Audit of Fraud
Fraud Detection Techniques & Forensic Audit

Case Studies
1) Fraudulent drawal and expenditure
2) Cyber Crimes (Vol.II)

Indian Audit & Accounts Department
Regional Training Institute
26/1, Civil Lines, Nagpur
E-mail: rtiaadnr_ngp@sancharnet.in
Phone: (0712) - 2545420, 2545816, 2545829
Fax: 0712-2562577
From PD’s Desk

As a part of our pursuit towards excellence in training in the area of “Audit of Fraud, fraud Detection techniques, and Forensic Audit”, we bring out a series of cases of frauds reported in the audit reports of the Comptroller and Auditor General of India, as case studies. Simultaneously, we also endeavor to consolidate the approach and methodology followed by fraudsters in committing them as well as the manner in which they were prevented/detected.

These case studies have been prepared based on the material reported under para 4.1.1 of the report of the Comptroller and Auditor General of India for the year ended 31 March 2001 (Civil) Government of Bihar and the material received from Cyber Crime Investigation Cell, Mumbai.

I take this opportunity to extend my sincere thanks to Shri Arun Kumar Singh, Principal Accountant General (Audit), Bihar, Patna, who made us available all the relevant documents of the case (para 4.1.1 of the report of the Comptroller and Auditor General of India for the year ended 31st March 2001 (Civil) Government of Bihar), whenever requested for. I am also thankful to him for arranging for validation of the facts reported and conclusions drawn in the case study.

I also thank Shri Mukund Pawar, Police Commissioner, Cyber Crime Investigation, Crime Branch, Mumbai for making us available case studies in marathi which were translated by my Core Faculty.

I commend the efforts of Smt.R.R.Shahare, Asstt.Audit Officer /Core Faculty in preparing the case study “Fraudulent drawal and expenditure” on the lines directed from time to time.

I hope that the readers would benefit from this. Their suggestions, if any, would help us in future such attempts.

Principal Director
<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Topic</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fraudulent drawal and expenditure</td>
<td>1-19</td>
</tr>
<tr>
<td>2</td>
<td>Fraud through Internet</td>
<td>20-22</td>
</tr>
<tr>
<td>3</td>
<td>Phishing Case</td>
<td>23-24</td>
</tr>
<tr>
<td>4</td>
<td>Porn E-mail</td>
<td>25-26</td>
</tr>
<tr>
<td>5</td>
<td>Hurting Religious Sentiments</td>
<td>27-28</td>
</tr>
<tr>
<td>6</td>
<td>Credit Card Fraud</td>
<td>29-30</td>
</tr>
<tr>
<td>7</td>
<td>Cheating through Internet</td>
<td>31-32</td>
</tr>
<tr>
<td>8</td>
<td>Opening Vulgar Profile on Internet</td>
<td>33</td>
</tr>
<tr>
<td>9</td>
<td>Defaming E-mail</td>
<td>34</td>
</tr>
<tr>
<td>10</td>
<td>Downloading Porn Video &amp; Pictures</td>
<td>35</td>
</tr>
<tr>
<td>11</td>
<td>Hacking</td>
<td>36</td>
</tr>
<tr>
<td>12</td>
<td>How to track E-mail Sender</td>
<td>37-39</td>
</tr>
</tbody>
</table>
Fraudulent drawal and expenditure-
A Case Study
**Fraudulent drawal and expenditure**

1. **Background**

   The Chief Conservator of Forest-cum-Chief Conservator of Wild Life, Bihar provided additional funds of Rs. 1.33 crores to the Divisional Forest Officer, Valmiki State Trading Division (VSTD), Betia on the request of the Conservator of Forest, Valmiki Tiger Project, Betia on 28th March 2001 without any requisition for such funds from the division to meet expenditure during 2000-01 on repair and maintenance of road, bridge and buildings and other contingent charges like telephone charges, electricity charges, liveries and other office expenses pertaining to two other divisions (Valmiki Tiger Project division I and II) which had no sanction of the Government for extension of their life till 31st March 2001 as the extension for operation of these divisions was accorded by the Government on the last day of the year i.e. 31st March 2001. There was neither sanction of the Government for such expenditure of the two divisions (Valmiki Tiger Project I and II) nor authorization of the Accountant General for operation of Letter of Credit for transacting activities of these two divisions during 2000-01.

2. **Fraud Environment**

   1. To meet the expenses of the division, the Government releases budgetary grant to the division on the last day (31st March 2001).
   2. As per provisions of the Financial Rules, Head of the Department was not empowered to divert/reappropriate the budgetary provision of one DDO to another DDO without the approval of the Government.
   3. Budgetary grants for any department are passed by Legislature.
4. Expenditure of Rs.82.88 lakh was shown by Divisional Forest Officer as incurred on unsanctioned construction and repair works by splitting the expenditure in small sums of Rs.5000 each to avoid sanction of competent authority.

