence folder as shown in Figure 72.

![Figure 72: Select Evidence](image1.png)

4. Evidence Information > then mentioned the case details as shown in figure 73.

![Figure 73: Evidence Information](image2.png)

5. Give the image file destination along with the image name then click on the finish button as shown in figure 74.

![Figure 74: Image file destination](image3.png)

6. After that you will see the image process completion message as shown in figure 75.

![Figure 75: Image Process Completion](image4.png)
7. After completion of the image process we will see the location folder, here we can see the image file along with the image log file and directory listing file as shown in Figure 76.

![Image File Along With the Image Log File](76)

8. Take two files as evidence as you can see the hash value of each evidence along with the full path as shown in figure 77.

![Hash Value of each Evidence along With the Full Path](77)

### 4.8 IMAGING (BIT STREAM IMAGING)

#### 4.8.1 Disk Imaging:

Disk imaging refers to copying the contents of a data storage device or medium and transferring this to another similar medium or device. In its original context, disk imaging implies the creation of an exact duplicate of a computer’s hard disk drive – including its programs, setup and data and then storing this in a special compressed file format. The primary use of disk imaging software is to provide quick and easy backups of computer software and data stored on hard disks. Disk imaging programs backup not only the data but also the computer system and configurations by capturing the image of an active computer system, its structure, registry programs, software, etc.

#### 4.8.2 Forensic Imaging

Forensic imaging refers to creating a bit-by-bit copy or bit stream of the data. Duplicate image means capturing every 1s and 0s on the hard drive, including slack space, unallocated space and the swap.

Types of Imaging:
- **Copy**: Copying data includes only file information, no slack space or unallocated space.
- **Backup**: Backing up of data means files copied for future restoration.
- **Image**: The Image is a file copy of a complete disk used for duplication or restoration.
- **Bit stream copy**: The bit stream copy used for forensics is the replica of all sectors, including every bit (1 and 0). This includes slack space, unallocated space, and swap space.

### Difference between Forensic Imaging and Cloning:

<table>
<thead>
<tr>
<th>Imaging</th>
<th>Cloning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usually refers to making a bit-by-bit copy of a disk partition, compressing it into a file and storing that compressed file image as a backup for future investigation.</td>
<td>Usually refers to creating a bit-by-bit copy of one disk and transferring that to another disk.</td>
</tr>
<tr>
<td>Disks created from imaging are not bootable.</td>
<td>The cloned disk is readily bootable.</td>
</tr>
<tr>
<td>The output is a file.</td>
<td>The output is a disk.</td>
</tr>
<tr>
<td>An imaged disk cannot be tampered.</td>
<td>A cloned disk can be easily tampered.</td>
</tr>
<tr>
<td>An imaged disk can be opened using specific tools such as Encase, FTK, Winhex, and ProDiscover.</td>
<td>A cloned disk needs no specific tools to be read.</td>
</tr>
</tbody>
</table>

| **Table 12:** Table of differences between Imaging & Cloning Procedures |

#### 4.8.3 Step Action of Imaging a Drive using FTK Imager 3.4.2.2

The FTK Imager is a free tool for forensic imaging and hash checking purpose.

FTK Imager is a Windows acquisition tool and it can be downloaded directly from the Access Data website (http://accessdata.com/) free of cost. FTK Imager is available in two formats “FTK Imager” and “FTK Imager Lite”. Both of the software has the same features and functions except that the Lite version can be run from a pendrive or external source hence setup is not required for this version. The version used for this exercise is FTK Imager Lite version 3.4.2.2.

**Usage:**

**Step 1:** To run the application, select the application **FTK Imager**, right-click on it and run as “Administrator”

**Step 2:** The application user interface would be displayed as shown in Figure 78.

![FTK Imager - Application User Interface](78)

Now to create an image, select the icon as shown in Figure 78

**Note:** In this demonstration, we would be using HP 8 GB pendrive to create the Image.

**Step 3:**

After clicking on the icon the next window would be displayed as shown in Figure 78.

**Step 4:**

After selecting the device type, click on “Next” button to proceed as shown in Figure 79
Select the drive for which you want to create an Image as shown below in Figure 80.

*Image log file contain the information pertaining to evidence details along with the image file hash value.
*Directory listing file contain many fields such as full path, hash value, creation date, modification date, access date, file size in byte, file deletion status.

Step 5: After clicking Finish click on the “Add” button as shown in Figure 82 to add the destination location to save the image.
Step 6: Select the image type to be created and click on the "Next" button as shown in Figure 83.

![Select Image Type](Image)

Figure 83: Select the Image type

Step 7: Fill in the evidence item information and click on the "Next" button as shown in Figure 84.

![Evidence Item Information](Image)

Figure 84: Fill in the evidence item information

Step 8: Fill the image destination folder location details and Image Filename details and click on the "Finish" button as shown in Figure 85.

![Select Image Destination](Image)

Figure 85: Fill the image destination folder location details

Step 9: After clicking on the Finish button, all the details will be added as shown in Figure 85. Click on the "Start" button to start the imaging process. The start and progress status of the Imaging process is displayed in Figures 86 and 87.

![Create Image](Image)

Figure 86: Create Image

* FTK Lite Image is the portable application which can run from external USB drive (no need to installation on the target computer).
Step 10: After completion of imaging, the hash value of the image will be calculated using the MD5 and SHA1 algorithm and will be displayed as shown in Figure 89.

Step 11: Click on the “Image Summary” as shown in Figure 90 for details of the pendrive such as model, serial number, number of sectors, cylinders etc.

