ડિજિટલ પુરાવા

એકત્રીકરણ, વિશ્લેષણ અને પ્રસ્તુતીકરણ

ગુજરાત પોલીસ

માર્ગદર્શિકા

संदेश

ગુજરાતનું પોલીસતંત્ર કાર્યક્ષમતા, વહીવટ અને ગુનાખોરી નિયંત્રણમાં ખૂબ જ અગ્રેસર રહેલ છે. પરંતુ, આધુનિક આવિષ્કારો, જેવા કે કોમ્પ્યુટર, ઇન્ટરનેટ, મોબાઈલ ફોન ની મદદથી પ્રણાલીગત આચરવામાં આવતા ગુનાઓની પદ્ધતિઓમાં ખૂબ જ પરિવર્તનો આવેલા છે. વધુમાં, ડિજિટલ પુરાવા ને એકત્ર, વિશ્લેષણ અને પ્રસ્તુત કરવા માટે આવશ્યક જ્ઞાન અને કૌશલ્ય પુરાવાનાં પરંપરાગત સ્રોતો કરતાં ભિન્ન છે. ગુજરાત પોલીસ સમક્ષ આ નવા પડકારો છે, જેને પહોંચી વળવા માટે આ માર્ગદર્શિકા પ્રસ્તુત કરવામાં આવે છે.

સમગ્ર પોલીસતંત્રને સાધન, સામગ્રી અને સવલતોથી સુસજ્જ બનાવવા જેટલું જ મહત્વ આવી માર્ગદર્શિકાના જ્ઞાનથી અવગત કરવાનુ છે. ઉપરોક્ત વિષય પર દેશમાં સ્થાનિક ભાષામાં

તૈયાર કરેલી આ પ્રથમ વિસ્તૃત માર્ગદર્શિકા નિ:શંકપણે સમગ્ર પોલીસતંત્રને ઉપયોગી નીવડશે.

આ પુસ્તિકા પ્રકાશિત કરવા બદલ ગુજરાત પોલીસ અકાદમી, આતંકવાદ વિરોધી દળ, અને ક્રાઈમ બ્રાંચ-અમદાવાદ શહેર ની ટીમો ને ગુજરાત પોલીસ વતી અભિનંદન આપુ છું.

આ પુસ્તિકાના પ્રકાશન બદલ ધન્યવાદ.

(શિવાનંદ ઝા)
પોલીસ મહાનિદેશક અને
મુખ્ય પોલીસ અધિકારી,
ગુજરાત રાજ્ય

પ્રસ્તાવના

કોમ્પ્યુટર અને ઇન્ટરનેટ આજે સમાજના તમામ પાસાઓને પ્રભાવિત કરી રહ્યા છે, અને સ્વાભાવિક પણે ફોજદારી ન્યાય વ્યવસ્થા પણ આ આધુનિક આવિષ્કારોની અસરોથી બાકાત રહી નથી. પોલીસ અધિકારીઓ/કર્મચારીઓ ને તપાસ કરનાર અમલદાર તરીકે દૈનિક ધોરણે ડિજિટલ પુરાવાઓની સમસ્યાઓ નો સામનો કરવો પડી રહ્યો છે અને ડિજિટલ પુરાવા ની સંવેદનશીલતા, એકત્ર કરવાની જટિલ પ્રક્રિયા, અને કાયદા ની ભિન્ન-ભિન્ન જોગવાઇઓના કારણે પોલીસ અધિકારીઓ અને કર્મચારીઓ તપાસમાં મુશ્કેલી અનુભવે છે.

શ્રી શિવાનંદ ઝા, પોલીસ મહાનિદેશક અને મુખ્ય પોલીસ અધિકારી, ગુજરાત રાજ્ય, દ્વારા આ પ્રશ્નનું નિવારણ કરવાના હેતુસર ડિજિટલ પુરાવા ને સંલગ્ન વિભિન્ન પાસાઓ નો સમાવેશ કરતી માર્ગદર્શિકા તૈયાર કરવાની અપાયેલ સૂચના અન્વયે ગુજરાત પોલીસ ને આ પુસ્તિકા પ્રસ્તુત છે.

આ માર્ગદર્શિકાનો મુખ્ય ઉદ્દેશ ઉપયોગકર્તાને નીચેની બાબતો વિષે માહિતગાર કરાવવાનો છે:

i. ડિજિટલ પુરાવાઓની મૂળભૂત પ્રકૃતિ
ii. ઈન્ફોર્મેશન ટેકનોલોજી એક્ટ અને ભારતીય પુરાવા અધિનિયમમાં ડિજિટલ પુરાવાઓને લગતી મૂળભૂત કાયદાકીય જોગવાઇઓ

iii. ડિજિટલ ફોરેન્સીકને લગતી આંતરરાષ્ટ્રીય પ્રચલિત અને માન્ય પદ્ધતિઓ

iv. ડિજિટલ પુરાવાની ઓળખ અને પ્રાથમિક પૃથક્કરણ (Analysis)

v. ડિજિટલ પુરાવાની વિશ્વસનીયતા અને સમ્પૂર્ણતા જળવાઇ રહે તે રીતે ભલામણ કરવામાં આવેલ પ્રમાણભૂત સંચાલન પ્રક્રિયા (SOP) અને તેનું દસ્તાવેજીકરણ (Documentation)

vi. વિવિધ સ્ત્રોતોમાંથી ડિજિટલ પુરાવા એકત્ર કરવા માટેની પ્રક્રિયા, જેમ કે, ઇ-મેઇલ, વિદેશ સ્થિત સોશિયલ મીડિયા સર્વર, MLAT/LR તૈયાર કરવા વગેરે

vii. મોબાઇલ ડિવાઈસ ફોરેન્સીક

viii. ગુજરાત પોલીસના વિવિધ એકમો સાથે ઉપલબ્ધ ડિજિટલ પુરાવાઓના સંગ્રહ માટેની સુવિધાઓ/સાધનો (Cyber Forensic Tools) ની માહિતી

પોલીસ અધિકારી/કર્મચારી દ્વારા માર્ગદર્શિકામાં દર્શાવેલ પદ્ધતિઓનું પાલન કેસની પરિસ્થિતી/આવશ્યકતાને આનુષંગિક રહ્શે. વધુમાં, આ માર્ગદર્શિકા પોલીસ અધિકારીઓ/કર્મચારીઓને ડિજિટલ પુરાવા બાબતે વૈશ્વિક રીતે માન્ય અને દેશના કાયદા સાથે સુસંગત પ્રક્રિયાઓ/પદ્ધતિઓથી અવગત કરાવવા માટે છે. આ માર્ગદર્શિકાનો ઉપયોગ કોઈપણ તપાસ કરનાર અમલદાર દ્વારા ન્યાયાલયમાં પુરાવાને પ્રસ્થાપિત કરવા અથવા ખંડન કરવા માટે કરવાનો રહ્શે નહી. ડિજિટલ પુરાવા અંગે પોલીસના ઉપયોગ માટે સ્થાનિક ભાષામાં તૈયાર કરવામાં આવેલ આ માર્ગદર્શિકા દેશભરમાં પ્રથમ પ્રયાસરૂપે

છે, અને આ પુસ્તિકામાં સમયાંતરે નવા પ્રકરણો ઉમેરવામાં આવશે અને સુધારા કરવામાં આવશે. આ પુસ્તિકા તૈયાર કરવા માટે નિમવામાં આવેલી સમિતિ ના સભ્યો, શ્રીમતી નિપુના તોરવને, શ્રી દિપાંકર ત્રીવેદી, શ્રી હિમાંશુ શુક્લા અને શ્રી દીપન ભદ્રન ને હું ધન્યવાદ આપુ છું.

મને વિશ્વાસ છે કે આ પુસ્તિકામાં સમાવેશ કરવામાં આવેલ માહિતી ગુજરાત પોલીસની ડિજિટલ પુરાવા સચોટ રીતે એકત્ર કરવાની કુશળતા માં વધારો કરશે.

કમલ કુમાર ઓઝા, ભા. પુ. સે.

અનુક્રમણિકા

પ્રકરણ-૧: ડિજિટલ પુરાવાને સંલગ્ન મહત્વપૂર્ણ કાયદાકીય જોગવાઇઓ

૧	ડિજિટલ પુરાવા: વ્યાખ્યા	૨
૨	ઇલેક્ટ્રોનિક પુરાવાની ગ્રાહ્યતા	૩
૨.૧	ભારતીય પુરાવા અધિનિયમ કલમ ૬૫-ખ: ઈલેક્ટ્રોનિક રૅકર્ડની ગ્રાહ્યતા	૫
૨.૨	કલમ ૬૫-ખ: ગ્રાહ્યતાની શરતો અને પ્રક્રિયા	૧૦
૨.૩	કલમ ૬૫-ખ અંતર્ગત સર્ટિફિકેટ આપવાની સત્તા અને સમાવિષ્ટ તથ્યો	૧૧
૨.૪	કલમ ૬૫-ખ હેઠળનું સર્ટિફિકેટ અમુક સંજોગોમાં ફરજીયાત નથીઃ આરોપી પાસે થી સીઝર	૧૫
૨.૫	કલમ ૬૫-ખની શરતો સર-તપાસ માં પૂર્ણ ના કરી શકાય	૧૭
૨.૬	કલમ ૬૫-ખ: માત્ર ગ્રાહ્યતા પૂરતું	૧૮
૨.૭	સર્ટિફિકેટ પછીથી પણ રજૂ કરી શકાય	૧૮
૩	વિદેશમાં રહેલ પુરાવા: મ્યુચ્યુઅલ લીગલ અસીસટન્સ ટ્રીટી (MLAT) અને લેટર્સ રોગેટરી(LR)	૧૯
૩.૧	ફોજદારી કાર્યરીતિ સંહિતા,૧૯૭૩ ની કલમ ૧૬૬ A અને ૧૦૫ હેઠળ વિદેશમાં તપાસ માટે લેટર્સ રોગેટરી (LR) / MLAT ઇશ્યુ કરવાની માર્ગદર્શિકા	૨૦
૩.૨	સક્ષમ કોર્ટ દ્વારા લેટર્સ રોગેટરી ઇશ્યુ કર્યા પછીની પ્રક્રીયા	૨૮

અનુક્રમણિકા

૪	ભારતમાં સ્થિત ઇલેક્ટ્રોનિક રૅકર્ડ ને રજૂ કરવા ફરજ પાડવાની રીત	૨૯
૫	ઇ-મેઇલ/એસએમએસ/ઇલેક્ટ્રોનિક સંદેશાની સાબિતી	૩૦
૬	દસ્તાવેજ વિશે નિષ્ણાંતનો અભિપ્રાય	૩૨
૭	તપાસ અધિકારી દ્વારા "પ્રિઝર્વેશન નોટીસ" ઇશ્યુ કરવી	૩૨
૮	ઇલેક્ટ્રોનિક પુરાવા ની ઝડતી અને જપ્તી (Search and Seizure) માટે કાયદાકીય જોગવાઇઓ	૩૪
૯	પુરાવા તરીકે CDR (Call Detail Record)	૩૫
૧૦	પુરાવા તરીકે આઈ.એમ.ઇ.આઇ(IMEI)	૩૫

પ્રકરણ-૨: ડિજિટલ પુરાવા: ઝડતી અને જપ્તી (Search and Seizure)ના મૂળ સિદ્ધાંતો

૧	ડિજિટલ ડિવાઈસ: ડિજિટલ પુરાવાના સ્ત્રોત	૩૭
૨	ડિજિટલ પુરાવાઓની મુખ્ય લાક્ષણિકતાઓ	૪૯
૩	પ્રવર્તમાન કાર્યપદ્ધતિ	૫૦
૩.૧	વર્તમાન કાર્યપદ્ધતિની ખામીઓ	૫૧
૪	ડિજિટલ પુરાવાઓની સંવેદનશીલતા	૫૩
૪.૧	ચેઇન ઑફ કસ્ટડી	૫૩
૪.૨	સ્થાયી ડેટા (Persistent Data) અને અસ્થાયી ડેટા (Volatile Data)	૫૫
૫	ડિજિટલ પુરાવા માટે સર્ચ અને વિશ્લેષણ	૫૫
૬	ડિજિટલ ડિવાઇસની ઓળખ અને પ્રારંભિક પ્રક્રિયા	૫૭

અનુક્રમણિકા

૬.૧	સામાન્ય સિદ્ધાંતો	૫૭
૬.૨	સ્થળ (Premises) અને ઉપલબ્ધ ડિવાઇસની પ્રાથમિક સમીક્ષા	૫૮
૬.૩	પ્રારંભિક પ્રક્રિયા	૫૯
૭	ડિજિટલ ડિવાઇસની જપ્તી (સીઝર) ની પ્રક્રિયા	૬૫
૭.૧	સીઝર/ ડિજિટલ પુરવાની જપ્તી	૬૬
૭.૨	ડિજિટલ પુરાવાનું તપાસ અધિકારી દ્વારા વિશ્લેષણ	૬૭
૭.૩	તપાસ અધિકારી દ્વારા વિશ્લેષણ પહેલા ડુપ્લીકેશન/બેકઅપ	૭૦
૮	હેશવેલ્યૂ:ડિજિટલ પુરાવામાં મહત્વ અને ગણતરી અંગેની પ્રક્રિયા	૭૪
૮.૧	ડિજિટલ પુરાવામાં અગત્યતા	૭૫
૮.૨	હેશવેલ્યૂની ગણતરી કરવાની પ્રક્રિયા	૭૭
૯	ડિજિટલ પુરાવાના સંગ્રહ માટે ની સાવચેતી	૭૭

પ્રકરણ-૩: સીસીટીવી (CCTV)

૧	સી.સી.ટી.વી. અને તેનુ પુરાવામાં મહત્વ	૮૧
૨	સી.સી.ટી.વી. ના પ્રકારો	૮૨
૩	સી.સી.ટી.વી. રેકોર્ડર ના પ્રકારો	૮૭
૩.૧	DVR રેકોર્ડર	૮૮
૩.૨	NVR રેકોર્ડર	૮૯
૪	ઘટના સ્થળ ની કાર્યવાહી	૯૧
૪.૧	બનાવ સ્થેળ લઇ જવા માટેનાં જરૂરી ઉપકરણ	૯૧

અનુક્રમણિકા

૪.૨	ફૂટેજ મેળવવા માટે નોડલ ઓફિસરને આપવા માટેની યાદી	૯૧
૪.3	ભારતીય પુરાવા અધિનિયમ ની કલમ ૬૫-ખ મુજબનું પ્રમાણપત્ર	૯૨
૪.૪	ઘટના સ્થળે પહોંચ્યા બાદ લેવામા આવતા પગલાઓ	૯૪
૫	પુરાવાના ભાગરૂપે ફૂટેજ મેળવવા માટેની કાર્યવાહી	૯૫
૫.૧	સી.સી.ટી.વી. રેકોર્ડર બાબતે લેવાની તકેદારીઓ	૯૫
૫.૨	સી.સી.ટી.વી. રેકોર્ડરમાંથી હાર્ડડ્રાઈવ /પેનડ્રાઈવમાં વિડીયો રેકોર્ડીંગની નકલ લેવા બાબત	૯૬
૬	DVR/NVR રેકોર્ડર તપાસના કામે કબ્જે લેતી વખતે	૯૮
૭	સી.સી.ટી.વી. બાબતનાં FSLમાં પૂછવાની પ્રશ્નોતરીનું ચેકલીસ્ટ	૧૦૨
૭.૧	DVR/NVRરેકોર્ડર બાબતનાં FSLમાં પૂછવાના પ્રશ્નો	૧૦૨
૭.૨	DVR/NVR રેકોર્ડરમાંથી હાર્ડ ડિસ્ક/પેન ડ્રાઈવ/DVD માં કરેલ કોપી બાબતના FSLમાં પૂછવાનાં પ્રશ્નો	૧૦3

અનુક્રમણિકા

૮	પેન ડ્રાઈવ ને ડી.વી.આર. સાથે જોડયા બાદ બેકઅપ(backup) અને નિકાસ(export) કરવા માટે ની પ્રક્રીયા	૧૦૪
૯	DVR/NVRરેકોર્ડર કમ્પનીના ડીફોલ્ટ યુઝરનેઈમ પાસવર્ડ	૧૧૦

પ્રકરણ-૪: ઇન્ટરનેટ અને IP Address

૧	વેબસાઇટ્સ, ફોરમ અને બ્લોગ્સને લગતાં ગુનાઓ	૧૧૫
૨	ઈ-મેઇલ સંચારનો ઉપયોગ થતો હોય તેવા ગુનાઓ	૧૧૮
3	ઈન્ટરનેટ ચેટ ધરાવતા ગુના	૧૨૧
૪	IP-એડ્રેસ ટ્રેસિંગ	૧૨3
૪.૧	ઈન્ટરનેટ પ્રોટોકોલ	૧૨૪
૪.૨	ઈન્ટરનેટ પ્રોટોકોલ (IP) ની મુખ્ય બે આવૃતિઓ	૧૨૪
૪.3	IP ઉપનેટવર્કો (IP Subnetworks)	૧૨૫
૪.૪	IP એડ્રેસની સોંપણી	૧૨૬
૫	ઈન્ટરનેટ પ્રોટોકોલ ડીટેઈલ રેકર્ડ (IPDR)	૧૨૯
૬	ટાઈમઝોનનું રૂપાંતર (Time Zone Conversion)	૧૩૦

પ્રકરણ-૫: સોશીયલ મીડિયા

૧	સોશીયલ મીડિયા: વ્યાખ્યા	૧33
૧.૧	સોશીયલ મીડિયાના વિવિધ પ્રકારો	૧33
૨	સોશીયલ મીડિયા સબંધિત પુરાવાઓ એકત્રિત કરવા	૧3૫
3	ફેસબુકમાંથી યુઝર ટ્રેસ કરવાની રીત	૧3૫

અનુક્રમણિકા

3.૧	પ્રાથમિક કાર્યવાહી	૧૩૫
3.૨	ફેસબૂક પાસેથી IP Log લેવા માટેના સ્ટેપ	૧૩૮
3.3	FACEBOOK તરફ થી માહિતી આવી છે કે તે ચેક કરવા	૧૪૧
૪	Instant Messengers અને End-to-End encryption	૧૪૭

પ્રકરણ-૬: ડિજિટલ પુરાવા: ઇ-વૉલેટ ફ્રોડ

૧	ઇ-વોલેટ શું છે?	૧૪૯
૨	ઇ-વોલેટ કઈ રીતે કામ કરે છે?	૧૫૦
3	ઇ-વોલેટ ના પ્રકારો	૧૫૧
3.૧	ક્લોઝ્ડ ઈ-વોલેટ	૧૫૧
3.૨	સેમી-ક્લોઝ્ડ ઈ-વોલેટ	૧૫૨
3.3	ઓપન વોલેટ	૧૫૨
૪	ઇ-વોલેટ એકાઉન્ટ ખોલાવવા માટે જરૂરી વિગતો	૧૫૨
૫	ઇ વોલેટ દ્વારા લેવામાં આવતી વિગતો	૧૫૩
૬	ઇ-વોલેટ કમ્પની દ્વારા આપવામાં આવતી વિગતો	૧૫૪
૭	ઇ-વોલેટ સંલગ્ન ક્યા પ્રકારના ગુના થાય છે?	૧૫૫
૮.	ઇ-વોલેટ ફ્રોડની તપાસ	૧૫૭
૯.	ઇ-વોલેટ કમ્પની તરફથી આવતી માહિતીના ફોર્મેટ	૧૬૦

અનુક્રમણિકા

પ્રકરણ-૭: મોબાઈલ ડિવાઈસ

૧	મોબાઈલ ડિવાઈસ માંથી કેવાં પ્રકારની માહિતી મેળવી શકાય	૧૭૭
૨	જપ્તી સમયે રાખવામાં આવતી સાવચેતી તેમજ પંચનામામાં નોંધવા લાયક બાબતો	૧૭૯
૨.૧	જ્યારે મોબાઈલ ચાલુ હાલતમાં હોય ત્યારે Airplane Mode ને On કરવાની રીત	૧૭૯
૨.૨	જો મોબાઈલ ડિવાઈસમાં લોક હોય	૧૮૦
૩	ફિંગરપ્રિન્ટ લોક /ફેશ લોક/ઈરિશ લોક દૂર કરવાની પધ્ધતિ	૧૮૫
૪	મોબાઈલ ડિવાઈસ: સર્ચ, સીઝર અને સંગ્રહ ની સામાન્ય માર્ગદર્શિકા	૧૯૧
૫	ટેબલેટ	૧૯૬

પ્રકરણ-૮: ગુજરાત પોલીસ પાસે ઉપલબ્ધ સોફ્ટવેર અને હાર્ડવેર

૧	સાયબર-ક્રાઈમ ઈક્વિપમેન્ટસ ગુજરાત પોલીસ	૧૯૯
૨	રાઈટ બ્લોકર કિટ (Write Blocker Kit)	૨૦૦
૩	ફોરેન્સિક વર્ક-સ્ટેશન	૨૦૧
૪	ફાલ્કન ડિસ્ક-ડુપ્લીકેટર	૨૦૨
૫	UFED (Universal Forensic Extraction Device)	૨૦૪

અનુક્રમણિકા

૬	XRY	૨૦૫
૭	EnCase સોફ્ટવેર	૨૦૬
૮	i2 iBase	૨૦૭
૯	FTK (Forensic Took Kit)	૨૦૮
૧૦	X1SD (Social E-Discovery Software)	૨૧૦

પ્રકરણ-૯: સાયબર અવેરનેસ (જાગૃતતા)

૧	OTP (One Time Password)	૨૧૧
૨	સિમ કાર્ડ બદલાવું (સિમ રિપ્લેસ)	૨૧૬
૩	ઓનલાઈન બેંકીંગ	૨૧૭
૪	ફેસબુક	૨૧૮
૫	વ્હોટ્સએપ	૨૨૦
૬	સેશીયલ મીડિયા	૨૨૧
૭	ઓનલાઈન જોબ	૨૨૨
૮	ઓનલાઈન લગ્ન સબંધી વેબસાઈટ	૨૨૩
૯	મોબાઈલમાં આવતા લખાણવાળા અજાણ્યા SMS	૨૨૪
૧૦	ઈ-મેલ	૨૨૫
૧૧	સંવેદનશીલ માહિતી	૨૨૭
૧૨	કોમ્પ્યુટર/લેપટોપ	૨૨૮
૧૩	પાસવર્ડ	૨૨૯
૧૪	ઓપરેટીંગ સીસ્ટમ અપડેટ	૨૩૦

પરિશિષ્ટ

પરિશિષ્ટ-૧: DRAFT MUTUAL LEGAL ASSISTANCE TREATY REQUEST ૨૩૩

પરિશિષ્ટ-૨: FORMAT FOR CERTIFICATE UNDER SECTION 65-B OF INDIAN EVIDENCE ACT, 1872 ૨૫૩

પરિશિષ્ટ-૩: LETTER ROGATORY (LETTER OF REQUEST) FOR EVIDENCE FROM SKYPE ૨૫૭

પરિશિષ્ટ-૪: PARAMETERS FOR INTERNET PROTOCOL DETAIL RECORD(IPDR) AND SYS LOG of NETWORK ADDRESS TRANSLATION (NAT) ૨૭૭

પરિશિષ્ટ-૫: PRESERVATION REQUEST ૨૭૯

પરિશિષ્ટ-૬: PERFORMA TO SEEK CDR/ SDR/ CAF/ IMEI/ ILD/ IPDR ૨૮૩

પ્રકરણ -૧

ડિજિટલ પુરાવાને સંલગ્ન મહત્વપૂર્ણ કાયદાકીય જોગવાઇઓ

પ્રકરણનો ઉદ્દેશ: કાનૂની કાર્યવાહી દરમ્યાન ડિજિટલ પુરાવા/ ઇલેક્ટ્રોનિક રેકર્ડની ગ્રાહ્યતા, વિશ્વસનીયતા અને સ્વીકૃતિ માટે કાયદામાં વિશેષ જોગવાઇઓ કરવામાં આવેલ છે. જેમ કે, ઇલેક્ટ્રોનિક રેકર્ડ ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ખ મુજબના પ્રમાણપત્ર સાથે ન્યાયાલય સમક્ષ રજૂ કરવાનું રહે છે.આથી તપાસ અધિકારીએ આ કાનૂની જોગવાઇઓ પ્રત્યે ધ્યાન આપવું અનિવાર્ય છે.

૨૦મી સદીમાં સૌથી નોંધપાત્ર અને પ્રભાવશાળી આવિષ્કાર થયો હોય તો તે કોમ્પ્યુટર અને ઈન્ફોર્મેશન ટેકનોલોજી. દેશના કાયદાઓએ પણ આ વાસ્તવિકતાની ગંભીરતાથી નોંધ લીધી છે, અને ઇલેક્ટ્રોનિક રેકર્ડને કાયદાની અદાલતમાં ગ્રાહ્ય પુરાવા તરીકે માન્યતા મળે તે હેતુથી ઈન્ફોર્મેશન ટેકનોલોજી એક્ટ ૨૦૦૦ પસાર કરવામાં આવેલ છે, જેના આધારે અન્ય કાયદાઓ જેવા કે ભારતીય દંડ સંહિતા(Indian Penal Code), ભારતીય પુરાવા અધિનિયમ (Indian Evidence Act) અને ફોજદારી કાર્યરીતિ સંહિતા(Criminal Procedure Code) વિગેરે કાયદાઓમાં પણ સુધારા લાવવામાં આવ્યા.

૧. ડિજિટલ પુરાવા: વ્યાખ્યા

ડિજિટલ પુરાવા અથવા ઇલેક્ટ્રોનિક પુરાવા એટલે ડિજિટલ સ્વરૂપે સંગ્રહિત અથવા પ્રસારિત કોઇપણ પ્રમાણિક/સાબિતી પૂરી પાડતી એવી માહિતી છે કે જેનો ઉપયોગ ન્યાયાલય સમક્ષ થઈ શકે છે.

ઈન્ફોર્મેશન ટેકનોલોજી એક્ટ, ૨૦૦૦ ની કલમ ૭૯-ક મુજબ પુરાવાના ઇલેક્ટ્રોનિક સ્વરૂપને આ પ્રમાણે વ્યાખ્યાયિત કરવામાં આવ્યું છે, "*કોઇપણ સાબિતી મૂલ્ય ધરાવતી એવી માહિતી કે જે ઇલેક્ટ્રોનિક સ્વરૂપે સંગ્રહિત કે પ્રસારિત કરવામાં આવેલ હોય કે જેમાં કોમ્પ્યુટર એવિડન્સ, ડિજિટલ ઑડિયો, ડિજિટલ વિડિયો, ડિજિટલ ફેક્સ મશીનનો સમાવેશ થાય છે.*"

ઈન્ફોર્મેશન ટેકનોલોજી એક્ટની કલમ 2(1)(t) અંતર્ગત ઇલેક્ટ્રોનિક પુરાવાની વ્યાખ્યા આ મુજબ કરવામાં આવી છે,"*ઇલેક્ટ્રોનિક સ્વરૂપમાં અથવા માઇક્રો ફિલ્મ અથવા કોમ્પ્યુટર જનરેટેડ માઇક્રોફિચ (micro fiche) માં સંગ્રહિત, પ્રાપ્ત થયેલ અથવા મોકલવામાં આવેલ ડેટા, રૅકર્ડ અથવા ડેટા જનરેટેડ, ઇમેજ કે સાઉન્ડ.*"

ઈન્ફોર્મેશન ટેકનોલોજી એક્ટ,૨૦૦૦ દ્વારા ભારતીય પુરાવા અધિનિયમની કલમ-૩ માં સુધારો કરવામાં આવ્યો છે જે અંતર્ગત ઇલેક્ટ્રોનિક રૅકર્ડને કોર્ટના નિરીક્ષણ માટેના પુરાવા તરીકે સમાવિષ્ટ કરવામાં આવેલ છે. ભારતીય પુરાવા અધિનિયમની

કલમ-3 અંતર્ગત પુરાવાની વ્યાખ્યા નીચે મુજબ કરવામાં આવી છે:

" 'પુરાવો' એ શબ્દનો અર્થ નીચે મુજબ થાય છે અને એ શબ્દમાં નીચેની બાબતોનો સમાવેશ થાય છે:

" જેની તપાસ ચાલતી હોય તે હકીકત સંબંધી કોર્ટ સાક્ષીઓને પોતાની સમક્ષ જે કથનો કરવાની પરવાનગી આપે અથવા તેમ કરવા ફરમાવે તે તમામ કથનો; આવા કથનો મૌખિક પુરાવો કહેવાય છે; "

કોર્ટ તપાસણી કરી શકે તે માટે રજૂ કરેલા તમામ ઇલેક્ટ્રોનિક રેકર્ડ સહિતના દસ્તાવેજો; આવા ઇલેક્ટ્રોનિક રેકર્ડ સહિતના દસ્તાવેજોને દસ્તાવેજી પુરાવો કહેવાય છે."

આ કલમ સ્પષ્ટ કરે છે કે ઇલેક્ટ્રોનિક રેકર્ડ એ કોર્ટમાં 'દસ્તાવેજી પુરાવો' છે.

<u>૨. ઇલેક્ટ્રોનિક પુરાવાની ગ્રાહ્યતા:</u>

ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ક માં ઇલેક્ટ્રોનિક પુરાવાની જોગવાઇ આપવામાં આવેલ છે, જે નીચે મુજબ છે:

" ઇલેક્ટ્રોનિક રેકર્ડને લગતાં રજૂ કરવામાં આવેલાં પુરાવાઓ કલમ ૬૫-ખ ની જોગવાઇઓ અનુસાર સાબિત કરી શકાય."

તપાસ કરનાર અધિકારીને કલમ ૬૫-ખ ની સ્પષ્ટ સમજ હોય તે જરૂરી છે, કારણ કે જ્યાં સુધી આ કલમની શરતોનું પાલન ના થાય

ત્યાં સુધી કોઇપણ ઇલેક્ટ્રોનિક પુરાવો અદાલતમાં ગ્રાહ્ય રહેશે નહી.

ઇલેક્ટ્રોનિક સ્વરૂપમાં રહેલ ડેટા સંગ્રહિત કરેલ તેમજ સાચવેલ હોવો જોઇએ. ઇલેક્ટ્રોનિક રેકર્ડ અર્થાત કોઇપણ માહિતી કે જે ઇલેક્ટ્રોનિક સ્વરૂપમાં રહેલ હોય. તેથી કોઇપણ ડેટા કે જે હાર્ડડ્રાઇવ, પેનડ્રાઇવ, સીડી, ડીવીડી કે પછી ઇન્ટરનેટ પર ઉપલબ્ધ હોય તે ઇલેક્ટ્રોનિક રેકર્ડ ગણાય છે. પેનડ્રાઇવમાં રહેલ કોઇ ફોટો, ફોન દ્વારા ક્લિક કરાયેલ ફોટો, ફોનમાં રહેલ 'whatsapp' મેસેજ, તેમજ મોબાઇલ સર્વિસ પ્રોવાઇડરના સર્વરમાં રહેલ કોલ ડિટેલ રેકર્ડ(CDR) આ બધાનો સમાવેશ ઇલેક્ટ્રોનિક રેકર્ડમાં થાય છે.

આવા કેસમાં મૂળ ડિવાઇસ કે જેમાંથી ઇલેક્ટ્રોનિક રેકર્ડ ઉત્પન્ન થયેલ હોય તેને પ્રાથમિક પુરાવો કહેવાય છે. ઉદાહરણ તરીકે સાઉન્ડ રેકર્ડર અથવા સીસીટીવી કેમેરા અને તેની સાથે સંકળાયેલ હાર્ડડિસ્ક કે જેનો ઉપયોગ કોઇ વિડિયો કે ઑડિયો ક્લિપને રેકર્ડ કરવા થયેલ હોય તો આવા ડિવાઇસ પ્રાથમિક પુરાવા છે. અન્ય ઉદાહરણ તરીકે આપણે વિશાળ સર્વરને લઇ શકીએ જ્યાં ડેટાનું નિર્માણ અને તેનો સંગ્રહ થતો હોય છે. આવા સર્વર પણ પ્રાથમિક પુરાવા તરીકે લાયક ઠરે છે. ઉદાહરણ તરીકે ફેસબુકનું સર્વર.

પુરાવાના કાયદાનો સામાન્ય નિયમ છે કે જ્યારે પ્રાથમિક પુરાવો ઉપલબ્ધ હોય ત્યારે ગૌણ પુરાવો ગ્રાહ્ય નથી. જો કે ઇલેક્ટ્રોનિક રેકર્ડ સંબંધી કેસોમાં આ સિદ્ધાંતને સખત રીતે લાગુ કરી શકાય

નહી કારણ કે દરેક કેસમાં વિશાળ સર્વર કે મૂળ ઉપકરણ (original device) ને કોર્ટ સમક્ષ પ્રસ્તુત કરવામાં આવે તેવી અપેક્ષા રાખી શકાય નહીં. જેમ કે કોર્ટની દરેક કાર્યવાહીમાં ફેસબુક સર્વર લાવવું શક્ય નથી. આ જ રીતે મોબાઇલ સર્વિસ પ્રોવાઇડરના સર્વરમાં સંગ્રહિત કોલ ડિટેલ રૅકર્ડ(CDR) એ પ્રાથમિક પુરાવો છે અને તપાસ અધિકારીને આપવામાં આવેલ કોપી/નકલ ગૌણ પુરાવો છે. તેથી સીડી/ડીવીડીના સ્વરૂપમાં મળેલ સોફ્ટ કોપી કે પ્રિન્ટઆઉટ તરીકે મળેલ કોઇ આઉટપુટ ગૌણ પુરાવા હોવા છતાં કોર્ટમાં ગ્રાહ્ય છે. પરંતુ ઇલેક્ટ્રોનિક રેકોર્ડ ન્યાયાલય સમક્ષ રજૂ કરતા પહેલા કેટલીક શરતોનું પાલન થવું જરૂરી છે.

આ શરતો એ સુનિશ્ચિત કરવાના દૃષ્ટિકોણથી બનાવવામાં આવેલ છે કે, ગૌણ પુરાવો એ મૂળ ઇલેક્ટ્રોનિક રૅકર્ડની સાચી અને સચોટ પ્રતિકૃતિ છે અને તેમાં કોઇપણ પ્રકારે ચેડા થયેલ નથી. આ શરતોને સુનિશ્ચિત કરવાના દૃષ્ટિકોણથી ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ખ (Information Technology Act, 2000 દ્વારા લાગુ પડેલ સુધારા) અમલમાં લાવવામાં આવેલ છે. ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ખ નીચે મુજબ છે.

૨.૧) ભારતીય પુરાવા અધિનિયમ કલમ ૬૫-ખ: ઈલેક્ટ્રોનિક રૅકર્ડની ગ્રાહ્યતા:

૧. આ કાયદામાં વિરૂદ્ધની કોઈ જોગવાઈ હોય તો પણ, ઈલેક્ટ્રોનિક સ્વરૂપે સંગ્રહાયેલી કોઈ પણ માહિતી કે જે કાગળ ઉપર પ્રિન્ટ તરીકે

કાઢવામાં આવેલ હોય,સંગ્રહવામાં આવી હોય,રેકર્ડ કરવામાં આવી હોય કે જેને (આ કલમમાં હવે પછી જેને કોમ્પ્યુટર આઉટપુટ તરીકે ઓળખવામાં આવશે.) કોમ્પ્યુટર સ્થિત ઓપ્ટિકલ અથવા ચુંબકીય માધ્યમની વ્યવસ્થા દ્વારા છાપીને તેની નકલ તૈયાર કરવામાં આવી હોય,ત્યારે એવી નકલો, એવી માહિતી અને પ્રસ્તુત કોમ્પ્યુટર સંબંધમાં આ કલમમાં જણાવેલી શરતોનું પાલન થતું હોય તો તે પણ દસ્તાવેજ છે,અને વધારાના પુરાવા કે અસલ દસ્તાવેજ રજૂ કર્યા વિના અસલ દસ્તાવેજના પુરાવા તરીકે જ્યાં સીધો પુરાવો જ ગ્રાહ્ય બની શકે તે હેતુ માટે તે કોઈપણ કેસમાં પુરાવા તરીકે ગ્રાહ્ય બની શકે છે.

૨.ઉપર પેટાકલમ-૧ માં જેનો ઉલ્લેખ કરવામાં આવ્યો છે તેવી કોમ્પ્યુટર સંબંધી શરતો નીચે પ્રમાણે છે.

(એ) *કોમ્પ્યુટરના ઉપયોગ સંબંધી નિયંત્રણ જે વ્યક્તિના હાથમાં હોય,તેવી વ્યકિત દ્વારા,એના ધંધા અંગેની તમામ માહિતી સંબંધિત સમયગાળા દરમિયાન નિયમિત રીતે તેમાં સંગ્રહવામાં આવી હોય કે તેનું વિશ્લેષણ કરી તેના ઉપર પ્રક્રિયા કરવામાં આવી હોય,અને એવા કોમ્પ્યુટરમાંથી જ એ માહિતી પ્રિન્ટઆઉટના સ્વરૂપમાં મેળવવામાં આવી હોય.*

(બી) *પ્રસ્તુત સમયગાળા દરમિયાન,ઈલેક્ટ્રોનિક રેકર્ડમાં સંગ્રહાયેલી એ માહિતી, અથવા અન્ય કોઈ માધ્યમ જેમાં એવી માહિતી જળવાયેલી હોય, તેમાંથી તે માહિતી એવા કોમ્પ્યુટરમાં એવી પ્રવૃત્તિ કે નિયમ*

પ્રમાણે નિયમિત રીતે દાખલ કે ફીડ કરવામાં આવેલ હોય.

(સી) *પ્રસ્તુત સમય દરમ્યાન કોમ્પ્યુટર કોઈપણ મુશ્કેલી વિના યોગ્ય રીતે કામ કરતું હતું , અને જો તે યોગ્ય રીતે કામ કરતું ન હોય અથવા તેમાંની પ્રક્રિયા બંધ થઈ હોય તો તે એવી સ્થિતિમાં નહિ હોય જેને કારણે એમાં સંગ્રહાયેલા ઈલેક્ટ્રોનિક રૅકર્ડ ઉપર વિપરીત અસર થાય.*

(ડી) *પ્રસ્તુત કોમ્પ્યુટરમાં એ ધંધા કે કામકાજના નિયમ પ્રમાણેની જે માહિતી સંગ્રહવામાં આવી હતી કે ફીડ કરવામાં આવી હતી,એમાંથી જ એ રૅકર્ડ સંબંધી માહિતી કે પ્રિન્ટઆઉટના સ્વરૂપમાં માહિતી મેળવવામાં આવેલ હતી.*

***3.** ઉપર પેટાકલમ-૨ ના ક્લોઝ (એ) માં જણાવ્યા પ્રમાણે ધંધા કે પ્રવૃત્તિ સંબંધી પ્રસ્તુત માહિતી કોમ્પ્યુટરમાં સંગ્રહ કરવાની અથવા તેના ઉપર પ્રક્રિયા થવાની કામગીરી પ્રસ્તુત સમયગાળા દરમિયાન તેમાં નિયમિત રીતે થતી આવી હતી, પછી ભલે ને એવી કામગીરી:-*

(એ) *એકી સાથે જોડાયેલાં અનેક કોમ્પ્યુટરમાં થતી હોય, અથવા*

(બી) *જુદાં જુદાં કોમ્પ્યુટરમાં એ કામગીરી વારાફરતી થઇ હોય, અથવા*

(સી) એક સાથે જોડાયેલાં અનેક કોમ્પ્યુટરોનાં જુદાં જુદાં સમુહોમાં વારાફરતી થતી હોય, અથવા

(ડી) એ સમયગાળા દરમિયાન એક કે વધુ કોમ્પ્યુટર અથવા એક કે વધુ કોમ્પ્યુટર સમુહોમાં અન્ય કોઈ રીતે એવી કામગીરી થતી હોય. ત્યારે પ્રસ્તુત સમયગાળા દરમિયાન એ હેતુ માટે ઉપયોગમાં લેવામાં આવેલાં કોમ્પ્યુટરો આ કલમના હેતુ માટે એક જ કોમ્પ્યુટર ગણાશે, અને આ કલમમાં નો તેનો સંદર્ભ એ રીતે જ સમજવાનો રહેશે.

૪. આ કલમની જોગવાઈઓને આધારે કોઈપણ પ્રકરણમાં પુરાવો રજૂ કરવાનો હોય, ત્યારે નીચે જણાવ્યા પ્રમાણેની વિગતોવાળું સર્ટિફિકેટ સામેલ કરવાનું રહેશે.

(એ) એવું વક્તવ્ય કે નિવેદન જેનું બનેલું છે, તે ઈલેક્ટ્રોનિક રૅકર્ડની ઓળખ કરાવતું હોય અને કઈ રીતે તેને પ્રિન્ટઆઉટના સ્વરૂપમાં બહાર કાઢવામાં આવેલ હતું.

(બી) એવું ઈલેકટ્રોનિક રૅકર્ડ જે સાધનો દ્વારા બહાર કાઢવામાં આવેલ હતું, તેની વિગતો, જેને આધારે યોગ્ય રીતે બતાવી શકાય કે એવું એ રૅકર્ડ કોમ્પ્યુટર માંથી બહાર કાઢવામાં આવેલ હતું.

(સી) પેટાકલમ-૨ માં જણાવ્યા પ્રમાણેની શરતોનું પાલન કરવા સંબંધે જે કરવું જરૂરી હતું તે કરવામાં આવ્યું હતું.

તેમજ કોમ્પ્યુટરની એ પ્રકારની કામગીરી સંબંધમાં જવાબદારી વાળો હોદ્દો સંભાળતી હોય કે સંબંધિત પ્રવૃત્તિની વ્યવસ્થા સંભાળતી હોય,(જે એ કેસના સંદર્ભમાં યોગ્ય હોય) તેની સહી થઈ હોય, તો એવા સર્ટિફિકેટ માટે તે પુરાવો બની રહે છે, અને સાથે આ પેટાકલમને સંબંધ છે ત્યાં સુધી એવા વક્તવ્ય કે નિવેદનમાં રજૂ થયેલી હકીકતની બાબતમાં એવી વ્યક્તિએ પોતાની શ્રેષ્ઠ જાણકારી અને માન્યતા પ્રમાણે ખરી હોવા બાબતનું એકરારનામું હોવું પર્યાપ્ત ગણાશે.

***૫.** આ કલમના હેતુઓ માટે,*

(એ) *કોમ્પ્યુટરમાં સંગ્રહવામાં આવેલી એવી માહિતી તે અંગેના યોગ્ય તેવા સ્વરૂપમાં કે ફોર્મેટમાં તેમાં સંગ્રહવવા માં કે ફીડ કરવામાં આવી હતી અને એ માહિતી તેમાં (માણસના માધ્યમ દ્વારા કે અન્ય રીતે) સીધી રીતે જ અથવા એ માટેના કોઇ યોગ્ય સાધન દ્વારા એમાં સંગ્રહ કરવામાં આવી હતી એમ માનવામાં આવશે.*

(બી) *અધિકારીક રીતે મળેલી એવી માહિતી કોમ્પ્યુટર ની રાબેતા મુજબની કામગીરી દરમિયાન તેમાં સંગ્રહવામાં આવી હોય કે કોમ્પ્યુટરની એવી રાબેતા મુજબની કામગીરી સિવાયની કોઇ પ્રક્રિયા કરવા માટે સંગ્રહવામાં આવી હોય, પરંતુ જો તે કોમ્પ્યુટરમાં યોગ્ય રીતે સંગ્રહવામાં આવી હોય તો તે પણ એની*

રાબેતા મુજબની કામગીરીના ભાગરૂપે થતી પ્રવૃત્તિ જ ગણાશે.

(સી) કોમ્પ્યુટરમાંથી પ્રિન્ટઆઉટ દ્વારા મેળવાયેલી માહિતી તેમાંથી (માણસના માધ્યમ દ્વારા અથવા તેના હસ્તક્ષેપથી) મેળવવામાં આવી હોય કે અન્ય સાધનોની મદદથી મેળવવામાં આવી હોય, તે એવા કોમ્પ્યુટરમાંથી જ મેળવવામાં આવી હોવાનું ગણાશે.

સ્પષ્ટીકરણ: આ કલમના હેતુ માટે અન્ય સ્ત્રોતમાંથી મેળવવામાં આવેલી માહિતીનો કોઇ પણ સંદર્ભ તે ગણતરી,સરખામણી કે અન્ય પ્રકારની પ્રક્રિયાની રીતે જ કરવામાં આવ્યો હતો એમ ગણાશે.