5. Balance amount of Rs. 50 lakh was spent on contingent charges and office expenses.

6. No vouchers for expenditure of Rs.1.33 crore were available in the division.

3. **Opportunity to prevent frauds**

   Controls which could have prevented/limited the fraud but were bypassed:

   3.1 As per provisions of the Financial Rules, Head of the Department was not empowered to divert or reappropriate funds from one D.D.O. to another specific D.D.O. because budgetary grants for the department are passed by Legislature.

   3.2 Vouchers for all the expenditure made from the grants were to be produced for audit.

   3.3 Sanction from competent authority was required to be obtained for incurring expenditure.

4. **Act of Fraud**

   Divisional Forest Officer, Valmiki State Trading Division, Betia released the entire amount of Rs. 1.33 crore to two Range Officers between 28th March 2001 and 30th March 2001. The entire amount of Rs.1.33 crore was exhibited in the division’s accounts as spent. Of this, expenditure of Rs.82.88 lakh was shown by Divisional Forest Officer as incurred on
unsanctioned construction and repair works by splitting the expenditure of Rs. 5000 each to avoid sanction of competent authority. The balance amount of Rs. 50 lakh was spent on contingent charges and office expenses. No vouchers for expenditure of Rs.1.33 crores were available in the division.

5. **Opportunity to detect fraud**

Audit Party of the office of Pr.Accountant General (Audit), Bihar, Patna conducted the audit of the records of Divisional Forest Officer, Valmiki State Trading Division (VSTD), Betia and conducted a test check of records for the period 2000-01. Audit found that Chief Conservator of Forest diverted the allotment of division I and II of all unit heads except salary amounting to Rs. 1.33 crore to the Divisional Forest Officer, Valmiki State Trading Betia and he also ordered to disburse the amount through his subdisburser to different range officers/foresters of division I and II of Valmiki Tiger Project, without the approval of the Government.

During test check of records audit noticed the following “red flags” (fraud indicators):

1. Diversion of budgetary grant to the tune of 1.33 crore without the approval of the Government.
2. The amount of Rs.1.33 crore was released through cheques to different range officers/foresters within three days i.e. between 28-3-2001 and 30-3-2001(end of the financial year).
3. Technical sanction was not accorded to any estimate.
4. Work order was not issued by the competent authority.
5. In spite of absence of Technical sanction and Work order, Divisional Forest Officer issued the cheques in favour of Range Officers as advances against work.

6. Against the demand of Rs.50.39 lakh by the Divisional Forest Officer Valmiki State Trading Division for the year 2000-01, the Conservator of Forest released the budgetary grant of Rs.1,99,07,600, which was prima facie irregular and unjustified.

6. Lessons learnt - preventive controls/detective controls

6.1 The financial provisions for drawal of funds in absence of proper sanction were not followed.

6.2 The prescribed accounting procedures namely,

i) drawal of bill with supporting vouchers

ii) Passage of bill by the competent authority before drawal of the cheques were not adhered.

6.3 Reappropriation of funds with proper sanction of the competent authority was not scrupulously followed. This led to diversion of funds for which they were not empowered which resulted in misutilisation of Rs.1.33 crores.

6.4 There were many procedural lapses, which gave scope for such fraudulent drawal reportedly.
7. **Enclosures for reference**:

i. Half Margin memo with reply  

ii. Details of expenditure  

iii. Letter of Conservator of Forest regarding deputation of officer  

iv. Letter of Conservator of Forest dt.27.3.2001 regarding reappropriation of funds /letter of credit of A.G.  

v. Action taken by the department.  

vi. Copy of Para 4.1.1 of the report of the Comptroller and Auditor General of India for the year ended March 2001 (Civil) Government of Bihar.
The chief conservator of forest, Meghalaya, had recommended the release of Rs. 1.93 crores to be made directly into the bank accounts of the different agencies. This recommendation was made in the interest of the conservation of the forest. The funds were to be used for the construction of new buildings and the purchase of machinery. The recommendation was approved and the funds were released as per the recommendation.
सेवा में,

बन प्रमुख पदाधिकारी सुनिश्चित करो जिन्होंने बाल जिला निदेश, बाल वोटिंग कराया गया हो।