Note: The detailed report is mentioned in table 13. The hash value must be saved to check the integrity of the image before forensic analysis and after forensics analysis.
4.9 DIGITAL FORENSIC ANALYSIS

The Investigative officer shall extract electronic evidence from the suspect digital devices using below artifacts and procedures as shown in Figure 91.

Table 13: Sample Case Study Summary of Imaging procedure using FTK Imager
5.0 Notices & Responses

The Investigative Officer shall refer to the prototype notices, search and seizure memos, 65(B) I.EA document, 91 Cr. P.C Notice, FSL forward notes, etc. below for acquiring information from different nodal agencies, intermediaries and witnesses.

Prototype Template for requesting certificate u/s 65B I.EA from the Telecom Service Provider (TSP)/Mobile Service Provider (MSP), Internet Service Provider (ISP)/Web Service Provider (WSP):

From
Investigation officer
(Office Address) .............

To
The Nodal officer
(Relevant MSP) .............

------------------------------------------------------------------------------------------------------------------------
U/s.91 Cr.P.C
Sir,

Sub: - Criminal Investigation - Want of Certified CDR as per sec 65(B) of I.EA - Requested- Regarding

Ref: _________________ C.R.No._______/_______

*******

You are requested to provide certified hard copies of the CDR/IPDR/IP/user logs for the number _______ for the period from _______ to _______ and the certificate under sec 65B of Indian Evidence Act for producing the same before the Court. It is also requested that the above mentioned CDR/IPDR/IP/user logs be preserved until the disposal of the case referred above at the court of law.

(Investigation officer)
INVESTIGATIVE WORKFLOW MANUAL ON CYBER HARASSMENT CASES

Module III – Legal Notice and Responses

Prototype Template for Seizure Memo form for Computer / Physical Storage Device

SEIZURE MEMO

1. Name of the party:

2. Place:

3. Computer System: (PC/Other)

4. Configuration of the Machine
   a) No. of Hard Disk:
   b) Capacity of Hard Disk:

5. Back-up device used by the party: (HDD/Other)

6. Operating System: (WINDOWS/DOS/LINUX/Other)

7. Passwords
   1) Log-in Password:
   2) Other Password:

8. Name of the Persons Operating the Computer:

   The victim had received explicit/abusive messages/photos/videos from the suspect and I have taken screenshots of such e-mails and I have downloaded the e-mail along with the e-mail header and have submitted the print outs of the same, I have submitted these documents.

   9. I reaffirm that I have taken screenshots, downloaded the e-mail along with its header and have submitted a copy of these documents. I am aware of how to use e-mails, taking care of e-mail attachments, taking screenshots, downloading e-mail header and taking printouts using a computer and a printer. The computer and printer that I used to perform the above-mentioned activities are working as expected to the best of my knowledge. I have taken these documents in the presence of the victim/complainant with their consent in the presence of two witnesses who can testify if required.

   10. I submit this certificate, along with the above-listed documents, I reconfirm that I have not made any changes to these documents (screenshots, header or printouts).

   Date:        Name of IO:

   Location:        Seal & Signature of IO:

Name, Address & Signature of Witness 1:

Name, Address & Signature of Witness 2:

Name, Address & Signature of the Custodian if any:

Prototype Template for Search & Seizure form for Computer / peripherals.

Computer / Peripheral Evidence Seizure Form

Crime No: _________________ Cyber Crime / PS: ______________

Date: __/__/______ State/UT: New Delhi

Name of the Investigating Officer:

Case Details:

Police Station:

Crime Number:

Seizure Memo Number:

Place of Seizure:

Time of Seizure:

Suspect Name:

Address:

Name of Person from whom evidences seized:

Address:

Way of Possession of Evidence

Name of Witness-1

Address:

Name of Witness-2

Address:

Evidence File Name:

Exhibit condition:

☐ Good  ☐ Damage/broken

Description of the Evidence Packaging after Seizure

☐ Sealed Container/Box

Encrypt/Unencrypt:

☐ Yes  ☐ No

If disk is encrypted/ locked then the password key

Remark if any:

Signature of Investigating Officer along with the department seal impression.
### Evidence Details

<table>
<thead>
<tr>
<th>Item Number</th>
<th>Device</th>
<th>Manufacturer</th>
<th>Model</th>
<th>Serial No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: 1</td>
<td>Desktop</td>
<td>Dell</td>
<td>OptiPlex5060</td>
<td>ABCD12345678</td>
<td>Black colour Dell Desktop in off condition.</td>
</tr>
</tbody>
</table>

### Computer – ON Condition

#### Computer Live Information

- **BIOS Date**
- **Actual Date**
- **Time zone**
- **Operating System**
- **RAM Size**
- **Hash Value (MD5)**
- **Software Used for RAM Dump**
- **Hash Value (SHA1 / SHA256)**

#### Hard Drive Information

- **Hard Drive Type**
- **Model**
- **Hash Value 1 (MD5)**
- **Software / Hardware Used for hashing**

#### Drive Information

- **Image File Name**
- **Storage Type**
- **Model**
- **Drive Size**
- **Hash Value 2 (SHA1 / SHA256)**
- **Write Blocker Used?**

### Computer – OFF Condition

#### Drive Information

- **Hash Value 2 (SHA1 / SHA256)**
- **Write Blocker Used?**

*In the remark section, IO can give details pertaining to the container/box, which he will use during the seizure time.*
**Digital Evidence Collection Form**

**Name of the Authorized Officer:**

**Name of the assessee:**

**Date:** Time: Premise Address:

**Examiner’s Name and Details:**

**Computer Information**

- Laptop
- Desktop
- Server
- File/Folder
- Others

**System State**

If switched On, What is visible on screen?