૨.૨) <u>કલમ ૬૫-ખ: ગ્રાહ્યતા ની શરતો અને પ્રક્રિયા:</u>

ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ખ કોર્ટમાં ઇલેક્ટ્રોનિક રેકર્ડના પુરાવાને રજૂ કરવાની શરતો અને પ્રક્રિયાઓ વિશે છે. કલમ ૬૫-ખ અંતર્ગત એ વાતનો સ્વીકાર કરવામાં આવ્યો છે કે, ઇલેક્ટ્રોનિક રેકર્ડના મૂળભૂત અને પ્રાથમિક પુરાવાને કોર્ટ સમક્ષ રજૂ કરવાની અપેક્ષા રાખી શકાય નહિ, અને જો તેવુ કરવામાં પણ આવે, તો ઇલેક્ટ્રોનિક પુરાવો બાઇનરી (Binary) સ્વરૂપમાં હોવાથી કોર્ટ તેને સમજી શકે નહિ. (બાઇનરી ભાષા એ કોમ્પ્યુટર સમજી શકે તેવી ભાષા છે - આમાં બધી માહિતી શૂન્ય અને એકથી બનેલી સંજ્ઞાઓમાં

સંગ્રહવામાં આવે છે). કલમ ૬૫-ખ નો મૂળ ઉદ્દેશ એ સુનિશ્ચિત કરવાનો છે કે, જો ઇલેક્ટ્રોનિક પુરાવાને લગતી અમુક શરતો અને પ્રક્રિયાઓનું પાલન કરવામાં આવ્યું હોય, તો કોમ્પ્યુટરમાંથી કાઢેલી નકલ, પ્રિન્ટઆઉટ (Printout) કે સીડી/ડીવીડી વગેરેમાંની માહિતી ગ્રાહ્ય ગણવામાં આવશે.

ઇલેક્ટ્રોનિક ડેટાની વિશ્વસનીયતાને જાળવી રાખવા માટેની કેટલીક શરતો કલમ ૬૫-ખ(૨) માં આપવામાં આવી છે. આ શરતો નીચેની બાબતો સુનિશ્ચિત કરવા માટે મૂકેલી છે:

એ) જે ડેટા વિશે વાત થઇ રહી છે, તેના સુધી કોઇ અનઅધિકૃત રીતે પહોંચી શક્યુ નથી (Data is not accessed illegally).

બી) કમ્પ્યુટર યોગ્ય રીતે જ કામ કરી રહ્યુ હતું અને તેથી ડેટાની નકલ સચોટ અને વિશ્વાસપાત્ર છે.

<u>૨.૩) કલમ ૬૫-ખ અંતર્ગત સર્ટિફિકેટ આપવાની સત્તા અને સમાવિષ્ટ તથ્યો:</u>

કોઇપણ ઇલેક્ટ્રોનિક રૅકર્ડનું આઉટપુટ, કોર્ટમાં ગ્રાહ્ય રહે તે માટે તેને પુરાવાના કાયદાની કલમ ૬૫-ખ(૪) અંતર્ગત અપાયેલ પ્રમાણપત્ર સાથે રજૂ કરવું જરૂરી છે. જે કમ્પ્યુટરમાંથી ડેટા લેવામાં આવ્યો છે, તે કોમ્પ્યુટરની જવાબદારી ધરાવનાર વ્યક્તિ દ્વારા જ આવું સર્ટિફિકેટ અપાયેલુ હોવું જોઇએ. આ સર્ટિફિકેટમાં કલમ ૬૫-ખ(૨)માં

આપેલી નીચેની શરતોનું પાલન થયુ છે તે પ્રમાણિત થયેલ હોવુ જોઇએ:

- ડેટા અને કોમ્પ્યુટર સિસ્ટમની વિશ્વસનીયતા,
- ઇલેક્ટ્રોનિક રેકર્ડના આઉટપુટને મેળવવાની પ્રક્રિયા,
- ઉપયોગમાં લેવાયેલ ડિવાઇસની ઓળખ અને વિગતો (તેમાં મૂળ ડિવાઇસનો પણ સમાવેશ થાય છે.)

આવા સર્ટિફિકેટનો મૂળ હેતુ સ્ત્રોતની વિશ્વસનીયતા અને માહિતીની પ્રમાણભૂતતાની ખાતરી કરવાનો છે કે જેથી કોર્ટ તેના પર વિશ્વાસ રાખી શકે. ઇલેક્ટ્રોનિક રેકર્ડમાં ચેડા અને ફેરફારની શક્યતાઓ વધારે હોવાથી, વધુ સાવચેતીની આવશ્યક્તા રહે છે. ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ખ અંતર્ગત આપવામાં આવતાં સર્ટિફિકેટનું સ્વરૂપ અનુસૂચિઓમાં આપવામાં આવેલ છે. પ્રશ્નો જેવાં કે, સર્ટિફિકેટ કેવી રીતે તૈયાર કરવું?, સર્ટિફિકેટ કોણે આપવું જોઇએ? અને સર્ટિફિકેટની ચોક્કસ માહિતી, કે જે ઇલેક્ટ્રોનિક રેકર્ડને ન્યાયાલય સમક્ષ સાબિત કરવાનું છે, તેના ચોક્કસ પ્રકાર અને કેસના તથ્યો પર આધાર રાખે છે.

ઉદાહરણ તરીકે, જો મોબાઇલ ફોનના કેમેરામાંથી લેવામાં આવેલો ફોટો સૌપ્રથમ લેપટોપ પર કોપી કરવામાં આવશે અને ત્યારબાદ તેની પ્રિન્ટ કાઢવામાં આવશે, તો આવા કિસ્સામાં માહિતીની આપ-લે કરવામાં આવી છે તે કડીની

વિશ્વસનીયતા સાબિત કરવા માટે સર્ટિફિકેટમાં ટ્રાન્સફર અને પ્રિન્ટિંગની પ્રક્રિયાનો ઉલ્લેખ કરવો પડશે. તેમજ આવું સર્ટિફિકેટ મોબાઇલ ફોન કે લેપટોપના સંચાલક/વાપરનાર દ્વારા જ તૈયાર કરીને અપાયેલું હોવું જોઇએ. આ સર્ટિફિકેટમાં કલમ ૬૫-ખ (૨) અને ૬૫-ખ (૪)ની શરતોનું ફરજિયાતપણે પાલન થયેલ હોવું જોઇશે. આ સર્ટિફિકેટમાં આઉટપુટ તૈયાર કરવા માટે વપરાયેલ મૂળ મોબાઇલ ફોન તેમજ અન્ય ડિવાઇસની ઓળખ આપવી પડશે, ઉદાહરણ તરીકે મોબાઈલ ડિવાઈસ ના IMEI અને લેપટોપ ના MAC Address વિગેરે. આવા કિસ્સાઓમાં મૂળ આઉટપુટની જાળવણી પણ અત્યંત જરૂરી છે.

કોલ ડિટેલ રૅકર્ડ(CDR)ના પુરાવાના કિસ્સામાં મોબાઇલ સર્વિસ પ્રોવાઇડરના નોડલ ઓફિસર જ કલમ ૬૫-ખ અંતર્ગત સર્ટિફિકેટ આપે છે (નોડલ ઓફિસર પોતે જ આ CDRની પ્રિન્ટઆઉટ કાઢીને પોલીસ સમક્ષ રજૂ કરશે.) પરંતુ જ્યારે ઇન્ટરનેટ પરની માહિતીને પુરવાર કરવાનું કહેવામાં આવે ત્યારે આ પ્રક્રિયા થોડી વધુ જટીલ બની જાય છે. આવા કિસ્સાઓમાં જે વ્યક્તિએ વેબસાઇટ/ઇ-મેઇલ પરથી પ્રિન્ટઆઉટ લીધી હોય તેણે પોતે સર્ટિફિકેટ આપવું પડશે. CCTV/DVR (ડિજિટલ વિડિઓરૅકર્ડર) માંથી નકલો લેવામાં આવી હોય તેવાં કિસ્સાઓમાં તે CCTV સિસ્ટમ/DVRના માલિક કે સંચાલકે સર્ટિફિકેટ આપવું જોઇએ, સાથે-સાથે જે

વ્યક્તિએ નકલ બનાવીને આપેલ છે તેણે પણ આ સર્ટિફિકેટ આપવાનુ રહેશે.

નામદાર દિલ્હી હાઇકોર્ટના કુંદનસિંહ વિ. રાજ્ય (MANU/DE/3674/2015)ના ચુકાદાને આધારે, એવાં કિસ્સાઓ કે જેમાં સર્વર/કમ્પ્યુટરમાં ડેટા લાંબા સમય સુધી સંગ્રહિત થાય છે, તેમાં જે વિસ્તૃતતાથી ‘કર્ણોપકર્ણનો સિદ્ધાંત’(the doctrine of hearsay) લાગુ પાડી શકાતો હતો તે વિસ્તૃતતાને ઇલેક્ટ્રોનિક પુરાવાના સંદર્ભમાં ઘણા અંશે લાગુ પડશે નહી. કોર્ટે એ હકીકતને માન્યતા આપી છે કે એવા કિસ્સા કે જેમાં વિવિધ સર્વરોમાં રહેલી વિશાળ માહિતી કે જેને વર્ષો બાદ સાબિત કરવાનું કહેવામાં આવે છે તે માહિતી જે કોમ્પ્યુટર સિસ્ટમમાં રહેલી છે તેના જે તે સમયનાં તમામ ઇન્ચાર્જ વ્યક્તિ પાસેથી આવું સર્ટિફિકેટ મેળવવું શક્ય ન પણ બને. આવા કિસ્સાઓમાં, જે વ્યક્તિઓએ ત્યારબાદ આવા કોમ્પ્યુટર્સનો હવાલો સંભાળ્યો હોય તેવી વ્યક્તિઓ ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ખ અંતર્ગત સર્ટિફિકેટ આપી શકશે. આનો અર્થ એવો થાય છે કે આવા ડિવાઇસના સંચાલનના સંદર્ભમાં જે વ્યક્તિ પુરાવા મેળવવાના સમયે જવાબદાર અધિકારીનો/સિસ્ટમ-એડમિનિસ્ટ્રેટરનો હોદ્દો ધરાવે છે તે વ્યક્તિ CCTV રેકોર્ડિંગ/CDR/સર્વર વગેરેનાં સંદર્ભમાં કલમ ૬૫-ખ અંતર્ગત સર્ટિફિકેટ આપી શકે.

નામદાર સર્વોચ્ચ ન્યાયાલયે અનવર પી.વી. વિ. પિ.કે. બશીર અને અન્ય (૨૦૧૪ ૧૦ SCC ૪૭૩) માં ઠરાવેલ છે કે ઇલેક્ટ્રોનિક પુરાવાને ગ્રાહ્ય બનાવવા માટે ૬૫-ખ અંતર્ગતનું સર્ટિફિકેટ ફરજિયાત છે. આ ચુકાદામાં કોર્ટે નોંધ્યુ કે પુરાવા અધિનિયમની કલમ ૬૫-ખ ની શરૂઆતમાં જ ‘બિનઅવરોધક જોગવાઇ’(non-obstante clause)છે. બિનઅવરોધક જોગવાઇ(non-obstante clause) એટલે એવી જોગવાઇ કે જેનાથી આ કાયદા અંતર્ગત કલમ ૬૫-ખ સાથે વિરોધાભાસ ધરાવતી બીજી કોઇ કલમો હોય, તો કલમ ૬૫-ખ હેઠળનું અર્થઘટન જ કાયદેસર ઠરશે. આથી ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ખ એ ગૌણ પુરાવાને લગતા સામાન્ય કાયદાની ઉપરવટ જાય છે, જે આ જ કાયદાની કલમ ૬૩ અને ૬૫ અંતર્ગત આવે છે. કલમ ૬૫-ખ એ ઇલેક્ટ્રોનિક રેકર્ડના પુરાવા સંબંધિત વિશેષ જોગવાઇ છે.

૨.૪) કલમ ૬૫-ખ હેઠળનું સર્ટિફિકેટ અમુક સંજોગો માં ફરજીયાત નથી: આરોપી પાસે થી સીઝર

એવા સંજોગો પણ આવી શકે છે કે જ્યારે ઈલેક્ટ્રોનિક રેકર્ડનું આઉટપુટ આરોપી પાસેથી જપ્ત કરવામાં આવે. દા.ત. ધરકપકડ કરતી વખતે આરોપી સ્વખુશીથી તેના ઈ-મેઈલ એકાઉન્ટમાંથી એક પ્રિન્ટઆઉટ કાઢીને પંચો રૂબરૂ આપે. શું આવા કિસ્સામાં આરોપીને પોતે જ સર્ટિફિકેટ રજૂ કરવાની ફરજ પાડી શકાય? અને જો તેમ થાય તો શું આમ કરવું એ

તેના પોતાના પર જ દોષારોપણ કરવામાં (Self-Incrimination)પરિણમે છે? જેના પરિણામ સ્વરૂપે, શું તે ભારતીય સંવિધાનના અનુચ્છેદ ૨૦(૩)ની વિરુદ્ધ નહી જાય? આ વિશે શફી મહોમ્મદ વિ. હિમાચલ પ્રદેશ રાજ્ય માં તારીખ ૩૦-૦૧-૨૦૧૮ના રોજ આપેલ ચુકાદામાં નામદાર સર્વોચ્ચ ન્યાયાલય દ્વારા નીચે મુજબ માર્ગદર્શન આપવામાં આવ્યું છે:

(11) The applicability of procedural requirement under Section 65B(4) of the Evidence Act of furnishing certificate is to be applied only when such electronic evidence is produced by a person who is in a position to produce such certificate being in control of the said device and not of the opposite party. In a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65of the Evidence Act cannot be held to be excluded. In such case, procedure under the said Sections can certainly be invoked. If this is not so permitted, it will be denial of justice to the person who is in possession of authentic evidence/witness but on account of manner of proving, such document is kept out of consideration by the court in absence of certificate under Section 65B(4) of the Evidence Act, which party producing cannot possibly secure. Thus, requirement of certificate under Section 65B(h) is not always mandatory.

(12) Accordingly, we clarify the legal position on the subject on the admissibility of the electronic evidence, especially by a party who is not in possession of device from which the document is produced. Such party cannot be required to produce certificate under Section 65B(4) of the Evidence Act. The applicability of requirement of certificate being procedural can be relaxed by Court wherever interest of justice so justifies.

આમ,આ ચુકાદા મુજબ,કલમ ૬૫-ખ અંતર્ગતના સર્ટિફિકેટની જરૂરિયાતને અમુક હદ સુધી હળવી બનાવી દેવામાં આવી છે અને ચુકાદામાં સૂચવવામાં આવ્યું છે કે કલમ ૬૫-ખ અંતર્ગતના સર્ટિફિકેટની જરૂરિયાત, અમુક શરતો હેઠળ, કાયમી રીતે ફરજિયાત નથી. ખાસ કરીને ત્યારે કે જ્યારે ઈલેક્ટ્રોનિક પુરાવો એવા પક્ષ દ્વારા રજૂ કરાયો હોય કે જે ડિવાઈસનો હવાલો ધરાવતો ન હતો. આથી, જ્યારે ઈલેકટ્રોનિક પુરાવો આરોપી પાસેથી જપ્ત કરવામાં આવ્યો હોય, તો ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ખ ની અંતર્ગતનું સર્ટિફિકેટ આરોપી પાસેથી મેળવવાનું રહેતુ નથી.

૨.૫) કલમ ૬૫-ખ ની શરતો સર-તપાસ માં પૂર્ણ ના કરી શકાય:

સર્ટીફિકેટ ના બદલામાં કોઇ સાક્ષી તેની સર તપાસમાં ઇલેક્ટ્રોનિક રૅકર્ડની કલમ ૬૫-ખ ની શરતોનું પાલન ન્યાયાલય સમક્ષ મૌખિક રીતે જુબાની આપી પૂર્ણ કરી શકે? આ પ્રશ્નનો ઉત્તર ના છે. જયારે પણ કાયદાની (statute) એવી

માંગ હોય કે કોઇ બાબત વિશિષ્ટ રીતે જ થવી જોઇએ તો તે તેવી રીતેજ થવી જોઇએ અને તેની રીત પરિસ્થિતિ મુજબ બદલી શકાય નહિ (cannot be circumvented). તેથી સાક્ષી સર તપાસમા આવી શરતોનું પાલન કરે છે એવુ માની લઇ ને ૬૫-ખ મુજબના પ્રમાણપત્રની જરૂરિયાત સંતોષાય જાય છે એમ માની લઇ શકાય નહિ.

૨.૬) કલમ ૬૫-ખ: માત્ર ગ્રાહ્યતા પૂરતું:

શું ૬૫-ખ અંતર્ગતનું પ્રમાણપત્ર ન્યાયલય સમક્ષ ઇલેક્ટ્રોનિક રૅકર્ડમાં રહેલી હકીકતોને નિર્ણાયક રીતે સાબિત/પ્રસ્થાપિત કરે છે? આનો ઉત્તર સ્પષ્ટ ના છે. કલમ ૬૫-ખ ની શરતો ઇલેક્ટ્રોનિક પુરાવાની ગ્રાહ્યતા માટેની પૂર્વશરત છે. ભારતીય પુરાવા અધિનિયમ ની કલમ ૬૫-ખ નું પાલન ન્યાયિક પ્રક્રિયા દરમ્યાન દસ્તાવેજ રજૂ કરવાની પરવાનગી (precondition for admissibilty of electronic records) આપે છે. ન્યાયાલયે દસ્તાવેજની પ્રસ્તુતતા, યથાર્થતા, ખરાપણું અને વિશ્વસનીયતા ચકાસવાની રહેશે.

૨.૭) સર્ટિફિકેટ પછીથી પણ રજૂ કરી શકાય:

ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ખ મુજબનું પ્રમાણપત્ર પ્રિન્ટઆઉટ/સીડી સાથે ફરજિયાત રજૂ કરવાનું રહેશે કે ત્યારપછી પણ રજૂ કરી શકાય? જો તપાસ કરનાર અમલદાર ચાર્જશીટમાં ઇલેક્ટ્રોનિક રેકર્ડ રજૂ કરી રહ્યા છે, તો સાથે ભારતીય પુરાવા અધિનિયમની કલમ

૬૫-ખ નુ સર્ટીફિકેટ રજૂ કરવાનું ફરજિયાત છે કે કેમ, તે બાબતે નામદાર દિલ્હી હાઇકોર્ટના કુંદનસિંહ વિ. રાજ્ય (MANU/DE/3674/2015) ના ચુકાદામાં સ્પષ્ટ કરવામા આવ્યું છે કે, "કલમ ૬૫-ખ મુજબનું પ્રમાણપત્ર પાછળથી પણ રજૂ કરી શકાય, અને ચાર્જશીટ સાથે જ રજૂ કરવુ જરૂરી નથી. સાક્ષી કે જેણે પુરાવા તરીકે ઇલેક્ટ્રોનિક રૅકર્ડ આપવાની તૈયારી બતાવી હોય તેને ભારતીય ફોજદારી કાર્યરીતિ સંહિતાની કલમ ૩૧૧ મુજબ પ્રમાણપત્ર રજૂ કરવાના હેતુથી ફરી બોલાવી શકાય. એવુ પણ થઇ શકે કે ચાર્જશીટ પછી પણ પ્રમાણપત્ર રજૂ કરી શકાય અને તે ભારતીય ફોજદારી કાર્યરીતિ સંહિતાની કલમ ૧૭૩(૮) મુજબ પૂરક ચાર્જશીટનો ભાગ બની શકે". નામદાર રાજસ્થાન હાઇકોર્ટના પારસ જૈન અને અન્ય વિ.રાજસ્થાન રાજ્યના ચુકાદા-[MANU/RH/1150/2015] માં સ્પષ્ટ કર્યું છે: "પુરાવા અધિનિયમની કલમ ૬૫-ખ મુજબનું પ્રમાણપત્ર રજૂ ન કરવું એ ઉપાય વિનાની ભૂલ નથી અને તે પછીથી પણ સુધારી શકાય તેમ છે". પરંતુ, હિતાવહ છે કે તપાસ કરનાર પોલીસ અધિકારી/કર્મચારી ઇલેક્ટ્રોનિક રેકર્ડ સાથે જ કલમ ૬૫-ખ મુજબનું પ્રમાણપત્ર/સર્ટીફિકેટ ન્યાયલય સમક્ષ રજૂ કરે.

<u>૩. વિદેશમાં રહેલ પુરાવા: મ્યુચ્યુઅલ લીગલ અસીસટન્સ ટ્રીટી (MLAT) અને લેટર્સ રોગેટરી (LR):</u>

ઇન્ટરનેટ કોઇપણ દેશની અધિકારક્ષેત્રની સીમાઓથી બંધાયેલ નથી. આથી સામાન્ય રીતે તપાસ દરમિયાન જોવા મળે છે કે

ડિજિટલ પુરાવા વિદેશનાં સર્વરમાં સ્થિત હોય છે. મોટાભાગની સોશિયલ મીડિયા વેબસાઇટ્સ (ઉદા. ફેસબુક), મેસેજ એપ્લિકેશન્સ (ઉદા.વોટ્સએપ) અને ઈ-મેઇલ (ઉદા.Gmail) વગેરેના સર્વર વિદેશમાં સ્થિત છે. ફોજદારી કાર્યરીતિ સંહિતા,૧૯૭૩ ની કલમ ૧૬૬-ક એ " ભારતની બહારનાં દેશોમાં તપાસ અંગે સક્ષમ સત્તાને વિનંતી પત્ર લખવા બાબત" સાથે સંબંધિત છે. ભારત સરકારનાં ગૃહ મંત્રાલય દ્વારા વિદેશમાંથી પુરાવા એકત્ર કરવા માટે એક વિસ્તૃત માર્ગદર્શિકા બહાર પાડવામાં આવી છે. પરંતુ તપાસ કરનાર અમલદારે સૌથી પહેલા એ તપાસ કરવાની જરૂરત રહે છે કે ઇલેક્ટ્રોનિક પુરાવા જે સર્વર/કોમ્પ્યુટર માં સંગ્રહિત છે તે ક્યા દેશ માં સ્થિત છે? તે જાણવા માટે ઇન્ટરનેટ પર ઘણી મફત સેવાઓ આપતી વેબસાઇટ્સ છે. www.dnsstuff.com આવી જ એક વેબસાઇટ છે. Domain Name Server (DNS), Universal Resource Locator (URL), અને Internet Protocol Address (IP Address) બાબતની તપાસ કરવાની પ્રક્રિયાની ચર્ચા આગામી પ્રકરણોમાં કરવામાં આવી છે.

3.1) ફોજદારી કાર્યરીતિ સંહિતા,૧૯૭૩ ની કલમ ૧૬૬ A અને ૧૦૫ હેઠળ વિદેશમાં તપાસ માટે લેટર્સ રોગેટરી (LR) / MLAT ઇશ્યુ કરવાની માર્ગદર્શિકા:

ફોજદારી કાર્યરીતિ સંહિતા,૧૯૭૩ ની કલમ ૧૬૬-ક માં વિદેશમાં સત્તાવાર તપાસ કરવા અને પુરાવા તથા સામગ્રી/દસ્તાવેજો એકત્ર કરવા માટે સક્ષમ કોર્ટ મારફત લેટર્સ

રોગેટરી (LR) મોકલવાની માર્ગદર્શિકા આપવામાં આવેલી છે. ભારત અને અન્ય દેશ વચ્ચે કરાયેલ મ્યુચ્યુઅલ લીગલ અસીસટન્સ ટ્રીટી (MLAT), સમજૂતીપત્ર (MOU) વગેરેની મર્યાદામાં રહીને આવા લેટર્સ રોગેટરી (LR) મોકલવામાં આવે છે. જો આવી કોઇ સંધિ અથવા સમજૂતીપત્ર અસ્તિત્વમાં ન હોય તો પણ બે દેશ એકબીજાને મદદ કરવાની બાંહેધરી હેઠળ પરસ્પર સહાય મેળવે છે. ક્રિમિનલ પ્રોસિજર કોડ (સીઆર.પી.સી.) ની કલમ ૧૦૫ સમન્સ/વોરન્ટ/ન્યાયિક પ્રક્રિયાઓની બજવણી(Service) સંદર્ભમાં વિદેશ ની સરકારો સાથે કેન્દ્ર સરકાર દ્વારા કરવામાં આવતી પારસ્પરિક વ્યવસ્થાની વાત કરે છે. ભારત અને અન્ય દેશો વચ્ચે કરવામાં આવેલ MLAT ની યાદી સીબીઆઇ (CBI) ની વેબસાઇટ પર ઉપલબ્ધ છે. અમુક કિસ્સાઓમાં ભારત અને અન્ય દેશ જો પરસ્પર સહાયનાં આંતરરાષ્ટ્રીય કન્વેન્શનનાં સહીકર્તા ના આધારે બંધનકર્તા હોય તો આવાં કન્વેન્શનની જોગવાઇઓનો પણ ઉપયોગ કરી શકાય છે. ભારત સરકારનાં ગૃહ મંત્રાલય દ્વારા લેટર્સ રોગેટરી (LR) માટે નીચે મુજબની માર્ગદર્શિકા બહાર પાડવામાં આવેલ છે.

એ. તપાસ એજન્સી દ્વારા સેન્ટ્રલ ઓથોરિટી જેવી કે ગૃહ મંત્રાલય (MHA) ની સંમતિ વગર કોઇપણ કોર્ટ સમક્ષ લેટર્સ રોગેટરી (LR) ઇશ્યુ કરવાની વિનંતી કરી શકાશે નહિ.

બી. જો લેટર્સ રોગેટરી (LR) મોકલવા અનિવાર્ય હોય તો સક્ષમ કોર્ટમાં અરજી દાખલ કરતાં પહેલા કેન્દ્ર સરકારની પરવાનગી મેળવવા માટે રાજ્યનાં ગૃહ વિભાગ મારફતે એક સ્વયં પ્રસ્તુત દરખાસ્ત ઉપસચિવશ્રી (કાયદા),આંતરિક સુરક્ષા વિભાગ, ગૃહ મંત્રાલય, લોકનાયક ભવન,નવી દિલ્હી-૧૧૯૯૯૩ ને ઉદ્દેશીને મોકલવાની રહેશે.

સી. ગૃહ મંત્રાલયને દરખાસ્ત મોકલતાં પહેલા સંબંધિત તપાસ એજન્સીએ એ બાબતની વિસ્તૃત ચકાસણી કરવી જોઇએ કે કેસનાં તર્કપૂર્ણ તારણ પર પહોંચવા માટે વિદેશમાં તપાસ કરવી સંપૂર્ણપણે જરૂરી છે. MLAT, MOU, વ્યવસ્થાઓ અથવા આંતરરાષ્ટ્રીય સંમેલનોની જોગવાઇઓ તેમજ વિનંતી કરાયેલ દેશના કાયદાની જરૂરિયાતો જેવી કે બેવડી ગુનાખોરીનો સિદ્ધાંત (Principle of Dual Criminality), પરસ્પર મદદની બાંહેધરી (Assurance of reciprocity) વગેરેનો અભ્યાસ કરવો જોઇએ કે જેથી આ પ્રકારની વિનંતી સંબંધિત દેશની કાનૂની જરૂરિયાતોને પૂરી કરે છે કે કેમ તે નક્કી કરી શકાય. MLATs ની યાદી CBI ની વેબસાઇટ પર ઉપલબ્ધ છે. એ સ્પષ્ટ રીતે દર્શાવવું મહત્વનું છે કે કઇ સંધિ, MOU, વ્યવસ્થા અથવા આંતરરાષ્ટ્રીય કન્વેન્શનની જોગવાઇને આધીન

રહીને આવી વિનંતી કરવામાં આવી છે? જ્યાં આ પ્રકારની દ્વિપક્ષીય કે બહુપક્ષીય વ્યવસ્થાઓ ઉપલબ્ધ નથી ત્યાં પરસ્પર મદદની બાંહેધરીનાં આધાર પર LR ઇશ્યુ કરવાં જોઇએ.

ડી. કેટલાક દેશો એવો આગ્રહ રાખે છે કે LR ચોક્કસ ભાષા કે ફોર્મેટમાં મોકલવામાં આવે. જો એમ હોય તો, આ માટેનો અભ્યાસ કરવો જોઇએ કે જેથી જે-તે દેશની જરૂરિયાતોનું પાલન થઇ શકે. જો જરૂરી જણાય તો આ માટે International Police Co-operation Cell (IPCC), CBI, નવી દિલ્હીની મદદ મેળવવી જોઇએ.

ઇ. MHA ની સંમતિ મેળવવા સબંધિત તપાસ એજન્સી નિમ્નલિખિત વિગતો ત્રણ નકલમાં મોકલશે:

I. આરોપ, આરોપીઓના નામ અને કરેલ ગુનાની કાયદાની કલમો સાથેની સંક્ષિપ્ત હકીકતો ધરાવતી સ્વંયસંપૂર્ણ નોંધ અને પ્રથમ માહિતી અહેવાલ (FIR) ની નકલ. FIR ગુજરાતી ભાષામાં હોય તો તેનું સ્પષ્ટ શબ્દોમાં લખાયેલ અંગ્રેજી ભાષાંતર હોવું જોઈશે.

II. વિદેશમાં તપાસ કરવાની આવશ્યકતા બાબત ની નોંધ સાથે, લેટર્સ રોગેટરી (Letter of Request) ઇશ્યુ કરવા ની જરૂરિયાત પર મુખ્ય સરકારી વકીલના કાનૂની અભિપ્રાયમાં સામેલ

હોવો જોઇએ. મુખ્ય સરકારી વકીલના અભિપ્રાયમાં લેટર્સ રોગેટરી (Letter of Request) જો ઇશ્યુ કરવામાં આવે તો તે MLAT અથવા MoU અથવા Arrangement અથવા આંતરરાષ્ટ્રીય કન્વેન્શન અંતર્ગત આવી જશે, અને દ્વિપક્ષીય-ગુનાખોરીના સિદ્ધાંત પર આધારિત જે તે દેશના કાયદામાં ગુનો બને છે કે કેમ? તે બાબતોની સ્પષ્ટ નોંધ હોવી જોઇએ. સાથો-સાથ, જે નિવેદન નોંધવા અથવા જે દસ્તાવેજ/સામગ્રી જપ્ત કરવા માટે અનુરોધ કરવામાં આવી રહ્યો છે, તેનુ ચાલુ તપાસમાં શું મહત્વ છે અને તેની તપાસમાં પ્રસ્તુતતા બાબતે પણ ટિપ્પણી કરી શકાય.

III. MLAT અથવા MoU અથવા Agreement અથવા Arrangement અથવા આંતરરાષ્ટ્રીય કન્વેન્શન અંતર્ગત લેટર્સ રોગેટરી કરવામાં આવેલ હોય તો તેને સબંધિત જોગવાઈઓનો ઉલ્લેખ કરવો. જો તે પારસ્પારિક્તાની ખાતરી માટેના કિસ્સામાં મોકલવામાં આવે તો તેનો પણ ઉલ્લેખ કરવા જોઇએ.

IV. સક્ષમ અદાલતમાં દાખલ કરવાની સૂચિત લેટર્સ રોગેટરીની દરખાસ્ત અરજી પણ સામેલ

કરી શકાય. અરજીમાં નીચેની વિગતોનો સમાવેશ કરવો:

i. કેસને લગતી સંક્ષિપ્ત હકીકતો, આરોપ, આરોપીઓના નામ તથા કરેલ ગુના માટે કાયદાની કલમો સાથેની પૃષ્ઠભૂમિ નોંધ અને બીડાણ તરીકે સ્પષ્ટ શબ્દોમાં લખાયેલ પ્રથમ માહિતી અહેવાલ **(FIR)** ની નકલ.

ii. વિનંતી કરાયેલ દેશ ખાતે કરવાની થતી તપાસની વિગતો. કોઈપણ દેશ ખોટી/અસ્પષ્ટ પૂછપરછ/તપાસ માટે મંજૂરી આપશે નહિ, તેથી તે બાબતની કાળજી રાખવી જોઈએ.

iii. દરેક સાક્ષીને ચકાસવા માટેની પ્રશ્નાવલી સાથે સાક્ષીની વિગતો, તેમની ઓળખ અને જો ઉપલબ્ધ હોય તો તેમનાં સરનામાં.

iv. એકત્રિત કરવાના દસ્તાવેજો/સામગ્રીનું અને તેની કાર્યવાહીનું વર્ણન.

v. તપાસ હેઠળ ગુના માં ભારતના કાયદા હેઠળ લાગતા આરોપો અને વિનંતી કરાયેલ દેશના કાયદાની સુસંગત કલમોનો સાર. જો લેટર્સ રોગેટરીના અમલ માટે વિનંતી કરેલ દેશના કાયદા હેઠળ

દ્વિપક્ષીય-ગુનાખોરીનો સિદ્ધાંત અથવા અન્ય કોઈ જરૂરિયાત ફરજિયાત હોય,તો તેનો સ્પષ્ટ ઉલ્લેખ હોવો જોઈશે.

vi. વિનંતી કરતાં દેશ દ્વારા આવી સહાય માટે **MLAT** અથવા MoU અથવા Agreement અથવા આંતરરાષ્ટ્રીય કન્વેન્શન વગેરેની જોગવાઈઓનો સાર.

vii. પ્રસ્તાવિત લેટર્સ રોગેટરી વિનંતી કરાયેલ દેશની તમામ જરૂરિયાતોનું પાલન કરશે, અને તે તપાસ રાજકીય, લશ્કરી,વંશીય અથવા ધાર્મિક બાબતની નથી તે અંગેનો એકરાર.

viii. **MLAT** અથવા MoU અથવા Agreement અથવા Arrangement અથવા આંતરરાષ્ટ્રીય કન્વેન્શન હેઠળ ન આવતા દેશ હોય તો પારસ્પરિક્તાની ખાતરી અંગેની દરખાસ્ત.

ix. લેટર્સ રોગેટરીનો અમલ કરવા વિનંતી કરાયેલ દેશમાં સત્તાધિકારીને મદદ કરવા તપાસ અધિકારી કે અન્ય અધિકારીની મુલાકાતની સૂચિત છે કે કેમ, તે બાબત ની દરખાસ્ત.

એફ. તપાસ એજન્સી દ્વારા લેટર્સ રોગેટરી તૈયાર કરતી વખતે નીચે મુજબની તકેદારી રાખવાની રહેશે.

i. દસ્તાવેજો, ફોટોગ્રાફ્સ અને વસ્તુઓ **(objects)** જો લેટર્સ રોગેટરી સાથે બીડેલ હોય તો, લેટર્સ રોગેટરી ના મુખ્ય ભાગમાં ઉક્તને સ્પષ્ટ રીતે ચિન્હિત તથા ઉલ્લેખિત કરવા જોઇશે કે જેથી વિનંતી કરેલ સત્તામંડળ એ સ્પષ્ટ રીતે જાણી શકે કે તેની સાથે શું કરવાની જરૂરિયાત રહે છે.

ii. તમામ બીડેલ કાગળો/દસ્તાવેજોની નકલો સ્પષ્ટ, સુવાચ્ય અને જો જરૂર જણાય તો જરૂરી ભાષામાં અનુવાદિત હોવી જોઈએ.

iii. લેટર્સ રોગેટરી યોગ્ય રીતે બીડેલ અને પેજ નંબર સાથેના હોવા જોઈએ.

iv. MLAT, MoU, Arrangement અથવા અન્ય કિસ્સામાં જો દર્શાવ્યા મુજબની ચોક્કસ ભાષામાં રજૂઆત કરવાની જરૂરિયાત હોય તો, અનુવાદક દ્વારા યોગ્ય રીતે સહી કરેલ અધિકૃત ભાષાંતરિત નકલો લેટર્સ રોગેટરીની અસલ નકલ સાથે બીડાયેલ હોવી જોઈએ.

v. લેટર્સ રોગેટરીની અસલ નકલની સાથે ઓછામાં ઓછી પાંચ નકલો તૈયાર કરવાની રહેશે. ભાષાંતરિત આવૃત્તિ (જો હોય તો) તેની સાથે કુલ ત્રણ નકલો ગૃહ મંત્રાલયને તથા એક

નકલ ઇન્ટરનેશનલ પોલીસ કો-ઓપરેશન સેલ (**IPCC-CBI)** ને મોકલવી જરૂરી રહેશે.

જી. ગૃહ મંત્રાલય જયારે યોગ્ય જણાશે ત્યારે **CBI** સાથે વિમર્શ કરીને લેટર્સ રોગેટરીને સક્ષમ કોર્ટ સમક્ષ રજૂ કરવા માટેની દરખાસ્તને સંમતિ પ્રદાન કરશે તથા પોતાના સંમતિપત્રની નકલ **IPCC-CBI**, નવીદિલ્હી ને મોકલશે.

એચ. ગૃહ મંત્રાલયની સંમતિ મેળવ્યા બાદ વિનંતી કરેલ દેશના સક્ષમ સત્તામંડળને સંબોધીને લેટર્સ રોગેટરી ઇશ્યુ કરવા માટે સક્ષમ કાર્યક્ષેત્ર ધરાવતી કોર્ટમાં એક અરજી દાખલ કરવાની રહેશે. સક્ષમ કોર્ટ એ નક્કી કરશે કે વિનંતી કરેલ દેશના સક્ષમ સત્તામંડળને સંબોધીને લેટર્સ રોગેટરી ઇશ્યુ કરવી કે કેમ?

આઇ. આવા કિસ્સામાં, જો વિનંતી સ્વીકારવામાં આવે છે તો કોર્ટ પોતાના સીલ અને ઓથોરીટી સાથેના લેટર્સ રોગેટરી ઇશ્યુ કરશે.

<u>૩.૨) સક્ષમ કોર્ટ દ્વારા લેટર્સ રોગેટરી ઇશ્યુ કર્યા પછી ની પ્રક્રીયા:</u>

સક્ષમ કોર્ટ દ્વારા લેટર્સ રોગેટરી ઇશ્યુ કર્યા બાદ તપાસ એજન્સી લેટર્સ રોગેટરી ની ત્રણ નકલો **IPCC-CBI**, નવી દિલ્હી ને તથા એક નકલ ગૃહ મંત્રાલયને મોકલશે. **IPCC-CBI,** નવી દિલ્હી, ગૃહ મંત્રાલયની જાણ હેઠળ ઇન્ડિયન

મિશન દ્વારા વિનંતી કરેલ દેશના સક્ષમ સત્તામંડળને તે નકલ મોકલી આપશે. વિનંતી કરેલ દેશથી લેટર્સ રોગેટરી ના અનુસંધાને જ્યારે ઇલેક્ટ્રોનિક પુરાવા મોકલવામાં આવે, તો તે તપાસ કરનાર અમલદારે **IPCC-CBI**, નવી દિલ્હી થી મેળવી લેવાના રહેશે અને સક્ષમ કોર્ટ સમક્ષ ચાર્જશીટ સાથે રજૂ કરવાના રહેશે.

ડ્રાફ્ટ **MLAT** વિનંતી અને ડ્રાફ્ટ **Letters Rogatory (Letter of Request)** પરિશિષ્ટ તરીકે જોડવામાં આવેલ છે.

૪. ભારતમાં સ્થિત ઇલેક્ટ્રોનિક રૅકર્ડ ને રજૂ કરવા ફરજ પાડવાની રીત:

ભારતીય ફોજદારી કાર્યરીતિ સંહિતાના પ્રકરણ-૭માં દસ્તાવેજી પુરાવા રજૂ કરવા માટે ફરજ પાડવાની રીતની જોગવાઇઓ આપવામાં આવેલ છે. હકીકતના ગુણને કારણે (By virtue of fact) ‘ઇલેક્ટ્રોનિક રૅકર્ડ’ દસ્તાવેજી પુરાવો છે, તપાસ અધિકારી ઇન્વેસ્ટિગેશન દરમ્યાન ઇલેક્ટ્રોનિક પુરાવા તરીકે તેનો ઉપયોગ કરી શકે છે. ભારતીય ફોજદારી કાર્યરીતિ સંહિતાની કલમ-૯૧ તપાસ અધિકારીને દસ્તાવેજ રજૂ કરવા સમન્સ કાઢવાની સત્તા આપે છે. તેમ છતાં ભારતીય ફોજદારી કાર્યરીતિ સંહિતાની કલમ-૯૧ પોસ્ટ અને ટેલિગ્રાફના તાબામાં રહેલા દસ્તાવેજોને લાગુ પડતી નથી. કોઇ કેસમાં જ્યારે પોસ્ટ અને ટેલિગ્રાફના તાબામાં રહેલા વિવરણ (details) મેળવવાના થાય ત્યારે ભારતીય

ફોજદારી કાર્યરીતિ સંહિતાની કલમ-૯૨માં યોગ્ય પદ્ધતિનો ઉલ્લેખ કરવામાં આવેલ છે. ભારતીય ફોજદારી કાર્યરીતિ સંહિતાની કલમ-૯૧ મુજબ આપવામાં આવતી નોટીસનો નમૂનો(ફોર્મેટ) પરિશિષ્ટ-૬ ના સ્વરૂપમાં જોડવામાં આવેલ છે. આના સંદર્ભમાં એ ધ્યાનમાં રાખવું જોઇએ કે તપાસ અધિકારી ભારતીય ફોજદારી કાર્યરીતિ સંહિતાની કલમ-૯૧ અંતર્ગતની નોટીસ ભારતમાં રહેલ ઇલેક્ટ્રોનિક દસ્તાવેજનો પુરાવા તરીકે રજૂ કરવાના કેસોમાં જ ઉપયોગ કરી શકે છે.

<u>૫. ઇ-મેઇલ/એસએમએસ/ઇલેક્ટ્રોનિક સંદેશાની સાબિતી:</u>

ઇ-મેઇલ, એસએમએસ અને અન્ય ઇલેક્ટ્રોનિક સંદેશાઓ મેટા-ડેટા ધરાવે છે, જે એકત્ર કરવાના રહે છે અને કોર્ટ સમક્ષ પુરાવા તરીકે રજૂ કરવામાં આવે છે. ઇ-મેઇલની બાબતમાં 'હેડર'નો મેટાડેટા તરીકે સમાવેશ થાય છે, જેને પુરાવાના ભાગરૂપે લેવો જોઇએ. ઇ-મેઇલના 'હેડર'માં IP એડ્રેસ, સમય, તારીખ હોઇ શકે. પુરાવા અધિનિયમની કલમ ૮૮-ક પણ ઇ-મેઇલ મેળવવાની બાબતમાં ચોક્કસ પૂર્વધારણાઓ રજૂ કરે છે, જે ઇ-મેઇલ પત્ર વ્યવહારની સાબિતી માટે ઉપયોગી થઇ શકે.

<u>કલમ ૮૮- A : ઇલેક્ટ્રોનિક સંદેશા સંબંધી માની લેવા બાબત.</u>

> *" અદાલત એવું માની લઇ શકશે કે જે વ્યક્તિને ઇલેક્ટ્રોનિક સંદેશો મોકલ્યાનું અભિપ્રેત થતુ હોય તે વ્યક્તિને, ઇલેક્ટ્રોનિક સંદેશો મોકલનાર વ્યક્તિ દ્વારા*

સંદેશો મોકલવા માટે તેના કોમ્પ્યુટરમાં સ્ટોર કરેલ સંદેશો, ઈલેક્ટ્રોનિક સંદેશો મોકલનાર સાધન (મેઈન સર્વર) દ્વારા મોકલનાર વ્યક્તિ દ્વારા મોકલાયેલ મૂળ સંદેશા પ્રમાણેનો છે, પરંતુ આવો સંદેશો મોકલનાર વ્યક્તિ સંબંધી અદાલત કશું માની લઇ શકશે નહિ."

સરળ રીતે કહીએ તો, આ કલમમાં માની લેવા બાબત એ છે કે 'X કોમ્પ્યુટર' થી ઇ-મેઇલ દ્વારા મોકલવામાં આવેલ મેસેજ 'Y કોમ્પ્યુટર' પર પ્રાપ્ત મેસેજની નકલ છે. આ જોગવાઈ હેઠળ કોર્ટ આવી ધારણા ન પણ બાંધે અથવા તેનું ખંડન પણ કરી શકે, કારણ કે આવી ધારણા રદબાતલ થઇ શકે તેવી શક્યતા છે. આ ઉપરાંત, આ કલમમાં સ્પષ્ટ છે કે મોકલનાર (સેન્ડર) ની ઓળખ બાબતની કોઇ ધારણા બાંધી શકાય નહિ.