प्रमुख पदाधिकारी
बाल जिला राजनीति अधिकृत

प्रभाव: पिछले पर्यावरण में वचनवाद के लिए वाल्मीकी भाषा प्रोत्साहन के बन के बालध्वनिकार्यों का बाल जिला के अधिकारक वाल्मीकी राजनीति अधिकृत प्रभाव के प्रतिकृति के हंसी में।

महासत्व,

प्रभाव को इन बाल्मीकियों नाम प्रोत्साहन की धज्ज

प्रभाव की स्वतंत्री राष्ट्रीय समारूह-कार से दशकार नव बालिका

में दी गई।

बालकार नाम प्रोत्साहन के नवाचार विधि बद्वारीत देखनी तथा रथ-पहाड़ी

कार्य के लिए गर योजना के बालध्वनिक राम का निष्क्रिय प्रभाव की स्वतंत्री पिछले पर्यावरण में लीग की गई है। उस विक्षेप में वाल्मीकी का भुगतान स्वतंत्र न करने गर वाल्मीकी योजना का निर्धारण सम्भव है।

उपाय का प्रतीक्षित है, जब राजनीति परिस्थिति में उपचार घटकी वहाँ वाल्मीकी भाषा का चलाया जा चला वाल्मीकी भाषा अधिकार के वाल्मीकी क्षेत्र वाल्मीकी कार्यों का अन्वेषण करने गर वाल्मीकी राजनीति अधिकृत प्रभाव के साथ बहे हैं।

बाल कार, 31 अगस्त, 2003 का प्रभावित प्रभाव पिछला जाने। वह बल्लोपीय प्रभावक उनके नेताओं के निराधार हेतु की बाल रखा है। इन्हें आवाज पदार्थवादी वोटिंग के लिए वाल्मीकी वाल्मीकी वोटिंग कराया जाएगा कार्यों के साथ बहे हैं।

बाल वादक के बावजूद वे बालवादियों के भुगतान का गर्दन मुनाफा लाना वर्तमान का है लीग कर नैतिक विकास के वाल्मीकी प्रभाव का उपचार घटकी निश्चित करने के लिए लीग करने की कार्यकर्ता दिनियाँ जारी करते हैं।

उस बल्लोपीय प्रभाव का विविध अभाव को समझने का लक्ष्य है बाल वादक के लिए कार्यों के बालवादियों निश्चित करने के लिए लिखें।
वर ने सहर बसाया तो लोगों को पुराने हो. वे हाल बना।

वे रहे हैं।

वे भी वातन्त्रकी के रूप में बने हुए हैं।
<table>
<thead>
<tr>
<th>Building</th>
<th>Rate Road</th>
<th>Wages</th>
<th>Contingency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Date</td>
<td>Amt(Rs.)</td>
<td>Date</td>
</tr>
<tr>
<td>29.01</td>
<td>29.01</td>
<td>2,00,000</td>
<td>29.01</td>
</tr>
<tr>
<td>15.01</td>
<td>15.01</td>
<td>4,00,000</td>
<td>30.01</td>
</tr>
<tr>
<td>20.01</td>
<td>20.01</td>
<td>1,50,000</td>
<td>30.01</td>
</tr>
<tr>
<td>31.01</td>
<td>31.01</td>
<td>3,00,000</td>
<td>30.01</td>
</tr>
<tr>
<td>15.01</td>
<td>15.01</td>
<td>3,00,000</td>
<td>30.01</td>
</tr>
<tr>
<td>02.01</td>
<td>02.01</td>
<td>5,00,000</td>
<td>30.01</td>
</tr>
<tr>
<td>03.01</td>
<td>03.01</td>
<td>1,50,000</td>
<td>30.01</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>26,51,000</td>
<td></td>
</tr>
</tbody>
</table>

Besides, Rs. 50 lakh was spent on contingent charges and office expenses.

\[ \text{Signature} \]
लेखन व लेखन संबंधित मामले के लिए, जातिविद प्रायोगिक प्रयोगात्मक,

जातिविद निर्देशन के अनुसार,

प्रत्येक जाति की प्राथमिकता और अर्थव्यवस्था

के लिए उपयोगी विभागों में विवरण देने का कार्य.