**System Info**

Make: Model: Serial No: Size: 

Whether Volatile Memory/RAM Memory was collected?

** Shut Down Type**

- Normal
- Power Plug Pulled
- Battery Removed (Laptop)

**Is the suspected media encrypted?**

- Yes
- No

**Type of encryption Software used**

- Seize
- Forensic Previewing
- Imaging
- Backup

**Details of Imaging Software/Version to be given**

**Is the hash value calculated?**

- Yes
- No

Algorithm:

- MD5
- SHA
- OTHERS

**MD5 hash value:**

**SHA hash value:**

**Other Authentication Method:**

**Storage Copy Details**

- Make: Model: Serial No:

**Hard disk Handling:**

- Seize
- Forensic Previewing
- Imaging
- Backup

**Is the hard disk replaced back?**

- Yes
- No

**Date:** Time:

**Is the signature of the witness taken?**

- Yes
- No

**Note by the AO regarding the potential evidences in the digital devices:**

---

**Crime No:** _________________

**Cyber Crime / PS:** ______________

**Date:** __/__/____

**State/UT:** New Delhi

---

**Mobile Seizure Form**

**Name of the Investigating Officer:**

**Case Details:**

**Police Station:**

**Serial Number:**

**Place & Time of Seizure:**

**Suspect Name:**

**Address:**

**Name of Person from whom evidences seized:**

**Address:**

**Way of Possession of Evidence**

**Name of Witness-1**

**Address:**

**Name of Witness-1**

**Address:**

**Exhibit condition:**

- Good
- Damage/broken

**Description of the Evidence Packaging after Seizure (Sealed Container/Box):**

**Description of the Evidence Packaging after Seizure (Sealed Container/Box):**

**Pin/password/pattern:**

- Yes
- No

If it is encrypted/locked then password key

**Remark if any:**

**Signature of Investigating Officer along with the department seal impression:**

---

*In this section ID should mention the way of mobile device possession along with the details of sealed container/box.*
### Device Details

<table>
<thead>
<tr>
<th>Type of Device</th>
<th>Feature Phone □</th>
<th>Smartphone □</th>
<th>Tablet □</th>
<th>Other □</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device System State</td>
<td>On (Unlocked) □</td>
<td>On (Locked) □</td>
<td>Off □</td>
<td>Rooted / Jail □</td>
</tr>
<tr>
<td>Password / PIN / Pattern</td>
<td>![Image of password screen]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Settings Applied

- **Mobile Device**
  - Manufacturer
  - Model Name
  - Model Number
  - IMEI 1
  - IMEI 2
  - FCC ID
  - S/N
  - IMEI
  - Mobile #
- **OS**
- **OS Version**

#### Internal Storage Capacity

- **Internal Storage**
- **External Storage**

#### SIM Card Present?

- **SIM Card Present** □
- **Memory Card Present** □

#### Dual SIM?

- **Dual SIM** □
- **CCID – 1**
- **CCID – 2**
- **IMSI – 1**
- **IMSI – 2**

---

### Mobile Devices Collection Form-Checklist

- **Name of the Authorized Officer:**
- **Name of the assessee:**
- **Date:** □
- **Time:** □
- **Premise Address:**

#### Examiner’s Name and Details:

- **If switched On, What is visible on screen?**
  - **On**
  - **Off**
  - **Hibernate/Standby**

#### System Info

- **Make:**
- **Model:**
- **Mobile Type:**
  - GSM □
  - CDMA □
  - 3G □
  - Others □
- **If Others Specify:**

#### Time Zone Setting:

- **Date/Time of Mobile Phone:**
- **Actual Date/Time:**

#### IMEI/MESID Number

- **IMEI/MESID Number:**

#### Mobile Serial Number (if any)

- **Operating System** (Including Version Number)

- **Is the SIM Card Present?**
  - **SIM Service Provider Name:**
  - **SIM Card Size:**
  - **IMSI Card Number:**

#### Mobile Phone State:

- **OFF**
- **OFFLINE**
- **NORMAL**
- **BATTERY PULLED**

#### Does the Assessee phone has the ability to access Internet?

- **Yes** □
- **No** □

#### Storage Copy Details:

- **Make:**
- **Model:**

#### Working Copy Details:

- **Make:**
- **Model:**

---

Bureau of Police Research & Development

National Cyber Crime Research & Innovation Centre
Module III – Legal Notice and Responses

Forwarding Proforma

Send the exhibits which require forensic examination and expert opinion to the designated laboratory in strong and sturdy packaging and in sealed condition along with duly filled in forwarding proforma (FSL/CFSL form), specimen seal impression and other relevant documents useful for the laboratory examination.