સીડી/પ્રિન્ટઆઉટ લેવામાં આવેલ હોય તે સંબંધિત સમયગાળા દરમિયાન ઇ-મેઇલ સાબિત કરનાર વ્યક્તિના કાયદેસરના નિયંત્રણ હેઠળ હતું તે કલમ ૬૫-ખ મુજબનું પ્રમાણપત્ર મેળવવું જરૂરી છે. (બાબુરામ અગ્રવાલ અને અન્ય વિ. ક્રિષ્નકુમાર ભટનાગર અને અન્ય.૨૦૧૩ IIAD(દિલ્હી) 441). અબ્દુલ રહેમાન કુંજી વિ. પશ્ચિમ બંગાળ રાજ્ય [MANU/WB/0828/2014]માં ઇ-મેઇલની ગ્રાહ્યતા નક્કી કરતી વખતે નામદાર કલકત્તા હાઇકોર્ટ દ્વારા એવું ઠરાવવામાં આવ્યું છે કે, ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ખ અને કલમ ૮૮-ક ને સાથે વાંચતા,

વ્યક્તિના ઈ-મેઈલ એકાઉન્ટમાંથી ડાઉનલોડ કરેલ તથા પ્રિન્ટ કરેલ ઇ-મેઇલને અદાલત સમક્ષ સાબિત કરી શકાશે.

૬. દસ્તાવેજ વિશે નિષ્ણાતનો અભિપ્રાય:

ભારતીય પુરાવા અધિનિયમ, ૧૯૭૨ ની કલમ ૪૫-ક મુજબ " કોમ્પ્યુટરમાં અથવા કોઇ બીજા ઇલેક્ટ્રોનિક કે ડિજિટલ પ્રકારે સંગ્રહિત અથવા પ્રસારિત થયેલ કોઇ માહિતીને લગતી કોઇ બાબતમાં કાર્યવાહી દરમિયાન ન્યાયલયે અભિપ્રાય બાંધવાનો હોય ત્યારે ઇન્ફર્મેશન ટેક્નોલોજી અધિનિયમ,૨000 (સન ૨000 ના ૨૧ મા) ની કલમ ૭૯-ક માં ઉલ્લેખવામાં આવેલ પુરાવા પરિક્ષકનો અભિપ્રાય એ પ્રસ્તુત હકીકત છે". ભારત સરકારે ડાયરેક્ટરેટ ઑફ ફોરેન્સીક સાયન્સ, ગુજરાતને " ઇલેક્ટ્રોનિક પુરાવાના પરિક્ષક" તરીકે જાહેર કરેલ છે. આથી DFS ગાંધીનગરના અધિકારીઓને ઇલેક્ટ્રોનિક પુરાવાના નિષ્ણાત તરીકે વલણ સ્પષ્ટ કરવા બોલાવી શકાશે.

૭. તપાસ અધિકારી દ્વારા " પ્રિઝર્વેશન નોટીસ" ઇશ્યુ કરવી:

ઇન્ફર્મેશન ટેક્નોલોજી એક્ટ, ૨000 ની કલમ ૬૭-ગ માહિતીનો સંગ્રહ અને સાચવણીનું વર્ણન કરે છે.

૬૭-ગ: મધ્યસ્થી દ્વારા માહિતીનો સંગ્રહ અને સાચવણી

૧. કેન્દ્ર સરકારની સુચના મુજબ મધ્યસ્થી આવી માહિતીને ચોક્કસ સમયગાળો, ચોક્કસ રીત અને ચોક્કસ ફોર્મેટમાં સંગ્રહ અને સાચવણી કરશે.

૨. કોઇ મધ્યસ્થી ઇરાદાપૂર્વક કે જાણી જોઇને પેટાકલમ (૧) નો ભંગ કરે તે ત્રણ વર્ષ સુધી લંબાવી શકાય તેવી સજા અને દંડને પાત્ર થશે.

ઉદાહરણ તરીકે ઇ-મેઇલ સર્વિસ પ્રોવાઇડર ૧૮૦ દિવસ સુધી મેટા-ડેટા સાચવી રાખે છે. એવા કેસોમાં જ્યાં તપાસ અધિકારી ૧૮૦ દિવસમાં ડેટા મેળવી શકતા નથી, ત્યાં પ્રિઝર્વેશન નોટીસ ઇશ્યુ કરવાની જરૂર ઊભી થાય છે. એવી પણ શક્યતા રહે છે કે આરોપી અથવા તેમના મદદગાર સર્વર માંથી ડેટા ડિલીટ કરી દે, જેથી સર્વિસ પ્રોવાઈડર ને તપાસ કરનાર અમલદાર દ્વારા 'પ્રિઝર્વેશન નોટીસ' આપવાની રહે છે. સરકારી કચેરીઓ અને કાયદા દ્વારા સ્થાપિત અન્ય સંસ્થાઓના કેસોમાં જ્યાં નેટવર્કનું સુપરવિઝન કરનાર વ્યક્તિ શંકાસ્પદ ન હોય, સંસ્થાનો વડો શંકા હેઠળ ન હોય, ત્યાં પણ એવીડન્સ પ્રિઝર્વેશન નોટીસ ઇશ્યુ કરી શકાય છે. ઘણીવાર તપાસ અધિકારી માટે તાત્કાલિક પુરાવો કબ્જે લેવા અંગેનો નિર્ણય કરવો શકય હોતો નથી. તપાસ અધિકારી માટે જેની પાસે આવુ સાધન કે માહિતી છે તે તેને સલામત કસ્ટડીમાં રાખે અને તેને જણાવવામાં આવે તે સમયે અને સ્થળે તપાસ અધિકારી પાસે રજૂ કરે તે માટે તપાસ અધિકારી દ્વારા આપવામાં આવેલ પ્રિઝર્વેશન નોટીસ ઘણી મદદગાર બની રહે છે. વિદેશ માં

સ્થિત સર્વરથી માહિતી મેળવવામાં ઘણો સમય લાગે છે, જેથી, એવા કિસ્સાઓમાં 'પ્રિઝર્વેશન નોટીસ' ઇશ્યુ કરવી હિતાવહ છે. પ્રિઝર્વેશન નોટીસ નો નમૂનો આ સાથે પરિશિષ્ટ-૫ માં આપેલ છે.

૮. ઇલેક્ટ્રોનિક પુરાવા ની ઝડતી અને જપ્તી (Search and Seizure) માટે કાયદાકીય જોગવાઇઓ:

ભારતીય ફોજદારી કાર્યરીતિ સંહિતાની કલમ ૧૬૫ તપાસ અધિકારીને વોરંટ વગર ઝડતી અને જપ્તી માટેની સત્તા આપે છે. તેમ છતાં આઇ.ટી.(IT) એક્ટની કલમો લગાવવામાં આવી હોય તો પોલીસ ઇન્સપેક્ટર કે તેનાથી ઉપરના હોદ્દાના પોલીસ અધિકારી જાહેર સ્થળોએ વગર વોરંટે પ્રવેશીને ઝડતી અને જપ્તી કરી શકે છે. આઇ.ટી.(IT) એક્ટ, ૨૦૦૦ ની કલમ ૮૦(૧) નીચે મુજબ છે.

૮૦: પોલીસ અધિકારી અને અન્ય અધિકારીઓની પ્રવેશ, તપાસ વગેરેની સત્તા બાબત

૧. ભારતીય ફોજદારી કાર્યરીતિ સંહિતા, ૧૯૭૩માં કઇ પણ દર્શાવ્યુ હોય તેમ છતાં પોલીસ ઇન્સપેકટર થી નીચેના હોદ્દાનાં ન હોય તેવા કોઇપણ પોલીસ અધિકારી અથવા કેન્દ્ર સરકાર દ્વારા આ સંદર્ભે નિયુક્ત કરવામા આવેલ કોઇ પણ કેન્દ્ર અથવા રાજ્ય સરકારનાં કોઇપણ અધિકારી કોઇપણ જાહેર સ્થળે જો કોઇ વ્યક્તિ આ કાયદા વિરૂદ્ધનું કોઇ કૃત્ય કરતો જોવા મળે અથવા કાયદાનો ભંગ કરતો

હોવાની વાજબી શંકા જાગે તો તેવા અધિકારી, કોઇપણ જાહેર સ્થળે પ્રવેશ કરી શકશે તથા તેવી વ્યક્તિની વગર વોરંટે ધરપકડ કરી શકશે.

<u>૯. પુરાવા તરીકે CDR (Call Detail Record):</u>

ઘણાં કેસોમાં કોલ ડીટેઈલ રેકર્ડસ અગત્યનાં પુરાવા હોય છે. State (N.C.T of Delhi) vs. Navjot Sandhu @ Afsan Guru ના કેસમાં નામદાર સુપ્રિમ કોર્ટ દ્વારા ગ્રાહ્ય અને વિશ્વસનીય પુરાવા તરીકે CDR પર આધાર રાખવામાં આવ્યો હતો. જો કે ભારતીય પુરાવા અધિનિયમની કલમ ૬૫-ખ મુજબ CDR સાથે તેનું પ્રમાણપત્ર હોવુ જોઈએ. CDRના પ્રિન્ટઆઉટ/સી.ડી. રજૂ કરવાના કિસ્સામાં મોબાઈલ સેવા ઉપલબ્ધકર્તા/પ્રદાતાના નોડલ અધિકારી દ્વારા પ્રમાણપત્ર આપવું જોઈએ. જો મોબાઈલ સેવા ઉપલબ્ધકર્તા/પ્રદાતા દ્વારા CDR ઈ-મેઈલ થી તપાસ કરનાર અમલદાર ને મોકલવામાં આવેલો હોય, તો તે ઈ-મેઇલ ની પ્રિન્ટઆઉટ/સી.ડી. કાઢનાર પોલીસ કર્મચારી/અધિકારી દ્વારા પણ પ્રમાણપત્ર આપવું જોઈએ.

<u>૧૦. પુરાવા તરીકે આઈ.એમ.ઇ.આઇ(IMEI):</u>

Gajraj vs. State (N.C.T of Delhi) [(2011)10 S.S.C 675]ના કેસમાં નામદાર સુપ્રીમ કોર્ટે નોંધ્યુ છે કે, મોબાઇલ હેન્ડસેટનો આઈ.એમ.ઇ.આઇ (IMEI) નંબર અનન્ય (unique) હોય છે અને

કોઈપણ બે મોબાઈલ હેન્ડસેટનાં આઈ.એમ.ઇ.આઇ (IMEI) નંબર સરખા હોતા નથી. દરેક વખતે મોબાઈલ હેન્ડસેટથી કોલ કરતી વખતે કોલ કરનાર તથા કોલ રીસીવ કરનારના નંબરની સાથે મોબાઇલના આઈ.એમ.ઇ.આઇ (IMEI) નંબર પણ મોબાઈલ સેવા ઉપલબ્ધકર્તા/પ્રદાતા દ્વારા રૅકર્ડ કરવામાં આવે છે. આથી, પુરાવાનો આ ભાગ કે જે આરોપી અને મૃતક વચ્ચે સંબંધ પ્રસ્થાપિત કરે છે તેને નામદાર સુપ્રિમ કોર્ટ દ્વારા નિર્ણાયક પ્રકારના પુરાવા (Conclusive nature) તરીકે માન્ય રાખેલ છે. જેથી, તપાસ કરનાર અમલદાર દ્વારા મોબાઈલ ફોન સંબંધિત પુરાવા, ઉદાહરણ તરીકે મોબાઈલ ફોનના માલિકીના પુરાવા, પ્રસ્થાપિત કરતા સમયે IMEI ની વિગતો જરૂર ધ્યાને લેવી જોઈએ.

નોંધ: કોમ્પ્યુટર્સ અને ઇન્ફોર્મેશન ટેક્નોલોજી ના ક્ષેત્રમાં ત્વરિત તકનીકી વિકાસને ધ્યાનમાં રાખીને ઇલેક્ટ્રોનિક પુરાવા સંબંધિત કાયદા અને તેના અર્થઘટન સતત પરિવર્તન હેઠળ છે. તેથી પોલીસ અધિકારીઓ અને કર્મચારીઓએ પોતાને આ ક્ષેત્ર માં થતા બદલાવો થી અદ્યતન રાખવા જોઇએ.

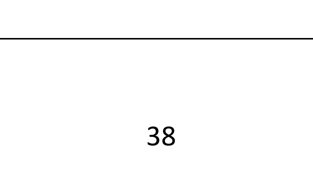
પ્રકરણ-૨

ડિજિટલ પુરાવા: ઝડતી અને જપ્તી (Search and Seizure) ના મૂળસિદ્ધાંતો

પ્રકરણનો ઉદ્દેશ: ડિજિટલ ડિવાઈસ, જેમ કે કોમ્પ્યુટર, સીસીટીવી-ડીવીઆર (CCTV-DVR), મોબાઈલ ફોન, પ્રિન્ટર, પેનડ્રાઈવ વગેરે, માંથી પુરાવા એકત્ર કરવા માટે સર્ચ અને સીઝર (ઝડતી અને જપ્તી) કરવાની માર્ગદર્શિકા.

૧. ડિજિટલ ડિવાઈસ: ડિજિટલ પુરાવાના સ્ત્રોત:

આજે દરેક ડિજિટલ ડિવાઇસીસ માં પુષ્કળ પ્રમાણમાં માહિતી સંગ્રહિત હોય છે. નીચેના ટેબલમાં કયા પ્રકારના ડિજિટલ ડિવાઇસીસ માં ક્યાં અને કેવી માહિતી સંગ્રહિત હોય છે તેનો ચિતાર આપવામાં આવેલ છે. જુદા જુદા ડિજિટલ ડિવાઈસમાં જુદી જુદી ટેક્નોલોજીનો ઉપયોગ થાય છે અને પુરાવા એકત્ર કરવાની રીત પણ ડિવાઈસમાં વપરાતી ટેક્નોલોજી ઉપર નિર્ભર રહે છે. જો કે, ડિજિટલ ડિવાઈસ માં તમામ ડેટા બાઇનરી (0 અથવા ૧) ના સ્વરૂપ માં સ્ટોર થાય છે, જેને ઉપયોગકર્તા સમઝી શકે તે રૂપ માં દર્શાવામાં આવે છે.

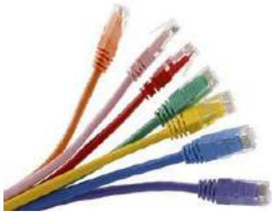
નં	ડિજિટલ ઉપકરણો	આધારભૂત પુરાવા
૧	ડેસ્કટોપ કૉમ્પ્યુટર કેબિનેટ	માહિતીને સંગ્રહ કરવા માટેના સ્ટોરેજ ડિવાઈસ, જેવા કે હાર્ડ ડિસ્ક, સીડી, ડીવીડી વગેરે કે જેમાંથી ગુનાહિત પ્રવૃત્તિઓ સાબિત થઇ શકે તેવી શક્યતા ધરાવતા પુરાવા મળી શકે.
૨	ડિસ્પ્લે મોનીટર અને મોબાઇલ સ્ક્રીન(જો ચાલુ હાલતમાં હોય તો) 	ગ્રાફિકલ ફાઈલ્સ, સ્ટીકી નોટ, કોમ્પ્યુટર સિસ્ટમના સમય સંબંધિત માહિતી વગેરે.

3	સ્માર્ટ કાર્ડ, ડોંગલ અને બાયોમેટ્રિક સ્કેનર્સ વગેરે	આ પ્રકારના ડિવાઈસમાં વ્યક્તિગત માહિતી સંગ્રહિત હોય છે, તથા લોગ, એક્સેસ લેવલ અને પરવાનગી સંબંધિત માહિતી મળી શકે છે.
૪	આન્સરિંગ મશીન	આ પ્રકારના ઉપકરણો વોઈસ સ્વરૂપે મોકલવામાં આવેલ સંદેશાઓનો સંગ્રહ કરે છે. સંદેશો ક્યા સમયે અને ક્યા દિવસે મોકલવવામાં આવેલો છે તેની માહિતી મળી શકે છે. તેમાં છેલ્લે કોલ કરેલા નંબર, મેમો, ફોન નંબર, અને નામ, કોલ કરેલા સંદેશાઓ પણ સંભવિત રીતે મળી શકે છે.

૫	ડિજિટલ કેમેરા 	વિવિધ પ્રકારના ડીજિટલ કેમેરામાં રહેલા સ્ટોરેજ મીડિયા, મેમરી કાર્ડમાં રહેલી વિવિધ માહિતી જેવી કે ફોટો, વિડિઓ, સાઉન્ડ, રીમુવેબલ મીડિયા તથા તેને સંબંધિત સમય અને દિવસ, GPS તથા metadata ની માહિતી મળી શકે છે.
૬	હેન્ડહેલ્ડ ડિવાઈસ (વ્યક્તિગત ડિજિટલ સહાયક, સ્માર્ટ ફોન, મોબાઈલ ફોન, ટેબલેટ) 	આવા ડિવાઈસમાંથી address book, નિમણૂંક કરેલી તારીખો, દસ્તાવેજો, ઈ-મેઈલ, ફોનબુક, લખાણ રૂપી તથા વોઈસરૂપી સંદેશાઓ, ઈ-મેઈલના પાસવર્ડ વગેરે જેવી માહિતી મળી શકે છે.

૭	હાર્ડ ડ્રાઈવ 	હાર્ડડ્રાઈવમાં અલગ-અલગ પ્રકારની ઘણી બધી માહિતી સંગ્રહિત હોય છે, તેથી તેમાંથી ઘણા ખરા આધારભૂત પુરાવાઓ મેળવી શકાય છે.
૮	લોકલ એરિયા નેટવર્ક (LAN), નેટવર્ક ઈન્ટરફેસ કાર્ડ(NIC) 	આ ડિવાઈસમાંથી MAC એડ્રેસ ને લગતી માહિતી મળી શકે છે.

૯	મોડેમ્સ, રાઉટર્સ, હબ, સ્વીચ	આ ડિવાઈસમાંથી કન્ફ્યુગરેશનની ફાઈલમાં રહેલી IP Address ને લગતી માહિતી મેળવી શકાય છે.
૧૦	સર્વર	આ પ્રકારના ડિવાઈસમાંથી, છેલ્લા સમયનું લોગ-ઇન, ઈ-મેઈલ, અપલોડ, ડાઉનલોડ થયા વિશેની માહિતી, ઉપયોગ કરેલા વેબપેજો વગેરે પ્રકારની માહિતી મળી શકે છે.

૧૧	નેટવર્ક કેબલ અને કનેક્ટર્સ 	નેટવર્ક કેબલનો ઉપયોગ તેની સાથે જોડાયેલા ડિવાઈસને શોધવા તથા જે તે ડિવાઈસનો પ્રકાર જાણવામાં ઉપયોગી નીવડે છે.
૧૨	પેજર્સ	એડ્રેસની માહિતી, લખાણરૂપી સંદેશાઓ તથા ફોન નંબર મળી શકે છે.
૧૩	પ્રિન્ટર્સ	વિવિધ પ્રકારના પ્રિન્ટરમાંથી છેલ્લે કાઢેલી પ્રીન્ટોની સંખ્યા, ઘણા-ખરા સમયે વપરાશના લોગ, સમય અને તારીખ,

		જો જે તે પ્રિન્ટર નેટવર્કમાં જોડાયેલું હોય તો તે નેટવર્કની માહિતી મળી શકે છે.
૧૪	દૂર કરી શકાય તેવા સ્ટોરેજ મીડિયા અને ઉપકરણો	આ પ્રકારના ડિવાઈસ મુખ્ય સાધનથી દૂર કરી શકાતા હોય છે. તે માહિતીનો સંગ્રહ કરવા માટે વપરાય છે અને તેમાંથી મહત્વના પુરાવાઓ મેળવી શકાય છે.
૧૫	સ્કેનર્સ	આ ડિવાઈસ કાગળો, ફાઈલને સ્કેન કરવા વપરાય છે. સ્કેનરમાં ફાઈલો કે કાગળો સ્કેન કર્યા હોય તેનો ડેટા સંગ્રહિત થતો હોય છે જે

		આધારે છેલ્લે કરેલી ફાઈલો/કાગળો સ્કેન કર્યા હોય તે તેમજ ફિંગરપ્રિન્ટ હોય તે વિગતો મળી રહે છે.
૧૬	ટેલિફોન	ઘણા બધા ટેલીફોન નામ, સંદેશા, મેમો, પાસવર્ડ,ફોન નંબર અને આવેલા કોલ વિશેની માહિતીને સંગ્રહિત કરે છે કેટલાક સેલ્યુલર ટેલીફોન વોઈસ રૅકર્ડર તરીકે પણ કામ કરતા હોય છે તો ક્યારેક કયા કયા નંબર ઉપર ફોન કરવામાં આવ્યો છે તે માહિતી પણ મેળવી શકાય છે.

૧૭	કોપિયર્સ (ઝેરોક્ષ)	કોપિયર્સમાં કેટલાક દસ્તાવેજો, બંને ભૌતિક અને ઇલેક્ટ્રોનિક,વપરાશકર્તા વપરાશ લૉગ્સ, સમય અને તારીખ, સ્ટેમ્પ્સ મળી શકે છે.
૧૮	સીડી અને ડીવીડી ડ્રાઈવો	આ ડિવાઇસમાં વિવિધ પ્રકારની માહિતી સ્ટોર કરી શકાતી હોય છે જેથી તેમાંથી પુરાવા મળી શકે છે.
૧૯	ક્રેડિટ કાર્ડ સ્કીમર્સ	આ પ્રકારના ડિવાઈસમાંથી કાર્ડધારકની માહિતી જેવી કે, કાર્ડ સમાપ્તિની તારીખ, વપરાશકર્તાનું નામ સરનામું, ક્રેડિટ કાર્ડ

		નંબર તથા અન્ય માહિતી મળી શકે છે.
૨૦	ડિજિટલ ઘડિયાળ (smart watch)	ડિજિટલ ઘડિયાળમાં સરનામાં પુસ્તિકા, નોંધો, નિમણૂંક તારીખો,ફોન નંબર, ઇ-મેઇલ વગેરે માહિતી સ્ટોર થયેલી હોય છે જે પુરાવા તરીકે મળી શકે છે.
૨૧	ફેક્સ મશીન	આ ઉપકરણોમાં ઇનબિલ્ટ મેમરી હોય છે. જે દસ્તાવેજ, કાગળો, ફાઈલોની ઝેરોક્ષ કરવાની હોય તે પ્રથમ સ્કેન કરવામાં આવે છે. ત્યારબાદ તેની માત્ર નકલ ઝેરોક્ષ કરવામાં આવે છે. સ્કેન થયેલ

		માહિતી, મેમરીમાંથી મેળવી શકાય છે.
૨૨	ગ્લોબલ પોઝિશનિંગ સિસ્ટમ(GPS) 	આ ઉપકરણમાં મુસાફરીના સ્થળના લોગ્સ, ઘરનું સ્થાન, અગાઉ જે સ્થળોએ મુસાફરી કરી હોય તે સ્થળો, રસ્તો તથા પોઇન્ટ કોઓર્ડિનેટ્સ, નામ વિગેરે સ્ટોર થતા હોય છે જે પુરાવા તરીકે મળી શકે છે.
૨૩	કીબોર્ડ અને માઉસ 	આવા ઉપકરણોમાં કોઈ માહિતી સ્ટોર થતી હોતી નથી પરંતુ તે ઉપર વ્યક્તિની ફિંગરપ્રિન્ટ પડી હોય તે મળી શકે છે.

૨૪	ક્લાઉડ ડાટા સર્વર	આ સુવિધા સ્માર્ટ ફોન અને ટેબલેટ માટે ઉપલબ્ધ હોય છે. ક્લાઉડ સર્વરમાં ફોનની તમામ માહિતી અપલોડ હોઈ શકે છે અને ગુનાથી સંબંધિત અગત્યના પુરાવા સ્ટોર હોઈ શકે છે.

આ યાદી સંપૂર્ણ નથી અને ડિજિટલ પુરાવા ઘણા બીજા ઉપકરણોના ભાગરૂપ બની રહ્યા છે. જેમ કે સ્માર્ટ ટેલિવિઝન, બુકરીડર, સ્માર્ટકાર્ડ વગેરે.

૨. ડિજિટલ પુરાવાઓની મુખ્ય લાક્ષણિકતાઓ:

- તે ઈલેક્ટ્રોનિક ઉપકરણો કે સર્વરમાં અપ્રગટ અને છુપા હોય છે.
- તે રાષ્ટ્રીય સીમાઓને સહેલાઈથી અને ઝડપથી ઓળંગી શકે છે.
- તે ખૂબજ સંવેદનશીલ, નાજૂક અને સહેલાઈથી પરિવર્તિત થઈ શકે, તેને નુકશાન કે તેનો નાશ પણ થઈ શકે અને તે સમયબાધ્ય પણ છે.

આવા જ કારણોસર આ પ્રકારના ડિજિટલ પુરાવાઓના દસ્તાવેજીકરણમાં, પુરાવાઓ ભેગા કરવામાં, સાચવવામાં અને તપાસ/વિશ્લેષણ કરવામાં ખાસ તકેદારી રાખવી જોઈએ.
ડિજિટલ પુરાવાઓ ખૂબ નાજૂક અને સંવેદનશીલ હોવાથી જરૂરી તકેદારી વગર ઉપકરણ/સર્વરમાંથી મેળવવામાં આવે તો પુરાવાઓની અધિકૃતતા અને પ્રામાણિકતાને હાનિ પહોંચે છે.
પરંપરાગત રીતે પ્રાકૃતિક કે દસ્તાવેજી પુરાવાઓ મેળવવામાં (પુરાવાઓની ઓળખ, ભૂસાઈ ગયેલા પુરાવાઓની પુન:પ્રાપ્તિ, આવા પુરાવાઓની ચકાસણી વગેરેમાં) જે મુશ્કેલીઓનો સામનો કરવો પડે છે તેના કરતાં અહીં ડિજિટલ પુરાવાઓની બાબતમાં અખંડિતતા જાળવવામાં પડતી મુશ્કેલીઓ કંઈક જુદા જ પ્રકારની છે. આ માર્ગદર્શિકા ડિજિટલ પુરાવાઓ જાળવવા માટે પાયાની કાર્યપદ્ધતિ સૂચવવા પ્રયત્ન કરે છે. આ પ્રકરણમાં દર્શાવેલ કાર્યપદ્ધત્તિ ઈલેક્ટ્રોનિક મીડિયા, સર્વર અને નેટવર્ક કે જ્યાં ડિજિટલ માહિતી/પુરાવા સંગ્રહિત હોઈ શકે ત્યાં સુધી પહોંચવા, મેળવવા, વિશ્લેષણ કરવા અને કબજે કરવાની પ્રક્રિયામાં મદદરૂપ થશે.

<u>3. પ્રવર્તમાન કાર્યપદ્ધતિ:</u>

હાલમાં તપાસ દરમ્યાન કોમ્પ્યુટર કે અન્ય વિજાણુ ઉપકરણ સુધી કેવી રીતે પહોંચવુ, કેવી રીતે ઉપયોગમાં લેવા અને તેમાંથી ડિજિટલ ડેટા કેવી રીતે પુન:પ્રાપ્ત કરવા વગેરે બાબતો અંગે કોઈ એકરૂપ કાર્યરીતિ અમલમાં નથી.

હાલમાં સામન્ય રીતે અપનાવામાં આવતી કાર્યરીતિ નીચે મુજબ છે:

- પુરાવા/માહિતીની નકલ હાર્ડકોપી (પ્રિંટ-આઉટ) માં લેવી અને કબજે કરવી.
- સીડી રાઈટર, પેનડ્રાઈવ, પોર્ટેબલ હાર્ડડ્રાઈવ દ્વારા ઓરિજિનલ હાર્ડડ્રાઈવમાંથી પુરાવાઓની નકલ મેળવવી.
- હાર્ડડિસ્ક, કોમ્પ્યુટર, મોબાઈલ ફોન વગેરે કબજે કરવા અને ઓફિસે લઈ જવા.
- કેટલીકવાર ફોરેન્સિક સોફ્ટવેર વગર પણ વિન્ડોઝ યુટિલિટી દ્વારા પુરાવાઓ કોપી કરી લેવામાં આવે છે.
- પોલીસ કર્મચારીઓ/અધિકારીઓ પુરાવારૂપે કબજે કરેલ તમામ સાધનો જેવા કે મોનિટર માઉસ વગેરે પણ FSL કચેરી તરફ મોકલી આપે છે.

<u>૩.૧) વર્તમાન કાર્યપદ્ધતિની ખામીઓ:</u>

આવી પદ્ધત્તિઓ ન્યાયની અદાલતમાં વિશ્વાસપાત્ર નથી. જો યોગ્ય કાર્યપદ્ધતિનું અનુસરણ ન થાય તો માહિતીની અખંડિતતા અને વિશ્વાસપાત્રતા સાથે બાંધછોડ કરવી પડે. એવી પદ્ધત્તિ અપનાવાથી, અમુક આધારો કે જેમાં જપ્ત કરેલ માહિતીની અખંડિતતાને કાયદાની અદાલતમાં પડકાર કરી શકાય છે, નીચે મુજબ છે:

- જ્યારે કોઈ સિસ્ટમને કોઈ ચોક્કસ તારીખે જપ્ત કરવામાં આવે,તેને ત્યારપછીના કોઈ સમયે તેની

માહિતી જોવા શરૂ/બૂટ(Boot) કરવામાં આવે ત્યારે છેલ્લે ખુલેલી ફાઈલોની તારીખ અને સમય આપોઆપ સુધરી/બદલી જાય છે. પ્રતિવાદી પક્ષ ટ્રાયલ વખતે જપ્ત થયેલ/પંચનામા મુજબના પુરાવા સાથે ચેડા થયેલ છે તેવો પડકાર કરી શકે છે.

- જો જપ્ત કરવામાં આવેલી સિસ્ટમ સ્વયં રીતે શરૂ નથી તથા તેની હાર્ડડિસ્ક અન્ય સિસ્ટમ સાથે જોડાયેલી છે, તો પણ ઓપરેટિંગ સિસ્ટમમાં એવી સ્વયંસંચાલિત કાર્યક્ષમતા હોય છે કે, જોડાયેલા બધાં માધ્યમોમાં તે લખાણ કરી શકે છે. તપાસકર્તાની સિસ્ટમ સાથે જોડાયેલી બધી જ નવી ડિસ્કમાં System Restore ટેગ સાથેના ફોલ્ડર બને છે. વધુમાં, તપાસકર્તાની સિસ્ટમમાં રહેલા એન્ટિવાયરસ સોફ્ટવેર જપ્ત થયેલ હાર્ડડ્રાઈવની ફાઈલને સ્કેન કરે છે, જે દરમિયાન તારીખ અને સમય બદલાશે. એન્ટિવાયરસ પ્રોગામ જપ્ત કરેલ ડિસ્ક પર રહેલ મહત્વના પુરાવાઓને કાઢી નાખી શકે છે અથવા અલગ-થલગ (quarantine) કરી શકે છે.

- કોઈ સિસ્ટમ કે હાર્ડડિસ્કમાં Write Protect ડિવાઈસના ઉપયોગ વગર કોઈ અન્ય રીતે પ્રવેશ કરવાથી ડિસ્કની હેશવેલ્યૂ (Hash Value) અથવા

ડિજિટલ ફિંગરપ્રિન્ટ (Digital Fingerprint) માં ફેરફાર થઈ શકે છે. આથી ડિસ્કમાં રહેલા પુરાવાઓ અગ્રાહ્ય પુરાવાઓ બની શકે છે.

અનુગામી પ્રકરણોમાં ડિજિટલ પુરાવાઓને મેળવવામાં તેની અખંડિતતા અને વિશ્વાસપાત્રતા સાથે કોઈ બાંધછોડ ન કરવી પડે તે માટેની કાર્યપદ્ધતિનો ઉલ્લેખ છે.

૪. ડિજિટલ પુરાવાઓની સંવેદનશીલતા:

ડિજિટલ પુરાવા ખૂબ જ સંવેદનશીલ હોય છે અને તેને હેન્ડલ કરવામાં થયેલ ભૂલથી કોર્ટમાં પુરાવા તરીકે તેમનું મહત્વ ઘટી શકે છે. આ માટે ડિજિટલ પુરાવા હેન્ડલ કરતા સમયે તપાસ અધિકારીએ જરૂરી તકેદારી રાખવી જોઇએ.

૪.૧) ચેઇન ઑફ કસ્ટડી

ચેઇન ઑફ કસ્ટડી એ પુરાવા એકત્રિત કરવાની એક એવી પદ્ધતિ છે જેમાં પુરાવાને કોર્ટમાં રજૂ કરવા માટે તેને કેવી રીતે એકત્રિત કરવા, સંગ્રહિત કરવા અને તેનું વિશ્લેષણ કેવી રીતે કરવું જોઇએ તે દર્શાવવામાં આવે છે. એક સ્પષ્ટ ચેઇન ઑફ કસ્ટડી એવુ દર્શાવે છે કે ડિજિટલ પુરાવાઓ વિશ્વાસપાત્ર છે. ઇલેક્ટ્રોનિક પુરાવા માટે ચેઇન ઑફ કસ્ટડી ને જાળવી રાખવું મહત્વપૂર્ણ છે કારણકે ડિજિટલ પુરાવાઓ ખૂબ જ સંવેદનશીલ હોય છે. આ ઉપરાંત તપાસ અધિકારીએ કેસ ડાયરીમાં ચેઇન

ઑફ કસ્ટડીનો સ્પષ્ટપણે ઉલ્લેખ કરેલો હોવો જોઇએ. ડિજિટલ પુરાવાની ચેઇન ઑફ કસ્ટડી બાબતે તપાસ અધિકારીએ પુરાવા મેળવવા સબંધે કરેલ તમામ કાર્યવાહી ફોરેન્સિક માન્ય પદ્ધતિ અનુસારની હોવી જોઇએ અને તમામ કાર્યવાહીની નોંધ કેસ-ડાયરીમાં થવી જોઇએ. **ચેઇન ઑફ કસ્ટડી બાબતે ધ્યાનમાં રાખવા જેવી બાબતો:**

૧. જપ્ત(સીઝ) કરેલ ડિજિટલ પુરાવાઓમાં કોઇપણ માહિતી ઉમેરાયેલ, બદલાયેલ કે ડીલીટ થયેલ ન હોવી જોઇએ.

૨. ડિજિટલ પુરાવાની જો નકલ(duplication) બનાવવામાં આવે તો એ નકલ સંપૂર્ણ રીતે થયેલ હોવી જોઇએ.

૩. વિશ્વાસપાત્ર અને સર્વમાન્ય નકલ(duplication) મેળવવાની યોગ્ય રીતનો ઉપયોગ થયેલો હોવો જોઇએ.

૪. બધા જ મીડીયા સલામત અને સુરક્ષિત હતા, અને તેમા છેડ-છાડ નો કોઇ અવકાશ ન હતો તે બાબતનુ ચોકસાઇપુર્વક પાલન થવું જોઇએ.

૪.૨) સ્થાયી ડેટા (Persistent Data) અને અસ્થાયી ડેટા (Volatile Data)

ડિજિટલ ઉપકરણોમાંથી બે પ્રકારના પુરાવાઓ મેળવી શકાય છે. સ્થાયી પુરાવા (Persistent Data) અને અસ્થાયી પુરાવા (Volatile Data)

- **સ્થાયી પુરાવા (Persistent Data)** આ એવા પુરાવા છે જે કોમ્પ્યુટર/ડિવાઈસ બંધ થાય તો પણ તેની હાર્ડડીસ્કમાં સ્ટોર થાય છે. ડોકયુમેન્ટ, ઇમેજીસ, ચેટલોગ, બ્રાઉઝર હિસ્ટ્રી, રજીસ્ટ્રી, ઓડીયો, વિડિયો એપ્લીકેશન, ઇ-મેઇલ, SMS/MMS, ફોન બુક, કોલ લોગ વિગેરે.
- **અસ્થાયી પુરાવાઓ (Volatile Data)** આ એવા ડેટા છે જે કોમ્પ્યુટર/ડિવાઈસ બંધ થાય અથવા તેનો પાવર કટ થાય ત્યારે મેમરીમાંથી ડિલિટ થઇ જાય છે. દા.ત. મેમરી, નેટવર્ક સ્ટેટસ, પ્રોસેસ રનિંગ, સમયની જાણકારી. એ વસ્તુનું જાણવું ખુબ જરૂરી છે કે અમુક કેસમાં જયાં અસ્થાયી પુરાવાઓ ખૂબ જ મહત્વના છે. પરંતુ કોમ્પ્યુટરના/ડિવાઈસના બંધ થવાથી આ અસ્થાયી પુરાવાનો નાશ અથવા તેને નુકશાન થઇ શકે છે.

પ. ડિજિટલ પુરાવા માટે સર્ચ અને વિશ્લેષણ:

કોઇપણ કોમ્પ્યુટરની તપાસ સરળ હોય છે પણ ઘણા કારણોથી તે એટલી જ જટીલ પણ છે કારણકે કોમ્પ્યુટરમાં હજારો ફોલ્ડર્સ હોય છે અને તપાસ અધિકારીને એ જાણકારી નથી હોતી કે કયા

ફોલ્ડર્સમાં, કઇ જગ્યાએ, કઇ માહિતી પડેલ હોય છે. છતાં પણ તપાસ અધિકારી ચાહે તો સંપુર્ણ ડેટાને જપ્ત (સીઝ) કરી શકે છે અને ત્યારબાદ બધા જ ડીવાઇસ અને કોમ્પ્યુટરને FSLમાં મોકલાવી શકે છે. પરંતુ જયાં સુધી FSL માંથી રીપોર્ટ નહી આવે ત્યાં સુધી તપાસ અધિકારી પુરાવાઓનું વિશ્લેષણ નહી કરી શકે. સંબંધિત અને ચોકકસ ડેટાની ઓળખ ખૂબ જ સમય માંગી લે તેવું કાર્ય છે અને સંભવત: મોટાભાગના કેસોમાં સ્થળ પર આ ઓળખ પૂર્ણ કરી શકાતી નથી.

આ માટે જ સંબંધિત અધિકારીએ સર્વ પ્રથમ જુદા-જુદા ડીવાઇસને સ્કેન કરવા જોઇએ અને ત્યારબાદ બધા જ ડીવાઇસને હસ્તગત કરવાને બદલે ફકત તે જ ઉપકરણો (ડીવાઇસ)ને સીઝ કરવા જોઇએ કે જે સંબંધિત પુરાવાઓ ધરાવતા હોય અને આ કાર્ય વચ્ચે એક ચોકકસ બેલેન્સ હોવુ જોઇએ. કારણ કે એક બાજુ ડીવાઇસમાંથી વિશાળ માહિતી જપ્ત (સીઝ) કરવાની છે જે કાર્યને વધારે જટીલ બનાવશે અને એ જ સમયે જયાં પણ સંબંધિત પુરાવાઓને શોધવાની સંભાવના હોય ત્યાં ડેટાને સીઝ કરવાની ખાતરી પણ કરવાની છે.

૬. ડિજિટલ ડિવાઇસની ઓળખ અને પ્રારંભિક પ્રક્રિયા:

૬.૧) સામાન્ય સિદ્ધાંતો:

જ્યારે ડિજિટલ પુરાવાઓ સાથે વ્યવહાર કરીએ ત્યારે નિમ્નલિખિત સામાન્ય ફોરેન્સીક અને કાર્યપ્રણાલીના સિદ્ધાંતો અનુસરવા જોઇએ:

- ડિજિટલ પુરાવાઓ એકત્રિત અને સુરક્ષિત કરવાની પ્રક્રિયા એવી રીતે કરવી કે જેથી તે પુરાવાની અખંડિતતાને (integrity of the evidence) અસર કરે નહિ.
- ડિજિટલ પુરાવાઓનું પરિક્ષણ કરનાર વ્યક્તિઓ આ હેતુ માટે તાલીમબદ્ધ હોવા જોઇએ.
- ડિજિટલ પુરાવાઓની જપ્તી (seizure), પરિક્ષણ, સંગ્રહ અથવા ટ્રાન્સફર વગેરેને લગતી પ્રવૃતિઓનું દસ્તાવેજીકરણ (documentetion) થવું જોઇએ, તથા તેનો કેસ-ડાયરીમાં ઉલ્લેખ થવો જોઇએ.

ડિજિટલ પુરાવાઓના એનાલીસીસ(પૃથ્થકરણ)નું પ્રથમ પગલું ડિજિટલ પુરાવાઓની આકરણી કરવી, મેળવવા, તેને ઇમેજ્ડ (imaged) કરવા વગેરે છે. ડિજિટલ પુરાવાઓની સમર્થતા(potential) નક્કી કરતી વખતે ઇન્ચાર્જ(તપાસ) અધિકારી નીચે આપેલ માર્ગદર્શિકામાંથી એવી કડી મેળવી શકે કે જે ડિજિટલ પુરાવાઓ મેળવવા અને ઇમેજ્ડ(imaged) કરવા જરૂરી છે.

૬.૨) સ્થળ (Premises) અને ઉપલબ્ધ ડિવાઇસની પ્રાથમિક સમીક્ષા:

ગુજરાત પોલીસ દ્વારા તપાસણી થનાર મોટા ભાગના કેસોમાં, માત્ર થોડાં ડિવાઇસીસ જપ્ત (seize) કરવાના રહે છે. જેમ કે, આરોપી કે ભોગ બનનારનાં મોબાઇલ ફોન. આ કેસોમાં ઘટનાસ્થળનો વિગતવાર સર્વે જરૂરી નથી. પરંતુ, જ્યારે પુરાવા ક્યા ડિવાઈસમા મૌજૂદ છે અથવા ડિવાઈસ મા કઈ જગ્યાએ ઉપલબ્ધ છે, ત્યારે સ્થળ અને ઉપલબ્ધ ડિવાઇસની પ્રાથમિક સમીક્ષાની જરૂરત હોય છે. નિમ્નલિખિત સામાન્ય સિદ્ધાંતો પુરાવાને સુરક્ષિત કરવામાં મદદ કરે છે, જેમ કે તાત્કાલિક ઇન્ટરનેટ કનેક્શનની સાથે wi-fi કનેક્શન ડિસકનેક્ટ કરવું.

ઘટનાસ્થળ(Premises) નીચે મુજબ હોઇ શકે:

૧. ઘરમાં રહેલા એક કે તેથી વધુ કોમ્પ્યુટર, હેન્ડ હેલ્ડ ડિવાઇસીસ (hand held devices);
૨. ઓફિસમાં રહેલા કેટલાક કોમ્પ્યુટર;
૩. બહોળા અને જટિલ નેટવર્ક સિસ્ટમ (complicated network of system)ધરાવતી કંપનીઓ કે ઓર્ગેનાઇઝેશનો.

ઘટનાસ્થળે, તપાસ અધિકારીએ કાળજીપૂર્વક ઘટનાસ્થળનો સર્વે કરવો, નિરીક્ષણ કરવું અને પરિસ્થિતિની આકરણી કરવી

અને આગળ પગલાં લેવા નિર્ણય કરવો જોઇએ. ડિજિટલ પુરાવાઓ વધારે નાજુક (fragile) છે અને તે સંખ્યાબદ્ધ ડિવાઇસીસ, લોકેશન અને વિવિધ પ્રકારના ફોર્મેટમાં ઉપલબ્ધ હોઈ શકે છે. આથી સ્થળથી ચાવીરૂપ ડિજિટલ ડિવાઇસને ઓળખવા માટે ઘટનાસ્થળની પ્રાથમિક સમીક્ષા ખૂબ જ જરૂરી છે. ઉદાહરણ તરીકે, કોઇપણ સંસ્થા કે જેની બહુવિધ શાખાઓ છે, એ જરૂરી નથી કે તે તમામ શાખાઓના ડિજિટલ પુરાવાઓ લેવા જ્યારે તે તમામ શાખાઓનો ડેટા તે સંસ્થાના મુખ્ય મથક ખાતેના કેન્દ્રીય ડેટાબેઝમાં/સર્વરમાં રહેલો હોય. આમ મુખ્ય મથક ખાતેનુ સર્વર કે જેમાં આ ડેટા સંગ્રહ કરવામાં આવ્યો છે તે ચાવીરૂપ ડિજિટલ ડિવાઇસ બની રહેશે.

<u>૬.૩) પ્રારંભિક પ્રક્રિયા:</u>

ડિજિટલ પુરાવાઓ મળવાની શક્યતા ધરાવતા ડિવાઇસની ઓળખ કર્યા બાદ તપાસણી અધિકારી કેસની જરૂરિયાત મુજબ નીચે દર્શાવેલ પગલાઓ લઇ શકે.