उपर्युक्त विषय में प्रतिष्ठित भाषा व्यक्ति के लिए जातिविदीय

आदेशों का पालन करना है।

जातिविद निर्देशक के एक कार्यक्रम में जातिविदीय

आदेशों का पालन करना है।

जातिविद निर्देशक के एक कार्यक्रम में जातिविदीय

आदेशों का पालन करना है।

जातिविद निर्देशक के एक कार्यक्रम में जातिविदीय

आदेशों का पालन करना है।

जातिविद निर्देशक के एक कार्यक्रम में जातिविदीय

आदेशों का पालन करना है।

जातिविद निर्देशक के एक कार्यक्रम में जातिविदीय

आदेशों का पालन करना है।

जातिविद निर्देशक के एक कार्यक्रम में जातिविदीय

आदेशों का पालन करना है।

जातिविद निर्देशक के एक कार्यक्रम में जातिविदीय

आदेशों का पालन करना है।

जातिविद निर्देशक के एक कार्यक्रम में जातिविदीय

आदेशों का पालन करना है।
To

The Dy. Accountant General (I.C.),
O/O the Pr. Accountant General (Audit),
Bihar, Patna.

Sub:- Information regarding receipts of vouchers from Valmiki State Trading Division, Bettiah.

Sir,

With reference to your letter No. I.C./D.P.Cell (2003-04)-97 dated 5.3.2004, I am to state that as per the Classified Abstract of Revenue and expenditure for the month of 3/01, total amount of Rs. 1,29,91,634.00 had been found booked against the Divisional Forest Officer, Valmiki State Trading Division, Bettiah in different Sub-head minor head under major head 2406- Forestry & Wild Life. The information regarding the two divisions (Valmiki Tiger Project I and II) nor was receipts of actual no. of Vouchers above Rs. 1000/- will be communicated later on as the same is not readily available.

Yours faithfully,

विषय:- केलिया के राजकीय व्यापार प्रमंडल ने एक करोड़ रूपयों लाख कवर करने की आवश्यकता के संबंध में।

प्रलंग:- आयका अदालत पत्र सं-डीओत० नो. रेफ. 1 सितिली/स्ट. आर. /2002-2003, दिनांक 8.8.2003. 27/73

महाशय,

निलेखनुसार उपहीक विषय आयका अदालत सरकारी पत्र के डीओतो नं. 50 रेफ. 1 सितिली/स्ट. आर. /2002-2003, दिनांक 8.8.2003 के प्रलंग में सुविधित करना है कि केलिया विश्वसनीय पटरीकन एवं फ्रेम की विभाग के कार्यालयों में करोड़ों से अधिक नक्सली का मानवता सहकर्मी द्वारा पद "किस्तिका" में प्रभावित हुआ। इस पर तक्षकैल्य केलिया मुख्य की संकेत, पटरा 1500 एम के 60 शाम। तथा तक्षकैल्य का लंबी, पल्ला भी अपने प्रदूषण को वापस करने की आशा तथा सरकार के द्वारा दिया गया।

इसके संयुक्त जोड़ प्रबंधन के स्पष्ट हुआ कि तक्षकैल्य गृहानुप्र घुटने का लंबी, विश्वास द्वारा मार्च के अंतिम सप्ताह में विश्वास के लिए वित्तपंचायत के अन्तर्गत सहकर्मी मटरों में आवंत बन संस्थान, बैलिया जगह दोनों दोनों दोनों दोनों दोनों दोनों दोनों दोनों ही की गयी और स्थानीय अधिकारियों को उल्लेखित कर सहकर्मी के सहायता द्वारा मार्च के अंतिम दिनों में ही गयी। आर्थिक अवस्था के द्वारा अपने मार्गों में सीधाता 60 पदों विभागितियों एवं कार्यालयों को विश्वास कर सहकर्मी के सहायता द्वारा मार्च के अंतिम दिनों में ही गयी। आर्थिक अवस्था के द्वारा निष्पादित हुआ की संयोग से विश्वास के लिए कार्यालयों को किस्मतित कर सहकर्मी के सहायता द्वारा मार्च के अंतिम दिनों में ही गयी।
पढारियों के निम्नांकनार्दी प्राप्त हो गयी है। ताया ही इन लबों के लिये प्राथमिक दायित्व करने के लिए वन संरक्षण, मेलिया को लिया गया है।

इस कौन्न के मंदिरनज़र विभिन्न विभागों को मेलिया के वन प्रमाणों तथा क्षेत्र निषेध-लक्ज-वन संरक्षण के कार्यालयों का प्रशिक्षण आयोजन करने का अनुशासन किया गया है। विभिन्न विभागों के साथ समायोजन निमित्त महाविद्यालय, बिहार, पटना आदि के प्रभारियों विभिन्न विभागों के जोध विभिन्न प्राप्त हो जाते हैं के बाद सरकार द्वारा समीक्षण रत्न मामले के नियमार्धक विभाग जाएगा।

शिवाय भाजन,

पीलीऩ करण।
सरकार के उप तथ्य।
CHAPTER IV
AUDIT OF TRANSACTIONS

4.1 Fraudulent drawal/ Misappropriation/ Embezzlement/ Losses

ENVIRONMENT AND FOREST DEPARTMENT

4.1.1 Doubtful expenditure

Expenditure of Rs 1.33 crore against advance payment in Valmiki State Trading Division, Betia was doubtful.