Crime No: _________________ Cyber Crime / PS: ______________
Date: __/__/____ State/UT: New Delhi

I. Nature of Crime

Nature of Crime: ____________________________________________________________________

Brief History: ____________________________________________________________________

Any other relevant details: ____________________________________________________________________

II – List of Exhibits for Examination

<table>
<thead>
<tr>
<th>Sr. No. / Barcode</th>
<th>Description of Exhibits</th>
<th>Who, where, and by whom found</th>
<th>Source of exhibits</th>
<th>Remarks</th>
</tr>
</thead>
</table>

III – Nature of Examination required

<table>
<thead>
<tr>
<th>Sr. No. / Barcode</th>
<th>Description of Exhibits</th>
<th>Nature of Examination required</th>
<th>Date or any keyword or Filter</th>
<th>Remarks</th>
</tr>
</thead>
</table>

Certificate of Authority

Certified that the Director has the authority to examine the exhibits sent to him in connection with Case No. ____________

Date: __/__/____ State: ______________

Certificate of Authority

Certified that the Director has the authority to examine the exhibits sent to him in connection with Case No. ____________

Date: __/__/____ State: ______________

5.1 SUGGESTED FORENSIC/INVESTIGATIVE TOOLS FOR COMBATING CSAM CRIMES

<table>
<thead>
<tr>
<th>S. No</th>
<th>Suggestive/Advisory Tools for Forensic Analysis/investigation</th>
<th>Tool Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Microsoft PhotoDNA</td>
<td>PhotoDNA creates a unique digital signature known as a hash of an image which is then compared against signatures (hashes) of other photos to find copies of the same image. PhotoDNA is an incredible tool to detect, disrupt and report the distribution of child exploitation material. Download Link: <a href="https://www.microsoft.com/en-us/photodna">https://www.microsoft.com/en-us/photodna</a></td>
</tr>
<tr>
<td>5.1</td>
<td>Sweetie 2.0 project</td>
<td>The Sweetie 2.0 software is used for mapping, measuring and combating online child abuse. One of the most innovative functions is the automation of responsive communication with online chat partners through a personalized chat robot in various communication channels. Download Link: <a href="https://www.terredeshommes.nl/en/sweetie-20-stop-webcam-childsex">https://www.terredeshommes.nl/en/sweetie-20-stop-webcam-childsex</a></td>
</tr>
</tbody>
</table>

## S. No | Suggestive/Advisory Tools for Forensic Analysis/Investigation | Tool Description
--- | --- | ---
1 | Thorn-Spotlight | Spotlight is a victim identification tool used by Law Enforcement Agencies to aid in juvenile sex trafficking investigations. Download Link: [https://www.thorn.org/spotlight/](https://www.thorn.org/spotlight/)
2 | Porn detection Sticks | The porn detection sticks are designed to scan all images and videos on your computer for illicit images. It’s nearly impossible to keep any computer connected to the internet clean from pornography, even with programs that are designed to prevent access to porn. The porn detection stick will not only scan your system for pornography, it will securely wipe any traces of such images and videos permanently. Download/Product View Link: [https://paraben-sticks.com/index.php/product/porn-detection-stick-for-windows-os/](https://paraben-sticks.com/index.php/product/porn-detection-stick-for-windows-os/)

### 5.2 SUGGESTED FORENSIC/INVESTIGATIVE WEBSITES AND PLUGINS RELATED TO CYBER HARASSMENT CRIMES

**Important Tools/Websites**

- https://cybercrime.gov.in/
- https://getsafer.io/
- [Spotlight Thorn.org/spotlight](https://www.thorn.org/spotlight)
- [https://osintframework.com/](https://osintframework.com/)
- [https://www.shodan.io/](https://www.shodan.io/)

**Suggestive Websites Name**

- https://cybercrime.gov.in/
- https://getsafer.io/
- [Spotlight Thorn.org/spotlight](https://www.thorn.org/spotlight)
- [https://osintframework.com/](https://osintframework.com/)
- [https://www.shodan.io/](https://www.shodan.io/)

---

### 5.3 REFERENCES

2. 50af96983a8
3. [https://research.icainline.org/volume68/number23/pwc.3887435.pdf](https://research.icainline.org/volume68/number23/pwc.3887435.pdf)
5. SOP_a_forensic_guide_for_crime_investigators by Lok Nayak Jayaprakash Narayan National Institute of Criminology and Forensic Science
6. SOP Guideline Manual for Searching & Seizure by SFSL Maharashtra
7. DSCII Cyber Crime Investigation Manual
8. 65(B) Circular by Tamil Nadu Police
6.0 CYBER HARASSMENT LAW PERSPECTIVES

Forbes defines online harassment or cyber harassment as repeated online expressions amounting to a "course of conduct" targeted at a particular person that causes the targeted individual substantial emotional distress and/or the fear of bodily harm.

In India, there is no concrete any definition of online harassment. Online harassment also encompasses sexual harassment which is defined under section 2(n) of the Sexual Harassment of Women at Workplace (prevention, prohibition, and redressal) Act 2013 as unwelcomed. Few terms in the Act include:

- contact and advances
- a demand or request for sexual favours
- making sexually coloured remarks
- showing pornography
- any other unwelcome physical, verbal or non-verbal conduct of sexual nature

6.1 CYBER HARASSMENT CASES AT A RISE

No one can deny the positive role of cyberspace in today’s world whether in political, economic or social spheres of life. But everything has some pros and cons. On one hand, Information Technology has been a boon as it has paved way for a new world of the Internet, business networking, e-commerce, etc. which is not only time saving and speedy but also easier to use. On the other hand, it has been used by people with a criminal band of mind to interfere with the internet accounts through various unauthorized techniques such as spoofing, phishing etc. and used the information to gain profits out of the target’s account.

Cyber-crime has been on a constant rise since its inception. It’s not that no laws are regulating it but sometimes the laws are not adequate and sometimes because of various loopholes in them the criminal escapes easily.

Cyber-crimes in India almost doubled in 2017, according to statistics released by the National Crime Records Bureau (NCRB). The data comes in the backdrop of India aspiring to become a trillion-dollar digital economy. Interestingly, cyber-crimes accounted for less than a percentage (0.43%) or 21,796 cases of a total of 50,07,044 cognizable crimes in 2017.