- તપાસ અધિકારીએ સ્થળ (premises) ને સુરક્ષિત કરી કોઇપણ વ્યક્તિને તેમની પરવાનગી વિના કોઇ કોમ્પ્યુટર અથવા ડિવાઇસનો ઉપયોગ કરવા મંજૂરી આપવી નહી. ઇન્ચાર્જ ઓફિસરે ઘટનાસ્થળ (premises) ખાતે ફિઝિકલી હાજર દરેક વ્યક્તિની નોંધ લેવી જોઇએ

અને ઘટનાસ્થળ (premises) સુરક્ષિત કરવામાં તેમની ભૂમિકા નોંધવી જોઇએ. મોટા ઓર્ગેનાઇઝેશનના કિસ્સામાં સિસ્ટમ સંચાલક કોણ છે તે પૂછપરછ કરવી જોઇએ અને તેમના મારફત ડિવાઇસની ઓળખ કરવી જોઇએ.

- **ઇન્ટરનેટ ડિસેબલ(બંધ) કરવું:** ઇન્ટરનેટ કનેક્શન તાત્કાલિક દૂર કરવું જોઇએ જેથી દૂરસ્થ(remote) ઇન્ટરનેટ પ્રવેશ દ્વારા ડેટામાં થતાં ફેરફાર અટકાવી શકાય.

ઇન્ટરનેટ કેવી રીતે ડિસેબલ(બંધ) કરવું:

- મોડેમ અને રાઉટરને સ્વિચ ઑફ કરવાં.
- તપાસ અધિકારી ઘટનાસ્થળ અથવા આસપાસનાં ક્ષેત્રમાં ઉપલબ્ધ wi-fi નેટવર્ક સ્કેન કરી શકશે.
- જો મોડેમ અથવા રાઉટર ન મળે તો LAN અથવા LAN કેબલ અનપ્લગ કરવો જોઇએ.

- **LAN ડિસેબલ (બંધ) કરવું**: જો શક્ય હોય તો LANને સર્વરમાંથી ડિસેબલ કરવું. જો નેટવર્કમાંથી કોઇપણ કાર્ય ન કરવાનું હોય જેમ કે પ્રિન્ટઆઉટ કાઢવી અથવા અન્ય કોઇ પ્રકારનો ડેટા એનાલિસિસ કરવો, તો બિનઅધિકૃત ડેટા પ્રવેશ અટકાવવા LAN ને ડિસેબલ કરવું જોઇએ.

LAN કેવી રીતે ડિસેબલ (બંધ) કરવું

- LAN સ્વિચને સ્વિચ ઓફ કરવી.
- અથવા Control Panel -> Network and sharing center -> Local Area Network -> Disable ના ક્રમ માં ઓપરેટ કરવા.
- જો સ્વિચ ના મળે અથવા સિસ્ટમમાં LAN નું સેટિંગ શોધી ન શકો તો અંતિમ વિકલ્પ LAN કેબલને સર્વરથી અનપ્લગ કરવો.

- **પાસવર્ડ એકઠા કરવાં**: કોમ્પ્યુટર/ ડિવાઇસ/ફાઇલમાં પ્રવેશ કરવા માટે ઘણાં પ્રકારના પાસવર્ડ હોય શકે. જેમ કે, કોમ્પ્યુટરના BIOS પાસવર્ડ, કોમ્પ્યુટરની ઓપરેટીંગ સિસ્ટમના (operating system)પાસવર્ડ, સ્માર્ટ ફોન કે ટેબલેટના પાસકોડ, whatsapp જેવી એપ્લીકેશનના પાસવર્ડ વગેરે. પાસવડ્ર્સના કેસમાં, માલિક પોતાના ડિવાઇસનો પાસવર્ડ પોતે જ પૂરો પાડે તે સારો વિકલ્પ છે. FSL માટે પણ ડિજિટલ ડિવાઇસનો પાસવર્ડ બ્રેક કરવો ખૂબ જ મુશ્કેલ છે. જો આરોપી પાસવર્ડ સ્વખુશી થી જાહેર કરે તો તેને પુરાવા તરીકે લેવા ભારતીય પુરાવા અધિનિયમની કલમ ૨૭ મુજબ પ્રક્રિયા કરવી જોઇએ. પાસવર્ડ જાહેર કર્યા સંબંધિત અનુરૂપ નોંધ પંચનામામાં કરવાની રહેશે.

- **જો કોઈ અસ્થિર(volatiles) માહિતી હોય તો તેને ઓળખો**: અસ્થિર માહિતી એ એક જીવંત સિસ્ટમ પરનાં ડેટાને સંદર્ભિત કરે છે, જે કોમ્પ્યુટર ઉપકરણને સંચાલિત કર્યા પછી અથવા સમય પસાર થવાને કારણે ડિલિટ થઈ જાય છે. સિસ્ટમ પર કરવામાં આવતી અન્ય ક્રિયાઓના પરિણામે અસ્થિર ડેટા(Volatile Data) ડિલિટ થઈ શકે છે. તેથી તપાસ અધિકારીએ સ્થિર માહિતી સાથે અસ્થિર માહિતી (જો તપાસ માટે નિર્ણાયક હોય) હસ્તગત કરવાનું વિચારવું જોઈએ. ઉદાહરણ તરીકે કેટલાક પ્રિન્ટરમાં છેલ્લાં પ્રિન્ટ થયેલ દસ્તાવેજ/ચિત્ર અસ્થિર મેમરીમાં સંગ્રહિત થાય છે અને પ્રિન્ટર બંધ થયા પછી આ અસ્થિર મેમરી ડિલિટ થઈ જાય છે. એવા કિસ્સમાં ડિવાઈસ ને સ્વીચ ઑફ ન કરવૂ જોઇયે, અને ચાલૂ સિસ્ટમ માંથી ફોરેંસિક ઇક્વિપ્મેંટ (ઉદાહરણ તરીકે: Write-Block Device) નો ઉપયોગ કરી ને ડેટાની નકલ કરવી જોઇએ.
- **અગત્યનાં તમામ મોબાઈલ ઉપકરણોને ઓળખો** : સંબંધિત મોબાઈલ ઉપકરણોને કબજે લેવા અને તે ખાતરી કરવી જોઈએ કે મોબાઈલ ડિવાઈસીસમાં માહિતી ડિલિટ કરવાં કોઈ અવકાશ નથી. જો મોબાઈલ ઉપકરણમાં કોઈ અસ્થિર ડેટા અસ્તિત્વમાં ન હોય તો મોબાઈલ સ્વિચ ઑફ મોડમાં રાખવો જોઈએ.
- **ક્લાઉડ હોસ્ટેડડેટા (Cloud Hosted Data):** અહિં ઘણાં ઓનલાઈન ડેટા સ્ટોરેજ પ્રોવાઈડર્સ હોય છે. જેમકે, Google,

yahoo, microsoft, dropbox વગેરે. મોટાભાગનાં સ્માર્ટફોનમાં ડેટા સમયાંતરે અપલોડ કરવામાં આવે છે અને ક્લાઉડ સર્વરમાં સ્ટોર થાય છે, જેમકે, iCLOUD. સ્માર્ટફોન અને કોમ્પ્યુટરમાંથી ડિલિટ કરેલ ફાઈલો ઘણીવાર ક્લાઉડ સર્વરમાં સ્ટોર કરવામાં આવે છે. યુઝરનેમ અને પાસવર્ડ વિના આવા પ્રોવાઈડર્સ પાસેથી ડેટા મેળવવામાં લાંબી કાયદાકીય પ્રક્રિયાનો સમાવેશ થાય છે. બેન્ડવિથ મર્યાદાઓ બેકઅપ પ્રક્રિયામાં સમય લાગે છે. જો કે તપાસ અધિકારી કેસનું મૂલ્યાંકન કરી શકે છે અને જરૂરિયાત મુજબ તે/તેણી ક્લાઉડમાં લોગ-ઈન થઈ શકે છે અને પાસવર્ડ બદલી શકે છે. જેથી કોઈપણ અન્ય લોકો ક્લાઉડમાંના ડેટાને નાબૂદ કરવા માટે સિસ્ટમમાં બહારથી પ્રવેશ કરી શકે નહીં. તમામ પ્રવૃત્તિઓની નોંધણી પંચનામામાં કરવામાં આવશે. જો કે પંચનામામાં બદલાયેલ પાસવર્ડનો ઉલ્લેખ કરવો જોઈએ નહિ અને તે ફક્ત કેસડાયરીમાં જ લખવામાં આવશે. (જેથી ચાર્જશીટ ફાઈલ કર્યા પછી આરોપી ને ચાર્જશીટ ની નકલ સાથે પંચનામા માંથી નવા પાસવર્ડ ના મળી શકે)

- **ટાઈમઝોન/સિસ્ટમ ટાઈમ:** મોટાભાગના ડિજિટલ ડિવાઈસમાં સિસ્ટમનો સમય સેટ કરવાની જોગવાઈ રહેલી હોય છે. ઉદાહરણ તરીકે સીસીટીવીમાં સિસ્ટમનો સમય વાસ્તવિક સમયથી અલગ હોઈ શકે અને તેનો તફાવત ન નોંધવાથી તે બાબત ન્યાયિક કાર્યવાહીમાં નુકસાનકારક બની શકે છે. વધુમાં વિવિધ ટાઈમઝોન જેમ કે ભારતીય પ્રમાણભૂત

સમય(IST), ગ્રીનવીચ સ્ટાન્ડર્ડ ટાઈમ(GMT), કોઓર્ડિનેટ યુનિવર્સલ ટાઈમ(UTC) આવેલા હોય છે. ઓનલાઈન એપ્લીકેશનોમાં ટાઈમઝોન પણ સુસંગત હોય છે. આથી ડિવાઈસને સ્વીચ ઑફ કરતાં પહેલા ડિવાઈસ કે એપ્લીકેશનના પંચનામામાં સિસ્ટમ ટાઈમ કે ટાઈમઝોન (પુરાવામાં જરૂરિયાત મુજબ) નોંધવા ખૂબજ અગત્યના છે.

- **USB મીડિયા કનેક્શનોની હિસ્ટ્રીની ઓળખ:** ઘણાં કેસોમાં આપણને જરૂરી કામના કાગળનો પ્રિન્ટેડ ભાગ મળી આવે છે પરંતુ આનુષંગિક/સંબંધિત દસ્તાવેજ નહીં. સ્થળ પરના તમામ પર્સનલ કોમ્પ્યુટરમાં શોધવા છતાં પણ આવા દસ્તાવેજોના નિશાન મળતાં નથી. આવી કોયડારૂપ પરિસ્થિતિને દસ્તાવેજના USB ડ્રાઈવ જેવા પોર્ટેબલ મીડિયા પર કરેલ સ્ટોરેજથી સમજાવી શકાય. આવા કેસોમાં સ્થળ પરના પર્સનલ કમ્પ્યુટરમાં USB ડિવાઈસ કરેલ છે કે નહિ તથા કેટલા સમય પહેલા કરેલ છે તે સુનિશ્ચિત કરવું ખૂબ જ અગત્યનું છે. આ પ્રકારની તપાસમાં USBDeview.exe ટૂલ મદદ કરી શકે છે. USBDeview.exe પરના ડબલ ક્લિકથી USB ડિવાઈસની હિસ્ટ્રી તમને દેખાડે છે. કેસ ની જરૂરત પ્રમાણે આ ટૂલ નો ઉપયોગ કરી USB ડિવાઈસ ઓળખી શકાય.
- કેટલાક કેસોમાં GPS ડેટા મહત્વપૂર્ણ છે, જેમકે અકસ્માતનો કેસ. આ પિરિસ્થિતિમાં ડિવાઈસ વાહનની ગતિ, સંબંધિત લોકેશનો, ટ્રાવેલ લોગ્સ, હોમ લોકેશન, અગાઉના ડેસ્ટિનેશન

વગેરે પૂરા પાડી શકે છે. આવી પરિસ્થિતિમાં, GPS ડિવાઈસને સ્વીચ ઑફ અને ડિસકનેક્ટ કરવામાં આવે તો, તે સુનિશ્ચિત થવું જોઈએ કે સ્વીચ ઑફ થાય તે પહેલા ડિવાઈસ નુ લોકેશન બદલાતું નથી. GPSના કિસ્સામાં, સ્થળની ભૂગોળ અને જ્યાં તે માઉન્ટ થયેલ છે તે સ્થાન પણ મહત્વપૂર્ણ છે (જેથી પ્રતિવાદી એ દાવો ન કરી શકે કે ઉપગ્રહોથી ડિવાઈસ યોગ્ય સંકેત મેળવતા ન હતા). તેથી પંચનામામાં ડિવાઈસની નજીકની કોઈ ઊંચી ઈમારત હોય તો તેનો ઉલ્લેખ કરવો જોઈએ.પંચનામામાં GPSના માઉન્ટનું સ્થાન પણ જણાવવામાં આવશે.

૭. ડિજિટલ ડિવાઇસની જપ્તી (સીઝર) ની પ્રક્રિયા:

ઉપર જણાવેલ મૂલ્યાકંન (એસેસમેન્ટ) પૂર્ણ કર્યા પછી, તપાસ અધિકારી તમામ ડિજિટલ ડિવાઈસનું મૂલ્યાકંન (એસેસમેન્ટ) કરશે. જે ડિવાઈસ કેસ માટે નિર્ણાયક છે તે જપ્ત(સીઝ) કરવાની જરૂર હોય અથવા નકલ કાઢવી (ઈમેજિંગ) જરૂરી હોય કે બેકઅપ લેવાની જરૂર હોયતો તેમ કરશે. જે કિસ્સામાં પુરાવા થોડાં સાધનોમાં ઉપલબ્ધ હોય (જેમ કે માત્ર એક જ મોબાઈલ ડિવાઈસ અથવા કોમ્પ્યુટર) અને/અથવા ફોરેન્સિક સહાય કે ટેકનિકલ સહાય સ્થળ પર ઉપલબ્ધ ન હોય તો ઈન્ચાર્જ અધિકારી નીચે જણાવ્યા મુજબ તે પુરાવા જપ્ત (સીઝ) કરશે અને જપ્તી (સીઝર) કર્યાના પંચનામા તૈયાર કરશે. જે સંજોગોમાં મહત્વના પુરાવાઓ પૂર્વ મૂલ્યાકંન (પ્રિ-એસેસમેન્ટ) સમયે શોધવા મુશ્કેલ હોય ત્યારે

ઈન્ચાર્જ અધિકારી પુરાવા જે ડિવાઇસીસમાં હોવાની શંકા હોય તે જપ્ત (સીઝ) કરી શકે છે. તેનાથી કાર્યભારણ (વર્કલોડ) વધશે પરંતુ કોઈ મહત્વનો પુરાવો છૂટી જશે નહિ.

૭.૧) સીઝર/ ડિજિટલ પુરવાની જપ્તી:

જો સ્થળ પર ટેકનિકલ સહાય ઉપલબ્ધ ન હોય તો ઇન્ચાર્જ અધિકારી ડિજિટલ પુરાવા સીઝ કરવાનું આયોજન કરશે તથા આ પુરાવા ફોરેન્સિક લેબોરેટરીમાં મોકલી આપશે જયાં તેનું એનાલીસીસ કરવામાં આવશે. યોગ્ય સીઝર મેમો અને પંચનામું ફરજિયાત કરવું અને નીચેની બાબતો ધ્યાનમાં રાખવી જોઈએ. :

- સર્ચ અને સીઝરની કાર્યવાહી દરમિયાન ટેકનિકલ જાણકારી ધરાવનાર એક વ્યક્તિ તથા અન્ય બે સ્વતંત્ર સાક્ષીઓ સ્થળ પર હાજર છે કે કેમ તેની ખાતરી કરવી.
- સાધનો, નેટવર્ક અને અન્ય સંદેશાવ્યવહારના (કોમ્યુનિકેશન) સાધનો સંબંધિત ટેકનિકલ માહિતીને યોગ્ય રીતે દસ્તાવેજકૃત કરવી.
- જો સિસ્ટમ ચાલુ(સ્વીચ ઓન) સ્થિતિમાં હોય તો સમય ઝોન (ટાઈમ ઝોન) કે સિસ્ટમ સમય કાળજીપૂર્વક નોંધી લેવો જોઈએ.
- કોઈપણ ઉપકરણ (ડિવાઈસ) ચાલુ (સ્વીચ ઓન) કરવું નહી.

- ઉપકરણ (ડિવાઈસ)ને એક અલગ નંબર આપવો અને તે જ નંબરથી પંચનામામાં તેનો યોગ્ય ઉલ્લેખ કરવો.
- ખાતરી કરો કે તમામ સંભવિત ડિઝિટલ ઉપકરણો (ડિવાઈસ) કે જે જપ્ત (સીઝ) કરવાની જરૂર છે તેની સંબંધિત સંદર્ભ સાથે ફોટોગ્રાફી થાય.
- જો હાર્ડ ડિસ્ક દૂર કરવામાં આવી હોય તો હાર્ડ ડિસ્ક ડ્રાઈવનો ફોટોગ્રાફ લેવો જોઈએ.
- પંચોને વિવિધ ઉપકરણો (ડિવાઈસ) વિશે પ્રાથમિક જ્ઞાન (જાણકારી) છે કે કેમ તેની ખાતરી કરવી.

૭.૨) ડિજિટલ પુરાવાનું તપાસ અધિકારી દ્વારા વિશ્લેષણ:

તપાસ અધિકારી જો સીધું જ ડિજિટલ ઉપકરણ જપ્ત કરે અને ફોરેન્સિક સાયન્સ લેબોરેટરીમાં તેની નકલ કરવા માટે મોકલવામાં આવે તો તેનાથી એ ફાયદો થશે કે કોઈપણ ડેટા(માહિતી) નષ્ટ થશે નહિ અને ડેટા(માહિતી)ની પ્રામાણિકતા નષ્ટ થવાની પણ ઓછમાં ઓછી શક્યતા રહેશે. જો કે, આ હંમેશા સલાહભર્યું નથી અને અમુક પરિસ્થિતિઓમાં કેસના હિતની વિરુદ્ધ જશે. તેમાંની કેટલીક પરિસ્થિતિ અહીં નીચે દર્શાવેલ છે.

- જ્યાં સુધી FSL દ્વારા પુરાવાની વર્કિંગકોપી પૂરી પાડવામાં નહીં આવે ત્યાં સુધી તપાસ અધિકારી આગળની વધુ તપાસ માટેની કડીઓ શોધી શકશે નહીં. જ્યાં વધુ

આરોપીઓ સામેલ હોય અને તપાસ માટેની કડીઓ ડિજિટલ ઉપકરણમાં ઉપલબ્ધ હોય તેવા કેસોમાં આ બાબત નિર્ણાયક રહેશે. ઉદાહરણ તરીકે, જો આરોપીએ પોતાના મોબાઇલ ફોન દ્વારા તેના સહ-આરોપીને ગુનાને લગતો કોઇ અગત્યનો વોટ્સએપ મેસેજ કર્યો હોય ત્યારે સીધું જ ડિજિટલ ઉપકરણ જપ્ત કરી અને FSL ને મોકલી આપવાથી, આગળની તપાસમાં વિલંબ થઈ શકે છે.

- એવા કિસ્સાઓમાં કે જ્યાં ડિજિટલ પુરાવા સર્વર્સ(Servers)માં સંગ્રહિત થઈ શકે છે અને આરોપી ડિજિટલ ઉપકરણ દ્વારા સર્વર સુધી પહોંચી શકે છે ત્યારે, જ્યાં સુધી તપાસ અધિકારી MLAT/LR અથવા Cr.P.C.ની કલમ-૯૧ ની પ્રક્રિયા પૂર્ણ કરે નહીં ત્યાં સુધી ડેટા(માહિતી) સર્વરમાંથી રીકવર કરી શકાશે નહીં. અન્યથા, તપાસ અધિકારીએ FSL દ્વારા લૉગ-ઇન આઇડી અને પાસવર્ડના રીકવરી માટેની રાહ જોવી પડશે. આ સમય દરમિયાન, આરોપી અથવા તેના સહયોગીઓ અન્ય ઉપકરણ દ્વારા લૉગ-ઇન કરી સર્વરમાંથી ડેટા(માહિતી) ડિલિટ કરી શકે છે. ઉદાહરણ તરીકે, જો કોઈ ઈ-મેઈલની રીકવરી કરવાની હોય તો, રીકવરી માટેના વિલંબના સમય દરમિયાન આરોપી અથવા તેના સહયોગીઓ દ્વારા કોઈ અન્ય મોબાઈલ કે કમ્પ્યુટરથી લૉગ-ઇન કરી તે ઈ-મેઈલ ડિલિટ કરી શકે છે.

- કોઈ કંપની કે ઓર્ગેનાઈઝેશનના મહ્ત્વના સર્વર જપ્ત કરવાથી તેમના માટે ઘણી સમસ્યાઓ ઊભી થઈ શકે છે. ઉદાહરણ તરીકે, સુરત સિટી પોલીસ કંટ્રોલ રૂમના સર્વરમાંથી CCTV ફૂટેજ માટે, સર્વરને જપ્ત કરવા વ્યવહારિક રીતે શક્ય નથી.
- જ્યારે ડેટા ઘણા બધા સાધનોમાં સંગ્રહિત હોય અને જરૂરી પુરાવા કયા ડિવાઇસ માં મૌજૂદ છે તે સ્પષ્ટ ન હોય, ત્યારે તમામ સાધનોની જપ્તી અવ્યવહારિક બને છે. ઉદાહરણ તરીકે, કોઈ સાયબર કાફેમાંથી થયેલ ઈ-મેઈલ માટે તમામ કોમ્પ્યૂટરોને જપ્ત કરવા અવ્યવહારુ છે.

આવા કિસ્સાઓમાં તપાસ અધિકારીએ સંબંધિત ડિજિટલ પુરાવા માટે ઉપકરણોનુ મૂળ-સ્થાને(ઈન-સાઈટ) વિશ્લેષણ કરવુ જોઈએ અને તે પછી આગળ પગલાં લેવા જોઈએ. જો કે ડેટાની સંવેદનશીલતા જોતા મૂળ-સ્થાને (in-situ) વિશ્લેષણ એ નાજૂક પ્રક્રિયા છે. મૂળ-સ્થાને વિશ્લેષણની પ્રક્રિયાની ચર્ચા અહીં નીચે કરેલ છે. તેવી જ રીતે, જો તપાસ અધિકારી ઉપકરણને FSLમાં મોકલતા પહેલાં, ઉપકરણનુ વિશ્લેષણ કરવાનુ પસંદ કરે તો, સમાન સાવચેતીઓ લેવી જોઈએ. ડિજિટલ પુરાવા માટે સર્વસામાન્ય નિયમ એ છે કે તપાસ અધિકારીએ મૂળ ઉપકરણ (ઓરીજનલ ડિવાઈસ) નું વિશ્લેષણ કયારેય ન કરવું જોઈએ અને વિશ્લેષણ માત્ર ડુપ્લીકેટ/બેક-અપ ફાઈલમાં જ

કરવું જોઈએ. ડેટાની પ્રામાણિકતા જાળવવા માટે આ ખૂબ જ મહત્વનું છે.

૭.૩) તપાસ અધિકારી દ્વારા વિશ્લેષણ પહેલા ડુપ્લીકેશન / બેકઅપ:

ડિજિટલ પુરાવાનાં વિશ્લેષણ માટે પ્રશિક્ષિત વ્યક્તિ આવશ્યક છે. ડિજિટલ પુરાવા એકત્ર કરવા માટે આવશ્યક કૌશલ્ય વિકસાવવા માટે ફોરેન્સિક સાયન્સ યુનિવર્સિટી, ગાંધીનગર વિવિધ તાલીમ અભ્યાસક્રમો ચલાવી રહી છે. **FSL** ને મોકલતા પહેલા તપાસ અધિકારી દ્વારા ડિજિટલ ડિવાઈસમાં ઉપલબ્ધ પુરાવાઓનું વિષ્લેષણ કરવાની જરૂર પડે ત્યારે, ડુપ્લીકેશન/બેકઅપ જરૂરી છે. તપાસ અધિકારી દ્વારા લેવાયેલ તમામ પગલાઓ પંચનામામાં દર્શાવવા જોઈએ.

ડુપ્લીકેશન અને બેકઅપ બે અલગ પ્રક્રિયા છે અને તેમાં નીચેના મહત્વનાં તફાવત છે:

- **લોજિકલ બેકઅપ**: લોજિકલ બેકઅપ લોજિકલ વોલ્યુમની ડિરેકટરીઓ અને ફાઈલોની નકલ કરે છે. તે કાઢી નાખેલ અથવા અસ્થિર સ્થાનમાં સંગ્રહિત શેષ ડેટા જેવા અન્ય ડેટાને ગ્રહણ (કેપ્ચર) કરતું નથી.
- **બિટ સ્ટ્રીમ ઈમેજિંગ/ફોરેન્સિક ઈમેજિંગ/કલોનિંગ**: ડિસ્ક ઈમેજિંગ/કલોનિંગ તરીકે પણ ઓળખાતી બિટ સ્ટ્રીમ ઈમેજિંગ ફ્રી જગ્યા અને અસ્થિર (Slack) જગ્યા સાથે મૂળ

મીડીયાની અક્ષરશ: નકલ કરે છે. ડિસ્ક ઈમેજિંગ સામાન્ય રીતે વધુ જગ્યા અને લાંબો સમય લે છે.

તપાસ અધિકારી પોતાની વિવેકબુદ્ધિ અનુસાર કોઈ ચોક્કસ ડિવાઈસની નકલ કરવી કે બેકઅપ લેવુ તે નક્કી કરશે અને તે નિર્ણય કેસના સંજોગો તથા જરૂરિયાત આધારિત હશે. ઈમેજિંગ એ લાંબી, સમય માંગી લેતી પ્રક્રિયા છે જેમાં સામાન્ય રીતે વધારે સંગ્રહ જરૂરી છે. ઈમેજિંગ માટે ખાસ સાયબર-ફોરેન્સિક સાધન જરૂરી છે. (જે સાયબર-ફોરેન્સિક સાધન ગુજરાત પોલીસ પાસે ઉપલબ્ધ છે અને તેની ક્ષમતાઓ પછીના પ્રકરણમાં દર્શાવેલી છે.) બેકઅપ એ ઝડપી અને મુદ્દાસર પ્રક્રિયા છે, તેમાં સંગ્રહ માટેની જરૂરિયાત નોંધપાત્ર રીતે ઓછી હોય છે. તેમ છતાં ડિજિટલ ડિવાઈસમાં એવો કોઈ સંવેદનશીલ ડેટા હોય કે જેને કાયદાની કોર્ટમાં પડકારી શકાય તો એ સિસ્ટમની બિટ-સટ્રીમ નકલ (ઈમેજ) કરવું સલાહભર્યું છે. ડેટા બેકઅપની એક બીજી ઉણપ એ છે કે નાશ કરેલી ફાઈલોને આ ડેટા બેકઅપમાંથી પુન:પ્રાપ્ત કરી શકાતી નથી.જો ઈન્ચાર્જ અધિકારીને ખાતરી હોય કે સિસ્ટમમાં નોંધપાત્ર નાશ કરેલી ફાઈલો છે તો તે સિસ્ટમનો ડેટા બેકઅપ લેવાને બદલે નકલ (ઈમેજ) કરવી જોઈએ. તેમ છતાં જયાં ફોરેન્સિક નિષ્ણાંતો/પ્રશિક્ષિત કર્મચારીઓ અને સાધનો મેળવવા મુશ્કેલ હોય ત્યારે ડેટા બેકઅપ ઘણું ઉપયોગી છે. બન્ને માંથી કઈ પ્રક્રિયા હાથ ધરવી એ તપાસ કરનાર કેસ ના તથ્યો અને જરૂરિયાત આધારે નક્કી કરશે.

જો તપાસ અધિકારી લોજિકલ બેકઅપ/ફોરેન્સિક ઈમેજિંગ (નકલ) લેવાનો નિર્ણય લે તો કેટલીક સાવચેતી લેવાની જરૂર છે:

- બેકઅપ દરમિયાન, મૂળ મીડીયાની સંકલિતતા જળવાવી જરૂરી છે. બેકઅપ દરમિયાન તપાસ અધિકારીએ લેખ બ્લોકર(write blocker)નો ઉપયોગ કરવો જોઈએ. (ગુજરાત પોલીસ પાસે ઉપલબ્ધ Write-blocker device અને તેનો ઉપયોગ વિશે પછીના પ્રકરણમાં ચર્ચા કરવામાં આવી છે.) ફોરેન્સિક ઈમેજિંગ/કલોનિંગ માટે પણ આ લાગુ પડે છે. Write-blocker device એ હાર્ડવેર અને/અથવા સોફ્ટવેર આધારિત સાધન છે, જે કોમ્પ્યુટરને તેનાથી જોડાણ કરેલા કોમ્પ્યુટર સ્ટોરેજ મીડિયા પર લખાણ કરતા અટકાવે છે, અને પુરાવાની અખંડતા ને નુકસાન થવાથી રોકે છે.
- બેકઅપ અથવા ઈમેજિંગ કર્યા પછી કોપી થયેલ ડેટા મૂળ ડેટાના બરાબર છે કે કેમ તેની ચકાસણી કરવી હિતાવહ છે.
- ડેટાની સંકલિતતા જાળવવા નકલ કરેલ ડેટાની હેશ-વેલ્યૂની ગણતરી કરવી સલાહભર્યું છે. પુરાવામાં એક બિટનો બદલાવ પણ હેશવેલ્યૂ બદલી શકે છે. હેશવેલ્યૂ અને તેની ગણતરી કરવાની પ્રક્રિયાની ચર્ચા હવે પછી કરવામાં આવશે. જો પુરાવાની હેશવેલ્યૂ ન બદલાય હોય

તો ડેટાની સંકલિતતા કાયદાની કોર્ટમાં જાળવી રાખવાનો દાવો કરી શકાય છે.

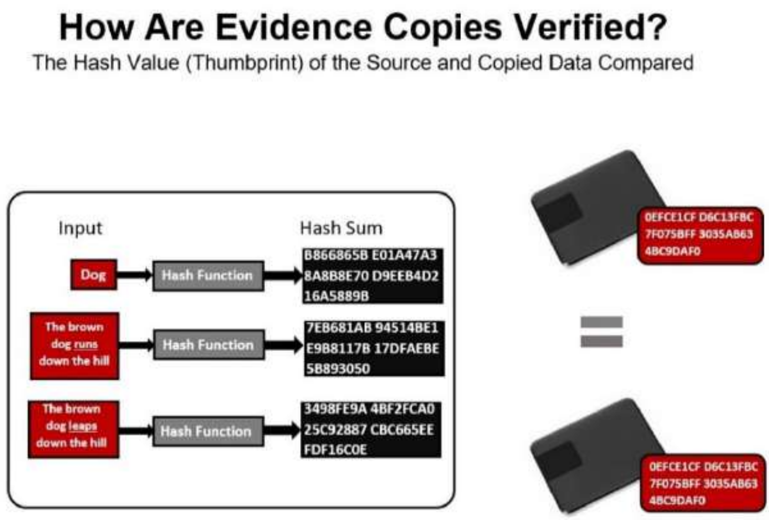
- બેકઅપ/ઈમેજ ફાઈલની બે નકલો બનાવો, એક અનુગામી વિશ્લેષણ માટે અને એક સંગ્રહ/સંદર્ભ માટે હશે.
- સંગ્રહ/સંદર્ભ માટે રાખવામાં આવેલ ફાઈલમાં વિશ્લેષણ કરવું નહી.
- વિશ્લેષણ માટે વાપરવામાં આવેલ ફાઈલમાં સામગ્રી પુરાવા મળે તો તપાસ અધિકારીએ કેસ ડાયરીમાં તેની નોંધ કરવી અને જરૂર હોય તો પ્રિન્ટ આઉટ/સી.ડી. પણ લઈ શકાય.

જુદા જુદા ઉપકરણોથી ફોરેન્સિકલી સાઉન્ડ રીતમાં માહિતી મેળવવા માટે કેટલાક રસ્તાઓ :

- **હાર્ડ ડ્રાઈવ (ડેસ્કટોપ/લેપટોપ/USB ડ્રાઈવ્સ)** : ડ્રાઈવ્સની નકલ કરવા ફોરેન્સિક સોફટવેર્સ/સાધનો જેમ કે એન્કેસ, સાયબર ચેક સ્યુટ, FTK નો ઉપયોગ કરવો. ડેટાની સંકલિતતાને સુરક્ષિત રાખવા માટે write blocker નો ઉપયોગ કરવાની ખાતરી કરો.
- **સ્માર્ટ ફોન**:એન્કેસ, સેલેબ્રાઈટ, પેરાબેન ડિવાઈસ જેવા સોફ્ટવેર/સાધનોનો ઉપયોગ કરો. આ કિસ્સામાં ચાલુ મોબાઈલ ફોન સાથે કામ કરતી વખતે સાવચેતી રાખવી જોઈએ, જેની ચર્ચા પછીના પ્રકરણમાં કરીશું.

૮. હેશવેલ્યૂ:ડિજિટલ પુરાવામાં મહ્ત્વ અને ગણતરી અંગેની પ્રક્રિયા:

હેશવેલ્યૂ એ કોઈ ફાઈલના ભાગ, ફાઈલ કે ફાઈલોના સમૂહ ને તેમાં સંગ્રહાયેલ ડેટા અંગેની લાક્ષણીકતા ને ધ્યાને લઇ, તેને સંક્ષિપ્તમાં દર્શાવતી એક અનન્ય વેલ્યૂ છે. જે મૂળભૂત રીતે ખૂબ મોટા ડેટાને મેથેમેટિકલ અલ્ગોરીધમ વાપરીને એક સંક્ષિપ્ત(નાની) વેલ્યૂ સ્વરૂપે રજૂ કરે છે. હેશવેલ્યૂ મેળવવા મુખ્યત્વે MD5 અથવા SHA અલ્ગોરીધમનો ઉપયોગ થાય છે. જેના દ્વારા મળતી હેશવેલ્યૂ અનન્ય(unique) હોય છે. 'હેશિંગ'નો મુખ્ય ઉપયોગ મૂળ ડેટાની અધિકૃતતા અને અખંડિતતા નક્કી કરવાનો છે. સામાન્ય રીતે હેશવેલ્યૂ 'C75491c89395de9fa4ed29affda0e4d29cbad290' જેવી દેખાતી હોય છે. હેશવેલ્યૂની લંબાઈ એક નાની ફાઈલથી માંડીને મોટી હાર્ડડીસ્ક માટે પણ સમાન હોઈ શકે છે તથા મૂળ ફાઈલ કે ડેટામાં થયેલ સામાન્ય ફેરફારથી પણ હેશવેલ્યૂ બદલાઈ જાય છે. હેશ વેલ્યૂ ને કોમ્પ્યુટર ફાઈલની ફીંગરપ્રીન્ટ કહી શકાય. રીસીવ કરેલ ડેટા ફાઈલની હેશ વેલ્યૂ ને મોકલી આપેલ ડેટા ફાઈલની હેશ વેલ્યૂ સાથે મેચ કરવાથી એ જાણી શકાય છે કે મોકલી આપેલ (મૂળ) ડેટા ફાઈલ સાથે કોઈ પણ પ્રકારના ચેડા થયેલ છે કે કેમ?



<u>૮.૧) ડિજિટલ પુરાવામાં અગત્યતા:</u>

ધી ઇન્ફર્મેશન ટેકનોલોજી એક્ટ, ૨૦૦૦ પણ આંતરરાષ્ટ્રીય-રીતે સ્વીકૃત હેશ-ફંક્શનને, ડેટાની વિશ્વસનીયતા પ્રમાણિત કરવા અંગેની એક વિશ્વસનીય પદ્ધતિ ગણે છે. જે અંગે કલમ-૩(૨) માં દર્શાવ્યાનુસાર,

> *સ્પષ્ટીકરણ: આ પેટા કલમના હેતુ માટે 'હેશફંક્શન' એટલે અલ્ગોરીધમ મેપિંગ અથવા અમૂક બીટ્સની સિક્વન્સનું અન્ય બિટમાં ભાષાંતર, જે સામાન્ય રીતે સંક્ષિપ્ત(નાનું) હોય છે. જેને 'હેશરીઝલ્ટ' તરીકે ઓળખવામાં આવે છે અને આવા ઈલેક્ટ્રોનિક રેકર્ડને*

જેટલી પણ વાર અલ્ગોરિધમને કરી ઈનપુટ તરીકે આપવામાં આવે ત્યારે ઈલેક્ટ્રોનિક-રૅકર્ડનું સમાન 'હેશ રિઝલ્ટ' આપે છે. જેના કારણે નીચેની બે બાબત અશક્ય બની જાય છે.

ક). અલ્ગોરીધમથી તૈયાર કરવામાં આવેલ હેશ રિઝલ્ટમાંથી મૂળ ઈલેક્ટ્રોનિક રૅકર્ડ ફરી મેળવવું.

ખ). અલ્ગોરીધમ વાપરવાથી બે ઈલેક્ટ્રોનિક રૅકર્ડનું એક સરખું 'હેશ રિઝલ્ટ' લાવવું.

વધુમાં કલમ-3ની જોગવાઈ અનુસાર, ઈલેક્ટ્રોનિક-રૅકર્ડની અધિકૃતતા માટે 'એસીમેટ્રિક-ક્રીપ્ટોસીસ્ટમ' અને હેશ ફંક્શનનો ઉપયોગ કરવામાં આવશે.

ઇન્ફર્મેશન ટેકનોલોજી (સર્ટિફાઇન્ગ ઓથોરીટીઝ) નિયમો ૨૦૦૦, અનુસાર હેશ-ફંક્શનની ઉપયોગીતા ડિજિટલ સિગ્નેચર અંગેની માહિતીની પ્રમાણભૂતતા નિર્ધારિત કરવા અંગેની તથા ડિજિટલ સિગ્નેચર બનાવવા તથા તેની ચકાસણી માટે અને ઈલેક્ટ્રોનિક રૅકર્ડમાં કોઈ અનિચ્છનીય ફેરફાર થયેલ ન હોવાની ખાતરી કરવાની છે. જેની ખાતરી ચકાસણીકાર દ્વારા ગણતરી બાદ મેળવેલ હેશ પરિણામ અને ડિજિટલ સિગ્નેચરમાંથી મેળવાયેલ હેશ પરિણામ સરખા હોય તેવા કિસ્સામાં થાય છે. ઇન્ફર્મેશન ટેકનોલોજી (સર્ટિફાઇન્ગ ઓથોરીટીઝ) નિયમો, ૨૦૦૦ના નિયમ-૬ અનુસાર MD5 તથા SHA-2 એ પ્રમાણભૂત અને સ્વીકૃત હેશફંક્શન છે.

જો તપાસ અધિકારી એવું દર્શાવવામાં સફળ થાય કે, મેળવેલ પુરાવાની હેશ-વેલ્યૂ બદલાયેલ નથી તો ડેટા કે પુરાવાની વિશ્વસનીયતા જળવાઈ રહે છે. આથી, જો તપાસ અધિકારી કોઈ ડિજિટલ પુરાવાનું વિશ્લેષણ કરતાં હોય ત્યારે આવા ઈલેક્ટ્રોનિક રૅકર્ડની હેશવેલ્યૂ પંચનામા અને કેસ ડાયરીમાં અચૂક દર્શાવવી જોઈએ.

<u>૮.૨) હેશવેલ્યૂની ગણતરી કરવાની પ્રક્રિયા:</u>

જ્યારે ગુજરાત પોલીસ પાસે ઉપલબ્ધ ફોરેન્સિક ટૂલ અથવા સોફ્ટવેર દ્વારા ઈમેજીંગની પ્રક્રિયા પૂર્ણ થાય ત્યારે આ ટૂલ કે સોફ્ટવેર દ્વારા ઓટોમેટીક-જનરેટ થતી હેશવેલ્યૂ પંચનામા માં અચૂક દર્શાવવી જોઈએ.

આ સિવાય હેશવેલ્યૂ ગણી આપતા ઘણા સોફ્ટવેર ઓનલાઈન ની:શુલ્ક ઉપલબ્ધ છે. જેમ કે, WINMD5 એ MD5 હેશ-ફંક્શન વાપરી હેશ-વેલ્યૂ ગણી આપતું ફ્રી-ઓનલાઈન ટૂલ છે.

<u>૯. ડિજિટલ પુરાવાના સંગ્રહ માટે ની સાવચેતી:</u>

ડિજિટલ પુરાવા મેળવ્યા પછી, તે ટ્રાયલ દરમ્યાન રજૂ કરવા સુધી ડિજિટલ ડિવાઈસ અને પુરાવા સાચવવાની જવાબદારી તપાસ કરનાર અમલદાર અને ક્રાઈમ રાઈટર હેડની હોય છે. ડિજિટલ ડિવાઈસ અને સ્ટોરેજ ની સંવેદશીલતાને ધ્યાને લેતા, ડિજિટલ

પુરાવાને નુકશાન ન થાય તે રીતે સાચવવાની જરૂરત રહે છે. તેથી, નીચે મુજબની માર્ગદર્શિકા સૂચવવામાં આવે છે:

- ડિજિટલ પુરાવા કાળજીપૂર્વક સંભાળો. જો ડિજિટલ પુરાવો કોઈ વાહનમાં મૂકીને એક ઠેકાણેથી બીજે ઠેકાણે લઈ જવાનો હોય તો ડિવાઈસને સીધો મૂકો જેથી તેને કોઈ ગંભીર ભૌતિક આંચકા ન આવે.
- ડિજિટલ પુરાવા ચુંબકીય સ્રોતો (લાઉડ સ્પીકર, ગરમ સીટ કે બારીઓ, પોલીસ રેડિયો) થી દૂર રાખો. તમામ ડિજિટલ ઉપકરણોની હાર્ડ ડિસ્ક ચુંબકીય ક્ષેત્રોથી સુરક્ષિત હોવી જોઈએ. એન્ટિ-સ્ટેટિક બેગ, જો ઉપલબ્ધ હોય તો તેમા કે મજબૂત કાગળની બેગ અથવા મજબુત કાર્ડબોર્ડ પેકેજીંગ અને વાયુયુક્ત પ્લાસ્ટિકની બેગમાં રાખો.
- રીમુવેબલ સ્ટોરેજ ફલોપી ડિસ્ક, મેમરી સ્ટિકસ, મેમરી કાર્ડ્સ, સીડી/ડીવીડી ને ચુંબકીય ક્ષેત્રોથી સુરક્ષિત રાખવા જોઈએ. તેમને વાળવા નહીં કે વાકાં કરવા નહીં. ફલોપી ડિસ્ક અથવા સીડી/ડીવીડી પર લેબ્લસ સીધા ન ચોંટાડો. અન્ય વસ્તુઓને ચુંબકીય ક્ષેત્રોથી સુરક્ષિત રાખવી જોઈએ.
- વસ્તુઓનું યોગ્ય રીતે પેકેજીંગ કરો અને બેગમાં સીલ કરો. વસ્તુઓને ભીની ન થવા દો.
- ઈલેકટ્રોનિક્સ ઉપકરણો પર એલ્યુમિનિયમના પાઉડરનો ઉપયોગ પુરાવાને નુકશાનકારક બની શકે છે અને તેનાથી પુરાવાનો નાશ પણ થઈ શકે છે.

- મુદ્દામાલ રૂમના સામાન્ય તાપમાને ભેજની કોઈ અસર કે ચુંબકીય પ્રભાવ જેવા કે રેડિયો રીસીવરથી સુરક્ષિત રીતે સંગ્રહિત હોવી જોઈએ. ધૂળ, ધ્રૂમ્રપાન, રેતી, પાણી, તેલ વગેરે પણ ઈલેકટ્રોનિક્સ સાધનો માટે હાનિકારક છે.
- કેટલાક ઉપકરણો બેટરીઓનો ઉપયોગ કરીને આંતરિક ડેટા (જેમ કે સિસ્ટમ પર સેટ કરેલ સમય અને તારીખ) સંગ્રહિત કરવા માટે સક્ષમ હોય છે. જો બેટરીને નિષ્ક્રિય થવા દેવામાં આવે તો, આંતરિક ડેટા નષ્ટ થશે. જો કે, જ્યારે ફોરેન્સિક પરીક્ષણ પહેલા લાંબા સમય માટે ઉપકરણને સંગ્રહિત કરવાનું થાય ત્યારે આ એક મહત્વપૂર્ણ બાબત છે અને કેસની જરૂરિયાત મુજબ તેની કાળજી રાખવી જોઈએ.

પ્રકરણ-૩

સીસીટીવી (CCTV)

પ્રકરણ નો ઉદ્દેશ: ક્લોઝ્ડ સર્કિટ ટેલિવિઝન (સીસીટીવી) સર્વેલન્સ અપરાધ નિયંત્રણ માટે કાર્યરત તકનીક છે, અને સીસીટીવી કેમેરા દ્વારા રેકર્ડ કરવામાં આવેલા ફૂટેજ ફોજદારી કાર્યવાહીમાં અગત્યનાં પુરાવાના સ્રોત બની ગયા છે. આ પ્રકરણમાં સીસીટીવી રેકર્ડીંગને પુરાવા તરીકે એકત્ર, વિશ્લેષણ અને પ્રસ્તુત કરવાની માર્ગદર્શિકા આપવામાં આવેલ છે.