On the request of the Conservator of Forest, Valmiki Tiger Project, Betia, the Chief Conservator of Forest-cum-Chief Conservator of Wild Life, Bihar provided additional funds of Rs 1.33 crore to the Divisional Forest Officer (DFO), Valmiki State Trading Division (VSTD), Betia on 28 March 2001 without any requisition for such funds from the division to meet expenditure during 2000-01 on repair and maintenance of road, bridge and buildings and other contingent charges (telephone and electricity charges, liversies, other office expenses) pertaining to two other divisions (Valmiki Tiger Project division I and II) which had no sanction of Government for extension of their life till 31 March 2001 as the extension for operation of the divisions was accorded by Government on the last day (31 March 2001) of the year. Further, there was no sanction of Government for such expenditure of the two divisions (Valmiki Tiger Project I and II), nor was there any authorisation of the Accountant General for operation of Letter of Credit for transacting activities of these two divisions during 2000-01.

Scrutiny of records of the DFO, VSTD, Betia revealed that DFO released the entire amount of Rs 1.33 crore to two Range Officers from 28 March 2001 to 30 March 2001. These Range Officers further advanced the amount to foresters on 31 March 2001 and the entire amount of Rs 1.33 crore was exhibited in the division's accounts as spent. Of this, expenditure of Rs 82.88 lakh was shown by DFO as incurred on unsanctioned construction and repair works by splitting the expenditure in small sums of Rs 5000 each to avoid sanction of competent authority. The balance amount of Rs 50 lakh was spent on contingent charges and office expenses. No vouchers for expenditure of Rs 1.33 crore were available in the division.

Thus, the entire expenditure of Rs 1.33 crore depicted as booked in the divisional accounts in March 2001 was prima facie doubtful. The DFO, VSTD, Betia stated (May 2003) that the matter was under investigation at the level of Principal Chief Conservator of Forests and the result would be communicated to audit in due course.
The matter was referred to Government (August 2003). The Deputy Secretary to Government, Environment and Forest Department stated (December 2003) that all the 60 officials involved had been placed under suspension and departmental proceeding against them had been initiated. Reference had been made to Government of India for action against the then Principal Chief Conservator of Forests who had retired and action had been initiated against two other officers of Indian Forest Service. He also stated that Conservator of Forests, Betia had been directed to lodge FIR with the Police against all of them.
Cyber Crimes (Vol.II)
Case No. 1

Fraud Through Internet

Brief History

The plaintiff, Shri Ajay, (Name has been changed) was in service at Abudhabi. He had received e-mail from unknown lady (Mrs. Rita Basu) through her e-mail ID ritabasu@epatra.com. This e-mail made Shri Ajay & Mrs. Rita Basu friends. She sent e-mail to the plaintiff inviting him in a hotel. The plaintiff did not turn up and he avoided sending mails to her. After that the plaintiff received a threatening e-mail from anonymous persons. The plaintiff was warned that if he did not send e-mails, the lady would commit suicide. By this, the plaintiff got perturbed and he informed her friend to convince Rita Basu to give up the idea of committing suicide. Ruchira Sengupta (friend of Rita Basu) had informed through email that Rita Basu had committed suicide and Kolkata police were investigating. It was further warned that if he wanted to take out his name from that case, he had to arrange for money. Ruchira Sengupta was pretending to save plaintiff from false case. She was seeking help of Advocate S. Sinha (name changed) in this case. Ruchira Sengupta had informed plaintiff to deposit money in Advocate S. Mitra’s bank account at State Bank of India Mahul Road, Chembur branch. In order to make him believe, an email in the name of kolkata police (cid@culeuttapolicel.in.box.as) and high court was sent to the complainant that investigations were going on in suicide case. The plaintiff got terrified with
this email & requested Ruchira Sengupta and Advocate S. Sinha to make patch up between Kolkata police and the High Court.

Ruchira Sengupta had informed plaintiff that she had succeeded in her attempt to patch up the case and added that he had to pay a big amount for that.