According to the NCRB record, India has recorded a massive increase of 63.5% in cybercrime cases in 2019. Cyber Harassment is one of the cyber-crimes. It impacts the affected individual not only physically but also mentally and emotionally. Factors such as poor social perception towards crime, cultural conflict and ignorance, subjective characteristics, freedom and remoteness of internet technologies and inadequacy of cyber legislation in preventing and penalizing the crime have facilitated the rapid growth and proliferation of cyber harassment cases in India. In addition to this victim’s lack of awareness, fear of being excluded from society, shame etc. there has been less reporting in such cases. According to the NCRB report, the crime against women has increased from 749 in 2014, 792 in 2015 to 930 cases in 2016. These are the cases reported; however, the conviction rate is pretty low.

Though there have been cases in the past related to cyber harassment but due to lack of evidence and inadequate knowledge of the person handling them a very low conviction rate has been observed in such cases. Earlier modules have dealt with the collection, handling and preservation of evidence and this module will help in applying the relevant section of Acts for various categories of cyber harassment crimes.

6.2 LEGAL PROVISIONS RELATED TO CYBER CRIME

Table 16 is intended to help the Investigating Officers understand the different IT acts and their scope while presenting a case in the court of law. The various possible acts dealing with cyber-crimes (cyber harassment cases) that can be applied are briefly tabulated for the convenience of Investigating Officer. Apart from this, various court judgments have been listed which the Investigating Officer can refer while handling similar cyber offences. This acts as a guide to proceed with such cases. Also, various committees and portals of the government from different domains have been mentioned which will further assist the Investigating Officer to carry investigations properly.

<table>
<thead>
<tr>
<th>Types of Cyber Harassment</th>
<th>Information Technology Act</th>
<th>Indian Penal Code</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Legal Provisions for punishments of cybercrimes in India</th>
<th>Supreme Court/ High Court/ other courts Judgments</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Anti-Bullying Committee in schools, as per CBSE guidelines</td>
<td>S-354D</td>
</tr>
</tbody>
</table>

- State v. Jayanta Kumar Das & Ors (2012)
- State v. Jogesh Kwatra (2014)
<table>
<thead>
<tr>
<th>Types of Cyber Harassment</th>
<th>Information Technology Act</th>
<th>Indian Penal Code</th>
<th>POCSO/ Indecent Representation of Women(Prohibition) Act/ Copyright Act etc.</th>
<th>Supreme Court/ High Court/ other courts Judgments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pranab Mukherjee’s daughter stalking case (2017)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Karan Girotra v. State(Bihar) Act 1989 S-3(4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Manish Khatra Case (2008)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Cyber Crime Prevention against Women and Children (Cyber) Act 2013 Dol</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• @CyberDost - Cyber Crime Departments/ Digital Portals</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Ministry of Electronics and Information Technology (MeIT), has issued an Advisory under Information Technology Act, 2000 for Online Matrimonial Websites service</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. The Young Persons (Harmful Publications) Act 1956 S-3 r/w S-6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. The Scheduled Cases and the scheduled Tribes (Prevention of Atrocities) Act, 1989 S-3(4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Sajay Sharma Bz.: State of UP Bible(2016) Dol</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• N/L Bloomberg Finance LP v. State of Karnataka(2013) Kar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Mghnsas BPO Fraud case (2005)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Andhra Pradesh Tax Case</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• State of Tamil Nadu v. Suharuni(2004) CMM Egmore</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NASSCOM v. Ajay SoodBzDrs (2005) Kar HC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Ministry of Women and Child Development has a dedicated e-mail address <a href="mailto:complaint-mecd@gov.in">complaint-mecd@gov.in</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• State v. Arunkumar(Kuma) Addin St, Del</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NaelanVidhwakarma v State of MP(2017)MP HC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Smt. Amini Chaudhary v State of MP(2013) MP HC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Sajeev Krishnan v. State of Kerala (2012) Ker HC</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Types of Cyber Harassment</th>
<th>Information Technology Act</th>
<th>Indian Penal Code</th>
<th>POCSO/ Indecent Representation of Women(Prohibition) Act/ Copyright Act etc.</th>
<th>Supreme Court/ High Court/ other courts Judgments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. The Scheduled Cases and the scheduled Tribes (Prevention of Atrocities) Act, 1989 S-3(4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Sajeesh Krishnan v. State of Kerala (2012) Ker HC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Ministry of Women and Child Development has a dedicated e-mail address <a href="mailto:complaint-mecd@gov.in">complaint-mecd@gov.in</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. The Scheduled Cases and the scheduled Tribes (Prevention of Atrocities) Act, 1989 S-3(4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Sajeesh Krishnan v. State of Kerala (2012) Ker HC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Ministry of Women and Child Development has a dedicated e-mail address <a href="mailto:complaint-mecd@gov.in">complaint-mecd@gov.in</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. The Scheduled Cases and the scheduled Tribes (Prevention of Atrocities) Act, 1989 S-3(4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Ministry of Women and Child Development has a dedicated e-mail address <a href="mailto:complaint-mecd@gov.in">complaint-mecd@gov.in</a></td>
<td></td>
</tr>
</tbody>
</table>
### Types of Cyber Harassment