૧. સી.સી.ટી.વી. અને તેનુ પુરાવામાં મહત્વ :

સી.સી.ટી.વી એટ્લે ક્લોઝ્ડ સર્કિટ ટેલીવીઝન, જેના દ્વારા નિર્ધારીત વિસ્તારનુ સતત વીડીયો રેકોર્ડીંગ કરી શકાય છે, ઘણા ગુનાહિત બનાવમાં કોઇ નજરે જોનાર સાહેદ હોતા નથી કે આરોપીની ઓળખ થઈ શકતી નથી. તેવા કિસ્સામાં સી.સી.ટી.વી કેમેરાની મદદથી કેટલા આરોપી હતા?, બનાવ માં કોઇ હથિયાર હતા કે કેમ?, કોઇ વાહન નો ઉપયોગ થયો છે કે કેમ?, આરોપી કઈ દીશા તરફ ગયેલ છે?, બનાવનો સમય અને તારીખ શુ હતી?, જેવા ઘણા પ્રશ્નોના ઉકેલ તેની આસપાસ રહેલા સી.સી.ટી.વી. કેમેરામાં રેકોર્ડ થઈ જવાના કારણે મળી જાય છે, અને આ વિડિયો રેકોડીંગનો ઉપયોગ વણ-શોધાયેલા બનાવો શોધવામાં તેમજ તપાસમાં પુરાવા તરીકે ખુબ મહત્વનો ભાગ ભજવે છે.

સી.સી.ટી.વી. કેમેરાના મુખ્ય ભાગો માં લેન્સકેમેરા જેના દ્વારા ચોક્કસવીસ્તાર નુ ચિત્ર રેકોર્ડ થાય છે, અને સી.સી.ટી.વી કેમેરા માટેના સ્ટોરેજ ડીવાઇસ માં સ્ટોર કરવામાં આવે છે, અને મોનિટર દ્વારા જીવંત નીરીક્ષણ તથા રેકોર્ડ થયેલ વીડીયોને નીહાળવા માટે થાય છે.

૨. સી.સી.ટી.વી. ના પ્રકારો:

અનુ. નં	**કેમેરા નું નામ**	**વર્ણન**
૧	**બુલેટ(BULLET)**	આ કેમેરાનુ નામ તેના બુલેટ જેવા આકાર ને કારણે બુલેટ કેમેરા રાખવામા આવ્યુ છે. આ કેમેરા નાના કદ અને સસ્તા ભાવ હોવાના કારણે ઘર તેમજ નાની દુકાનો માં જોવા મળે છે. બુલેટ કેમેરા દ્વારા ફક્ત નીર્ધારીત વીસ્તારનુ જ રેકોર્ડીંગ થાય છે.

૨	**ગુંબજ(DOME)**	ગુંબજ જેવા આકાર ને કારણે આ કેમેરા નુ નામ ડોમ કેમેરા રાખવામાં આવેલ છે. આ કેમેરાના આકાર ના કારણે કઇ દીશાનુ વીડીયો રેકોર્ડીંગ થાય છે તે સમજવુ અઘરુ પડે એ માટે આ કેમેરા ઉપયોગી છે. સામાન્ય રીતે આ કેમેરા બિલ્ડીંગ, હોટલો, બેંક, રેસ્ટોરેંટ જેવી જગ્યાઓમાં લગાવામાં આવે છે.
3	**ડીસક્રિટ(DISCRETE)**	ડીસક્રિટ સી.સી.ટી.વી.એ ગુપ્ત પ્રકારનો કેમેરો છે, જેનો બાહ્ય આકાર તથા રૂપ ખ્યાલ ન આવે તેઓ રાખવામા આવે છે.

૪	**ઇન્ફ્રારેડ(INFRARED)**	ઇન્ફ્રારેડ કેમેરા અંધારામા તેમજ રાત્રિના સમયે બોડી ટેમ્પરેચર ના આધારે ઇન્ફ્રારેડ દ્વારા ચિત્ર છબીઓ મેળવે છે.આ કેમેરાને ઓળખવા માટે તેના લેન્સ ની સામે મોબાઈલ કેમેરો ઓન કરી જોશો તો લેન્સ માં લાઈટ બ્લીન્ક થતી મોબાઈલ સ્ક્રીન પર જોવા મળશે , જે નરી આંખે જોઈ શકાશે નહિ.
૫	**દિવસ/રાત્રિનો** **(DAY/NIGHT)**	સામાન્ય રીતે રાત્રીના અથવા અંધકારમાં સી.સી.ટી.વી. દ્વારા થયેલુ વીડીયો રેકોર્ડીંગ સ્પષ્ટ આવતુ નથી પરંતુ ડે- નાઇટ કેમેરા દ્વારા રાત્રી નુ વીડીયો રેકોર્ડીંગ સ્પષ્ટપણે લઇ શકાય છે. આ કેમેરા ને ઓળખવા માટે તેના લેન્સ ની ફરતે **LED** આવેલી હશે જે **LED** જોતા લાલ રંગ ની ચાલુ અવસ્થામાં હશે .

૬	**વેરીફોકલ(VARIFOCAL)** 	વેરીફોકલ કેમેરા દ્વારા દુરના ચિત્ર પણ સ્પષ્ટ રીતે લઇ શકાય છે. તેમજ ચોક્કસ વિસ્તારનુ ફોકસ ગુમાવ્યા વગર ઝૂમ-ઇન અને આઉટ કરી શકાય છે.
૭	**આઇ.પી. કેમેરા (IP CAMERA)** 	આઇ.પી. કેમેરા દ્વારા થતા વીડીયો રેકોર્ડીંગને ઇન્ટરનેટ માધ્યમ દ્વારા કોઈપણ જગ્યાએ જોઈ શકાય છે, તેમજ વીડીયોરેકોર્ડીંગ સ્ટોર પણ કરી શકાય છે. આ કેમેરા નું વિડીયો રેકોર્ડીંગ એન.વી.આર. રેકોર્ડરમાં રેકોર્ડ કરવામાં આવે છે. આ એન.વી.આર. વિડીયો રેકોર્ડરમાં હાર્ડ ડ્રાઈવ આવેલ હોય છે જે રેકોર્ડરનાં કંપનીના સર્વર સાથે જોડાયેલ હોય છે જેથી ઈન્ટરનેટનાં માધ્યમ દ્વારા આ વિડીયો રેકોર્ડીંગ કોઈ પણ જગ્યાએ જોઈ શકાય છે.

૮	**વાયરલેસ (WIRELESS)**	વાયરલેસ કેમેરાને ડી વી આર રેકોર્ડર સાથે કેબલ વગર જોડી શકાય છે જેની રેઈન્જ ૧૦૦ ફૂટ થી ૪૫૦ ફૂટ હોઈ છે.આ કેમેરા વાઇફાઈ નેટવર્ક થી જોડાયેલ હોઈ છે.
૯	**પીટીઝેડ(PTZ)**	પીટીઝેડ (પેન-ટિલ્ટ-ઝૂમ કેમેરા) કેમેરાની ખાસિયત એ છે કે તે પ્રોગ્રામેબલ છે અને મેન્યુઅલી નિયંત્રિત કરી શકાય, ઝૂમ-ઇન અને આઉટ કરી શકાય છે તેમજ ચારેય દિશા નું રેકોર્ડીંગ પણ કરી શકાય છે.
૧૦	**હાઇડેફિનેશન(HD)**	હાઇડેફિનેશન કેમેરાનો ઉપયોગ મોટે ભાગે ઉચ્ચ જોખમ ધરાવતી સંસ્થામાં થાય છે. જેના ઉચ્ચ રીઝોલ્યુશન લેન્સ થી, સારી ગુણવત્તાવાળુ વિડીયો રેકોર્ડીંગ કરી શકાય છે.

<u>૩. સી.સી.ટી.વી. રેકોર્ડર ના પ્રકારો :</u>

સી.સી.ટી.વી. રેકોર્ડર બે પ્રકાર છે: DVR રેકોર્ડર અને NVR રેકોર્ડર. DVR રેકોર્ડરમાં વિડિયો ઈન નો પોર્ટ રાઉન્ડ પ્રકારનો હોય છે. જયારે NVR રેકોર્ડરમાં વિડિયો ઈન નો પોર્ટ લેન પ્રકારનો હોઇ છે. સી.સી.ટી.વી. રેકોર્ડરમાં USB પોર્ટ આપેલો હોઈ છે જ્યા હાર્ડ ડિસ્ક/પેનડ્રાઈવ ડેટા કેબલથી કનેકટ કરી વિડિયો રેકોર્ડીંગ કોપી કરવામાં આવે છે.

સી.સી.ટી.વી. વિડીયો રેકોર્ડરની વિડીયો ફાઇલ .mov, .divx, .mpg, .avi, .mp4, .mp5, વગેરે પ્રકારની હોય છે. જે સી.સી.ટી.વી. વિડીયો રેકોર્ડરની હાર્ડ ડીસ્કમાં સ્ટોર થતી હોય છે. આ રેકોર્ડરોમાં કંપનીનુ ડીફોલ્ટ વિડીયો પ્લેયર આવેલ હોય છે, જેમા સ્ટોર થયેલી ફૂટેજ જોઇ શકાય છે. તેમજ કોપી કરેલી વિડીયો ફૂટેજ ને લેપટોપ અથવા કોમ્પ્યુટરમાં જોવા માટે VLC player, Total Video player, GOM player, જેવા વિડીયો પ્લેયરમાં જોઈ શકાય છે. આ બધા વિડીયો પ્લેયર ઇન્ટરનેટ થી ડાઉનલોડ કરી શકાય છે. પરંતુ, અમુક વખતે પ્રોપ્રાઈટી સોફ્ટવેર પ્લેયર પણ સી.સી.ટી.વી. માં વીડિયો પ્લે કરવા માટે વપરાઈ શકે છે, તેવા સંજોગો માં સી.સી.ટીવી. ફૂટેજ પ્લે કરવા માટે તેજ પ્રોપ્રાઈટરી સોફ્ટવેર પ્લેયર ની જરૂરત પડે છે.

૩.૧) DVR રેકોર્ડર :

ડી.વી.આર. (ડિજિટલ વિડિયો રેકોર્ડર) નો ઉપયોગ સી.સી.ટી.વી. કેમેરા દ્વારા કરવામાં આવતા રેકોર્ડીંગને સ્ટોર કરવા તેમજ ઓપરેટ કરવા માટે ઉપયોગ કરવામાં આવે છે. તેમાં 1 થી 4 ઓડિયો માઇક્રોફોન ઈનપુટ અને 4 થી 32 વિડીયો ચેનલો હોય છે, જેના દ્વારા સી.સી.ટી.વી. કેમેરા અને ઓડિયો ડીવાઈસ કનેક્ટ કરી શકાય છે. જેટલી વિડીયો ચેનલ ડી.વી.આર.માં હોય તેટલા કેમેરા ચલાવી શકાય છે, તેમજ યુ.એસ.બી. પોર્ટ સ્ટોરેજ ડીવાઈસ કનેક્ટ કરી ડેટા કોપી કરવા માટે આપેલા હોય છે અને લેન પોર્ટ ડી.વી.આર. ને અપડેટ કરવા માટે ઈન્ટરનેટ નું જોડાણ થઇ શકે તે માટે આપવામાં આવેલ હોય છે. ડી.વી.આર. ની સ્ટોરેજ કેપેસિટી ૫૦૦ જીબી થી લઇ ૧૬ ટીબી સુધી ની હોય છે.

DVR RECORDER

૩.૨) NVR રેકોર્ડર :

એન.વી.આર. (નેટવર્ક વિડીયો રેકોર્ડર) નો ઉપયોગ આઈ.પી. કેમેરા દ્વારા થતા વિડીયો રેકોર્ડીંગને સ્ટોર કરવા માટે થાય છે એન.વી.આર.માં લેન પોર્ટ આવેલ હોય છે જેની સાથે આઈ.પી. કેમેરા જોડી શકાય છે. એન.વી.આર. રેર્કોડર ની અંદર જ તેની સ્ટોરેજ હાર્ડ-ડ્રાઇવ હોય છે. જેની અંદર વિડીયો રેકોર્ડીંગ સ્ટોર થતુ હોય છે. એન.વી.આર. રેકોર્ડરની સ્ટોરેજ કેપેસિટી ૫૦૦ જીબી થી લઇ ૧૬ ટીબી સુધીની હોય છે. તેમજ એન.વી.આર. રેકોર્ડર જે કંપનીનુ હશે તેના આઇ.પી. યુઝર આઇ.ડી અને પાસવર્ડ કંપની દ્વારા આપેલા હોય છે. તેમજ આ રેકોર્ડરમાં લેન પોર્ટ આવેલો હોય છે, જેમાં ઈન્ટરનેટ કનેક્શન આપેલ હોય તો કંપનીના આઇ.પી. લીન્ક ઇન્ટરનેટ વેબ બ્રાઉજરમાં નાખી તેના યુઝર આઈ.ડી. અને પાસવર્ડથી લોગ-ઇન થઇ વિડીયો રેકોર્ડીંગ કોઈ પણ જગ્યા જોઈ શકાય અથવા થયેલ વિડીયો રેકોર્ડીંગ ડાઉનલોડ કરી શકાય છે. તેમજ કોઇપણ જગ્યાએ સર્વર રાખી આ વિડીયો ફૂટેજ સ્ટોર પણ કરી શકાય છે પણ તેના માટે N.V.R. રેકોર્ડર અને સર્વરમાં ઈન્ટરનેટ કનેકશન હોવું જોઈએ અને કોપી થતી વખતે ઈન્ટરનેટ કનેકશન લોસ્ટ ના થવું જોઈએ.

OK
NVR RECORDER

HOME
WORK
I.P CAMERA
NVR RECORDER
INTERNET
ANY WHERE
SYSTEM
SERVER

<u>NVR સર્વર</u>

<u>૪. ઘટના સ્થળ ની કાર્યવાહી :</u>

<u>*૪.૧) બનાવ સ્થેળ લઇ જવા માટેનાં જરૂરી ઉપકરણ:*</u>

બનાવ સ્થળે જતી વખતે સાથે કંપનીની સીલબંધ હાર્ડ ડીસ્ક, પેન ડ્રાઇવ, ડી.વી.ડી, સી.ડી જેની ખરીદી પોલીસ સ્ટેશનનાં નામવાળા બીલ થી થયેલ હોય, તપાસનાં કામે કોપી કરવા માટે હાર્ડ ડીસ્ક, લેપટોપ, કી-બોર્ડ, માઉસ, HDMI કેબલ, USB એક્સટેનશન કેબલ, મોનીટર સ્ક્રીન સાથે લઇ જવી કારણ કે અમુક સ્થળે સી.સી.ટી.વી રેકોર્ડર સાથે મોનીટર હોતુ નથી તેમજ સી.સી.ટી.વી. રેકોર્ડર ને ઓપરેટ કરવા માટે માઉસ અને કી- બોર્ડ હોતા નથી.

<u>*૪.૨) ફૂટેજ મેળવવા માટે નોડલ ઓફિસરને આપવા માટેની યાદી :*</u>

વિષય : CCTV ફૂટેજ તથા એક વર્કિંગ કોપી એવીડન્સ એક્ટ ૬૫(ખ) ના ફોર્મ સાથે આપવા બાબત.

સવિનય

સાથે..પોલીસ સબ ઇન્સપેક્ટર ....અમદાવાદ શહેર નાનો વિનંતી રીપોર્ટ કે,......................કંપની ની પેન ડ્રાઇવ/હાર્ડ ડ્રાઇવ જેની સ્ટોરેજ કેપેસીટી........................જી.બી. તથા વર્કિંગ કોપી માટેની................................કંપનીની પેન ડ્રાઇવ/હાર્ડ ડ્રાઇવ જેની સ્ટોરેજ કેપેસેટી..............છે. તેમા .... નંબરના ગુના/જા.જોગ/એ.ડી ના કામે તા. / /૨૦૧૮ થી લઇ તા. / /૨૦૧૮ ના કલાક / વાગ્યા સુધીની CCTV ફૂટેજ એવીડન્સ એક્ટ ૬૫(ખ) ના ફોર્મ સાથે ફૂટેજની કોપી તેમજ

વર્કિંગ કોપી આપેલી પેન ડ્રાઇવ/હાર્ડડ્રાઇવમાં કોપી કરી આપવા વિનંતી છે. જે આપ સાહેબને વિદિત થાય.

તા. / /૨૦૧૮

પોલીસ સબ ઇન્સપેક્ટર

....

.....

અમદાવાદ શહેર

૪.૩) ભારતીય પુરાવા અધિનિયમ ની કલમ ૬૫-ખ મુજબનું પ્રમાણપત્ર:

જ્યારે વિડિયો રેકૉર્ડિંગ ની કોપી લેવામા આવે એટલે કે આ વીડીયો રેકૉર્ડિંગ ગૌણ પુરાવો હોય તેવા કિસ્સા માં DVR/NVR રેકોર્ડરના માલિક / ઓપરેટર / નેટવર્ક એડમીન / IT પાસેથી તેમની સહીવાળુ 65 (બી) નું સર્ટીફીકેટ લેવુ પડશે. બાકી DVR/NVR રેકોર્ડર કબ્જે કરવાનુ હોય તે કિસ્સા માં આ સર્ટીફીકેટ ની જરુરિયાત રહેતી નથી. પરંતુ પંચો રૂબરૂ પંચનામું કરીને **પંચનામામાં હેશ-વેલ્યુ કાઢીને તેનો ઉલ્લેખ કરવો અને કબ્જે કરવું.**

પ્રમાણપત્રનો નમૂનો

(ભારતીય પુરવા અધિનિયમ, ૧૮૭૨ ની કલમ ૬૫-ખ (૪) (સી) અંતર્ગત)

આથી પ્રમાણીત કરવામાં આવે છે કે.................................... પોલીસ સ્ટેશન ફસ્ટ ગુના.રજી / જા.જોગ / એ.ડી નં .... મુજબના બનાવની તપાસના કામે તમો પોલીસ દ્વારા માંગેલ છે તે (૧) A કેમેરો તા :……\……\……કલાક....\.... (૨) B કેમેરો તા :……\……\……કલાક....\.... (3) C કેમેરા તા :……\……\……કલાક....\.... ના ફૂટેજ તપાસ ના કામે જરુરી હોય જે અંગેના સી.સી.ટી.વી ફૂટેજને સાંકળતો ઈલેક્ટ્રોનિક ડીવાઈસમાંનો રેકર્ડ રૂપાંતરીત ડેટાની ....કંપનીની હાર્ડ ડિસ્ક / પેન ડ્રાઈવમાં (૧) **Acctv.wmv** (૨) **Bcctv.wmv**(3) **Ccctv.wmv** ની ફાઈલો વાળુ રેકર્ડ રૂપાંતરીત નીચે સહી કરનાર દ્વારા...........નામ/માલીકી વાળાની..............જગ્યા પરથી............. કંપનીના DVR / NVR રેકર્ડરના ફૂટેજના મેઇન સર્વરમાથી રૂપાંતરીત કરી સાચો ઉત્પાદિત કરેલ છે.

તેમજ એ પણ પ્રમાણીત કરવામાં આવે છે કે ડેટા ની ઇલેક્ટ્રીક ડીવાઈસની રૂપાંતરીત પ્રક્રીયા મારા સંપુર્ણ નિયંત્રણ હેઠળ હતી અને સુવ્યવસ્થિત કાર્યરત રહેલ તેમજ મૂળ ડેટા પ્રમાણે બરાબર છે અને ફેરફાર કરવામાં આવેલ નથી.

વધુ માં એ પણ પ્રમાણીત કરવામાં આવે છે કે હાર્ડ ડીસ્ક / પેન ડ્રાઈવમાં હકીકત વાળો રૂપાંતરીત ડેટા કલમ ૬૫-ખ-૨(એ) થી ૬૫-ખ-૨(ડી) માં દર્શાવેલ શરતોને અનુસરીને સંપુર્ણ સંતોષકારક રીતે કરવામાં આવેલ છે. ઉપર ની દર્શાવેલ વિગતો સાચી છે .

તા :-

સ્થળ:-

(નોડલ ઓફિસર)

૪.૪) ઘટના સ્થળે પહોંચ્યા બાદ લેવામા આવતા પગલાઓ:

- સૌથી પહેલા બનાવસ્થળ જાણવું તેમજ બનાવ બનવાનો સમય તેમજ તારીખ મેળવવી તથા ફરિયાદી કે સાહેદ પાસેથી બનાવમાં ઉપયોગમા લેવાયેલ વાહનનું વર્ણન તથા આરોપીનું વર્ણન તેમેજ પહેરવેશની માહિતી મેળવવી.
- બનાવ સ્થળે આવવા તથા જવા માટેના તમામ પોઈન્ટ નોધી અલગ અલગ ટીમ બનાવી બધા પોઈન્ટ તરફ કોઈ સી.સી.ટી.વી. કેમેરા આવેલા છે કે કેમ તેની માહિતી મેળવવી.
- બનાવ સ્થળ તથા એન્ટ્રી અને એક્ઝીટ પોઈન્ટ પર આવેલા સી.સી.ટી.વી. કેમેરાનો પ્રકાર જાણવો તેમજ તેનું વિડીયો રેકોર્ડીંગ જે ડી.વી.આર. માં થતું હોય તે ક્યા પ્રકાર નું છે અને ક્યાં આવેલું છે અને તેની માહિતી તેના માલિક / ઓપરેટર / નેટવર્ક એડમીન / ITના માણસ પાસે થી મેળવવી તથા જ્યાં કોઈ ઓપેરટર ના હોય ત્યાં તે સી.સી.ટી.વી. કેમેરા લગાવી

ગયેલ ટેકનીકલ ઓપેરેટર, કંપનીના ટેકનીકલ પર્સનનો સંપર્ક કરવો.

- ડી.વી.આર. સાથે જોડાયેલ મોનીટરમાં તેના માલિક / ઓપરેટર / નેટવર્ક એડમીન / ITના માણસ દ્વારા સૌ પ્રથમ મોનીટરમાં દર્શાવતી તારીખ તથા સમય અને ખરેખર ની તારીખ અને સમય સરખી છે કે કેમ? તે ચકાસવું અને જે કોઈ ફેરફાર હોઈ તે નોંધી લેવો.
- બનાવના સંભવિત સમયના પહેલા થી લઇ અને બનાવ બન્યા પછી ના સમય સુધીના વિડીયો રેકોર્ડીંગ અને જો આ તારીખ અને સમય માં ફેરફાર હોય તો તે ફેરફાર ની ગણતરી કર્યા બાદ ઓપરેટર દ્વારા આ વિડીયો રેકોર્ડીંગ મોનીટરમાં ચકાસવા અને શક્ય હોય તો ફરિયાદી કે સાહેદ ને સાથે રાખી ચકાસવા જેથી તે શંકાસ્પદ વસ્તુઓ જણાવી શકે.
- આ વિડીયો રેકોર્ડીંગમાં કોઈ શંકાસ્પદ તેમજ પુરાવા માં ઉપયોગી ફૂટેજ મળી આવે તો તેની તારીખ અને સમય નોંધી લેવી તેમજ તેને પુરાવાના ભાગ રૂપે કબજે કરવી .

<u>૫. પુરાવાના ભાગરૂપે ફૂટેજ મેળવવા માટેની કાર્યવાહી:</u>

<u>*૫.૧) સી સી ટી વી રેકોર્ડર બાબતે લેવાની તકેદારીઓ :*</u>

- સી.સી.ટી.વી. રેકોર્ડરને તેના જાણકાર ઓપરેટર / નેટવર્ક એડમીન / IT નો માણસ પાસેજ ઓપરેટ કરાવુ.

- સી.સી.ટી.વી. રેકોર્ડરમાં અમુક સીમિત સમયગાળા ના દિવસોનું જ રેકોર્ડીંગ થતુ હોય છે જેથી ફૂટેજનું ઓવરરાઇટ થતા પહેલા બેકઅપ લઇ લેવું તેમજ પુરાવા તરીકે જરુરિયાત હોય તો ત્વરિત કાર્યવાહી કરવી.
- વાસ્તવિક વર્તમાન તારીખ અને સમય (સંદર્ભ ઘડિયાળમાંથી) નોંધ કરો. જો તપાસ માટે ચોક્કસ સમય મહત્વના હોય તો http://www.nplindia.in/time-and-frequency-standards વેબસાઈટ માંથી ચોક્કસ સમય મેળવી શકો છો.
- ડીફોલ્ટ ID અને PAASWORD તેના જાણકાર ઓપરેટર / નેટવર્ક એડમીન / IT નો માણસ પાસેથી મેળવી લેવા અને જો ના મળી શકે તો તે કિસ્સામા ૨ (બે) થી વધુ વખત ID અને PAASWORD નાખવો નહીં.
- તપાસના કામે વિડીયો ફુટેજ લીધેલા હોય તો બીજી જગ્યા ના વિડીયો ફુટેજ લેતા પહેલા પેન ડ્રાઈવ/ હાર્ડડ્રાઈવ ફોર્મેટ કરી બીજી જગ્યાના વિડીયો ફુટેજ કોપી કરવા.

<u>૫.૨) સી.સી.ટી.વી. રેકોર્ડરમાંથી હાર્ડડ્રાઈવ /પેનડ્રાઈવ માં વિડીયો રેકોર્ડીંગ ની નકલ લેવા બાબત:</u>

- FSLમાં મોકલી શકાય તે માટે એક સીલબંધ હાર્ડડીસ્ક/પેનડ્રાઈવ અને વર્કિંગ કોપી (જે તપાસનાં કામે આપણા માટે ઉપયોગી બની શકે) માટે એક જુદી હાર્ડ

ડીસ્ક/પેન ડ્રાઈવ ખરીદવી, અને એક કરતા વધુ ડી.વી.આર. માંથી ફૂટેજો લેવાની હોય તે મુજબ ખરીદવી. તેમજ આ હાર્ડ ડીસ્ક/પેનડ્રાઈવ ને કોઈ પણ ડીવાઈસ સાથે કનેક્ટ કરવી નહીં.

- આ ખરીદેલી હાર્ડ ડીસ્ક /પેનડ્રાઈવ નાં બીલની નકલ તપાસમાં સામેલ રાખવી.
- સૌપ્રથમ ઓપરેટર / નેટવર્ક એડમીન / IT ના માણસ ને ફૂટેજ મેળવવા માટેની યાદી આપવી તેમજ તેની સાથે કોપી કરવા માટે સીલબંધ હાર્ડ ડીસ્ક/ પેન ડ્રાઈવ આપવી.
- કોપી કરેલ તમામ વિડીયો ફૂટેજ ફાઇલની હેશ-વેલ્યુની તેમજ જે સોફ્ટવેર દ્વારા હેશ-વેલ્યુ કાઢવામાં આવેલ હોઈ તે સોફ્ટવેર નું નામ અને વર્ઝનની વિગતની નોંધ પંચનામામાં કરવી.
- તમામ ફાઇલની હેશ-વેલ્યુ વાળા પત્રક પર પંચોની તેમજ તપાસ કરનાર અધિકારીની સહી લેવી .
- કોપી થઈ ગયેલ હાર્ડ ડીસ્ક/ પેન ડ્રાઈવ ને કોઈ પણ ડીવાઈસ સાથે કનેક્ટ કર્યા વગર પંચો રૂબરૂ હાર્ડ ડીસ્ક/ પેન ડ્રાઈવનાં સંપૂર્ણ વર્ણન સાથે સીલ કરી કબ્જે કરવી અને વર્કિંગ કોપી કરેલી હાર્ડ ડીસ્ક/ પેન ડ્રાઈવનો ઉપયોગ તપાસના કામે કરી શકાય છે.
- તેમજ જેની પાસેથી સી.સી.ટી.વી. ફૂટેજ કોપી કરી હાર્ડ ડીસ્ક/ પેન ડ્રાઈવમા લેવામાં આવેલ છે તેમની પાસેથી ભારતીય પુરાવા અધીનાયમ ૧૮૭૨ ની કલમ ૬૫-ખ મુજબની

સહીવાળું સર્ટીફિકેટ પંચનામા વખતે મેળવી લેવું અને તપાસમાં સામેલ રાખવું.

- આ વર્કિંગ કોપી કરેલી હાર્ડ ડીસ્ક/ પેન ડ્રાઈવ માં આવેલ વિડીયો ફૂટેજનું વિશ્લેષણ કરી તેના આધારે એફ.એસ.એલ.માં પુછવા અંગેના પ્રશ્નો અંગેની પ્રશ્નોત્તરી તૈયાર કરવી, જેથી તપાસના કામે જરૂરીયાત મુજબના પુરાવાઓ મેળવી શકાય છે.
- આ પંચો રૂબરૂ કબ્જે કરેલ સીલબંધ હાર્ડ ડીસ્ક/ પેન ડ્રાઈવ, પંચનામાંની પ્રમાણિત નકલ, એફ.આઇ.આર. ની પ્રમાણિત નકલ, પુરાવા અધીનાયમ ૧૮૭૨ ની કલમ ૬૫-ખ મુજબની સર્ટીફિકેટની પ્રમાણિત નકલ તેમજ એફ.એસ.એલ. માં પુછવાં માટેની પ્રશ્નોત્તરીવાળું પત્રક એફ.એસ.એલ. ખાતે મોકલી આપવું.

<u>૬. DVR/NVR રેકોર્ડર તપાસના કામે કબ્જે લેતી વખતે:</u>

- DVR/NVR રેકોર્ડર ને જ્યારે પુરાવા તરીકે કબ્જે કરવા નુ હોય ત્યારે DVR/NVRના મૉનિટર માં જે તારીખ અને સમય અને ખરેખરના વાસ્તવિક તારીખ અને સમય વચ્ચેનો ફેરફારની નોંધ પંચનામામાં કરવી. જો તપાસ માટે ચોક્કસ સમય મહત્વના હોય તો http://www.nplindia.in/time-and-frequency-standards વેબસાઈટ માંથી ચોક્કસ સમય મેળવી શકો છો.

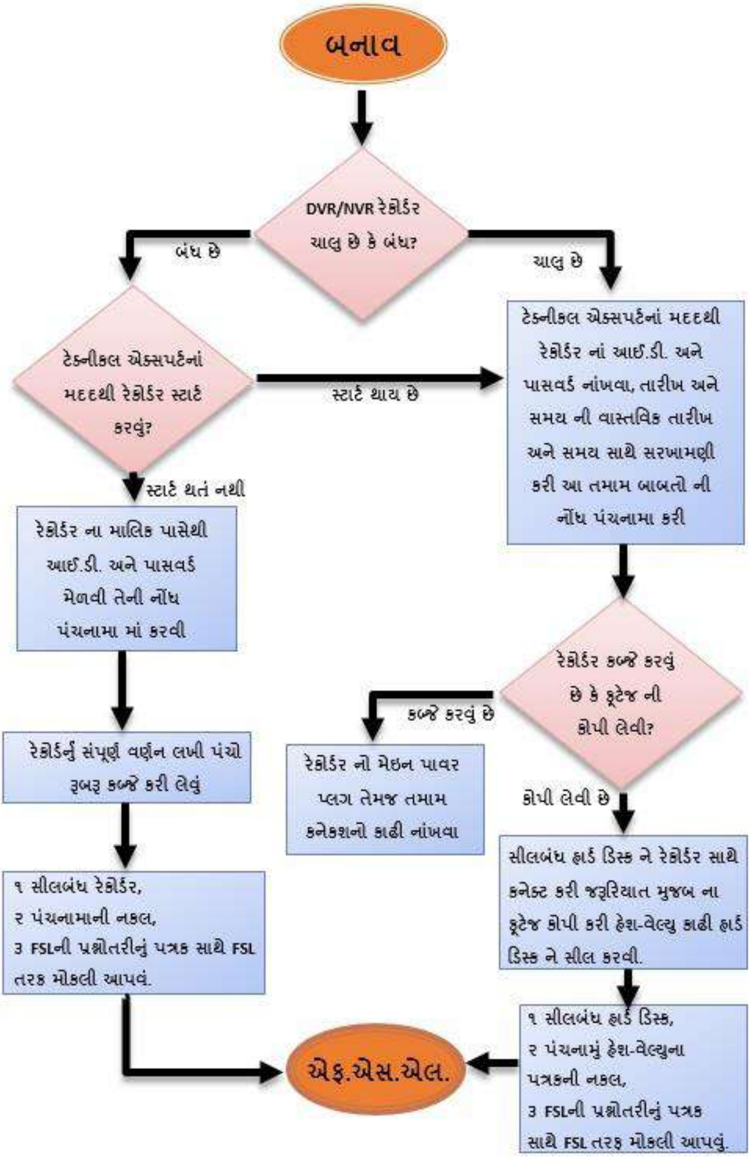
- DVR/NVR રેકોર્ડરના ID અને PASSWORD માલિક / ઓપરેટર / નેટવર્ક એડમીન / ITના માણસો પાસેથી મેળવવા. તેનાં ID અને PASSWORD ની નોંધ પંચનામામાં કરવી. અને DVR/NVRરેકોર્ડર ચાલૂ કે બંધ હાલત માં છે તેની નોંધ પણ કરવી.
- ID અને PASSWORD માલિક / ઓપરેટર / નેટવર્ક એડમીન / ITના માણસો પાસેથી મળી શકે તેમ ના હોય તો પંચો રૂબરૂ કંપનીના ડિફોલ્ટ ID અને PASSWORD નાખવા અને તેનાથી રેકોર્ડર અનલોક થઈ જાય તો તે ID અને PASSWORD ની નોંધ પંચનામામાં કરવી.
- ત્યારબાદ DVR/NVR રેકોર્ડરની મુખ્ય પાવર સ્વીચ બંધ કરી પાવર પ્લગ કાઢી નાખવો અને ત્યાર બાદ કેમેરા ના તેમજ મોનીટરના તમામ કનેક્શનો DVR/NVR રેકોર્ડરમાંથી કાઢી નાખવા.
- DVR/NVR રેકોર્ડરના પાવર ચાર્જર પણ સાથે અચૂકપણે લઈ લેવું.
- DVRછે કે NVRતેની વિગત રેકોર્ડર પર લખેલી હોય છે. તેમ છતા આઇ.પી. કેમેરા અને જો રેકોર્ડરમાં પાછળના ભાગે લેન પ્રકાર ની વિડિયો ચેનલ સોકેટ હશે તો તે NVR રેકોર્ડર છે, અને વર્તુળાકારમાં વિડિયો ચેનલ હશે તો તે DVR રેકોર્ડર છે.

NVR RECORDER

DVR RECORDER

- આ DVR/NVRરેકોર્ડર પર લખેલી તમામ વિગતો જેવી કે કમ્પનીનું નામ , સિરિયલ નં , મેન્યુફેક્ચર તારીખ, સ્ટોરેજ કેપેસિટી, જોડેલા સી.સી.ટી.વી. કેમેરાની સંખ્યા જેવી વિગતો પંચનામામાં નોંધવી.

આ DVR/NVRરેકોર્ડર અને તેના પાવર ચાર્જરને પંચો રૂબરૂ સીલબંધ કવરમાં સીલ કરી ,પંચનામાંની પ્રમાણિત નકલ, એફ.આઇ.આર ની પ્રમાણિત નકલ તેમજ એફ.એસ.એલ માં પુછવા માટેની પ્રશ્નોત્તરીવાળું પત્રક સાથે એફ.એસ.એલ ખાતે મોકલી આપવું.


બનાવ
DVR/NVR રેકોર્ડર ચાલુ છે કે બંધ?
બંધ છે
ચાલુ છે
ટેક્નીકલ એક્સપર્ટનાં મદદથી રેકોર્ડર સ્ટાર્ટ કરવું?
સ્ટાર્ટ થાય છે
ટેક્નીકલ એક્સપર્ટનાં મદદથી રેકોર્ડર નાં આઈ.ડી. અને પાસવર્ડ નાંખવા, તારીખ અને સમય ની વાસ્તવિક તારીખ અને સમય સાથે સરખામણી કરી આ તમામ બાબતો ની નોંધ પંચનામા કરી
સ્ટાર્ટ થતું નથી
રેકોર્ડર ના માલિક પાસેથી આઈ.ડી. અને પાસવર્ડ મેળવી તેની નોંધ પંચનામા માં કરવી
રેકોર્ડર કબ્જે કરવું છે કે ફૂટેજ ની કોપી લેવી?
કબ્જે કરવું છે
રેકોર્ડરનું સંપૂર્ણ વર્ણન લખી પંચો રૂબરૂ કબ્જે કરી લેવું
રેકોર્ડર નો મેઇન પાવર પ્લગ તેમજ તમામ કનેકશનો કાઢી નાંખવા
કોપી લેવી છે
સીલબંધ હાર્ડ ડિસ્ક ને રેકોર્ડર સાથે કનેક્ટ કરી જરૂરિયાત મુજબ ના ફૂટેજ કોપી કરી હેશ-વેલ્યુ કાઢી હાર્ડ ડિસ્ક ને સીલ કરવી.
૧ સીલબંધ રેકોર્ડર, ૨ પંચનામાની નકલ, 3 FSLની પ્રશ્નોતરીનું પત્રક સાથે FSL તરફ મોકલી આપવું.
૧ સીલબંધ હાર્ડ ડિસ્ક, ૨ પંચનામું હેશ-વેલ્યુના પત્રકની નકલ, 3 FSLની પ્રશ્નોતરીનું પત્રક સાથે FSL તરફ મોકલી આપવું.
એફ.એસ.એલ.

૭. સી.સી.ટી.વી. બાબતનાં FSL માં પૂછવાના પ્રશ્નોતરીનું ચેકલીસ્ટ:

FSL માં પ્રશ્નોતરી કરતી વખતે બનાવની અંદરની તમામ વિગતોનું વર્ણન કરવું જેમ કે ઉપયોગ થયેલા હથિયારો, કેટલા ઇસમો હતા, તેમના પહેરવેશનું વર્ણન, તેના શરીર નો બાંધો, વાહનનું વર્ણન, બનાવ ની વિગત, વગેરે.

૭.૧) DVR/NVR રેકોર્ડર બાબતનાં FSL માં પૂછવાના પ્રશ્નો :

- આપેલા DVR/NVR રેકોર્ડરમાં રહેલી વિડીયો ફૂટેજમાં કોઈપણ પ્રકારની છેડછાડ થયેલ છે કે કેમ ?
- આપેલા DVR/NVR રેકોર્ડરના તારીખ અને સમય ચકાસી આ તારીખ અને સમયમાં કોઈ ફેરફાર કરેલ છે કેમ ?
- આપેલા DVR/NVR રેકોર્ડરના તારીખ અને સમય સાથે વાસ્તવિક તારીખ અને સમયમાં કેટલો તફાવત છે ?
- કલાક ....\..... તારીખ .....\.....\.........નાં અરસામાં .... બનાવ બનેલ હોય જે બનાવને લગતા વિડીયો ફૂટેજ DVR/NVR રેકોર્ડરમાં છે. જે વિડીયો ફૂટેજમાં ઇસમોના ચિત્રો સ્પષ્ટ કરી આપવા .
- આપેલા DVR/NVRરેકોર્ડર અથવા કોપીમાં કલાક ...\..... તારીખ .....\.....\......... નાં અરસામાં .... બનાવ બનેલ હોઈ તે બનાવમાં વપરાયેલ વાહનના રજીસ્ટ્રેશન નંબર સ્પષ્ટ કરી આપવા અને વાહનનો પ્રકાર, મોડેલ નંબર, કંપની જોઈ શકાય તેવા ચિત્રો સ્પષ્ટ કરી આપવા.

૭.૨) DVR/NVR રેકોર્ડરમાંથી હાર્ડ ડિસ્ક/પેન ડ્રાઈવ/DVD માં કરેલ કોપી બાબતના FSL માં પૂછવાનાં પ્રશ્નો:

- આપેલા હાર્ડ ડિસ્ક/પેન ડ્રાઈવ/DVD કોપીમાં રહેલી વિડીયો ફૂટેજમાં કોઈ પણ પ્રકારની છેડછાડ થયેલ છે કે કેમ ?
- આપેલા હાર્ડ ડિસ્ક/પેન ડ્રાઈવ/DVD કોપીમાં રહેલી (૧).............WMV નામવાળી ફાઈલમાં કલાક ...\..... તારીખ .....\.....\.........નાં અરસામાં .... બનાવ બનેલ (૨).............WMV નામવાળી ફાઈલમાં કલાક ...\..... તારીખ .....\.....\.........નાં અરસામાં .... બનાવ બનેલ હોઈ જે બનાવમાં રહેલા ઇસમોના ચેહરાઓના ચિત્રો સ્પષ્ટ કરી આપવા .
- આપેલા હાર્ડ ડિસ્ક/પેન ડ્રાઈવ/DVD કોપીમાં રહેલી (૧).............WMV નામવાળી ફાઈલમાં કલાક ...\..... તારીખ .....\.....\.........નાં અરસામાં .... બનાવ બનેલ (૨).............WMV નામવાળી ફાઈલમાં કલાક ...\..... તારીખ .....\.....\.........નાં અરસામાં .... બનાવ બનેલ હોઈ તે બનાવ માં વપરાયેલ વાહનના રજીસ્ટ્રેશન નંબર સ્પષ્ટ કરી આપવા અને વાહનનો પ્રકાર, મોડેલ નંબર, કંપની જોઈ શકાય તેવા ચિત્રો સ્પષ્ટ કરી આપવા .

૮. પેન ડ્રાઈવ ને ડી વી આર. સાથે જોડયા બાદ બેકઅપ (backup) અને નિકાસ (export) કરવા માટે ની પ્રક્રિયા:

(૧) વેબ બ્રાઉઝર દ્વારા ડીવીઆર નો ઍક્સેસ મેળવી શકાય છે. તે પછી વેબ બ્રાઉઝર ખોલો, ડીવીઆર ના IP address ને ઇનપુટ કરો અને પછી Enter દબાવો. લૉગ-ઇન ઈન્ટરફેસ દેખાય છે તેમાં યુઝરનેમ નામ અને પાસવર્ડ ઇનપુટ કરો, અને લૉગ-ઇન બટન ક્લિક કરો.

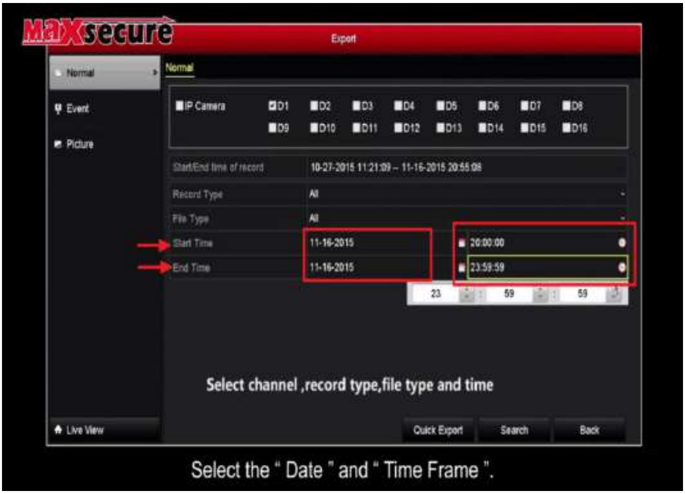
(૨) માઉસ ની જમણી / રાઈટ બટન દબાવો અને Menu પર ક્લિક કરો.

(૩) ઓપન થયેલ વિન્ડો માંથી Export બટન પર ક્લિક કરો.

(૪) ઓપન થયેલ વિન્ડોમાં બધી ચેનલ ની માહિતી મળી જશે ત્યાર બાદ કેસ ની જરૂરિયાત મુજબ ની ચેનલ શોધો અને નોંધ કરો.

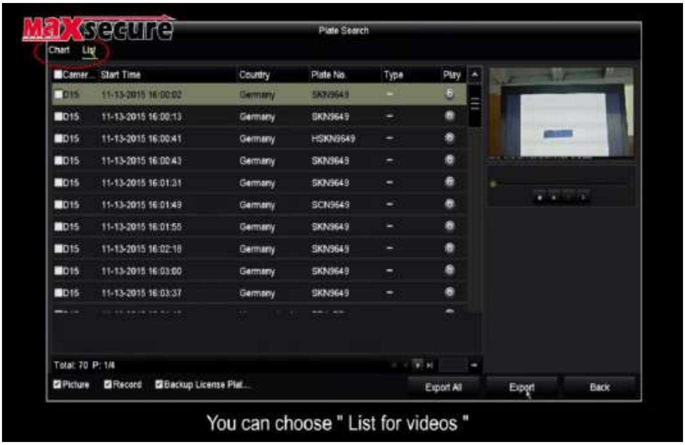
(૫) બધી ચેનલ ની લીસ્ટ માંથી જરૂરિયાત મુજબ ની ચેનલ પર ટીક માર્ક કરો અને બાકીની ચેનલ પરના ટીક માર્ક દુર કરો.