After that the plaintiff received email from (second) unknown girl friend (who live in America & her email ID was Drsudeshana@mail2 Doctor.com) communicating her desire to meet him at Dubai when she returns from New York. It was managed to feel the plaintiff that this Dr. lady started from New York & thereafter she was missing. After that the plaintiff received another email from email ID nyc police usa@usa.net. Because of this, the complainant felt that the email was really received from New York. It was stated by the police in the email that Dr. Sudeshana was missing and complaint to that effect and police were investigating that matter. The missing lady was from Kolkata. Kolkata police and New York police were investigating the matter jointly and they were suspecting the plaintiff. After taking the plaintiff in to confidence he was informed that the missing lady was a relative of one Member of Parliament and if he complaints then the plaintiff had to pay big amount. The plaintiff got frightened and contacted Advocate S. Sinha. Mr Sinha advised him to deposit Rs.20 lakhs in his account. Accordingly plaintiff deposited the amount. The plaintiff was given to understand that Chandigarh police are investigating kidnapping case of one lady and he may be arrested in that case. Again the
plaintiff telephoned Advocate S. Sinha and he was asked to deposit amount in bank. Accordingly the amount was deposited. Such an atmosphere was created that the plaintiff was required in so many cases by the police and Rs75 lakhs were ripped off from him. The plaintiff had taken loan from the bank as his money from savings account got exhausted. In spite of paying this much amount, he was being troubled by the ladies so he came from Abu Dhabi to Mumbai for making complaint with Mumbai police. The cyber crime branch of Mumbai police registered a case as above as told by the plaintiff.

The officers from cyber crime cell had obtained following IP addresses from the headers of the emails.

1. Cement Company ltd. Mumbai
2. Cement Company Nerul, Navi Mumbai

The account holder Pranab Parimal Sinha was arrested. The property worth Rs.90 lakhs was recovered from him out of Rs1 crore 25 lakhs gulped by him.

Present Status of Case

The case was in Killa Court No37 and case is subjudice.

Lessons to Learn

- Police officer should note that the person is unknown in cyber world
- In cyber crime the benefit of being unknownness is utilized and the email is sent in the persons name who are not in existence.
Case No. 2

Phishing Case

Brief History

On 9-3-2004, a complaint was received from one of the ICICI bank customers, that through e-mail and phone ICICI bank is enquiring about their password and e-mail I.D. & whether support@icici.com it belongs to their bank.

When the bank conducted a preliminary enquiry it was found that the enquiry was made through email i.d. support@icici.com by the bank. Vide this e-mail the customers accounts were checked and for this their user i.d., login password, transaction password etc. were asked (The transaction password is given to the user when the subscriber conducts monetary transactions through internet). The e-mail link web page http://infinity/icicibanks.co.in/verify.jsp belongs to ICICI bank and is for the customers to obtain information by visiting this site. The site http://infinity.icicibanks.co.in/verify.jsp link has been linked to the web site of ICICI bank and the information therein instead of going to w.w.w.all.about.notebook.com goes to another link and gets saved. And hence the bank started to make enquiries in the matter. At the end of the enquiry it came to the knowledge that the said site did not belong to the bank but was a fake site created specifically. So ICICI bank notified its customers not to part with their user i.d., log in i.d., transaction password through the web page through a notice
displayed on the bank’s website. A complaint was lodged in by the ICICI bank in the instant case.

When enquired it was found that the said e-mail was forwarded from America and the company (IPS) that gave the ISP was in America only. This e-mail was also diverted to China. Inquiries were made from America and China but reply is still awaited.

Lessons to learn

- It is very important to note that attempts to obtain personal identity of persons are being made in the world.
- Culprits can transfer money from one account to another using user i.d. and password obtained in this way through internet.
- You can ascertain from the bank, the P.C. through which money has been ordered to be transferred from one account to another (means I.P.Address and date and time of that I.P. Address).
Case No. 3

Porn E-Mail

Brief History

On 19-12-2003 at 10.22 a complainant Ku. Shalini Chavhan (changed name) went to Cyber Café at Bandra(West) and checked her email i.d. shalini_chavhan1@rediffmail.com. Here she found that she had received unknown email from email i.d. @rediffmail.com. This email i.d. displayed that the sender was having her porn photographs and porno writings. Then the same person sent an e-mail on 22\textsuperscript{nd} December, 2003 and threatened her that he will send her photos to her house in the village. When this happened repeatedly, the complainant came to the investigation cell to lodge a complaint of the above crime.

As soon as the crime was registered, the Cyber Crime Investigation Cell Officer understood that, Hasim Khan (changed name) was in possession of her porn photographs. When one of her friends Shri Dinesh was contacted, it was learnt that Hasim Khan reside at Villeparle, Mumbai. Police party from Cyber Crime Investigation Cell and two witnesses went to his residence and raided the house and seized three photographs and the girl in the photo was looking like Shalini.

When detail enquiry was made from Ramesh Rai(Changed name)it was found that the said e-mail was sent by one Shyam Agarwal.
Lessons to Learn

- E-mail sender is not surely known from the name of the e-mail sender. Police Officers should always remember that crime is committed keeping this in view.