<table>
<thead>
<tr>
<th>Legal Provisions for punishments of cybercrimes in India</th>
<th>Supreme Court/ High Court/ other courts Judgments</th>
<th>Committees formed/ Advisory issued by Government Departments/ Digital Portals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Technology Act</td>
<td>POCOSO/ Indecent Representation of Women(Prohibition) Act/ Copyright Act etc.</td>
<td>Committees formed/ Advisory issued by Government Departments/ Digital Portals</td>
</tr>
<tr>
<td>Indian Penal Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revenge Porn</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-46E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-67</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-67A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-67B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-354C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-354D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-354A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-292</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-294</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-506</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-507</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-509</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Indecent Representation of woman</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-4 r/w S-6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Aneemesh Bakshi v Bengal CID(2018) JM, WB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. State v Harish@Chirag (2013) Addin SJ, Del</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Table 16: Legal provisions related to cyber crimes

### 6.3 References:

#### 6.3.1 Acts:
- Information Technology Act, 2000
- Indian Penal Code, 1860
- Protection of Children from Sexual Offences (POCSO) Act, 2012
- The Indecent Representation of Women (Prohibition) Act, 1986
- Copyright Act, 1957
- Young Persons (Harmful Publications) Act, 1956
- The Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act, 1989

#### 6.3.2 Websites for cases and Committees:
- https://indiankanoon.org/
- https://www.manupatrafast.com/
- https://www.prsindia.org/
- https://indiankanoon.org/doc/35556724/
- https://www.cybercrime.gov.in
- http://ncwapps.nic.in/onlinecomplaintsv2/
7.0 CYBER SAFETY & AWARENESS

Cyber harassment awareness is crucial for protecting the safety of victims all over the world. For this, parents, students and law enforcement agencies should all be provided education and awareness about the warning signs of cyber harassment and to proactively take steps to prevent it.

7.1 STALKER’S STRATEGIES

Stalkers use many strategies to scare and trap their victims. Following are few tactics used:

• Frequent calls, e-mails, texts and messages to make a contact with the victim.
• Following them through social media platforms, apps, GPS etc.
• Spreading online rumours through fake images, videos.
• Damage their reputation and image.
• Account and password hacking and executing financial frauds.
• Gathering of information through the internet.

7.2 HARASSMENT WARNING SIGNS

- Considerable increase or decrease in usage of a mobile, laptop or tablet.
- Frequent emotional responses such as sadness, anger or happiness
- Hiding of the device screen when others are close by
- Sudden deactivation of their social media accounts or opening of new ones
- Increased concern about their reputation
- Failure to take responsibility for their actions

7.3 ONLINE MONITORING

- More computer or tablet use
- More texting
- Overly emotional (laughing, anger, upset, depressed)
- Hiding phone or computer screen
- Sits alone isolated
7.4 CYBER HARASSMENT - HARMFUL EFFECTS

- **Physical Ailments:** Headache, stomachache, ulcers, changes in eating habits like skipping meals etc.
- **Psychological Disorders:** Anxiety, stress, depression, insomnia
- **Fearful and Powerless:** a heightened sense of fear because they feel unsafe even at home and no power to give it back to them
- **Anger and Bitterness**
- **Lack of self-confidence, self-esteem**
- **Suicide Ideation**

7.5 PREVENTIVE STEPS

Prevention programs aim to prevent the victim from being harassed and what steps and actions are to be taken to avoid and tackle the victim. Parents and educators should remain vigilant and apply the following tips to prevent online harassment.

**Do’s**
- Frequent password change of social media accounts
- Undergo Internet privacy and safety programs
- Acceptable policies (no harassment)
- Use encryption
- Maintain social media hygiene
- Keep software updated
- Do not leave your computer logged in and unattended

**Don’t**
- Don’t overshare
- Do not leave data unattended
- Do not attack or insult anyone while participating in discussion groups.

7.6 POST INCIDENT STEPS ARE TO BE TAKEN IN CASE ANY WARNING SIGNS ARE OBSERVED

**Steps**
- **Conversation**
  - Talk to learn what is happening, how it started, and who is involved.
- **Support**
  - Parents, peers, teachers should help and guide the victims to recover from harassment impact.
- **Record the evidence**
  - Include text messages, e-mails, screenshots, IP addresses, dates and time as well.
- **Report**
  - Report the problem to school authorities, local police, Online Portal, other LEAs, service providers.
  - Keep social media accounts private so that user has full control on his public data.
- **Block**
  - Block or filter messages from the harasser immediately and if they create new accounts, block them too.

7.7 REPORTING PROCEDURE - CYBER HARASSMENT CASES

Platforms on which reporting can be done are:
- National Cyber Crime Reporting Portal
- Social Media Platforms
- Local Police / LEAs
- School Administration
- Online Service Providers

7.7.1 National Cyber Crime Reporting Portal

These crimes are to be reported on the “National Cyber Crime Reporting Portal” which is an initiative by the Government of India. This is a platform for victims to file a complaint against cyber-crime with all the relevant and accurate information of crime which is further used by the law enforcement agencies/ police for action.

The portal provides an option for two categories of crime: one for reporting crimes against women and
children and the other for general cyber-crime as shown in Figure 97.

Following are the steps taken to report cyber-crime on the reporting portal:

**Step 1:** Open the National Cyber Crime Reporting Portal and click on “File a Complaint” as shown in Figure 97.

**Step 2:** Accept the terms and conditions and choose the type of report you want to file: Cybercrime related to Women/Child or other cybercrime shown in Figure 98-100.

**Step 3:** The victim can report his/her complaint anonymously without fear from anyone and the same can be tracked anytime.