(૬) કેસ ની જરૂરિયાત પ્રમાણે Start Time (ફૂટેજ ચાલુ થવાનો સમય / તારીખ) અને End Time (ફૂટેજ પુરા થયેના સમય / તારીખ) સિલેક્ટ કરો.



(૭) ત્યાર બાદ નીચે રહેલ Search બટન પર ક્લિક કરો.

(૮) Search પર ક્લિક કર્યા બાદ નીચે મુજબ ની સ્ક્રીન જોવા મળશે તેમાં દરેક રેકોર્ડ થયેલા ફૂટેજ નું પૂરું લીસ્ટ આવી જશે તેમાંથી કેસ ની જરૂરિયાત પ્રમાણે ના ફૂટેજ સિલેક્ટ કરો અને નીચે રહેલ Export બટન પર ક્લિક કરો.



(૯) ત્યાર બાદ નીચે મુજબ ની સ્ક્રીન જોવા મળશે. તેમાં આપણે સાથે લઇ ગયેલા સ્ટોરેજ ડિવાઈસને સિલેક્ટ કરો અને જે ફોરમેટમાં વિડીયો જોઇએ છે એ ફોરમેટ સિલેક્ટ કરો. બને ત્યાંસુધી MP4 કે AVI ફોરમેટ સિલેક્ટ કરવું. અને ત્યારબાદ Export બટન પર ક્લિક કરો.

(૧૦) ત્યાર બાદ Export થવાનું શરુ થઈ જશે અને પ્રોસેસ પૂરી થાય ત્યાં સુધી રાહ જોવી.

(૧૧) Export સંપૂર્ણપણે થઇ જાય ત્યાર બાદ નીચે મુજબ ની વિન્ડો જોવા મળશે.

જો ઘટનાસ્થળે બેકઅપ(backup) અને નિકાસ(export) લેવા માં કોઈ સમસ્યા થાય તો નિષ્ણાંત નો સંપર્ક સાધો અથવા ડિવાઈસને સાથે લઇ જવું અને જે તે નિષ્ણાંત ને આપવું. તે દરમિયાન તેને યોગ્ય લેબલ આપવુ અને નોંધ લેવી.

૯. DVR/NVRરેકોર્ડર કમ્પનીના ડીફોલ્ટ યુઝરનેઈમ પાસવર્ડ:

મેનુફેક્ચરર નું નામ	યુઝરનેઈમ	પાસવર્ડ
3xLogice	Admin	12345
ACTi	Admin or admin	123456
American Dynmics	admin	Admin
Arecont Vision	admin	no set password

Avigilon	admin	Admin
Axis	Root	pass or no set password
Basler	admin	Admin
Bosch	service	Service
Bosch	Dinion	no set password
Brickcom	admin	Admin
Canon	root	Model# of camera
CBC Ganz	admin	Admin
Cisco	no default	no set password
CNB	root	Admin
Costar	root	Root
Dahua	admin	Admin
Digital Watchdog	admin	admin
DRS	admin	1234
DVTel	Admin	1234
DynaColor	Admin	1234
FLIR	admin	fliradmin
Foscam	admin	[leave blank]

GeoVision	admin	Admin
Grandstream	admin	admin
GVI	Admin	1234
HIKVision	admin	12345
Honeywell	Administrator	1234
IOImage	admin	admin
IPX-DDK	root	Admin or admin
IQInvision	root	system
JVC	admin	Model# of camera
LTS Security	admin	123456
March Networks	admin	[leave blank]
Merit Lilin Camera	admin	pass
Merit Lilin Recorder	admin	1111
Messoa	admin	Model# of camera
Mobotix	admin	meinsm
Northern	admin	12345

Panasonic	admin	12345
Panasonic	admin1	password
Pelco	admin	admin
PiXORD	admin	admin
PiXORD	root	pass
QVIS	Admin	1234
Samsung	root	4321 or admin
Samsung	admin	4321 or 1111111
Sanyo	admin	admin
Sentry360	Admin	1234
Sony	admin	admin
Speco	root	Root
Speco	admin	Admin
StarDot	admin	Admin
Starvedia	admin	no set password
Toshiba	root	ikwb
Trendnet	admin	admin
UDP	root	unknown

Ubiquiti	ubnt	ubnt
W-Box	admin	wbox123
Wodsee	admin	[leave blank]
Verint	admin	admin
VideoIQ	supervisor	supervisor
Vivotek	root	no set password

પ્રકરણ-૪

ઇન્ટરનેટ અને IP Address

પ્રકરણનો ઉદ્દેશ: વિવિધ ગુનાઓ ની તપાસ માં ઇન્ટરનેટ અને સંલગ્ન સેવાઓ થી અગત્ય ના પુરાવા મેળવી શકાય, અને ઇન્ટરનેટ આધુનિક સમય માં તપાસ નુ અભિન્ન અંગ બની ગયેલ છે. આ ક્ષેત્ર માંથી આધારભૂત પુરાવા એકત્ર કરવા સારૂ આ પ્રકરણમાં માર્ગદર્શિકા આપવામાં આવી છે.

૧. વેબસાઇટ્સ, ફોરમ અને બ્લોગ્સને લગતાં ગુનાઓ:

જ્યારે કોઇ ગુનો વેબસાઇટ પર મુકેલ પુરાવાને લગતો હોય તો આવા પુરાવાને મેળવવા માટેની સૌથી સરળ રીત છે કે કોઇ તાલીમબદ્ધ વ્યક્તિની મદદ લઇને વેબસાઇટની મુલાકાત લઇ પુરાવાની નકલ મેળવવી જોઇએ. આ માટે આ બાબતનાં તપાસ અધિકારીએ વેબસાઇટનું એડ્રેસ મેળવવું. ઉ.દા.https://police.gujarat.gov.in અથવા વેબસાઇટનું કોઇ ચોક્કસપેજઉ.દા.https://police.gujarat.gov.in/dgp/CMS.aspx?Content_id=3678. જ્યારે આવો પુરાવો મેળવવા માટેની કાર્યવાહી કરવામાં આવે છે ત્યારે તે બાબત ખૂબ જરૂરી છે કે પંચનામા અને કેસ ડાયરીમાં તપાસકર્તા દ્વારા આ તમામ ઓડીટ ટ્રેલની નોંધ કરવી. વેબસાઇટની કોપી કરવા માટે વેબસાઇટની મુલાકાત લેવી અને વિડિયો કેપ્ચર સોફ્ટવેરનો ઉપયોગ કરીને

સંબંધિત પેજીસને રૅકર્ડ કરવા જેથી વેબસાઇટની મુલાકાત સમયે તે કેવી દેખાય છે એ દ્રશ્યમાન થાય. જો વિડિયો કેપ્ચર સોફ્ટવેર ઉપલબ્ધ ન હોય તો આ વેબપેજીસના સ્ક્રીનશોટ લઇને પણ સાચવી શકાય. વેબપેજીસને મેળવવા માટે વેબસાઇટ કોપી સોફ્ટવેરનો ઉપયોગ કરવો અથવા પ્રત્યેક વેબપેજને સેવ કરવાં એ પણ સલાહભર્યું છે. વેબપેજીસને કોપી કરવા અને તેનાં વિઝ્યુઅલ રૅકર્ડ મેળવવાથી વેબપેજનો કોડ પણ સુરક્ષિત રહે છે જે પાછળથી ઉપયોગમાં આવી શકે છે. જો તપાસકર્તા અધિકારીને એમ જણાય કે ઉપરોક્ત પદ્ધતિને અનુસરવાથી વેબસાઇટ પરથી પુરાવો નષ્ટ થઇ જશે તો બે પંચની હાજરીમાં ઉપલબ્ધ કોઇ પણ રીતે (પ્રિન્ટ, સ્ક્રીનશોટ અથવા વેબપેજ સેવ કરવા) પુરાવાની કોપી કરી લેવી જોઇએ. ઉપરોક્ત પગલાં લેતા પહેલાં આ કામ માટે નિષ્ણાત વ્યક્તિની સેવાઓ મેળવવાના પ્રત્યેક પ્રયત્નો કરવા જોઇએ. માહિતીને સચોટ રીતે મેળવવામાં નિષ્ફળ રહેવાથી તપાસ પર ગંભીર અસર પડી શકે છે. સાઇટની મુલાકાત લઇને પુરાવા કબજે કરવાના સાથો-સાથ અધિકારક્ષેત્રમાં જરૂરી એવી કોઇપણ કાયદાકીય કાર્યવાહી જેવી કે MLAT/LR/SECTION 91 ની નોટિસ દ્વારા વેબસાઇટના માલિકને પુરાવા આપવા સત્તાવાર વિનંતી પણ કરવાની હોય છે. આ પ્રક્રિયા કરતા પહેલા, આ વેબસાઈટ ક્યા સર્વર માં હોસ્ટેડ છે, અને આ સર્વર ક્યા દેશ માં સ્થિત છે તે જાણવુ જરૂરી છે. આ જાણવા માટે Domain Name Server ની તપાસ માટે અનેક ફ્રી-વેબટુલ્સ ઉપલબ્ધ છે, ઉ.દા. www.dnsstuff.com. એવા ફ્રીટૂલ્સ થી વેબપેજ ના સર્વર અને

જિયો-લોકેશન મેળવી શકાય. તે મેળવ્યા પછી, અગાઉ ના પ્રકરણ માં જણાવ્યા અનુસાર MLAT/LR/SECTION 91 ની નોટીસ ની પ્રક્રીયા હાથ ધરવી.

વેબસાઇટ હોસ્ટ કરનાર સર્વિસ પ્રોવાઇડરને વિનંતી કરવાથી વેબપેજ અથવા પોસ્ટ કોણે બનાવી છે? તેનો પુરાવો મેળવી શકાય છે. હોસ્ટ દ્વારા યુઝરની વિવિધ માહિતી જેવી કે નામ, સરનામું, ફોન નંબર, બેંકની માહિતી, ઇ-મેઇલ સરનામું વગેરેનો રેકર્ડ રાખવો એ સામાન્ય બાબત છે. વેબસાઇટ પર કેટલીક પ્રવૃતિઓ કોણે કરી છે? ઉ.દા. વેબસાઇટ પરથી સામાન ખરીદવા અથવા મેસેજ પોસ્ટ કરીને કોઇ છેતરપીંડી કરવામાં આવી હોય, તે ઓળખવા માટે વેબસાઇટના રેકર્ડ પરથી શકમંદની શોધ કરવી સંભવ છે. જ્યારે કોઇપણ યુઝર ઇન્ટરનેટનો ઉપયોગ કરેછે ત્યારે તેને એક અનન્ય સરનામું જેને IP Adress કહેવાય છે એ ફાળવવામાં આવે છે અને સર્વીસ પ્રોવાઇડર કોઇપણ IP Adressને સંલગ્ન માહિતી જેવી કે સમય, તારીખ અને યુઝરની ઓળખનો રેકર્ડ રાખે છે. જ્યારે યુઝર એક વેબસાઇટની મુલાકાત લે છે અને કોઇ પ્રવૃત્તિ કરે ઉ.દા. લોગ-ઇન કરે, મેસેજ પોસ્ટ કરે અથવા કોઇ ખરીદી કરે તો વેબસાઇટ દ્વારા યુઝરના IP Adress ની માહિતી રેકર્ડ કરી લેવામાં આવે છે. આ માહિતી મેળવ્યા પછી, IP Adress થી user ને ટ્રેસ/ઓળખવાની પ્રક્રીયા આગળ જણાવવામાં આવી છે.

૨. ઈ-મેઇલ સંચારનો ઉપયોગ થતો હોય તેવા ગુનાઓ:

સામાન્ય રીતે ઇ-મેઇલ મોકલવા-મેળવવાની બે પદ્ધતિઓ છે. પ્રથમ પદ્ધતિમાં વેબ બ્રાઉઝરનો ઉપયોગ કરીને ઇ-મેઇલ એક્સેસ કરવામાં આવે છે. ઉદા. હોટમેલ, વિન્ડોઝલાઇવ, યાહુ અથવા ગુગલની વેબસાઈટ. આ પદ્ધતિમાં ઇ-મેઇલ વેબ મેઈલ સર્વરમાં સ્ટોર થાય છે અને યુઝર બ્રાઉઝરની મદદથી વાંચી શકે છે. બીજી પદ્ધતિમાં આઉટલુક કે વિન્ડોઝ મેઈલ જેવા પ્રોગ્રામનો ઉપયોગ કરી ઇ-મેઇલ એક્સેસ કરી શકાય છે, જેમાં મેઈલ યુઝરના કોમ્પ્યુટરમાં ડાઉનલોડ થયાબાદ લોકલ સિસ્ટમમાં સ્ટોર થાય છે. જે કેસમાં પુરાવા તરીકે, પોલીસ જેને ટ્રેસ કરવા માંગતી હોય તેવા વ્યક્તિ દ્વારા મોકલેલ ઈ-મેઈલ હોય ત્યારે ચાવીરૂપ પુરાવો તે ઈ-મેઈલના Full Internet Header માંથી મળે છે. ઈન્ટરનેટ મારફતે મોકલાયેલ દરેક ઈ-મેઈલ સામાન્ય રીતે એક હેડર ધરાવતું હોય છે, જે સામાન્ય યુઝર માટે વિઝીબલ હોતું નથી. આ હેડરમાં ઇ-મેઇલ મોકલનારનું IP Address તથા ઇ-મેઇલના સંપૂર્ણ રૂટની વિગતો હોઈ શકે છે. જ્યાં ખોટી વિગતોથી બનાવેલ ઇ-મેઇલ એડ્રેસથી ઇ-મેઇલ મોકલાયેલ હોય તેવા કિસ્સાઓમાં પણ ઇ-મેઇલ મોકલનારને Full Internet Header ની મદદથી ઘણીવાર ઓળખી શકાય છે. Full Internet Header મેળવવા માટે બનાવનો અહેવાલ કરનાર કે ઇ-મેઇલ મેળવનાર વ્યક્તિ ઇ-મેઇલ અંગેની કઈ પદ્ધતિ વાપરે છે એવી વિગતથી માહિતગાર હોવી જોઈએ. જો વેબ આધારિત પદ્ધતિ વાપરવામાં આવતી હોય તો વેબમેલ હોસ્ટ

(ઉદા. હોટમેલ, યાહૂ વગેરે) અથવા જો પ્રોગામ વાપરવામાં આવતો હોય તો આ પ્રોગામનો વર્ઝન નંબર. પ્રોગમનો વર્ઝન નંબર Help →About મેનુમાંથી મળી શકે. દરેક વેબમેલ સર્વિસ પ્રોવાઇડર તથા ઇ-મેઇલ પ્રોગ્રામ Full Internet Header સાથે અલગ અલગ રીતે વર્તે છે. આથી જો તપાસ અધિકારી અથવા યુઝર Full Internet Header ને કેવી રીતે દર્શાવવું તે બાબતથી અજાણ હોય તો તેઓએ વેબમેલ સર્વિસ પ્રોવાઇડર અથવા પ્રોગામ અંગેની વિગતો, ટેકનિકલ અથવા તાલીમ પામેલ વ્યક્તિને મોકલી આપી તેઓની પૂરતી સલાહ મેળવવી જોઈએ. જયારે હેડર મળી જાય ત્યારે હેડર સાથેના ઇ-મેઇલની પ્રિન્ટ કાઢી સેવ કરી લેવી જોઈએ. કેસની ગંભીરતા તથા ઇ-મેઇલ ના પુરાવા તરીકેના મહત્વ અનુસાર ઇ-મેઇલ પુરાવાને સંગ્રહિત કરવા તથા જાળવી રાખવા ફોરેન્સિક નિષ્ણાતોનો અભિપ્રાય મેળવવો જોઈએ. જયારે Full Internet Header ની માહિતી મળી જાય ત્યારે તાલીમ પામેલ અથવા ટેકનિકલ પોલીસ અધિકારી, ઇ-મેઇલ મોકલનારના IP Address ની મદદથી આવી વ્યક્તિ વિરુદ્ધ તપાસ હાથ ધરી શકે છે. (IP Address અંગેની પદ્ધતિની હવે પછી ચર્ચા કરેલ છે.)

જયારે શંકાસ્પદનું ઇ-મેઇલ એડ્રેસ જાણમાં હોય પરંતુ Full Internet Header મેળવી શકાય તેવો ઇ-મેઇલ પ્રાપ્ય ન હોય ત્યારે ઇ-મેઇલ એડ્રેસના યુઝર અને એના લોકેશનની ઓળખ કરવી શક્ય છે. ઇ-મેઇલ સર્વિસ પ્રોવાઇડર યુઝરના પ્રથમવાર IP

Address રજીસ્ટ્રેશન સમયે તથા ત્યારબાદના સમયગાળામાં IP Addressની લોગ-ઇન હિસ્ટ્રીની સાથે સાથે યુઝર અંગેની અન્ય માહિતીનો પણ રૅકર્ડ રાખતા હોય છે જે અંગે ઇ-મેઇલ સર્વિસ પ્રોવાઇડરની કચેરીના સત્તાધીશ વ્યક્તિને વિનંતી કરી ઇ-મેઇલ એડ્રેસ સંબંધિત વિગતો મેળવી શકાય છે. (જીવનું જોખમ અને આતંકવાદ વગરેને સંલગ્ન એવા ઘણા કિસ્સાઓમાં લો એન્ફોર્સમેન્ટ એજન્સી ના ઓફીશિયલ ઇ-મેઇલ મારફતે કરવામાં આવેલ અરજીઓમાં ઇ-મેઇલ સર્વિસ પ્રોવાઈડર વળતો જવાબ આપે છે. વેબ સર્વિસ પ્રોવાઈડર્સની વેબસાઈટ પરથી નીતિ અંગેની માર્ગદર્શિકા તથા વિનંતી અરજી અંગેની પદ્ધતિ વિષે માહિતી મેળવી શકાય છે.) ઘણા કિસ્સાઓમાં આરોપી ની પૂછ-પરછ થી તપાસ એજન્સીને યુઝરના/આરોપીના ઇ-મેઇલ એકાઉન્ટની Id-login અને password મળે છે, અને તે આધારે ઈ-મેલ એક્સેસ કરી શકાય છે (જે ભારતીય પુરાવા અધિનિયમની કલમ ૨૭ અનુસાર આરોપીના કિસ્સામાં સ્વીકાર્ય છે.) આરોપી ના વેબ-બ્રાઉઝર માં મૌજૂદ ઈ-મેઈલ ને THUNDERBIRD CLIENT જેવી એપ્લીકેશનના માધ્યમથી ડાઉનલોડ કરી શકાય અને તેવા કિસ્સામાં ટેકનિકલ વ્યક્તિ અથવા ફોરેન્સિક અધિકારીને બોલાવવા એ સલાહભર્યું છે. ત્યારબાદ સંબધિત ડિજિટલ પુરાવાની પ્રિન્ટઆઉટ અને ડિજિટલ કોપી અગાઉના પ્રકરણોમાં સૂચવ્યા મુજબની પદ્ધતિ અનુસાર જપ્ત કરવી જોઈએ.

૩. ઈન્ટરનેટ ચેટ ધરાવતા ગુના:

વપરાશકર્તા ઈન્ટરનેટ પર ચેટ કરવા માટે ઘણા બધા ડિવાઈસ વાપરી શકે છે. ચેટ કરવા માટેની મુખ્ય ત્રણ રીત છે: વેબસાઇટ ચેટની વ્યવસ્થા વાપરીને, દા.ત. ફેસબુક; વિન્ડોસ લાઈવ મેસેન્જર જેવા ઈનસ્ટન્ટ મેસેન્જર પ્રોગ્રામ વાપરીને; અથવા સામાન્ય રીતે ઘણો ઓછો વપરાશ ધરાવતા ઈન્ટરનેટ રીલે ચેટ (IRC) દ્વારા. જ્યારે કોઇ એવો બનાવ નોંધાય છે, જેમા ચેટનો ઉપયોગ થયો હોય ત્યારે તપાસ કરનાર અમલદાર ને ગુનામાં કઇ પદ્ધતિના ચેટનો ઉપયોગ થયો છે તેની ખાતરી કરવી જરૂરી છે. દા.ત. ચેટ હોસ્ટ કરતી વેબસાઇટનું નામ શું છે તથા તેનું પૂરું IP Address અથવા તેમાં કયો પ્રોગ્રામ વપરાયો છે. મહ્ત્વના પુરાવા કે જે સુનિશ્ચિત કરવા જોઇએ:

- શંકાસ્પદ પાર્ટીની ઓળખ આપી શકે એવી કોઇપણ માહિતી, અને
- કોઇપણ ચેટની સામગ્રી.

જો ચેટ વેબ આધારિત હોય તો વેબસાઇટની વિગતો, કોઇપણ ચેટરૂમનું નામ અને શંકાસ્પદ વપરાશકર્તા નું નામ વગેરેને ચેટની ગતિવિધિના સમય અને તારીખ સાથે સુસંગઠિત પણે મેળવવું જોઇએ. જો ચેટ સોશિયલ નેટવર્કીંગ સાઇટ દ્વારા કરવામાં આવતી હોય તો વપરાશકર્તા મોટાભાગે યુનિક આઇડી નંબર તથા યુઝર નેમ ધરાવતો હશે. જ્યારે વપરાશકર્તા ની પ્રોફાઇલ જોવામાં આવે અથવા માઉસના પોઇન્ટરને યુઝરનેમ પર લઇ જવામાં આવે

ત્યારે સામાન્ય રીતે આ વેબ બ્રાઉઝરના એડ્રેસબારમાં દેખાશે. જો ચેટ ઇન્સ્ટન્ટ મેસેન્જર પ્રોગ્રામ દ્વારા થયેલ હોય ત્યારે શંકાસ્પદનું યુઝરનેમ સંકળાયેલ ઇ-મેઇલ એડ્રેસ (કે જે સામાન્ય રીતે વ્યકિતના કોન્ટેક્ટ લીસ્ટમાં ઉપલબ્ધ હોય છે.) સાથે મેળવવું જોઇએ. સામાન્ય રીતે વપરાશકર્તાનું કોન્ટેક્ટ લીસ્ટ ઇન્ટરનેટ સાથે જોડાયેલ કોઇ કોમ્પ્યુટરમાંથી પ્રાપ્ત કરી શકાય છે, આથી જો એવું માનવામાં આવે કે વપરાશકર્તાનું કોમ્પ્યુટર ફોરેન્સિક તપાસ માટે જાળવવાનું હોય ત્યારે તેનો ઉપયોગ તેમાંથી કોન્ટેક્ટ લીસ્ટ મેળવવા માટે થવો જોઇએ નહીં. સામાન્ય રીતે વપરાશકર્તા ની પાસે ચેટલોગ ને સેવ કરવા માટેનો વિકલ્પ હોય છે, પરંતુ ડીફોલ્ટ સેટીંગમાં લોગ સેવ કરવાનું તે વિકલ્પ બંધ હોય છે. જો વપરાશકર્તા પાસે પુરાવો ધરાવતા હોય તેવા ચેટ લોગ્સ સેવ હોય તો પુરાવો ભેગા કરવા માટે લોગને રીમુવેબલ મીડીયામાં સેવ કરવી જોઇએ, જો રીમુવેબલ મીડીયા ઉપલબ્ધ ન હોય તો તેની પ્રિન્ટ કાઢવી જોઇએ. વપરાશકર્તા કમ્પ્યુટરની સાથે સાથે અન્ય ઘણા પ્રકારના ડીવાઇસનો ઉપયોગ કરીને ચેટ કરી શકે છે. જ્યારે કેસના સંજોગો સમર્થનકર્તા હોય ત્યારે શંકાસ્પદના કોન્ટેક્ટની વિગતો અને ચેટની સામગ્રીના પુરાવા પુન: પ્રાપ્ત કરવા માટે એક અંતિમ વપરાશકર્તા ડીવાઇસ ફોરેન્સિક તપાસ માટે જમા કરી શકાય છે. જ્યારે શંકાસ્પદની યુઝર ડીટેઇલ્સ મેળવવામાં આવે ત્યારે કોન્ટેક્ટ પ્રોવાઇડર/ચેટ સર્વિસ પ્રોવાઇડરને યોગ્ય વિનંતી કરીને શંકાસ્પદની ઓળખ કરવી શક્ય છે. જો ચેટ IRC નો

ઉપયોગ કરીને કરવામાં આવી હોય તો નીચેની વિગતો મેળવવી જોઇએ:

- વપરાયેલ IRC પ્રોગ્રામ,
- IRC સર્વરનું નામ,
- ચેનલ અને કોઇ વપરાશકર્તા નામો.

ફોરેન્સિક નિષ્ણાત પાસેથી વધારાની સલાહ મેળવવી જોઇએ.

૪. IP-એડ્રેસ ટ્રેસિંગ:

મોટાભાગનાં ઈન્વેસ્ટીગેશન માં કોમ્પ્યુટર અથવા વ્યક્તિએ જે IP-એડ્રેસનો ઉપયોગ કર્યો હોય તેની ઝીવણવટભરી તપાસ (ટ્રેસિંગ) ની જરૂર રહે છે. ઉદા. લોગ ફાઇલને અથવા ઈ-મેઇલનાં હેડરનું પૃથ્થકરણ (Analyze) કરવાથી શંકાસ્પદ કોમ્પ્યુટરનાં IP-એડ્રેસનું રહસ્ય છતું કરે છે. WHOIS ને સર્ચ કરવાથી કોઈ એક ચોક્કસ IP એડ્રેસ અથવા IPએડ્રેસ જૂથને જે સંસ્થાએ રજીસ્ટર કર્યું છે તેની ઓળખ મળે છે. ઘણાં કિસ્સાઓમાં આ સંસ્થાઓ ઈન્ટરનેટ સર્વિસ પ્રોવાઈડર (ISP) હોય છે. શંકાસ્પદ ISP ઘણા ગ્રાહકોમાંનો એક હોય શકે. આવી પરિસ્થિતિમાં, સુસંગત તારીખ અને સમય સાથે જેને તેમણે શંકાસ્પદ IP એડ્રેસની ફાળવણી કરી હોય તે ગ્રાહકની વિસ્તૃત માહિતી પુરી પાડવા માટે ISP ને વિનંતી કરવાની રહેશે. અનુગામી પ્રકરણ કે જે ‘સોશિયલ મીડિયા ઈન્વેસ્ટીગેશન’ પર છે તે IP એડ્રેસ ટ્રેસિંગ દ્વારા end-user ની ઓળખ કરવાની રીતનું વર્ણન કરે છે. એ સમજવું જોઈએ કે IP

એડ્રેસ સ્થાયી કે અસ્થાયી (Static or dynamic) હોઈ શકે પરંતુ યોગ્ય પ્રક્રિયાના અનુસરણ કરવા થી end-user ને ઓળખી શકાય.

૪.૧) ઈન્ટરનેટ પ્રોટોકોલ:

ઈન્ટરનેટ-પ્રોટોકોલ (IP) ઈન્ટરનેટ નો મુખ્ય સંચાર પ્રોટોકોલ છે જે ડેટા પેકેટો ને તેના ઉદગમ-સ્રોત (હોસ્ટ) થી તેના ગંતવ્ય સુધી કેવળ સરનામાંના આધારે મોકલે છે. ઈન્ટરનેટ પ્રોટોકોલનું મુખ્ય કાર્ય ઉદગમ સ્થાનના હોસ્ટના ડેટા પેકેટો ને તેના પોતાના સરનામાં અને ગંતવ્ય સ્થાનના સરનામાં આપીને તેને એક કે (જરૂરી હોયતો) એકથી વધુ IP નેટવર્કોમાં તેનું રાઉટીંગ કરાવી તેને તેના ગંતવ્યસ્થાને મોકલે છે. આ પ્રક્રિયાને અંજામ આપવા ઈન્ટરનેટ પ્રોટોકોલે પેકેટોનું બંધારણ અને સરમાના પધ્ધતિ વિકસાવી છે જે મુખ્ય બે કાર્યો કરેછે : હોસ્ટની ઓળખાણ અને તાર્કિક સ્થાન સેવા પૂરી પાડે છે.

૪.૨) ઈન્ટરનેટ પ્રોટોકોલ (IP) ની મુખ્ય બે આવૃતિઓ:

IP ની મુખ્ય આવૃત્તિ ઈન્ટરનેટ પ્રોટોકોલ ૪ (IPv4) છે, જે ઈન્ટરનેટનો પ્રભાવશાળી પ્રોટોકોલ છે. તેના અનુગામી ઈન્ટરનેટ પ્રોટોકોલ ૬ (IPv6)છે. IPv4 એડ્રેસ પ્રણાલીમાં તેના એડ્રેસો ૩૨ બીટના હોય છે અને તેઓ શક્ય એટલા અનન્ય ૪૨૯૪૯૬૭૨૯૬ (૨^૩૨) એડ્રેસો ધરાવે છે. IPv4એ તેના

કેટલાક એડ્રેસોને ચોક્કસ હેતુઓ (જેમકે અંગત નેટવર્ક માટે ~૧૮ મિલિયન એડ્રેસો કે મલ્ટીકાસ્ટ એડ્રેસો (~૨૭૦ મિલિયન)) માટે અનામત કર્યા છે. IPv4ના એડ્રેસો પ્રમાણભૂત રીતે ડોટ-ડેસીમલ પધ્ધતિથી લખવામાં(દર્શાવામાં) આવે છે, જેમાં ચાર દશાંશ (Decimal) સંખ્યાઓ (જેનો વિસ્તાર ૦ થી ૨૫૫ વચ્ચે) ટપકા (ડોટ) વડે અલગ પડેલ હોય છે. દા.ત. 172.16.254.1. એડ્રેસનો દરેક એક ભાગ ૮ બીટ્સ (ઓક્ટેટ)ને દર્શાવે છે. તકનીકી લખાણ અને અમુક કિસ્સાઓમાં IPv4ને વિવિધ રીતે એટલે કે હેક્ક્ષાડેસીમલ, ઓક્ટેલ કે બાઈનરી સ્વરૂપે પણ પ્રદશિત કરાય છે. બીજી રીતે કહીએતો, આ IP એડ્રેસો વૈશ્વિક રીતે અનન્ય હોય છે. .

૪.૩) IP ઉપનેટવર્કો (IP Subnetworks):

IPv4 અને IPv6 બંનેમાં IP નેટવર્કોને ઉપનેટવર્કોમાં વિભાજીત કરી શકાય છે. આ માટે, IP એડ્રેસને તાર્કિક રીતે બે વિભાગમાં સ્વીકૃત કરાયા છે. નેટવર્ક પૂર્વગ અને હોસ્ટ ઓળખકર્તા કે ઇન્ટરફેસ ઓળખકર્તા (IPv6). સબનેટ માસ્ક કે CIDR નો ઉપયોગ IP **એડ્રેસને** નેટવર્ક અને હોસ્ટ વિભાગમાં કેવી રીતે વહેચવા તે માટે થાય છે. સબનેટ માસ્કનો ઉપયોગ IPv4 માંજ થાય છે. IPv4 અને IPv6 બંને CIDR

ધારણા અને પધ્ધતિનો ઉપયોગ કરે છે. આ પ્રમાણે, નેટવર્કે ઉપયોગમાં લીધેલ બીટ્સ ને IP એડ્રેસ બાદ એક સ્લેશ બાદ એક સંખ્યા(દશાંશ) તરીકે દર્શાવાય છે આને રાઉટીંગ પૂર્વગ પણ કહેવાય છે. દા.ત. IPv4 ના એક એડ્રેસ ૧૯૨.૧૬૮.૪૭.૫ અને તેનું સબનેટ માસ્ક ૨૫૫.૨૫૫.૨૫૫.૦ હોયતો, તેને ૧૯૨.૧૬૮.૪૭.૫/૨૪ તરીકે દર્શાવાય જ્યાં પહેલા ૨૪ બીટ્સ IP એડ્રેસમાંથી જે તે સબનેટનો નેટવર્ક ID દર્શાવે છે.

૪.૪.) IP એડ્રેસની સોંપણી:

જયારે હોસ્ટની બુટીંગ(સોફ્ટવેર સિસ્ટમનું હાર્ડવેરમાં સ્થાપન થવાની ક્રિયા) પ્રક્રિયા વખતે હોસ્ટ પર નવા IP એડ્રેસની સોંપણી અથવા સોફ્ટવેર કે હાર્ડવેરમાં રૂપરેખાંકિત કરેલ કાયમી IP એડ્રેસની સોંપણી થાય છે. IP એડ્રેસના સ્થાયી માળખુ સ્થિર IP એડ્રેસના (Static IP Addresing) ઉપયોગ તરીકે પણ ઓળખાય છે. આથી વિપરીત, જો દરેક વખતે નેટવર્કના હોસ્ટને નવા જ IP એડ્રેસ આપવાનો હોયતો આ પધ્ધતિને ગતિશીલ IP એડ્રેસિંગ (Dynamic IP Addressing) કહેવાય છે.

- પદ્ધતિઓ: સ્થિર IP એડ્રેસની સોંપણી હોસ્ટોને વ્યવસ્થાપક દ્વારા જાતે આપવામાં આવે છે. ચોક્કસ

પધ્ધતિ પ્લેટફોર્મ પ્રમાણે બદલાય છે. આના વિપરીત ગતિશીલ IP એડ્રેસો જે કોઈ કમ્પ્યુટરના ઇન્ટરફેસ દ્વારા કે કોઈ હોસ્ટના સોફ્ટવેર (ZeroConf) કે ડાયનેમિક હોસ્ટ કોન્ફીગરેશન પ્રોટોકોલ (DHCP) વાળા સર્વરની મદદથી સોંપણી થાય છે.

- **ગતિશીલ એડ્રેસિંગનો ઉપયોગ**: LAN માં ઘણાબધા હોસ્ટને IP ની જાતે સોંપણી કરવી એ નેટવર્કના વ્યવસ્થાપક માટે ખૂબ જ સમય અને ધ્યાન માગી લે છે. ઉપરાંત તેમાં વધતા ઘટતા હોસ્ટની સંખ્યા તેના વ્યવસ્થાપન માં ખૂબ જ ચીવટાઈ માંગી લે છે DHCP સર્વરનો ઉપયોગ કરી વ્યવસ્થાપક એક ચોક્કસ IP ની શ્રેણીને પોતાના નેટવર્કના હોસ્ટો માટે ખુલ્લી કરે છે. આ રૂપરેખાંકિત કરેલા સર્વર દ્વારા તે હોસ્ટોને IP એડ્રેસ ઉપરાંત ગેટવે એડ્રેસ, DNS એડ્રેસ, WINS સર્વર IP એડ્રેસ વિ. ની સોંપણી કરી શકે છે. DHCP સર્વર દ્વારા અપાતા IP એડ્રેસો ચોક્કસ મુદ્દત (વ્યવસ્થાપક દ્વારા નક્કી કરેલ) પછી બદલાય છે. કોઈ કિસ્સામાં કોઈક હોસ્ટનો IP એડ્રેસ સ્થિર કરવો હોયતો પણ DHCP સર્વર દ્વારા જે તે હોસ્ટનો MAC એડ્રેસ અનામત કરી તેને કાયમી ધોરણે IP એડ્રેસ આપી શકાય છે. DHCP એડ્રેસિંગ નો ઉપયોગ ડાયલ-અપ અને કેટલીક ઈન્ટરનેટની વ્યવસ્થા કરતી ISP પોઈન્ટ-ટુ-પોઈન્ટ પ્રોટોકોલ દ્વારા કરે છે.

- **સ્ટીકી ગતિશીલ એડ્રેસ:** સ્ટીકી ગતિશીલ એડ્રેસનો ઉપયોગ ઈન્ટરનેટની વ્યવસ્થાપક કંપનીઓ DSL કે કેબલ અને મોડેમ દ્વારા અપાતા ઈન્ટરનેટ માટે કરે છે આવા કિસ્સામાં ભાગ્યેજ IP એડ્રેસમાં ફેરફાર થાય છે. મોડેમને એક વાર મળેલ IP એડ્રેસ જ્યાં સુધી મોડેમ બંધ કરવામાં નથી આવતું ત્યાં સુધી તે રહે છે. તેને આપેલ IP એડ્રેસની મુદ્દતમાં ISP દ્વારા વારંવાર વધારો કરાય છે.
- **સ્વયં રૂપરેખાંકિત એડ્રેસ:** સ્થિર કે ગતિશીલ(DHCP) IP એડ્રેસોની ગેરહાજરીમાં કેટલીક ઓપરેટિંગ સિસ્ટમ (જેવીકે વિન્ડોસ) પોતાના ઇન્ટરફેસને APIPA (ઓટોમેટીક પ્રાઈવેટ IP એડ્રેસિંગ)ની મદદથી IP ની સોંપણી કરે છે.
- **સ્થિર એડ્રેસિંગનો ઉપયોગ:** સ્થિર એડ્રેસિંગના ઉપયોગ કેટલાક નેટવર્ક સ્થાપત્ય માટે થાય છે. ઇન્ટરનેટ પર પ્રકાશિત થયેલ સર્વરો મોટે ભાગે સ્થિર એડ્રેસિંગ નો ઉપયોગ કરે છે કારણકે DNS દ્વારા શોધ કરતા જે તે સર્વરના IP એડ્રેસ સ્થિર હોયતો તેની સાથે જોડાણ થવાની ક્રિયા ઝડપી બને છે.

ઉપરોક્ત તથ્યોને ધ્યાનમાં રાખીને જ્યારે કોઈ પણ IP એડ્રેસ ની તપાસ કરવાની હોય છે, ત્યારે IP એડ્રેસ ક્યા પ્રકાર ના છે તે ચકાસવાની જરૂરત રહે છે. પોલીસ અધિકારી/કર્મચારી IP એડ્રેસ ના પ્રકારની તપાસ અને પ્રાથમિક વિશ્લેષણ ફ્રી વેબટૂલ્સ વાપરીને

કરી શકે, ઉ.દા. www.ip2address.com, વગેરે. IP એડ્રેસ ના પ્રકાર જાણ્યા પછી, પોલીસ અધિકારી/કર્મચારી ને Internet Service Provider (ISP), ઉ.દા. વોડાફોન, સ્પીડિગો, વગેરે, પાસે થી end-user ની માહિતી મેળવવાની પ્રક્રીયા હાથ ધરવાની રહે છે. ISP પાસે થી માહિતી મેળવવાની પ્રક્રિયામાં પ્રશ્નો અને તથ્ય IP એડ્રેસના પ્રકારના આધારે પૂછવાના રહે છે. ઉ.દા. જો IP એડ્રેસ ડાયેનિમિક પ્રકાર નો છે, તો ટાઈમ-ઝોન કંવર્સન સાથે સમય અને તારીખ જરૂર થી ISP ને જણાવવુ. આગામી પ્રકરણમાં ISP થી IP એડ્રેસ લગતી માહિતી મેળવવાની પ્રક્રીયા વધુ વિસ્તાર થી જણાવવામાં આવી છે.

<u>૫. ઈન્ટરનેટ પ્રોટોકોલ ડીટેઈલ રેકર્ડ (IPDR) :</u>

કમ્યુનિકેશન અને આઈ.ટી. મંત્રાલય, ભારત સરકારે ૦૧-૧૦-૨૦૧૩ના રોજ ઈન્ટરનેટ પ્રોટોકોલ ડીટેઈલ રેકર્ડ (IPDR) અને SYS LOG of Network Address Translation (NAT) ને સંગ્રહ કરવા માટે બધા ઈન્ટરનેટ સર્વિસ પ્રોવાઈડરે અનુસરવાના માપદંડ આપ્યા હતા (પરિશિષ્ટ માં સામેલ છે). તપાસ કરનાર અધિકારી ઈન્વેસ્ટિગેશન માટે ભારતીય ફોજદારી કાર્યરીતિ સંહિતાની કલમ ૯૧ અથવા કલમ ૯૨ મુજબની નોટીસ આપીને IPDR અને SYS LOG ની માંગણી (requisition) કરી શકે છે. એવા કિસ્સાઓમાં કે જ્યાં IP એડ્રેસ પરથી મહત્વની માહિતી મળી શકે તેમ હોય, તો ઈન્વેસ્ટિગેટિંગ ઓફીસર તકનિકી વ્યક્તિ (technical person) ની

મદદથી સાધન/વ્યક્તિ (device/user) ની ઓળખ કરવા માટે IPDR અને SYS LOG ની માંગણી (requisition) કરી શકે છે.

<u>૬. ટાઈમઝોનનું રૂપાંતર (Time Zone Conversion):</u>

ટાઈમઝોન અને તેનું રૂપાંતર(conversion) એ આરોપી અને ગુનાહિત કાર્ય કે બનાવ વચ્ચે સંબંધ સ્થાપવા માટે અત્યંત જરૂરી છે. ટાઈમઝોન એ પૃથ્વીનું એક એવું ક્ષેત્ર છે જેનો એકસરખો પ્રમાણભૂત (standard) ટાઈમ હોય, જેને સામાન્ય રીતે લોકલ ટાઈમ કહેવામાં આવે છે. સામાન્ય રીતે, જુદાં-જુદાં ટાઈમઝોનના લોકલ ટાઈમ (UTC) ને Greenwich Mean Time સાથે ઓફસેટ (વધારો-ઘટાડો) કરીને ગણવામાં આવે છે, લોકલ ટાઈમ એટલે UTC વત્તા જે-તે સ્થાનનો હાલનો ટાઈમ ઝોન. મોટાભાગના ઓનલાઈન સર્વરના ટાઈમઝોન તેના ભૌગોલિક સ્થાન/લોકલ ટાઈમ સાથે સિંક્રોનાઈજ્ડ (સુમેળ) હોય છે. સાયોંગિક પુરાવા તરીકે અપરાધ અને તેના બાદની ક્રિયાઓનો ચોક્કસ સમય સ્થાપિત કરવા માટે તે સિસ્ટમના ટાઈમ ઝોનને જાણવું ખૂબ જ મહત્વનું છે. અમુક ભૌગોલિક ક્ષેત્રો ના ટાઈમઝોન વચ્ચેનો તફાવત 12 કલાક કરતાં વધુ હોઈ શકે, દા.ત. India અને USA. આથી ગુનો થયાની તારીખ પણ બદલાઈ શકે છે. આ વાત ખૂબ જ મહત્વપૂર્ણ અને નિર્ણયાત્મક છે, ખાસ કરીને ફેસબુક પોસ્ટ્સ, ઈ-મેઈલ, વગેરે સંબંધિત કિસ્સાઓમાં. દા.ત. ઈ-મેઈલ મોકલ્યાનો સમય ૧૨:30 IST (Indian Standard Time) હોય, પણ માહિતીનો સંગ્રહ તે ઈ-મેઈલ સર્વિસ પ્રોવાઈડરના સર્વરના લોકલ ટાઈમ પ્રમાણે થયો

હોય. તેથી ટાઈમઝોનનું રૂપાંતર તારીખ સાથે જરૂરી બની જાય છે. લોકલ ટાઈમનું ISTમાં રૂપાંતર અને તેનું ઉલટું કરવા માટે ઘણી બધી ઓનલાઈન વેબસાઈટ ઉપલબ્ધ છે.

પ્રકરણ – ૫

સોશીયલ મીડિયા

પ્રકરણનો ઉદ્દેશ: આ પ્રકરણમાં સોશીયલ મીડિયાથી પુરાવા એકત્ર કરતી વખતે રાખવાની તકેદારી, જરૂરી કૌશલ્ય, અને તકનીકની ચર્ચા કરવામાં આવેલ છે.

૧. સોશીયલ મીડિયા: વ્યાખ્યા

સોશીયલ મીડિયા એવા પ્રકારની ઈન્ટરનેટ એપ્લિકેશનો માટે જિનેરિક ટર્મ છે કે જે ઑન-લાઈન યુઝર્સ ને માહિતી અપલોડ કરવા, share કરવા, ચર્ચા કરવા કે અપલોડ થયેલી માહિતી પર કોમેન્ટ કરવા, વગેરે જેવી સુવિધાઓ પૂરી પાડે છે. સમાજના મોટી સંખ્યામાં લોકો વિવિધ પ્રકારના સોશીયલ મીડિયા પ્લેટફોર્મ, જેવા કે ફેસબુક, વોટ્સએપ, લિન્ક્ડ-ઈન, ટ્વીટર, ઈન્સ્ટાગ્રામ, મેસેન્જર, ના માધ્યમથી એકબીજા સાથે સંપર્કમાં રહે છે, અને માહિતીની આપ-લે કરે છે. આ તમામ માધ્યમોને સોશિયલ મીડિયા કહેવામાં આવે છે.