- Whenever a porn e-mail is sent, from the I.P. address in the header of the e-mail, the police officers will learn, from which P.C. this e-mail is sent. It is pertinent to note that there is a relation between the user of the P.C., P.C and other evidences.
Case No. 4

Hurting Religious Sentiments

A complaint was lodged by one Shri Abdul Khalid Painter Heenashahin, Bank Corporator, resident of Balbheem Chowk, Beed that he and other witnesses saw on a URL www.hinduunity.org a website the picture showing a pig writing the muslim religious book “Kuran”. In muslim religion the pig is thought of as very impure. Since this picture was hurting the religious sentiments of muslim society, a crime was registered in Beed police station under section 113/04 section 295(a) of Indian Penal Code, on 27th April 2005.

The investigating officers questioned the witnesses who saw this incidence. Further, at the orders of Director General of Police Maharashtra, the case was sent for investigation to Cyber Crime Investigation Branch, Mumbai.

On investigation it was found that the website belonged to Shri Rohit Yasman of United States of America. An arrangement is made in this website that any reader can express his thoughts through this website. That is why one person using the site www.ezboard.com sent the said picture to this website. Since the sites www.hinduunity.org and www.ezboard.com are operating from America, under Indian Penal Code Section 166(b), a letter under the signature of Chief Metro Judicial Magistrate through the Foreign Ministry, Government of India,
New Delhi, was sent to Law and Judiciary Department in America, with a request to investigate and report the matter.

It was also requested to name the owner of the website, date and time of creation of website, I.P. Address as well as log records of the website.

Whether the said picture was a part of website? Or was it posted by someone on this site. When was it posted, where was it created or posted (IP and Postal address).

Who is the person who created or posted this picture? Similarly who is the person that sent this message or created this message?

Law and Judiciary Department of America reported that since their Constitution gives freedom of speech, this information cannot be parted with.

**Lessons Learnt:**

- It is very serious issue to note that a new medium has been created to hurt the religious sentiments.

- Even residing out of India, a person is able to do this act.
Case No. 5

Credit Card Fraud

Brief History

Indian Railway has given the facility of booking the railway tickets online through Internet. In order to get the ticket, one has to log on to the website www.irctc.co.in and fill up relevant information. After that for making payment he has to enter his credit card number and date of expiry of his credit card. After that fare of the ticket is debited to that credit card. The accused has taken the advantage of this system and purchased many railway tickets giving the information of the credit card of different people. They have sold these tickets illegally to public. This way they have cheated Indian Railways Catering and Tourism Corporation by Rs.1, 04,758.

Investigation

The accused in this forgery case have logged on to the website www.irctc.co.in from a Cyber Café in Andheri as seen from the IP address. During the course of inquiry, names and address of the accused were obtained from the persons who have traveled on these tickets.

The IRCTC distributes the tickets through Courier Services from their Headquarters at New Delhi. The employees of the Courier Service at Mumbai had shown the places where they had delivered the tickets. During the
identification parade, the employees of the Courier Service at Mumbai and owners of Cyber Café had identified the accused.

**Lessons to learn**

- While making the purchasing through Internet, one has to give the Credit Card number and date of expiry of Credit Card. This information can be obtained by anybody and misused. People and Police should be aware of this.

- Police officers should know that such types of crimes are generally took place from Cyber Café.
Case No. 6

Cheating through Internet

Brief History

Sohonet India Pvt Ltd., a Chennai based company, had placed an advertisement about self employment for the unemployed retired persons and housewives on their website. It was mentioned in the advertisement that the work of data conversion and editing would be given. By doing this work, they may earn Rs.15,000 to Rs.1,80,000. People may enroll themselves for the job and purchase packages of different kind.

Accordingly People have purchased such type of packages. The company had supplied software and related information for conversion of data to the people. As directed by the company, the people had registered their names on the website of the company. The company had forwarded the data to be processed to the people on line. The people after carrying out required processing sent the data back to the company. But the company refused to pay the amount due to them by stating various reasons i.e. no data accuracy, exceeded time limit etc. In this way, the company had cheated thousands of people by not paying their due remuneration.

Investigation

The accused in this case have been arrested.
Lessons to learn

- The Police Officers should spread the awareness among the people about the companies offering job to the people on computers and to ensure the chances of completing the work in a prescribed time
Case No. 7

Opening Vulgar Profile on Internet

Brief History

Mr. X had complained that somebody had opened a profile of his daughter on a website shadi.com. The content in that was vulgar.