**Step 4:** Enter the details required: Complaint and incident details, suspect details as shown in Figure 100.

**Step 5:** Submit the report.

### 7.7.2 Social Media Reporting

Report the matter on your social media account where the harassment has taken place. On every platform, there is an option to block the person and report the post/tweet or any undesirable image or
video. An example of reporting the same on Twitter is shown in Figure 101.

7.7.3 Local Police/LEAs Reporting

Victims can report harassment matter to Local Police or Law Enforcement Agencies if it involves taking photos, videos that invade someone’s privacy, hate crimes, pornography and threats of violence. Police would take the appropriate steps to stop the harassment and track the victim.

7.7.4 School Administration

Taking the matter to a teacher, school counsellor, or principal can help to curb the effect of cyber harassment committed by another classmate.

School staff can help the child/victim to feel safe in the class and cope with the harassment effects.

7.7.5 Online Service Providers

If there is a violation of online service providers terms of service agreements, then the victim should review the terms of service to pinpoint what specific terms violate which clauses of the agreement. The same can be done by reporting and sharing feedback in the respective online service provider’s help section. An example of Google account reporting is shown in Figure 102 below.

7.8 VICTIM COUNSELLING

Professional counsellors are people who help victims overcome their pain and self-esteem issues by using different methods and strategies which help the victim to express themselves. They play an important role in eliminating cyber harassment effects by providing counselling sessions to students, parents, teachers, addressing issues and working on their solutions.

Practices used by counsellors can be divided into categories mentioned in Figure 103:
7.8.1 Student Counselling

Help them Speak Out: People who have been victims of cyber harassment are reluctant to speak out about their incidents. This may be because of their fear of embarrassment. Counsellors help and encourage them in improving their openness and speak out about their problems.

Addressing Issues: Healthy discussions with students about their feelings of being victimized, understanding emotions, identifying their weaknesses and strengths and determining causes of cyber harassment.

Workshops and Training: Including anger management, social skill building, decision making, boosting self-confidence/ self-esteem, stress management, goal setting, coping skills etc. A few of them are shown in Figure 104.

7.8.2 Parent-Driven Counselling

Practices which are to be followed by parents are shown in Figure 105.

Parental Control: Educating children about signs of harassment, how to monitor their child by using parental control applications, filtering the internet content, applying privacy settings may help them to control their child.

Preventive Steps: Counselors should have conversation with parents and recommend them steps they should take at home to protect their child.

Safe Use of Technology: Imparting them knowledge about use of technology, safety software, password protection etc.

7.8.3 School-Driven Counselling

Practices which are to be followed by Schools are shown in Figure 106.

Develop Guidelines: Anti-cyber harassment instructions and policies should be developed and implemented including a prevention plan in order to restrict the use of internet and limit harassment cases.

Educate: Counsellors should educate students and teachers about harmful effects and preventive measures of cyber harassment, encourage students to report incidents to their peers, school administration, parents or teachers.

Peer help program: Counsellors can appoint student leaders to interact with classmates and let them share their experiences. Peers should be receptive enough and encourage open communication. This would help to connect with them more easily and create a safe atmosphere which would in turn bring togetherness.

7.9 Cyber Crime Categories, Symptoms and Actionable Steps (Victim’s Perspective)

<table>
<thead>
<tr>
<th>Categories</th>
<th>Symptoms</th>
<th>Action Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Bullying</td>
<td>• Being emotional or upset</td>
<td>• Conversation</td>
</tr>
<tr>
<td></td>
<td>• Avoid gatherings</td>
<td>• Block</td>
</tr>
<tr>
<td></td>
<td>• Physical health affected</td>
<td>• Record the evidence</td>
</tr>
<tr>
<td></td>
<td>• Decrease in academic performance</td>
<td>• Report</td>
</tr>
<tr>
<td>Cyber Teasing</td>
<td>• Hurtful messages</td>
<td>• Talk with trusted adults or</td>
</tr>
<tr>
<td></td>
<td>• Get upset by the interaction</td>
<td>supportive peers.</td>
</tr>
<tr>
<td></td>
<td>• Repeatedly communication</td>
<td>• Stop communication</td>
</tr>
<tr>
<td></td>
<td>• Feeling of powerless</td>
<td>• Follow guidelines on healthy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and respectful communication</td>
</tr>
<tr>
<td>Cyber Stalking</td>
<td>• Frequent and inappropriate messages online</td>
<td>• Change e-mail id or passwords</td>
</tr>
<tr>
<td></td>
<td>• Following/ Chasing all social media account</td>
<td>• Collect the evidence of</td>
</tr>
<tr>
<td></td>
<td>• Too much and unwanted communication</td>
<td>conversations</td>
</tr>
<tr>
<td></td>
<td>• Monitoring extensively</td>
<td>• Block the stalker</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Report</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>• Withdrawal from your bank</td>
<td>• Change your passwords</td>
</tr>
<tr>
<td></td>
<td>• Unfamiliar account or charges on your credit report</td>
<td>• Notify financial institution</td>
</tr>
<tr>
<td></td>
<td>• If cards goes missing</td>
<td>about the fraud</td>
</tr>
<tr>
<td></td>
<td>• Missing e-mails or bills</td>
<td>• Freeze your cards immediately</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create a theft report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Review your transactions for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>more information</td>
</tr>
</tbody>
</table>
1. Learn to Identify Suspected Phishing Emails. There are some qualities that identify an attack through an email:
   - They duplicate the image of a real company.
   - Copy the name of a company or an actual employee of the company.
   - Include sites that are visually similar to a real business.
   - Promote gifts or the loss of an existing account.