૧.૧) સોશીયલ મીડિયાના વિવિધ પ્રકારો:

સોશીયલ મીડિયાના ઘણાબધા પ્રકારો છે.

(૧) FACEBOOK: ફેસબુક એ એક પ્રખ્યાત સોશીયલ નેટવર્કીંગ વેબસાઈટ છે કે જેની પર કોઈ વ્યક્તિ પોતાના નામ, નંબર, ઈમેલ આઈડી વગેરે વિગતો આપીને પોતાનું

નામ(આઇ-ડી) રજીસ્ટર્ડ કરાવે છે, ત્યારબાદ આવા રજીસ્ટર થયેલા યુઝર્સ ને પ્રોફાઈલ બનાવવી, ફોટાઓ અને વિડીયો અપલોડ કરવા, સંદેશાઓ મોકલવા જેવી સુવિધાઓ મેળવી શકે છે.

(૨) LINKED IN: લિન્ક્ડ-ઇન એક એવી સોશીયલ વેબસાઈટ છે જે ખાસ કરીને વ્યવસાય સમુદાય/વ્યાવસાયિકો માટે બનાવવામાં આવી છે. આનો મુખ્ય હેતુ આ મીડિયા પર રજીસ્ટર્ડ થયેલા રજીસ્ટર યુઝર્સને પ્રોફેશનલો જોડે ઓળખાણ/સમ્પર્ક કરાવી આપવાનો છે.

(3) WhatsApp: સંદેશાની આપ-લે કરવા માટે ની એપ્લીકેશન છે. જે એકબીજા જોડે વાત કરવાની, માહિતી ની આપ-લે કરવાની, માહિતી અપલોડ કરવાની, વોઈસ કોલિંગ તથા વિડીયો ચેટ કરવા જેવી સુવિધાઓ પૂરી પાડે છે.

(૪) Instagram: આ એવા પ્રકારનું સોશીયલ નેટવર્કિંગ પ્લેટફોર્મ છે કે જે ફોટાઓ અને વિડીયોને અપલોડ/શેર કરવાની સુવિધા પૂરી પાડે છે.

(૫) Twitter: Twitter મફત માઈક્રોબ્લોગીંગની સુવિધા પૂરી પાડે છે જે રજીસ્ટર કરેલા સભ્યોને tweet કરવાની તથા એકબીજા ને ફોલો કરવાની સુવિધા પણ આપે છે.

<u>૨. સોશીયલ મીડિયા સંબંધિત પુરાવાઓ એકત્રિત કરવા:</u>

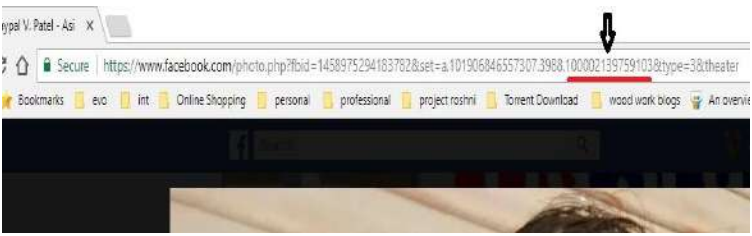
સોશીયલ મીડિયા વિવિધ પ્રકારના હોઈ શકે છે અને તેમનાથી પુરાવા એકત્ર કરવા માટે લેવામાં આવતા પગલાઓ પણ અલગ-અલગ હોય છે. સોશિયલ મીડિયા વેબસાઈટ્સ પર થી content ડાઉનલોડ કરવા માટે અગાઉના ચેપ્ટરોમાં દર્શાવેલ કાર્યરીતી અપનાવવી જોઇએ. પરંતુ સોશિયલ-મીડિયા બાબતની મોટા ભાગની તપાસોમાં સર્વ-પ્રથમ IP-Address ટ્રેસ કરી યુજરને ઓળખવાની જરૂરીયાત રહે છે. જેથી, અનુગામી ભાગમાં ફેસબુક માંથી યુઝર ટ્રેસ કરવાની રીત વિગતવાર દર્શાવવામાં આવી છે.

<u>3. ફેસબુકમાંથી યુઝર ટ્રેસ કરવાની રીત:</u>

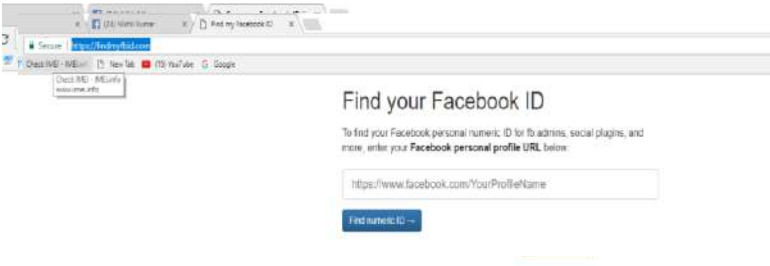
<u>3.૧) પ્રાથમિક કાર્યવાહી:</u>

- www.facebook.com પેજ ખોલવુ અને LOG-IN થવું.
- LOG-IN થયા બાદ ફરિયાદી દ્વારા જણાવેલ વિવાદિત એકાઉન્ટ ઓળખવું.
- વિવાદિત એકાઉન્ટ/આઈ-ડી જો યુનિક નામનું હશે તો તુરંત મળી જશે પણ જો કોમન નામ હશે તો શોધવું મુશ્કેલ પડશે. (ઉ.દા તરીકે **"Ramesh Patel"** નામનાં મોટી માત્રમાં users હશે.)
- ફરિયાદી/અરજદાર ને પ્રથમ વિવાદિત અકાઉન્ટની લિંક માટે પુછો.

- અરજદાર પાસેથી વિવાદિત એકાઉન્ટના નામ દ્વારા અથવા તો તેને આવેલા મેસેજના screenshots પરથી પણ ઓળખી શકાશે.
- બ્રાઉઝર ના URL (યુ.આર.એલ) માં જઈ વિવાદિત એકાઉન્ટ ના URL ને કોપી કરવું.
- દરેક Facebook ID નો એક યુનિક ન્યૂમેરિકલ આઈ ડી નંબર હોય છે. જેને **૨(બે)** રીતે શોધી શકાશે.
    1. વિવાદિત એકાઉન્ટ/આઈડી નાં પ્રોફાઈલ ફોટો ઉપર ક્લિક કરવાથી ઉપર URL માંથી મેળવી શકાશે. નીચે બતાવ્યા મુજબ પ્રોફાઈલ ફોટો ઉપર ક્લિક કરવાથી નીચે મુજબની URL દેખાશે. જેના અંતમાં પૂર્ણવિરામ(.) અને (&) ની વચ્ચે નાં આંકડાને યુનિક ન્યૂમેરિકલ આઈ ડી નંબર કહે છે. નીચેના ફોટામાં લાલ કલરથી લાઈન કરેલ યુનિક ન્યૂમેરિકલ આઈ-ડી નંબર સૂચવે છે.



2. www.findmyfbid.com નામ ની સાઇટ પર જઈને ઉપર વિવાદિત એકાઉન્ટ/આઈડીની URLકોપી કરીને paste કરી Find Numeric ID ઉપર ક્લિક કરવાથી ન્યૂમેરિકલ આઈ-ડી નંબર મેળવી શકાશે.



- વિવાદિત id માં જે વાંધાજનક મેસેજ અથવા picture હોય તેના screenshots લેવા ખુબજ જરૂરી છે. આ screenshots ફરિયાદી પાસેથી મેળવી લેવા અથવા જાતે મેળવી લેવા. ઉપરોક્ત તમામ પ્રક્રીયા પંચો ના રૂબરૂમાં કરવી અને પ્રક્રીયાના પંચનામા કરવા હિતાવહ છે.
- ત્યાર બાદ ફેસબુક પાસે થી માહિતી મેળવવા માટે નો પત્ર તૈયાર કરવો. જેમાં પોલીસ સ્ટેશન નો સિક્કો જરૂરી છે . આ લેટર ને PDF તરીકે સેવ કરવો કારણ કે Facebook અમુક ફોરમેટમાંજ માહિતી સ્વીકારે છે. (sample letter પ્રમાણે)

- આ તમામ data હવે Facebook માં upload કરવો. જેથી Facebook પાસે થી વિવાદિત એકાઉન્ટ/આઈ-ડી ની માહિતી મળી શકે. જેની process નીચે પ્રમાણે રહેશે.

<u>૩.૨) ફેસબૂક પાસેથી iplog લેવા માટે ના સ્ટેપ:</u>

- સૌપ્રથમ browser માં જઈ ને https://www.facebook.com/records/x/login આ URL ટાઇપ કરીને એન્ટર પર ક્લિક કરવું .
- આ કરવા પર એક નવું page ખુલશે જે આપને પૂછશે કે શું આપ એક Authorized Law Enforcement Agency છો? એટલે કે શું આપ એક પોલીસ અધિકારી છો તેની પૃચ્છા કરશે.
- આપે "I am an authorized law enforcement agent and this is an official request" ઓપ્શન પર ટીક માર્ક કરી આપેલ ખાનામાં આપના પોલીસ સ્ટેશનનુ ઈ-મેલ આઈડી એન્ટર કરીને "Request Access" બટન પર ક્લીક કરવું.
- આમ કરવા પર તમારા પોલીસ સ્ટેશનના રજીસ્ટર્ડ ઇ – મેલ આઈ-ડી ઉપર Facebook દ્વારા એક લિંક મોકલવામાં આવશે આ લિંકની અવધી ૧ કલાકની હોય

છે. આ સમયમાં લિંક ઓપન કરવામાં ના આવે તો બધી પ્રક્રિયા ફરીથી કરવી પડશે.

- આ લિંક ઉપર ક્લિક કરવાથી એક નવું પેજ ખુલશે.
- જે પોલીસ સ્ટેશન આ કાર્યવાહી પહેલીવાર કરતા હશે તો તેમણે પ્રથમ વાર રજીસ્ટ્રેશન details નાખવાની રહેશે જેમકે કયું પોલીસ સ્ટેશન? તેના ઇન્ચાર્જ અધિકારી ? વિગેરેની વિગત.
- બાદ RECORD REQUEST બટન પર ક્લિક કરવાથી એક નવુ પેજ ખુલશે જેમાં વિગત વાર માહિતી ભરવાની રેહશે.

1. Internal Case Reference Number–કેસ નંબર (ઉ.દા. તરીકે JPR/98/Pooja/2017). આમાં ત.ક.અ., અરજી/ગુન્હા નંબર/ ફરીયાદી અને વર્ષ ની વિગત નો ટૂંકમાં સમાવેશ થાય છે.
2. Legal Process-આપેલ ડ્રૉપડાઉન મેનુ માંથી Section-91 Request સિલેક્ટ કરવું.
3. Nature of Case-કેસ ને લાગતું સિલેક્ટ કરવું.
4. Legal Process Signed Date-ફોર્મ ભરતા હોય એ દિવસની તારીખ.
5. Request Due Date-ઉપર નાખેલ તારીખ બાદના ૧૦ દિવસની તારીખ.
6. Accounts
   - ફેસબુક

- વિવાદિત ફેસબુક આઈ.ડી. જોવા મળ્યું હોય તેવી કોઈ પણ જૂની તારીખ અથવા આઈ.ડી. ચાલુ જ હોય તો આજ ની તારીખ.
- વિવાદિત ફેસબુક આઈ.ડી. નું URL
- આ ત્રણે ડીટેલ નાખી ADD બટન પર ક્લિક કરવું.

7. Requesting Records Between-જે તારીખો વચ્ચે ના લૉગ મેળવવા હોય તે તારીખો નાખવી (શરૂઆત અને આખરની તારીખો સિલેક્ટ કરવી.)
8. Documentation-
    - ફેસબુક નો લેટર સિલેક્ટ કરવો (જે pdf ફૉર્મેટ માંજ હોવો જોઈએ)
    - વિવાદિત id માં જે વાંધાજનક મેસેજ અથવા picture હોય તેના Screenshots એક-એક સિલેક્ટ કરવા.
9. I attest that I am a law enforcement agent authorized to request account records and all the information I have provided is accurate. ની આગળ આવેલ ચેકબોક્સ પર રાઇટ ક્લિક કરી SUBMIT પર ક્લિક કરવું અને કેસ SUBMIT થઈ જાય તેની રાહ જોવી. કેસ

SUBMIT થઈ ગયા નો મેસેજ screen પર દેખાશે.

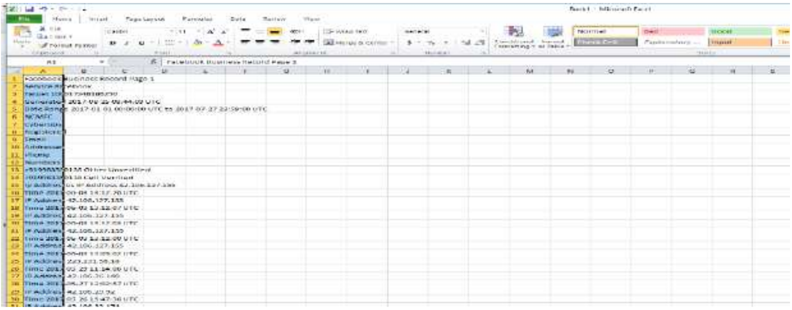
10. કેસ SUBMIT કર્યા બાદ HOME ઉપર ક્લિક કરવાથી સૌથી પ્રથમ દેખાતો કેસ તમારો કેસ છે જેની ડાબી બાજુએ જણાવેલ Facebook કેસ નંબર નોંધી લેવો અને વારંવાર FACEBOOK તરફ થી માહિતી આવી છે કે નહી તે ચેક કરતાં રહેવું.

3.3) <u>FACEBOOK તરફ થી માહિતી આવી છે કે તે ચેક કરવા:</u>

- સૌપ્રથમ browser માં જઈ ને **https://www.facebook.com/records/x/login** આ URL ટાઇપ કરીને એન્ટર પર ક્લિક કરવું .
- આ કરવા પર એક નવું page ખુલશે જે આપને પૂછશે કે શુ આપ એક Authorized Law Enforcement Agency છો કે શું? આપ એક પોલીસ અધિકારી છો તેની પુષ્ટિ કરશે.
- આપે "**I am an authorized law enforcement agent and this is an official request**"ઓપ્શન પર ટીક માર્ક કરી આપેલ ખાના માં અપના પોલીસ સ્ટેશન નું ઈ-મેલ આઈડી એન્ટર કરીને "Request Access"બટન પર ક્લીક કરવું.

- આમ કરવા પર તમારા પોલીસ સ્ટેશનના રજીસ્ટર્ડ ઇ – મેલ આઈ-ડી ઉપર Facebook દ્વારા એક લિંક મોકલવામાં આવશે જેની અવધી ૧ કલાકની હોય છે.
- આ લિંક ઉપર ક્લિક કરવા થી એક નવું પેજ ખુલશે.
- HOME ઉપર ક્લિક કરવાથી તમારા કેસનુ સ્ટેટસ જાણી શકાશે
    1. જો સ્ટેટસમાં OPEN બતાવે તો FACEBOOK તરફ થી PROCESS હજુ પેન્ડીંગ છે તેવું સમજવું.
    2. જો સ્ટેટસમાં REJECT બતાવે તો FACEBOOK તરફ થી PROCESS REJECT થઈ છે તેવું સમજવું.
    3. જો સ્ટેટસમાં RESOLVED બતાવે તો FACEBOOK તરફ થી માહિતી આવી ગઈ છે તેવું સમજવું અને DOWNLOAD RECORD PDF પર CLICK કરવું.

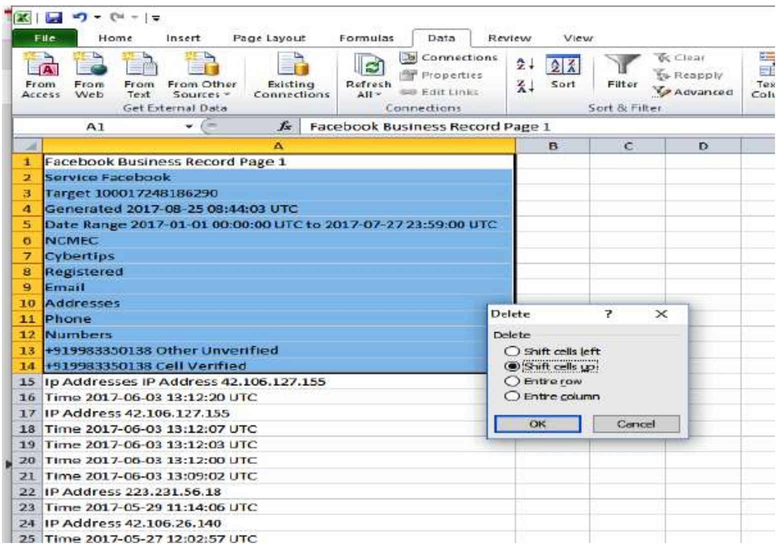
- DOWNLOAD RECORD PDF પર ક્લિક કરવાથી ફેસબુક દ્વારા મળેલ આઈ. પી. ની વિગત (PDF ફાઇલ) સેવ કરવાની રહેશે . આ ફાઇલ માં આઈ .પી. ની વિગત હોય છે અને તેમાં ઘણા આઈ.પી. લોગ હોઈ શકે. અમુક આઈ.પી. એડ્રેસ રિપીટ



થતા હશે પણ તારીખ અને ટાઈમ જુદા હશે. આ ફાઈલ માં દર્શાવેલ ટાઈમ યુટીસી (Universal Time Co-ordinated) ટાઈમ આપેલો હશે જેને IST (ઇન્ડીયન સ્ટાન્ડર્ડ ટાઇમ) માં ફેરવવો. જેના માટે PDF ફાઇલ માથી આઇપી લૉગ કોપી કરીને Excelsheet માં પેસ્ટ કરવી .

- જે કૉલમ માં પેસ્ટ કર્યું હોય તે કૉલમ સિલેક્ટ કરી મેનૂ બાર માં DATA ઓપ્શન પર કિલક કરી તેમાં Remove Duplicate ઓપ્શન પર કિલક કરવું.
- નવા open થયેલા popup મેનૂ માં દર્શાવેલ Column-A સિલેક્ટ રાખી ok પર ક્લિક કરવું.

- ડુપ્લીકેટ વેલ્યુ રિમુવ થયા બાદ કોલમમાં યુનિક વેલ્યૂ જ રહશે.
- કોલમ-A માંથી IPAddress સિવાય ની rows ડિલીટ કરવી.
    - ➢ સૌ પ્રથમ વાર IPAddress લખ્યું હોય તેના ઉપરની rows સિલેક્ટ કરી right ક્લિક કરી delete સિલેક્ટ કરવું.
    - ➢ Delete પર સિલેક્ટ કરવાથી ઓપન થયેલ મેનુ માં થી shifts cellsup સિલેક્ટ કરી ok પર ક્લિક કરવું.
- હવે columnA માં રહેલ વેલ્યૂ/ડેટા ને ચડતા ક્રમમાં ગોઠવવા. એના માટે column –A સિલેક્ટ કરી data મેનુ માં જવું અને Sort નામ ના સબ મેનુ માંથી A-Z સિલેક્ટ કરવું.



- આવું કરવા થી IPAddress સિવાય ની દરેક rows નીચે આવી જશે. આવી વધારા ની દરેક rows સિલેક્ટ કરી ડિલીટ કરી દેવી.
- Column-A માં થી numeric IP Address અલગ કરવા.
- ફેસબુક તરફથી આપવામાં આવેલ IP કઇ કંપનીના છે તે જાણવા માટે ગુગલ પર WHATISMYIPADDRESS, IP2LOCATION, IP LOCATOR જેવી વેબસાઇટ ખોલી ફેસબુકમાંથી આવેલ IP સિલેકટ કરી ઉપર જણાવેલ વેબસાઇટમાં જઇ આ IP કઇ સર્વિસ પ્રોવાઇડર કંપનીના છે તે જોઇ લેવું. જેથી નીચે મુજબ આઇપીનુ લોકેશન તેમજ આઇએસપીની વિગતો બતાવશે.

Domain and IP bulk lookup tool

223.231.56.18
42.106.127.155
42.106.26.140
42.106.29.92
42.106.33.174
42.106.127.155

Additional DNS record type to lookup for domains None Lookup

IP	Domain	Country	Region	City	ISP	ASN
223.231.56.18		India	34	Patna	Bharti Airtel Ltd. AS for GPRS Service	AS45609
42.106.127.155	42-106-127-155.live.vodafone.in	India			Vodafone Essar Ltd., Telecommunication - Value Added Services	AS38266
42.106.26.140	42-106-26-140.live.vodafone.in	India	16	Pune	Vodafone Essar Ltd., Telecommunication - Value Added Services	AS38266
42.106.29.92	42-106-29-92.live.vodafone.in	India			Vodafone Essar Ltd., Telecommunication - Value Added Services	AS38266
42.106.33.174	42-106-33-174.live.vodafone.in	India	09		Vodafone Essar Ltd., Telecommunication - Value Added Services	AS38266
42.106.127.155	42-106-127-155.live.vodafone.in	India			Vodafone Essar Ltd., Telecommunication - Value Added Services	AS38266

➢ ઉપરોક્ત આઇએસપી (સર્વિસ પ્રોવાઇડર) એ આ આઇપી કોને ક્યારે વપરાશ માટે આપેલા છે. તે જાણવા માટે સર્વિસ પ્રોવાઇડર કંપનીને સબસ્ક્રાઇબરને લેટર લખી મોકલવો.

PERFORMA FOR CDR/SDR/IMEI/IP ADDRESS

Outward No.Brinda/1087/2016,
Crime Branch, Ahmadabad City.
Date:27.07.2017.

To,
Deputy Commissioner of Police,
Crime Branch, Ahmadabad City.

Subject: To provide IP subscriber detail. (Vodafone)

1	Name of the Police Station	D.C.B. Police Station, Ahmadabad City.
2	C.R. No. Section	G/725/DCP/Crime/LA/1087/16, Date:31.12.2016 of the DCP Crime Branch, Ahmedabad City.
3	Place, Date and Time where offence occurred.	-----
4	Name of the I.O.	PSI J P Rojiya, Cyber Cell, Crime Branch, A.bad City.
5	Short detail of the offence	Facebook Fake Profile (Brinda Barot).
6	If any public safety order/anti national activity/ Order office of the Comm. of Police	-----
7	Which type of information needed.	Please provide subscriber detail of the following IP Addresses in one day.

IP Address

Sr. No.	IP Address	Date	Time (IST)
1	1.39.84.139	27.02.2016	19:13:36
2	1.39.85.46	16.04.2016	11:55:13
3	1.39.87.85	07.04.2016	12:20:06
4	1.39.99.108	28.03.2016	20:48:45
5	1.39.99.27	05.04.2016	11:47:00

(J P Rojiya)
Police Sub Inspector
Cyber Crime Cell
Crime Branch, Ahmadabad City.

Permission Granted and forwarded to Vodafone

(Deepan Bhadran)
Deputy Commissioner of Police
Crime Branch, Ahmedabad City.

- ઉપરોકત લેટર તૈયાર કરવા માટે આઇપી એડ્રેસ તથા ફેસબુક તરફથી આવેલ આઇપી તથા આ આઇપીમાં ૦૫:૩૦:૦૦ કલાક ઉમેરેલ ટાઇમ સાથે આઇપી જે કંપનીના હોઇ તે કંપનીને જે તે ઝોન ડીસીપીશ્રી/જિલ્લા પોલીસ અધીક્ષક મારફતે મોકલી આપવો.
- Internet Service Provider દ્વારા સબસ્ક્રાઈબરના મોબાઈલ નંબર/સરનામા આપવામાં આવશે, જેના આધારે તપાસ કરનાર અમલદાર દ્વારા આગળની કાર્યવાહી કરવાની રહે છે.
- ઉપરોક્ત પ્રક્રીયાની તપાસ કરનાર અમલદાર દ્વારા કેસ-ડાયરીમાં નોંધ કરવાની રહે છે.

આ પ્રમાણે અન્ય સોશિયલ મીડિયા માંથી પણ આઈ.પી. એડ્રેસ ની તપાસ કરી શકાય.

૪. Instant Messengers અને End-to-End encryption

વોટ્સએપ વપરાશકર્તાઓ વચ્ચેના સંદેશાને એન્ડ ટૂ એન્ડ એન્ક્રિપ્શન પ્રોટોકોલથી સુરક્ષિત કરવામાં આવે છે જેથી તૃતીય પક્ષો અને વોટ્સએપ સર્વર તેમને વાંચી શકતા નથી અને સંદેશાઓને ફક્ત પ્રાપ્તકર્તા દ્વારા ડિક્રિપ્ટ કરી શકાય છે. જેથી, વોટ્સએપ ના સર્વર થી MLAT/LR દ્વારા ડેટા મેળવવાનું મુશ્કિલ હોય છે. પરંતુ, IPDR ડેટા ના આધારે ડિવાઈસ થી ક્યારે-ક્યારે વોટ્સએપ મેસેજ પસાર/રિસીવ થયા છે, તે તપાસ કરી શકાય.

પ્રકરણ ૬

ઇ-વૉલેટ ફ્રોડ

પ્રકરણ નો ઉદ્દેશ: ઇ-વૉલેટ એટલે વ્યવસાયિક વ્યવહારો માટે મની પાર્ક કરવા બેન્કો દ્વારા શરૂ કરાયેલી સુવિધા. જે હવે સાયબર ક્રિમિનલ્સના નિશાને છે. આ પ્રકરણમાં ઈ-વૉલેટ ફ્રોડના કેસોમાં ડિજિટલ પુરાવા એકત્ર કરવાની રીત, જરૂરી કૌશલ્ય, અને તકનીકની ચર્ચા કરવામાં આવેલ છે.

૧. ઇ-વોલેટ શું છે?

- વોલેટ સામાન્ય ભાષામાં પર્સ છે કે જેમાં તમે તમારા પૈસા અને વ્યક્તિગત માહિતી જેવી કે ડ્રાઇવિંગ લાઇસંસ, પાન કાર્ડ, વિગેરે રાખી શકો છો. એવીજ રીતે ઇ-વોલેટ પણ એક પ્રકાર ની ઈલેક્ટ્રોનિક, ઇન્ટરનેટ પર આધારિત પેમેંટ સિસ્ટમ છે કે જે નાણાકીય વ્યવહારો અને વ્યક્તિગત માહિતીનો સંગ્રહ કરે છે.
- ઇ-વોલેટ એટલે ઈલેક્ટ્રોનિક વોલેટ કે જેમાં ઇન્ટરનેટના માધ્યમથી કોમ્પ્યુટર કે સ્માર્ટ ફોન દ્વારા ઓનલાઇન વ્યવહારો કરી શકાય છે.
- ઇ-વોલેટ ની મદદથી ઓનલાઇન શોપિંગ કરવું, મોબાઇલ રીચાર્જ કરાવવો, બિલ જેવા કે વીજળી, મોબાઇલ, ગેસ, વિગેરે ભરવા, મુસાફરી કરવા માટે ટેક્સી, બસ કે રિક્ષા બૂક

કરાવવી, વિમાનની ટિકિટ માટે ચૂકવણી કરવી, ઇન્સ્યોરન્સ પ્રીમિયમ ભરવા વિગેરે વ્યવહારો કરી શકાય છે.

<u>૨. ઇ-વોલેટ કઈ રીતે કામ કરે છે?</u>

- ઈ-વોલેટ એક પ્રકારના ડેબિટકાર્ડ કે ક્રેડિટકાર્ડ ની જેમ કામ કરે છે. ભારતમાં ઇ-વોલેટ ને રિઝર્વ બેંક ઓફ ઈન્ડિયા કે જે ભારતમાં બેંકોનુ નિયમન કરે છે, એના પ્રમાણે પ્રીપેડ પેમેંટ-ઇન્સ્ટ્રુમેન્ટ (PPI) પણ કહેવામાં આવે છે.
- ઇ-વોલેટમાં ઉપભોક્તા કેશ લોડ કરે છે. આ કેશ લોડ કરવા નેટ બૅન્કિંગ મારફતે એ પોતાના બેન્ક એકાઉન્ટ અથવા ક્રેડિટકાર્ડ કે ડેબિટકાર્ડ નો ઉપયોગ કરે છે અથવા તો પોતે POS(પોઈન્ટ ઓફ સેલ) પર જઈને કેશ લોડ કરે છે. પોઈન્ટ ઓફ સેલ એટલે ઇ-વોલેટ સંચાલિત કરતાં રીટેલર ની જગ્યા.
- કેશ લોડ કર્યા પછી એ નાણા કોઈ પેમેંટ કરવા અથવા તો ટ્રાન્સફર કરવા વાપરી શકાય છે. આવા ઇ-વોલેટ માં રજિસ્ટ્રેશન ચાર્જિસ અથવા કેશ લોડીંગ ચાર્જિસ લગાડવામાં આવતા હોય છે.
- ઇ-વોલેટ માં મુખ્યત્વે બે પાર્ટ છે સોફ્ટવેર અને માહિતી (information). સોફ્ટવેર પાર્ટ વ્યક્તિગત માહિતીનો સંગ્રહ કરે છે અને ડેટાની સુરક્ષા અને એન્ક્રિપસન પ્રદાન કરે છે, જ્યારે માહિતી પાર્ટ ઉપભોક્તા દ્વારા આપવામાં આવેલી વિગતોનો એક ડેટાબેઝ છે જેમાં તેઓના નામ, સમ્પર્કનું સરનામું, ચુકવણી પદ્ધતી, ચૂકવવાપાત્ર રકમ, ક્રેડિટ કે ડેબિટ કાર્ડ ની વિગત વિગેરે સામેલ છે.

3. ઇ-વોલેટ ના પ્રકારો:

રિઝર્વ બેંક ઓફ ઈન્ડિયાના નિયમો અનુસાર ભારતમાં ત્રણ પ્રકારના ઇ-વોલેટ છે.

3.૧) ક્લોઝ્ડ ઈ-વોલેટ:

ક્લોઝ્ડ ઇ-વોલેટ એટલે કોઈ કંપની પોતાના ગ્રાહકોની સગવડ માટે, તેના પ્લૅટફૉર્મ પર લેવડ દેવડ કરવા માટે ઓફર કરે તેવા વોલેટ છે. ખાસ કરીને ઘણીબધી શોપિંગ, હોટેલ, પ્લેન કે ટૅક્સી માટેની બુકિંગ સર્વિસ આ પ્રકારના વોલેટ ઓફર કરતી હોય છે. કોઈ કારણોસર જો આપણે બૂકિંગ કે ઓર્ડર કેન્સલ કરીએ તો આપણા નાણા રિફંડ તરીકે એજ વોલેટ માં જમા થાય. આ નાણા બેન્ક એકાઉન્ટ માં ટ્રાન્સફર ના કરી શકાય પણ ભવિષ્યમાં એ સાઇટ પર કોઈ ખરીદી કરીએ તો આ નાણાનો ઉપયોગ કરી શકાય. આવા વોલેટ ને રિઝર્વ બેંક ઓફ ઈન્ડિયાના નિયમન ની જરૂર પડતી નથી. બુકમાય શો, મેકમાય ટ્રીપ, ઉબેર, ઓલા વિગેરે આ પ્રકારના ક્લોઝડ ઇ-વોલેટ ની સુવિધા આપે છે.

૩.૨) સેમી-ક્લોઝ્ડ ઈ-વોલેટ:

સેમી-ક્લોઝ્ડ ઈ-વોલેટ એટલે એવા વોલેટ જેમાં આપણે ખાતું ખોલાવીએ, વાપરનારના વોલેટમાં રૂપિયા જમા કરાવી, એ વોલેટ સર્વિસે જે કંપનીઓ સાથે કરાર કર્યા હોય તેના માટે વાપરનાર મોબાઇલ વોલેટથી ચુકવણી કરી શકે છે. આ પ્રકારના વોલેટમાં પણ રૂપિયા જમા કર્યા પછી પરત બેન્ક ખાતામાં લઈ જઇ શકતા નથી કે જરૂર પડે ત્યારેએ વોલેટનો ઉપયોગ કરીને રોકડા રૂપિયા મેળવી શકાતા નથી. ફ્લિપકાર્ટ, ફ્રી ચાર્જ, મોબીક્વીક, પેટીએમ વિગેરે આ પ્રકારના **ક્લોઝ્ડ** વોલેટની સુવિધા આપે છે.

૩.૩) ઓપન વોલેટ:

ઓપન વોલેટ એટલે એવા વોલેટ કે જેનો ઉપયોગ ઓન લાઇન કે ઓફ લાઇન ખરીદી માટે થઈ શકે, જ્યાં કાર્ડ સ્વીકારાતા હોય ત્યાં પણ તેનો ઉપયોગ થઈ શકે. આ પ્રકારના વોલેટ ફક્ત બેન્ક ઓફર કરી શકે છે. ભીમ એપ, એરટેલ મની, એમ-પેસા, પે ઝેપ, વિગેરે આ પ્રકારનાં ઓપન વોલેટની સુવિધા આપે છે.

૪. ઇ-વોલેટ એકાઉન્ટ ખોલાવવા માટે જરૂરી વિગતો:

- ઉપભોક્તાનુ આખું નામ
- ઉપભોક્તાનો ઈમેલ આઈ ડી
- રજિસ્ટર્ડ મોબાઇલ નંબર

- ઉપભોક્તાની બેન્ક એકાઉન્ટ ડીટેલ અથવા તો ક્રેડિટ કાર્ડ/ડેબિટ કાર્ડ ડીટેલ
- ફુલ કે.વાય.સી. (Know Your Customer) માટે આધાર કાર્ડ
- પાન કાર્ડ, પાસપોર્ટ વિગેરે

રિઝર્વ બેંક ઓફ ઈન્ડિયાના નવા નિયમ પ્રમાણે ભારતમાં ઇ-વોલેટ ને **ફુલ કેવાયસી** સાથે લિન્ક કરવાનુ રહેશે. પહેલા **આંશિક કેવાયસી** પર વોલેટ લિન્ક થતાં હતા જેમાં ઉપભોક્તાના મોબાઇલ નંબર પર કે ઈ-મેઇલ આઈડી પર વેરિફીકેશન કોડ આવતો જેને વેરિફાય કરવાનો રહેતો હતો પણ હવે ઇ-વોલેટને આધાર કાર્ડ સાથે જોડીને આધાર સાથે લિન્ક મોબાઇલ મારફતે આવેલા વન ટાઇમ પાસવર્ડ(OTP)થી વેરિફાય કરવાનો રહેશે. જેને ફુલ કે.વાય.સી. કહેવાય છે. આંશિક કે.વાય.સી. વાળા વોલેટમાં મહિને દસ હજાર રૂપિયા સુધી લોડ કરી શકાય છે, જ્યારે ફુલ કેવાયસી વાળા વોલેટમાં એક લાખ રૂપિયા સુધી લોડ કરી શકાય છે.

૫. ઇ વોલેટ દ્વારા લેવામાં આવતી વિગતો:

ઉપભોક્તા જ્યારે આવા ઇ-વોલેટ પોતાના મોબાઇલમાં ડાઉનલોડ કરે છે અને વાપરવાનું ચાલુ કરે છે ત્યારે ઇ-વોલેટ દ્વારા ઉપભોક્તાની નીચે મુજબની માહિતી એકત્ર કરવામાં આવે છે.

- ઉપભોક્તાનું નામ અને સરનામું કે જે કેવાયસી ડોક્યુમેન્ટસમાં હોય તે.
- ઉપભોક્તાનો મોબાઈલ નંબર
- ઉપભોક્તાની બેન્ક એકાઉન્ટ અથવા તો ક્રેડિટ/ડેબિટ કાર્ડ ડીટેઇલ.
- ઉપભોક્તાનું ઈમેલ એડ્રેસ
- ઉપભોક્તાનું IP એડ્રેસ
- ઉપભોકતાની ડિવાઇસ ડીટેલ જેના પર વોલેટ ડાઉનલોડ કરવામાં આવ્યું છે
- ઉપભોક્તાનું જીપીએસ લોકેશન જો ઉપભોક્તા દ્વારા મોબાઇલ સેટિંગ્સમાં જઈને પરવાનગી આપવામાં આવી હોય તો
- ઉપભોક્તાના મોબાઇલ કૉન્ટૅક્ટ જો ઉપભોક્તા દ્વારા પરવાનગી આપવામાં આવી હોય તો
- ઉપભોક્તાની વેબ સર્ચ હિસ્ટરી જો ઉપભોક્તા દ્વારા પરવાનગી આપવામાં આવી હોય તો

<u>૬. ઇ-વોલેટ કમ્પની દ્વારા આપવામાં આવતી વિગતો:</u>

ઇ-વોલેટ કંપની દ્વારા નીચે મુજબની માહિતી માત્ર કાયદો અને વ્યવસ્થા જાળવતી એજન્સીઓને આપવામાં આવે છે. પોલીસ એના ઓફિસિયલ ઈ-મેઈલ આઈડી પર થી માહિતી માંગી શકે છે.

- ઉપભોક્તાનુ નામ અને સરનામું જે કે.વાય.સી. ડોક્યુમેંટ્સ માં હોય તે

- ઉપભોક્તાનો મોબાઈલ નંબર
- ઉપભોક્તાની બેન્ક એકાઉન્ટ અથવા ક્રેડિટ/ડેબિટ કાર્ડ ડીટેઇલ.
- ઉપભોક્તાનુ ઈમેઇલ એડ્રેસ
- ઉપભોક્તાનુ IP એડ્રેસ
- ઉપભોક્તાની ટ્રાન્જેક્શન ડિટેઇલ્સ જેવી કે બેન્કનુ નામ, ટ્રાન્જેક્શનની તારીખ અને સમય, જે એકાઉન્ટ કે વોલેટ માં રૂપિયા ટ્રાન્સફર થયા છે એનું નામ અને નંબર, ટ્રાન્જેક્શનની રકમ, વિગેરે.
- ઉપભોકતાની ડિવાઇસ ડીટેઇલ જેના પર વોલેટ ડાઉનલોડ કરવામાં આવ્યું છે
- મરચન્ટ ડીટેઇલ એટલે વેપારીની માહિતી જેની પાસેથી ઇ-વોલેટ મારફતે કોઈ ખરીદી કરવામાં આવી હોય.

<u>૭. ઇ-વોલેટ સંલગ્ન ક્યાં પ્રકાર ના ગુના થાય છે ?</u>

- ઓન-લાઈન બેન્કિંગ સિસ્ટમ નો ઉપયોગ કરવા માટે બેન્ક તરફથી યુઝરનેમ અને પાસવર્ડ આપવામાં આવે છે અને ઓન-લાઇન ટ્રાન્સફર કરવા માટે વન ટાઇમ પાસવર્ડ (OTP) ખાતાધારકના રજિસ્ટર્ડ મોબાઇલ નંબર પર મોકલવામાં આવે છે. આ વન ટાઇમ પાસવર્ડ સિસ્ટમ માં એડ કર્યા બાદજ ઓનલાઇન ટ્રાન્જેક્શન થાય છે.
- ઠગ ટોળકી ઇન્ટરનેટના માધ્યમનો ઉપયોગ કરીને યેન કેન પ્રકારે ભોગ બનનારનો યુઝરનેમ અને પાસવર્ડ મેળવી લે છે

અને તે પછી ભોગ બનનારના નામના બોગસ દસ્તાવેજ બનાવે છે અને ભોગબનનાર જે કંપનીનુ સિમકાર્ડ વાપરે છે એના ડિસ્ટ્રીબુટર પાસે જઈને સિમ કાર્ડ પડી ગયું હોવાનું બહાનું બનાવીને બોગસ દસ્તાવેજ આપીને નવું સિમકાર્ડ મેળવી લે છે અને પછી ઓન લાઈન ટ્રાન્જેક્શન કરે છે જેથી OTP નવા સિમકાર્ડ માં આવે છે અને આસાનીથી ટ્રાન્જેક્શન કરીને ફ્રોડ કરે છે. આ ટ્રાન્સફર કરેલા રૂપિયા ઘણા ઇ-વોલેટમાં ટ્રાન્સફર કરી દેવામાં આવે છે અને આ ઇ-વોલેટ મારફતે શોપિંગ કે મોબાઇલ રીચાર્જ કરવામા એ રૂપિયા બારોબાર બીજા ઇ-વોલેટ કે બેન્ક ખાતા માં ટ્રાન્સફર કરી દેવામાં આવે છે.

- ઠગ ટોળકી જે લોકો બેન્કિંગ સિસ્ટમથી અજાણ હોય એમને મુખ્ય ટાર્ગેટ બનાવે છે. ઠગ ટોળકી આવા લોકોને કોલ કરીને બેન્કથી વાત કરું છું કે ઇન્સ્યોરન્સ કંપનીથી વાત કરું છું એમ કહીને વિશ્વાસમાં લઈને એમના એટીએમ કાર્ડ કે ડેબિટ કાર્ડ ની સંપૂર્ણ વિગતો જેવી કે કાર્ડ નંબર, એક્સપાયરી ડેટ, સી.વી.વી. નંબર મેળવી લે છે અને પછી OTP પણ માંગી લે છે. આ બધી વિગતો મેળવ્યા બાદ ઓન-લાઇન ફ્રોડ ટ્રાન્જેક્શન કરે છે અને વિવિધ ઇ-વોલેટમાં રૂપિયા ટ્રાન્સફર કરી દે છે.
- આજકાલ આવી ઠગ ટોળકી દ્વારા ક્લોનિંગ કાર્ડ વાપરીને પણ ફ્રોડ કરવામાં આવે છે. ક્લોનિંગ કાર્ડ એટલે ખાતાધારક ના કાર્ડની ડુપ્લિકેટ કોપી. ઓછા જાણીતા રેસ્ટોરન્ટ કે દુકાનમાં અથવા તો એટીએમ મશીનમાં કાર્ડ ક્લોનિંગ મશીન લગાવી

દે છે એટલે જ્યારે ઉપભોક્તા આવી જગ્યાએ કાર્ડ સ્વાઇપ કરે તો એના કાર્ડની માહિતી કાર્ડ ક્લોનિંગ મશીનમાં આવી જાય છે જેના પરથી નવું ક્લોનિંગ કાર્ડ બનાવીને ઓન લાઇન ફ્રોડ ટ્રાન્જેક્શન કરીને ઇ-વોલેટો માં રૂપિયા ટ્રાન્સફર કરી દેવામાં આવે છે.

- ઘણી બધીવાર આવી ઠગટોળકી દ્વારા ઈમેઇલ દ્વારા ઈનામ ની લાલચ આપી, લોટરીની લાલચ આપી, લગ્ન ની લાલચ, વિગેરે લાલચ આપી ઠગટોળકી દ્વારા ઓન-લાઇન ફ્રોડ ટ્રાન્જેક્શન કરાવી આવા ઇ-વોલેટો માં રૂપિયા જમા કરાવવામા આવે છે.

૮. ઇ-વોલેટ ફ્રોડ ની તપાસ:

- ઇ-વોલેટ પાસે માહિતી માંગવા માટે સૌથી પહેલા ફરિયાદીનું બેન્ક સ્ટેટમેંટ જોવું, જેથી ખબર પડે કે ફરિયાદીના રૂપિયા કઈ કંપનીના ઇ-વોલેટમાં ટ્રાન્સફર થયા છે. બેન્ક સ્ટેટમેંટ માટે સૌથી પહેલા ફરિયાદી જે બેન્ક નુ ક્રેડિટ/ડેબિટ કાર્ડ વાપરતો હોય તેને સી.આર.પી.સી. ની કલમ-91 મુજબની નોટીસના અધારે ખોટા ટ્રાન્જેક્શનની માહિતી મેળવવી.
- બેન્ક સ્ટેટમેંટના આધારે આવેલી માહિતીમાં જે જે કંપની ના વોલેટમાં રૂપિયા ગયા હોય તે કંપનીઓ ને ટ્રાન્જેક્શન અટકાવી દેવા તથા આ ટ્રાન્જેક્શન કોણે કરેલ છે અને ટ્રાન્જેક્શન થી કોને લાભ થયેલ છે તેનું નામ, સરનામું,

મોબાઇલ નંબર, ઈમેલ આઈડી, આઈપી એડ્રેસ વિગેરેની માહિતી માંગવાની રહેશે.