Investigation

During the investigation, it was learnt that the profile was prepared in a Cyber Café. The Cyber Café was identified from the IP address. The persons who had prepared the profile were also identified and one of them was arrested. The case was registered in the court of Law.

Lessons to learn

- These types of crime took place because the Cyber Café did not keep the record of the users. In such type of crimes, the investigation has to be carried out using the circumstantial evidences. If the Cyber Café maintains name of user, address and time of usage of computer then this can be used to identify the accused persons.

- It is necessary to control Cyber Café. There should be a law/rules for them. The Police Officers should guide the Cyber Café in these cases.
Case No. 8

Defaming Email

Brief History
The Cyber Crime investigating department receives complaints from people or companies that they or their officers had received defaming emails from others.

Investigation
The IP address of the computer through which the email was received could be obtained but the person who had send the email could not be identified.

Lessons to learn

- The Cyber Café did not maintain the name, address and other information. There is no law or rule in existence.
- The companies either small or big also did not maintain the information about the user and time.
Case No. 9

Downloading of Porn Video & Pictures.

Brief History

Suspected criminal, at his shop, made arrangement for downloading of porn video & pictures on Mobile phone. The mobile multimedia card was used for downloading. The criminal was caught red-handed while downloading the porn video & picture on mobile phone.

Lesson to learn:

- The Computer & information technology is widely used for illegal & anti-social purpose.
- Downloaded porn video clipping & pictures on mobile phone are rapidly transmitted all over through MMS, Blue tooth, E-Mail etc.
- The people who are transmitting the video clipping require lot of patience, skill & knowledge.
Case No 10

Hacking

Brief History:

A renowned company had hosted Web-mail on E-mail service providers Server. This Web-mail was exclusively used by the employees of the company for internal communication. Unique usernames & passwords were being used for the said purpose. One of the employees got the email id of another employee and got access to the e-mail box of the employee. He changed the setting and all received e-mails were diverted to his own e-mail box. In this way the company employee had hacked the e-mail account

Lesson to learn:

- User ID & password never be similar.
- A Proper security features need to be established while providing passwords.
- The crime like Hacking can be done by any person who has ordinary knowledge of computer.
HOW TO TRACK E-MAIL SENDER

The sender of the E-mail & path used by him/her can be tracked from E-mail header. Every e-mail service provider provides the facility for Full Header.

Click of Full Header option.

Procedure:

1. Open Inbox
2. Open E-mail
3. Click on Header
4. Note the e-mail here. It will look like as under;

Return-Path: <vijay_jr@hotmail.com>
Delivered-To: lgbhute1@fl.p3.mail.in.rediffmail.com@rediffmail.com
Received: (qmail 24268 invoked from network); 4 Aug 2007 16:18:21 -0000
Received: from unknown (HELO rediffmail.com) (220.226.195.202)
by 0 with SMTP; 4 Aug 2007 16:18:21 -0000
Received: (qmail 15983 invoked from network); 4 Aug 2007 16:18:09 -0000
Received: from unknown (HELO bay0-omc3-s1.bay0.hotmail.com)
(65.54.246.201)
by 0 with SMTP; 4 Aug 2007 16:18:09 -0000
Received: from hotmail.com ([65.55.153.116]) by bay0-omc3-
s1.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.2668);
Sat, 4 Aug 2007 09:19:32 -0700
Received: from mail pickup service by hotmail.com with Microsoft
SMTPSVC;
Sat, 4 Aug 2007 09:19:31 -0700
Message-ID: <BAY142-F360E78A7A996F758BFB6EDE5EB0@phx.gbl>
Received: from 65.55.153.123 by by142fd.bay142.hotmail.msn.com with
HTTP;
Sat, 04 Aug 2007 16:19:30 GMT
To track e-mail IP Address, the e-mail header should be read from bottom to top. The first IP-address being the IP-address from where the original e-mail was sent. It is very important to note the e-mail date and time. Against X-OriginalArrivalTime the date & time of the e-mail has been mentioned. Against X-Originating-IP: the ip address of the sender computer is mentioned.

**Identification of Sender**

1. Open [www.allnettools.com](http://www.allnettools.com)
2. Click on Tool
3. Enter IP address of sender & Click on Go. Internet service provider by which the IP address was assigned will be displayed alongwith its address is on the screen.
4. Send the letter to Internet service provider requesting him to provide for the name of the user, its address & telephone number.

The ISP will submit above information to the requesting agency.

Following are the some more websites who provide the name of ISP just submitting the IP Address of sender.

www.All-nettools.com

www.Arin.com

www.apnic.com

www.eAmnesia.com

www.RIPE.com