---

### Preventive Security Measures for Phishing Attacks

1. Learn to Identify Suspected Phishing Emails. There are some qualities that identify an attack through an email:
   - Promote gifts or the loss of an existing account.
   - Include sites that are visually similar to a real business.
   - They duplicate the image of a real company.
   - Copy the name of a company or an actual employee of the company.

---

### References

- [https://files.eric.ed.gov/fulltext/EJ1182235.pdf](https://files.eric.ed.gov/fulltext/EJ1182235.pdf)
- [https://www.connectsafely.org/tips-to-help-stop-cyberbullying/](https://www.connectsafely.org/tips-to-help-stop-cyberbullying/)
- [https://www.pandasecurity.com/mediacenter/panda-security/how-to-handle-online-harassment/](https://www.pandasecurity.com/mediacenter/panda-security/how-to-handle-online-harassment/)
• https://www.ccohs.ca/oshanswers/psychosocial/cyberbullying.html
• https://www.takebackthetech.net/be-safe/cyberstalking-strategies
• https://americanspcc.org/cyberbullying-learn-the-signs/
• https://www.verywellfamily.com/what-are-the-effects-of-cyberbullying-460558
• https://www.thehindubusinessline.com/info-tech/a-parental-control-app-for-tracking-kids-online-activities-ep/article24175094.ece#
• https://www.pandasecurity.com/mediacenter/security/10-tips-prevent-phishing-attacks/

Annexure-A

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Name of the service provider</th>
<th>Area Of Operation</th>
<th>E-mail ID/Reporting Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Facebook</td>
<td>All India</td>
<td><a href="https://www.facebook.com/records/login/">https://www.facebook.com/records/login/</a></td>
</tr>
<tr>
<td>2</td>
<td>Instagram</td>
<td>All India</td>
<td><a href="https://www.facebook.com/records/login/">https://www.facebook.com/records/login/</a></td>
</tr>
<tr>
<td>3</td>
<td>Pinterest</td>
<td>All India</td>
<td><a href="https://help.pinterest.com/en/law-enforcement">https://help.pinterest.com/en/law-enforcement</a></td>
</tr>
<tr>
<td>4</td>
<td>Twitter</td>
<td>All India</td>
<td><a href="https://legalrequests.twitter.com/forms/landingDisclaimer">https://legalrequests.twitter.com/forms/landingDisclaimer</a> E-mail ID: <a href="mailto:lawenforcement@twitter.com">lawenforcement@twitter.com</a></td>
</tr>
<tr>
<td>5</td>
<td>Google/Gmail/</td>
<td>All India</td>
<td><a href="mailto:gitanjli@google.com">gitanjli@google.com</a>, <a href="mailto:lis-apac@google.com">lis-apac@google.com</a></td>
</tr>
<tr>
<td>6</td>
<td>Microsoft</td>
<td>All India</td>
<td><a href="mailto:indiacc@microsoft.com">indiacc@microsoft.com</a></td>
</tr>
<tr>
<td>7</td>
<td>Rediff</td>
<td>All India</td>
<td><a href="mailto:legal@rediff.co.in">legal@rediff.co.in</a></td>
</tr>
<tr>
<td>8</td>
<td>Sify</td>
<td>All India</td>
<td><a href="mailto:leasupport@sifycorp.com">leasupport@sifycorp.com</a></td>
</tr>
<tr>
<td>9</td>
<td>Skype</td>
<td>All India</td>
<td><a href="mailto:lerm@skype.net">lerm@skype.net</a></td>
</tr>
<tr>
<td>10</td>
<td>Flipkart</td>
<td>All India</td>
<td><a href="mailto:murthy.sn@flipkart.com">murthy.sn@flipkart.com</a>,</td>
</tr>
<tr>
<td>11</td>
<td>Amazon</td>
<td>All India</td>
<td><a href="mailto:police-inquiries@amazon.in">police-inquiries@amazon.in</a>,</td>
</tr>
<tr>
<td>12</td>
<td>yahoo</td>
<td>All India</td>
<td><a href="mailto:robinfe@yahoo-inc.com">robinfe@yahoo-inc.com</a></td>
</tr>
<tr>
<td>13</td>
<td>Paytm</td>
<td>All India</td>
<td><a href="mailto:cybercell@paytm.com">cybercell@paytm.com</a></td>
</tr>
<tr>
<td>14</td>
<td>mobikwik</td>
<td>All India</td>
<td><a href="mailto:risks@mobikwik.com">risks@mobikwik.com</a></td>
</tr>
</tbody>
</table>
## Annexure-B

### Form To Report Cyber Harassment Incident

1. **Complainant Details**
   - Name
   - Address
   - E-mail id
   - Mobile No.

2. **Type of Incident (tick whichever is applicable)**
   - Cyber Bullying
   - Cyber Teasing
   - Cyber Stalking
   - Cyber Defamation
   - Identity Theft
   - Catfishing
   - Doxing
   - Swatting
   - Trolling
   - Revenge Porn

3. **Date and Time of incident (specify time zone)**

4. **Description of incident**

5. **Details of harasser (if known)**
   - Name
   - Address
   - E-mail id
   - Mobile No.

6. **Evidence Available (Tick Applicable)**
   - Original E-mail
   - E-mail header
   - SMS
   - MMS
   - Facebook Screenshots/URL
   - Twitter Message/Handle
   - YouTube video/URL
   - Website URL/screenshot
   - WhatsApp Message/screenshot
   - audio/video message