- "**NOTICE UNDER SECTION CRPC-91**" ના આધારે એક લેટર બનાવવાનો રહેશે. આ લેટર અંગ્રેજીમાં બનાવવો જરૂરી છે કેમકે લગભગ બધીજ ઇ-વોલેટ કંપનીઓનું હેડ ક્વાર્ટર ગુજરાત રાજ્યની બહાર આવેલુ છે. લેટર પર પોલીસ સ્ટેશનનો ગોળ સિક્કો મારીને લેટર ને સ્કૅન કરીને ઇ-વોલેટ કંપનીના ઈમેઇલ આઈડી પર મોકલવાનો હોય છે. ઇ-વોલેટનો ઈમેઇલ આઈડી કંપની ની contact us માં આપેલો હોય છે. અહિયા આ પ્રકરણ ના અંત માં લગભગ બધાજ નોડલના ઈમેઇલ આઈડી અને કૉન્ટૅક્ટ નંબર આપેલા છે.
- લેટરમાં બનાવની ટૂંકી વિગત અને થયેલ ફ્રોડ ટ્રાન્જેક્શનની વિગત દર્શાવવી.

Notice Under Section CRPC – 91

Outward No.JPR/673/2017
Cyber Crime Cell, Crime Branch,
Ahmedabad, Gujarat
Date: 10/08/2017

To,
security@paytm.com
cybercell@paytm.com

Subject: Provide details of fraudulent transaction.

I, the undersigned, Police Sub Inspector J P Rojiya, Cyber Crime Cell, Crime Branch, Ahmedabad, Gujarat.

I am investigation officer of the criminal application no. G/725/DCP/CRIME/LA/673/2017. The complainant was cheated by telling him that loan amount of 5 lacs has been approved in his name from Bajaj Finance and to process it he will have to pay certain amount which he will have to pay via Paytm in the mobile number 8506923938. In this matter the complaint holds PAYTM A/C under his mobile number 9909821252.

Transaction date	Wallet Txt ID	Amount(Rs.)	Company Name	Beneficiary Mobile Number
17/06/2017	11517635590	168	Bajaj Finserv Limited	8506923938
17/06/2017	11509465826	5000	Bajaj Finserv Limited	8506923938
17/06/2017	11509451298	5000	Bajaj Finserv Limited	8506923938
17/06/2017	11509432406	5000	Bajaj Finserv Limited	8506923938
17/06/2017	11509312234	1500	Bajaj Finserv Limited	8506923938

So, please provide details of merchant Name, merchant id, Beneficiary name, address, contract details, Device information, trip history and IP Address.

So it is requested you to provide this information as soon as possible.

Thanking you,

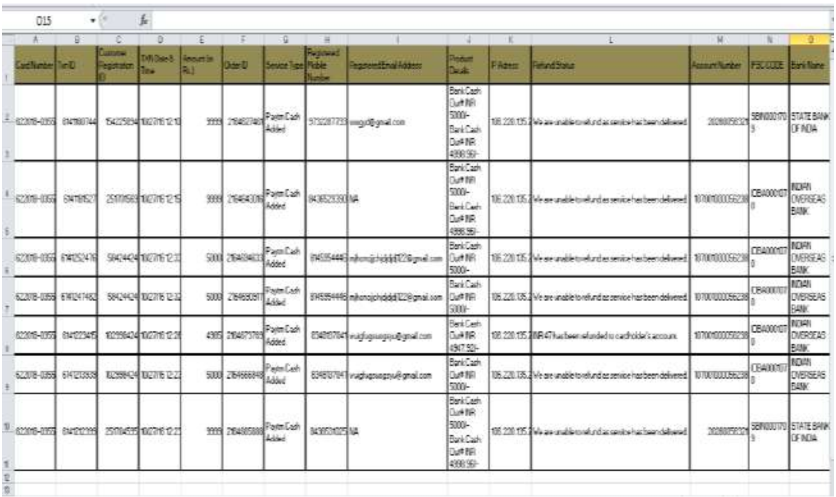
(J.P.Rojiya)
Police Sub Inspetor
Cyber Crime Cell
Crime Branch,Ahemedabad City,
Gujarat, India

My Office Address is :

Cyber Crime Cell, Crime Branch,
Bunglow no.15, Near IPS Mess,
Airport road, Shahibaug
Ahmedabad City, Gujarat, India.
pi-cybercrime-ahd@gujarat.gov.in
9898118843

૯. ઇ-વોલેટ કમ્પની તરફથી આવતી માહિતીના ફૉર્મેટ :

- લેટરના જવાબમાં ઇ-વોલેટ કંપની ઓફિશિયલ ઈમેઇલ આઈડી પર માહિતી મોકલે છે.
- અલગ અલગ ઇ-વોલેટ કંપની પાસેથી આવતી માહિતી અલગ અલગ ફૉર્મેટમાં હોય છે પણ એમાં રહેલી માહિતી લગભગ એક સરખી હોય છે.
- નીચે અમુક ઇ-વોલેટમાંથી આવતી માહિતીના ઉદાહરણ આપવામાં આવ્યા છે.
- **Pay Tm**



Card Number	Txn ID	Customer Registration ID	TXN Date & Time	Amount (in Rs.)	Order ID	Service Type	Registered Mobile Number	Registered Email Address	Product Details	IP Address	Refund Status	Account Number	IFSC CODE	Bank Name
[illegible]	[illegible]	[illegible]	10/27/16 12:[illegible]	9999	[illegible]	Paytm Cash Added	[illegible]	[illegible]@gmail.com	Bank Cash Out# INR 5000/- Bank Cash Out# INR 4998.96/-	106.220.135.2	We are unable to refund as service has been delivered	[illegible]	SBIN0001709	STATE BANK OF INDIA
[illegible]	[illegible]	[illegible]	10/27/16 12:[illegible]	9999	[illegible]	Paytm Cash Added	[illegible]	NA	Bank Cash Out# INR 5000/- Bank Cash Out# INR 4998.96/-	106.220.135.2	We are unable to refund as service has been delivered	[illegible]	IOBA0001070	INDIAN OVERSEAS BANK
[illegible]	[illegible]	[illegible]	10/27/16 12:[illegible]	5000	[illegible]	Paytm Cash Added	[illegible]	[illegible]@gmail.com	Bank Cash Out# INR 5000/-	106.220.135.2	We are unable to refund as service has been delivered	[illegible]	IOBA0001070	INDIAN OVERSEAS BANK
[illegible]	[illegible]	[illegible]	10/27/16 12:[illegible]	5000	[illegible]	Paytm Cash Added	[illegible]	[illegible]@gmail.com	Bank Cash Out# INR 5000/-	106.220.135.2	We are unable to refund as service has been delivered	[illegible]	IOBA0001070	INDIAN OVERSEAS BANK
[illegible]	[illegible]	[illegible]	10/27/16 12:[illegible]	4985	[illegible]	Paytm Cash Added	[illegible]	[illegible]@gmail.com	Bank Cash Out# INR 4947.52/-	106.220.135.2	INR 47 has been refunded to cardholder's account.	[illegible]	IOBA0001070	INDIAN OVERSEAS BANK
[illegible]	[illegible]	[illegible]	10/27/16 12:[illegible]	5000	[illegible]	Paytm Cash Added	[illegible]	[illegible]@gmail.com	Bank Cash Out# INR 5000/-	106.220.135.2	We are unable to refund as service has been delivered	[illegible]	IOBA0001070	INDIAN OVERSEAS BANK
[illegible]	[illegible]	[illegible]	10/27/16 12:[illegible]	9999	[illegible]	Paytm Cash Added	[illegible]	NA	Bank Cash Out# INR 5000/- Bank Cash Out# INR 4998.96/-	106.220.135.2	We are unable to refund as service has been delivered	[illegible]	SBIN0001709	STATE BANK OF INDIA

- ## Pay u money

From: Gurpal Kumar [mailto:gurpal.kumar@payu.in]
Sent: 11\12\2014 3:44 PM
To: READER CRIME AHD(GoG-Home Dept.)
Cc: 'PAYU'
Subject: RE: SR 16730 - 3375 PSI BH KOROT.pdf [Support #238633]

Hi All,
Please find below detail

PayU ID	Date	Merchant URL	Transaction ID	Transaction Fee	Payment Gateway	Bank Name	Status	Product Info	Customer Name	Customer Phone	Customer IP Address	Name on Card	Card Number	Bank Reference No
114818765	13/06/2014 06:42:42	www.mapdal.com	2125003102	17567.00	SBIPG	Credit Card	Transaction Successful	22468353	chandan kr jha	8376977964	223.176.196.128	j K KAPADIYA	517653XXXXXX3000	201401362341

Thanks and Regards,
Gurpal Kumar

From: care@payumoney.com [mailto:care@payumoney.com]
Sent: Thursday, December 11, 2014 1:39 PM
To: disputes@payu.in
Cc: gurjodhpal.singh@payumoney.com; vivek.yadav@payu.in; vishwas.singh@payu.in; care@payumoney.com
Subject: Re: SR 16730 - 3375 PSI BH KOROT.pdf [Support #238633]

- ## Free Charge

From: Risk [mailto:risk.team@freecharge.com]
Sent: 10/05/2016 11:52
To: READER CRIME AHD(GoG-Home Dept.)
Subject: Re: [#3671763] SR 8988 - 1265 PI JSG

Dear Sir

This is in regards to your mail concerning unauthorized transaction. Please note that the transaction amount has been completely used by end user
We have suspended his FreeCharge account to prevent any future misuse.
User has utilized the amount to avail the following services and the beneficiary details are listed below. We hope this information will help you for further investigation.

Order Id	PG ID	Amount	Card No	IP Address	Email ID	Transaction Date & Time	Registered Mob No.	Status
OC-3148467089-1462360900465	579437348	10000	459151XXXXXX8346	223.231.59.197	kumar101@gmail.com	5/4/2016 16:54	8292068279	User created Virtual card (card # 557783XXXXXX4436) by using Wallet amount & has utilized entire amount on different Merchant's Website

Regards,
Dispute Management Team
www.freecharge.in

On Fri, 6 May at 12:09 PM , care@freecharge.com <care@freecharge.com> wrote:
Dear Sir,

We have suspended Fraudulent person FreeCharge account to prevent any future misuse. Beneficiary details will be shared shortly.

Regards,
Dispute Management Team

P.S: To ensure safe online transaction, refrain yourself from sharing your account / card information with anyone.

On Thu, 5 May at 7:38 PM , READER CRIME AHD(GoG-Home Dept.) <reader-crime-ahd@gujarat.gov.in> wrote:

- **OXIGEN**

From: Fraud Control [mailto:fraud.control@myoxigen.com]
Sent: 30 August 2017 16:18
To: READER CRIME AHD(GoG-Home Dept.)
Subject: Re:[## 643917 ##] Fwd: SR 12078 - 1877 PI JSG

Dear Sir/Madam,

Please find enclosed IP details and refund details.

Transaction ID	Date	PayU ID	Amount	Status	Customer Name	Card Number	Customer Phone	Customer IP Address	Balance left
Mob6867091	19/07/2017 18:31:10	6289965288	4000	Captured	Oxigen	652196XXXXXX1460	919102277605	223.230.220.160	0

Transaction details attached in PDF for your reference.

Fraud can be reported at fraud.control@myoxigen.com

Regards
Neeraj Kumar
Risk & Fraud management
Oxigen Services India Private Limited, An ISO 9001:2008 certified company ; www.myoxigen.com; www.oxigenwallet.com
Building No 94, Institutional Area, Sector 32 Gurgaon, 122001 Haryana.
---- On Tue, 1 Aug 2017 12:42:05 +0530 care@oxigenwallet.com wrote ----

- આમ ઇ-વોલેટના જવાબ થી જે માહિતી મળે છે તેના આધાર પર લાભકર્તાનો મોબાઇલ નંબર અને નામ મળી રહે છે. આ મોબાઇલ નંબરના આધારથી ઠગબાજ સુધી પહોચી શકાય છે પરંતુ આવા કિસ્સાઓમા જોવા મળતા ઠગબાજ બહુ હોશિયાર હોય છે અને ડમી સિમકાર્ડ અને ડમી નામ વાપરતા હોય છે. તેથી આવા ઠગબાજ સુધી પહોચવા માટે આઈપી એડ્રેસ ખૂબ ઉપયોગી નીવડે છે.
- ઇ-વોલેટ તરફથી આપવામાં આવેલ IP કઇ કંપનીના છે તે જાણવા માટે ગુગલ પર WHATISMYIPADDRESS, IP2LOCATION, IP LOCATOR જેવી વેબસાઇટ ખોલી ઇ વોલેટ માંથી આવેલ IP સિલેકટ કરી ઉપર જણાવેલ વેબસાઇટમાં જઇ આ IP કઇ સર્વિસ પ્રોવાઇડર કંપનીના છે તે જોઇ લેવું.

ઉપરોકત આઇએસપી (સર્વિસ પ્રોવાઇડર) આ આઇપી કોને ક્યારે વપરાશ માટે આપેલા છે તે જાણવા માટે સર્વિસ પ્રોવાઇડર કંપનીને સીડીઆર/આઇપીડીઆર આપવા લેટર મોકલવો.

પ્રકરણ ૭

મોબાઈલ ડિવાઈસ

પ્રકરણ નો ઉદ્દેશ: ગુનામાં ઉપયોગ કરેલ મોબાઈલ ડિવાઈસને જપ્ત કરી ગુનાની તપાસને સાંકળતાં ઘણાં પુરાવા અથવા ગુનાને લગતી ઘણી બાબતો જાણી શકાય છે. આ પ્રકરણમાં મોબાઈલ ડિવાઈસ માંથી માહિતી એકત્ર, વિશ્લેષણ અને પ્રસ્તુત કરવાની રીતની ચર્ચા કરવામાં આવી છે.

૧. મોબાઈલ ડિવાઈસ માંથી કેવાં પ્રકારની માહિતી મેળવી શકાય:

કોઈ પણ મોબાઈલ ડિવાઈસ માંથી ગુનાને લગતી નીચે મુજબની માહિતી મેળવી શકાય છે.

- ડાયલ, રિસીવ અને મિસ્ડકોલ ની માહિતી
- લખેલાં, મોકલેલા, અથવા સંગ્રહ કરેલા મેસેજની માહિતી
- કોન્ટેક્ટ નંબરની માહિતી
- કોલ રેકોર્ડિંગ્સ (જો કોલ રેકોર્ડિંગ એપ્લિકેશન હશે તો)
- કેમેરા દ્વારા ખેચેલી તસ્વીરો, વિડિયો અને ડૉક્યુમેન્ટસ
- બીજાએ મોકલેલી માહિતી, જેવી કે તસ્વીરો, વિડીયો, ડૉક્યુમેન્ટસ,
- વેબ બ્રાઉઝરથી ઓપન કરેલી વેબસાઈટની માહિતી
- યૂ ટ્યુબમાં અપલોડ તેમજ ડાઉનલોડ કરેલા વિડિયોની માહિતી

- કઈ કઈ અપ્લિકેશન નો ઉપયોગ કરે છે એની માહિતી
- ડિવાઈસમાં કયુ ઈ-મેઇલ વાપરી રહેલ છે તે ઈ-મેઇલ આઈડીની માહિતી
- સોશિયલ મિડિયાને લગતી માહિતી, જેમ કે ફેસબુક, વ્હોટ્સ-એપ, ટ્વીટર, ઈન્સ્ટાગ્રામ, ટેલીગ્રામ, વિગેરે
- ગુન્હા સાથે સંકળાયેલા બીજા શંકાસ્પદ વ્યક્તિઓની માહિતી અને તેઓ સાથે થયેલ સંદેશાવ્યવહાર અને કોલની માહિતી વિગેરે....

૨. જપ્તી સમયે રાખવામાં આવતી સાવચેતી તેમજ પંચનામામાં નોંધવા લાયક બાબતો:

કોઈપણ પ્રકારના ઘટનાસ્થળ પર જો કોઈ મોબાઈલ ડિવાઈસ મળે તો નીચે મુજબના નિયમો અનુસાર માહિતી ની નોંધ અચૂકપણે લેવી, જેથી કરીને તે ડિવાઈસની ઓળખ અને તેમાં રહેલી માહિતીને નુકસાન ન પહોંચે. તેમજ જપ્ત કરેલ તમામ ડિવાઈસ કે વસ્તુઓને વ્યવસ્થિત લેબલિંગ કરી પંચનામાની પ્રક્રિયા પૂર્ણ કરીને FSL માટે મોકલી આપવી.

1. મોબાઈલ ડિવાઈસને ફિજીકલ નુકશાન કે ડેમેજ ન થાય તેની સાવચેતી રાખવી.
2. સૌ પ્રથમ મોબાઈલ ચાલુ છે કે બંધ હાલતમાં તે ચકાસી લેવું.
3. મોબાઈલ ડિવાઈસ બંધ હોય ત્યારે તેને ચાલુ કરવાનો પ્રયત્ન કરવો નહિ.

4. જો મોબાઈલ ડિવાઈસ બંધ હોય ત્યારે પંચો રૂબરૂ મોબાઇલના માલિક દ્વારા ફોન ચાલુ કરાવીને મોબાઈલ ડિવાઇસનું લોક ખોલાવી તેનુ પંચનામું કરી મોબાઈલમાં Airplane Mode ને on કરી દેવો.
5. જો મોબાઈલ ચાલુ હાલતમાં હોય તો Airplane Mode on કરી દેવું. (Airplane Mode on કરવાની પ્રક્રિયા નીચે જણાવેલ છે)

<u>૨.૧) જ્યારે મોબાઈલ ચાલું હાલત માં હોય ત્યારે Airplane Mode ને On કરવાની રીત:-</u>

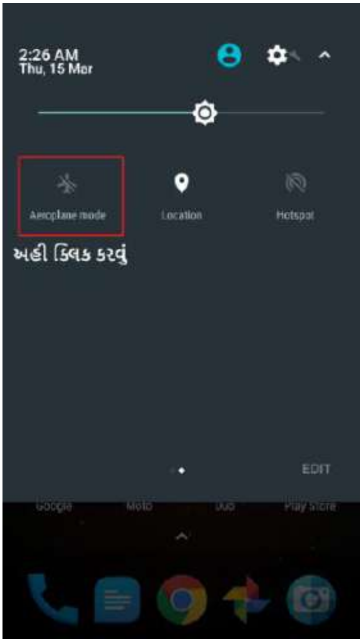
જો મોબાઈલ ચાલુ હાલતમાં હોય તો ચકાસણી કરો કે નોટીફીકેશન વિન્ડો ખુલે છે કે નહિ? (કારણ કે ઘણા મોબાઈલ ડિવાઈસ એવા હોય છે કે મોબાઈલમાં લોક હોય તો Airplane Mode ને On કરી શકાય છે તેમજ ઘણાં મોબાઈલ ડિવાઇસમાં લોક હોય ત્યારે તેમાં Airplane Mode ને On કરી શકાતો નથી, જેની વિસ્તૃત જાણકારી નીચેનાં મુદાઓમાં બતાવેલ છે.)

૨.૨) જો મોબાઈલ ડિવાઈસમાં લોક હોય:

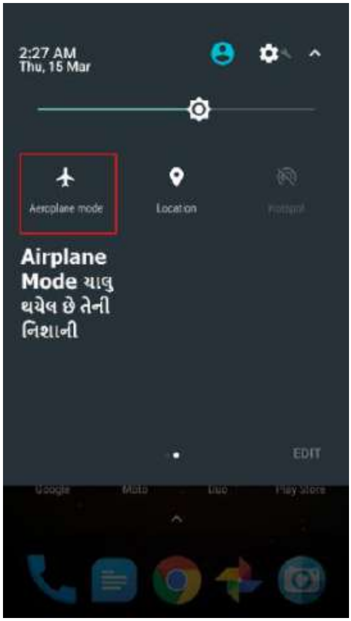
જો મોબાઈલ ડિવાઈસમાં લોક હોય તેમજ નોટીફીકેસન વિન્ડો ખુલતું હોય અને Airplane Mode ને ON કરી શકાતું હોય ત્યારે નીચે મુજબનાં સ્ટેપ્સને અનુસરવું.

➔ સૌપ્રથમ મોબાઈલ ડિવાઈસમાં ઉપરથી નોટિફિકેશન વિન્ડો ને નીચે swipe કરવું.

➔ તેમાં દર્શાવેલ Airplane Mode ની નિશાની પર ક્લિક કરવું



➔ ક્લિક કરવાથી Airplane Mode On થઇ જશે.

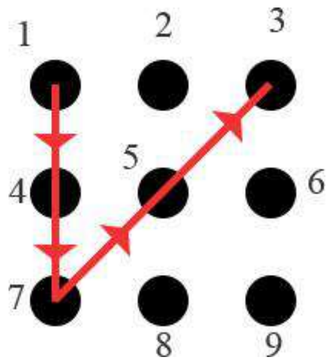


જો મોબાઈલ ડિવાઈસ લોક હોય અને નોટીફીકેશન વિન્ડો ખુલતું હોય અને Airplane Mode ને ON કરી શકાતું ન હોય ત્યારે નીચે મુજબનાં સ્ટેપ્સને અનુસરવું:-

- ➔ સૌપ્રથમ તો આ મોબાઈલ ડિવાઈસનો યુઝર કોણ છે તે જાણવાનું રહેશે.
- ➔ જો સ્થળ પર મોબાઈલ ડિવાઈસનાં યુઝર હાજર ન હોય ત્યારે મોબાઈલ ડિવાઇસને જે તે સ્થિતિમાં રાખી પંચનામાંની પ્રક્રિયા કરીને FSL મા મોકલવું.

- ➔ જો સ્થળ પર મોબાઈલ ડિવાઈસનાં યુઝર હાજર હોય તો તેમની પાસેથી મોબાઈલ ડિવાઈસનાં પીનકોડ/પાસવર્ડ/પેટર્ન લોકની માહિતી મેળવીને તેની નોંધ કરવી અને તપાસ કરતાં અધિકારીશ્રીએ પંચો રૂબરૂમાં તે મોબાઈલ ડિવાઈસને મોબાઇલનાં યુઝર દ્વારા પીનકોડ/પાસવર્ડ/પેટર્ન લોક અનલોક કરાવી લેવું અથવા પીનકોડ/પાસવર્ડ/પેટર્ન લોક નો પંચનામાં ઉલ્લેખ કરવો.

  (તપાસ કરતા અધિકારીશ્રી એ ધ્યાનમાં રાખવું કે કોઈપણ પ્રકારના ડેટા ડિલીટ/ટ્રાન્સફર/ફોર્મેટ/કોપી કરે નહિ તેની તકેદારી રાખવી)
- ➔ મોબાઈલ ડિવાઈસમાં જ્યારે પેટર્ન લોક હોય ત્યારે મોબાઈલ ડિવાઈસનાં યુઝર પાસેથી પેટર્ન લોકની ડિઝાઇન મેળવીને નોંધ કરવા માટે નીચે મુજબની ટેકનીકનો ઉપયોગ કરીને પંચનામાં મા ઉલ્લેખ નીચે મુજબ કરવો.



ઉપર્યુક્ત પેટર્નની નોંધ લેવા પ્રત્યેક dots ને અનુરૂપ નંબર આપી દેવા. તથા રફ ચિત્ર બનાવી દેવું. તેમાં પેટર્નની દિશા આપવાનું ખાસ ધ્યાન રાખવું.તથા જેમ જેમ જે નંબરના dot પરથી પેટર્ન પસાર થાય તે નંબરની નોંધ લેતી જવી. ઉપર ઉદાહરણ માં પેટર્નનો નંબર ની ભાષા માં રૂપાંતર નીચે મુજબ થશે.

1→ 4 → 7 → 5 → 3

- ➔ પિનકોડ/પાસવર્ડ/પેટર્ન ને મોબાઈલ યુઝર દ્વારા અનલોક કરી દીધા બાદ આગળના મુદ્દામાં દર્શાવેલ રીત મુજબ Airplane Mode ને On કરી દેવું.
- ➔ મોબાઈલ ડિવાઈસમાં જ્યારે ફિંગરપ્રિન્ટ લોક/ફેશ લોક/ઈરિશ લોક હોય ત્યારે તપાસ કરનાર અધિકારીશ્રીએ પંચોની રૂબરૂમાં તે મોબાઈલ

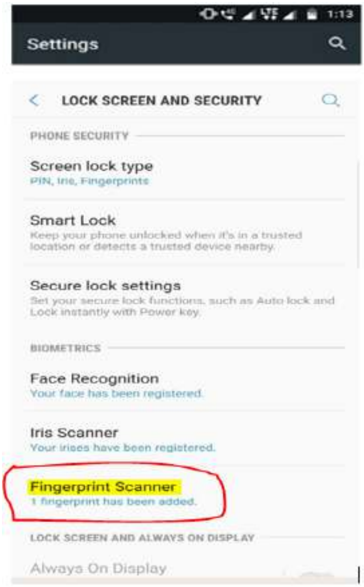
ડિવાઈસમાં જે પ્રકારનું લોક હોય તેને મોબાઇલનાં યુઝર પાસેથી અનલોક કરાવી લેવું. (ધ્યાનમાં રાખવું કે યુઝર કોઈપણ પ્રકારનાં ડેટા ડિલીટ/ટ્રાન્સફર/ફોર્મેટ કરે નહિ તેની તકેદારી રાખવી) તેમજ જે પ્રકારનુ લોક રાખવામાં આવેલ હોય તેનો પણ પંચનામાં મા ઉલ્લેખ કરવો.

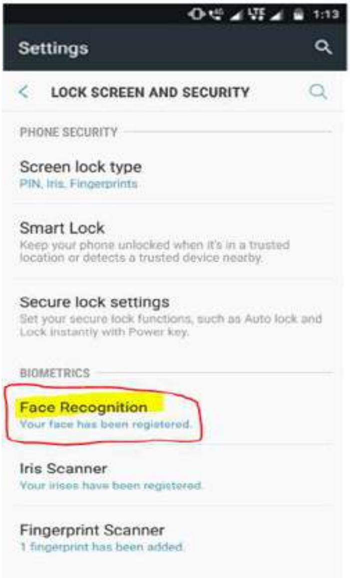
<u>નોંધ:-</u> જ્યારે અમુક કિસ્સામાં મોબાઈલ યુઝરને ફિંગરપ્રિન્ટ લોક/ફેશ લોક/ઈરિશ લોક રીમુવ કરતાં ન આવડતું હોય ત્યારે નીચે મુજબના સ્ટેપ્સ અનુસરવા.

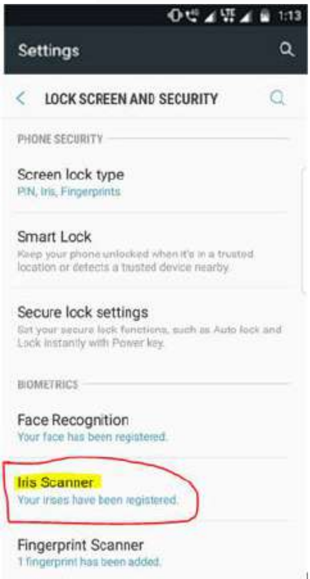
<u>3. ફિંગરપ્રિન્ટ લોક /ફેશ લોક/ઈરિશ લોક દૂર કરવાની પધ્ધતિ:</u>

➔ All Application પર જઈને settings ઓપન કરો. settings માં નીચે સ્ક્રોલ કરીને Lock screen and Security ટેબ શોધો અને તેને ઓપન કરો.

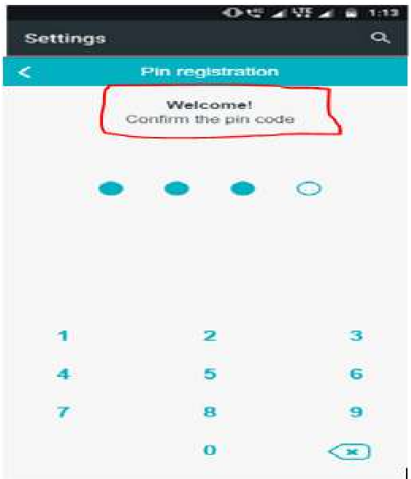
➔ ત્યાર બાદ Fingerprint/Face Recognition/Iris scanner મેનુ પર ક્લિક કરો



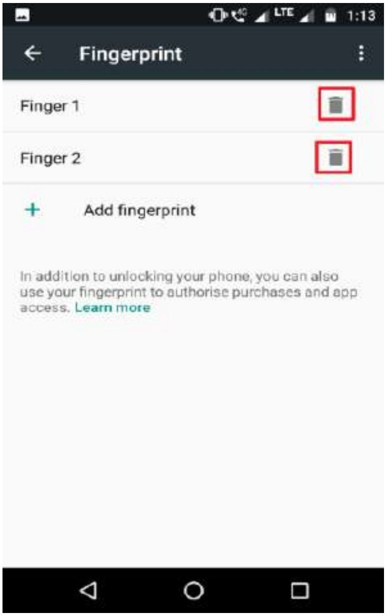

1:13
Settings
LOCK SCREEN AND SECURITY
PHONE SECURITY
Screen lock type
PIN, Iris, Fingerprints
Smart Lock
Keep your phone unlocked when it's in a trusted location or detects a trusted device nearby.
Secure lock settings
Set your secure lock functions, such as Auto lock and Lock instantly with Power key.
BIOMETRICS
Face Recognition
Your face has been registered.
Iris Scanner
Your irises have been registered.
Fingerprint Scanner
1 fingerprint has been added.

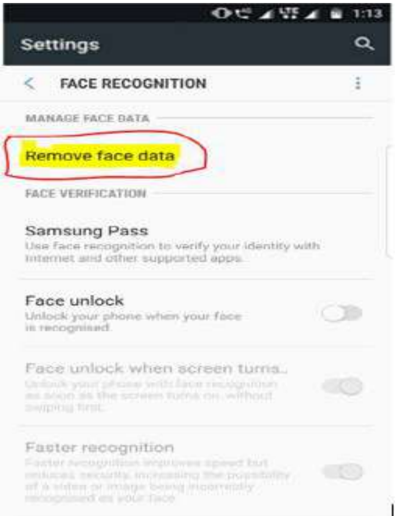

1:13
Settings
LOCK SCREEN AND SECURITY
PHONE SECURITY
Screen lock type
PIN, Iris, Fingerprints
Smart Lock
Keep your phone unlocked when it's in a trusted location or detects a trusted device nearby.
Secure lock settings
Set your secure lock functions, such as Auto lock and Lock instantly with Power key.
BIOMETRICS
Face Recognition
Your face has been registered.
Iris Scanner
Your irises have been registered.
Fingerprint Scanner
1 fingerprint has been added.

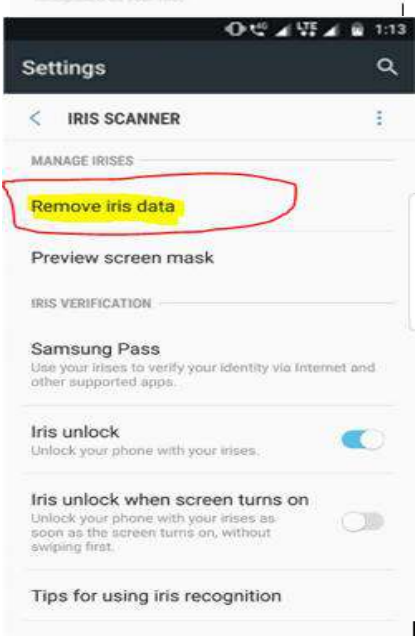
➔ તેના પર ક્લિક કરવાથી જો કોઈ Pattern/પીન કોડ પૂછે તો મોબાઈલ ના યુઝર ને પૂછીને તે નાખવો.



➔ ઓપન થયેલ વિન્ડો માં જેટલી પણ fingerprint હોય તેની બાજુમાં રહેલ ડીલીટ બટન પર ક્લિક કરવાથી જે તે ફિંગરપ્રિન્ટ/ફેશ લોક/ઈરિશ લોક રિમૂવ થઈ જશે..




1:13
Settings
FACE RECOGNITION
MANAGE FACE DATA
Remove face data
FACE VERIFICATION
Samsung Pass
Use face recognition to verify your identity with internet and other supported apps.
Face unlock
Unlock your phone when your face is recognised.
Face unlock when screen turns...
Faster recognition


1:13
Settings
IRIS SCANNER
MANAGE IRISES
Remove iris data
Preview screen mask
IRIS VERIFICATION
Samsung Pass
Use your irises to verify your identity via Internet and other supported apps.
Iris unlock
Unlock your phone with your irises.
Iris unlock when screen turns on
Unlock your phone with your irises as soon as the screen turns on, without swiping first.
Tips for using iris recognition

➔ ફિંગરપ્રિન્ટ/ફેશ લોક/ઈરિશ લોક રિમૂવ કરવાથી મોબાઈલ અનલોક થઈ જશે અને આગળ દર્શાવેલ રીત મુજબ Airplane Mode ને On કરી દેવું.

૪. મોબાઈલ ડિવાઈસ: સર્ચ, સીઝર અને સંગ્રહ ની સામાન્ય માર્ગદર્શિકા:

a) જ્યારે વધારે સંખ્યામાં મોબાઈલ ડિવાઈસ મળી આવે ત્યારે બધાં મોબાઈલ ડિવાઈસ માંથી મળેલ સિમ કાર્ડ, મેમરી કાર્ડ, બેટરી છૂટા રાખવા નહિ,કે જેથી બધી વસ્તુઓ એક બીજા સાથે ભળી ન જાય.

b) જો મોબાઈલ ફિજીકલી ડેમેજ્ડ હાલતમાં અથવા પાણીથી પલળેલો હોય તો મોબાઈલને ચાલુ કરવાનો પ્રયત્ન કરવો નહિ.

c) મોબાઈલ ડિવાઈસ નો રંગ, મોબાઈલ બનાવનાર કમ્પનીનું નામ, IMEI નંબર, મોબાઈલ નંબર, IMSI નંબર, મેમરી કાર્ડની વિગત અને બાહ્ય સ્થિતિની પંચનામા માં નોંધી કરવી.

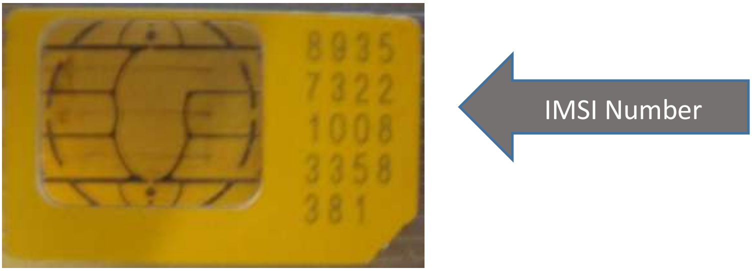
d) જો મોબાઈલ બંધ હાલતમાં હોય તો તેનાં પાછળનાં ભાગે દર્શાવેલો IMEI નંબર લખેલો હોય તો તે નોંધી લેવો. ઘણાં મોબાઈલ ડિવાઈસમાં પાછળનાં ભાગે IMEI નંબર લખેલો હોતો નથી ત્યારે મોબાઈલની બેટરી કાઢી તે મોબાઈલનો IMEI નંબર મેળવી લેવો જે નંબર જાણવા માટે બેટરી વાળી જગ્યાએ જોવું,

ત્યાં મોડલ નંબર તથા IMEI નંબર જોવા મળે તેની નોંધ કરી લેવી (આ IMEI નંબર મોબાઈલ ની પાછળના ભાગ માં બેટરી દૂર કરતાં 15 અંકનાં નંબર નું સ્ટીકર જોવા મળશે, જે નંબર IMEI નંબર કહેવામા આવે છે.)

<u>નોંધ:-</u> જો મોબાઈલ ડિવાઈસનું મોડેલ જાણવા ન મળે ત્યારે IMEI નંબર ઉપર થી જાણી શકાય છે, તે માટે નીચે જણાવેલ વેબસાઇટ ઉપર જઈને IMEI નંબરના ચેક બોક્ષ માં 15 અંકનો IMEI નંબર નાખવાથી મોબાઈલ ડિવાઈસનાં મોડેલ ની માહિતી મળી રહેશે. વેબસાઈટ :- http://www.imei.info/

e) જ્યારે ડબલ સીમ વાળો મોબાઈલ ડિવાઈસ હોય ત્યારે તેમાં બે સિમ કાર્ડો મળી આવે તો તે બંને સિમ કાર્ડો કયા સિમ-ટ્રે (ખાનામાં) માં હતા તે ખાસ જોવાનું રહેશે તેમજ તે સિમ ટ્રે નં-1 અને સિમ ટ્રે નં-2 મુજબ

બે IMEI ની નોધ કરવાની રહેશે, તેમજ આ સિમકાર્ડો ઉપર લખેલ IMSI નંબર જે 15 અંક નો હશે તે તથા તે સીમ કાર્ડોના સર્વિસ પ્રોવાઈડરની માહિતી વિગેરેની નોંધ કરી લેવી.



f) મોબાઈલ ડિવાઈસની સાથે જો કોઈ કેબલ કે કોઈ પણ બીજી વસ્તુ મળી આવે તો એને પણ જપ્ત કરવી. જપ્ત કરેલ મોબાઈલ ડિવાઈસ તથા દરેક વસ્તુ પર યોગ્ય લેબલ લખીને ચીપકાવવું.

g) આ ઉપરાંત ઉપર બતાવેલ પ્રક્રિયા પૂર્ણ થતાં મોબાઈલમાં સિમ કાર્ડ તેમજ બેટરી જે હાલત માં હતા તે જ હાલતમાં પાછા ફિટ કરી ને મોબાઈલને પેકિંગ પંચનામું કરી FSL માટે રવાના કરવાનો રહેશે.

h) મોબાઈલ ડિવાઈસ ની સાથે જો કોઈ કેબલ કે કોઈ પણ બીજી વસ્તુ મળી આવે તો તે પણ જપ્ત કરવી. જ્યારે બનાવવાળી જગ્યાએથી એક કરતાં વધું મોબાઈલ ડિવાઇસ કે અન્ય સાધનો કબ્જે કરવામાં આવે ત્યારે દરેક વસ્તુ પર યોગ્ય માર્કથી લેબલ લગાડી પંચનામામાં દરેક ડિવાઈસ અને અન્ય સાધનનો ઉલ્લેખ કરી કબ્જે કરવા.

i) અમુક કિસ્સામાં જ્યારે મોબાઈલ ડિવાઈસ Lock હોય છે અને તે મોબાઈલ નો કોઈ યુઝર ન મળી આવે ત્યારે તેને Unlock કરવો શક્ય ન હોય ત્યારે મોબાઈલનું પંચનામું કરી FSL મોકલી આપવો.

j) જે જગ્યાએથી બનાવ બનેલ હોય ત્યાં તપાસ કરતાં અમુક સમયે એવા મોબાઈલ ડિવાઈસ મળી આવે છે

જેમાં બેટરી હોતી નથી, તેવાં સમયે IMEI નંબરની પંચો રૂબરૂ પંચનમામાં નોંધ કરવી.

k) જે જગ્યાએથી બનાવ બનેલ હોય ત્યાં તપાસ કરતાં અમુક સમયે માત્ર સિમ કાર્ડ મળી આવે છે ત્યારે તે સિમ કાર્ડનો નંબર જાણવા માટે કોઈ પણ અન્ય મોબાઈલ ડિવાઈસમાં તે સિમ કાર્ડને લગાવવું નહિ અને તે સિમ કાર્ડને પંચો રૂબરૂ જે કંપનીનું સિમ કાર્ડ હોય તે તેમજ તેનો IMSI નંબર પંચનામામાં નોંધી લેવા.

l) પંચનામાની કામગીરી પૂર્ણ થઇ ગયા બાદ કોઈપણ પ્રકાર ના ફેરફાર ના થાય તે માટે તેમાં કોઈપણ જાતની application કે ફાઇલ open કરવી નહિ. આવું કરવાથી ઘણીવાર મહત્વના પુરાવાઓ ભૂંસાઈ જવાની, હેશ વેલ્યુ અને ટાઈમિંગ ચેન્જ થઇ જવાની શક્યતા રહે છે.

m) જિલ્લામાં જ્યારે કોઈ બનાવ બનવા પામે અને તેમાં ગુન્હાનાં કામે અથવા ગુન્હો શોધવામાં મદદરૂપે મોબાઈલ ડિવાઈસ મળી આવે તેવાં સમયે રેન્જમાં ફાળવેલ UFED મોબાઈલ ફોરેન્સિક હાર્ડવેર સાધન બનાવવાળી જગ્યા પર મંગાવી લેવું કે જેની મદદથી મોબાઈલમાં રહેલી જરૂરી માહિતીઓને ડિજિટલ પુરાવાનાં ભાગ રૂપે મેળવી શકાય.

n) ઉપરોક્ત જણાવેલ મોબાઈલ ડિવાઇસ માં Airplane Mode ને On કરવાં, મોબાઈલને અનલોક કરવાં, IMEI નંબરની તેમજ સિમકાર્ડની માહિતી મેળવવાં, મોબાઈલ ફિઝિકલ ડેમેજ કે બંધ ની સ્થિતિમાં હોય વિગેરે સંજોગોમા ગુનો શોધવાનાં કામે ડિજિટલ પુરાવા મેળવવા મોબાઈલ ડિવાઈસ કે અન્ય કોઈ પણ વસ્તુને FSL મોકલવા માટે સમગ્ર પ્રક્રિયા પંચો રૂબરૂ કરી પંચનામામાં તેનો ઉલ્લેખ કરવો.

<u>૫. ટેબલેટ:</u>

ટેબ્લેટ કોમ્પ્યુટર જે સામાન્ય રીતે નાની સાઈઝમાં હોય છે, જે પોર્ટેબલ પર્સનલ કોમ્પ્યુટર છે. ટેબલેટ એ મોબાઇલ ઓપરેટિંગ સિસ્ટમ અને એલસીડી ટચસ્ક્રીન અને એક પાતળા, ફ્લેટ પેકેજમાં રિચાર્જ બેટરી સાથેની બનાવટમાં હોય છે. આ એક પોર્ટેબલ ડિવાઇસ હોવાથી કોઈ પણ વ્યક્તિ તેને સહેલાઈથી ક્યાંય પણ સાથે રાખી શકે છે. ટેબ્લેટની તુલના એક પ્રકારે મોબાઈલ ડિવાઇસ સાથે પણ કરી શકાય છે.

ટેબ્લેટ ઓપરેટિંગ સિસ્ટમનાં પ્રકારો:-

I. Android OS
II. Apple iOS (iPad)
III. Window OS

- કોઈ પણ કંપનીનાં ટેબ્લેટની ઓળખ માટે તેમાં ૧૫ અંકનો યુનિક IMEI નંબર હોય છે, જેનાં પર થી કઈ

કંપની અને કયા મોડેલનું ટેબ્લેટ છે તે જાણી શકાય છે.

- ટેબ્લેટમાં સિમ કાર્ડનો વિકલ્પ છે, જેથી તેનાં વડે મોબાઈલની જેમ ફોન થઈ શકે છે.
- ટેબ્લેટને મોબાઈલ ડિવાઇસ અને કોમ્પ્યુટરનો સમાન ઉપયોગ કરી શકાય છે.

<u>નોંધ:-</u> ટેબ્લેટ એક મોબાઈલ ફોન જેવું ડિવાઈસ છે, જેથી મોબાઈલ ડિવાઈસની જપ્તી માટે જે પ્રક્રિયા **જણાવેલ** છે તે પ્રક્રિયાને ટેબ્લેટ માટે અનુસરવી. જેવી કે ટેબ્લેટ માંથી કેવાં પ્રકારની માહિતી મેળવી શકાય, ટેબ્લેટની જપ્તી સમયે રાખવામાં આવતી સાવચેતી, Airplane Mode ને ON કેવી રીતે કરવું, ટેબ્લેટ જ્યારે લોક હોય ત્યારે તેને અનલોક કરવાનાં મુદ્દા, IMEI નંબર કેવી રીતે મેળવવો.

<u>પ્રકરણ–૮</u>

<u>ગુજરાત પોલીસ પાસે ઉપલબ્ધ સોફ્ટવેર અને હાર્ડવેર</u>

<u>પ્રકરણ નો ઉદ્દેશ:</u> ડિજિટલ પુરાવા એકત્રીકરણ માટે અમુક સંજોગો માં ખાસ સાધનો અને સોફ્ટવેરની જરૂરત પડે છે. આ પ્રકરણનો ઉદ્દેશ ગુજરાત પોલીસ પાસે ઉપલબ્ધ હાર્ડવેર અને સોફ્ટવેર, અને તેની ઉપયોગિતા અંગે અવગત કરાવવાનો છે.

<u>૧. સાયબર-ક્રાઈમ ઈક્વિપમેન્ટસ ગુજરાત પોલીસ:</u>

અગાઉનાં પ્રકરણોમાં અનેક જગ્યા ડિજિટલ પુરાવા એકત્ર અને વિશ્લેષણ કરવા માટે ભિન્ન-ભિન્ન હાર્ડવેર અને સોફ્ટવેરનો ઉલ્લેખ કરવામાં આવેલ છે. ડિજિટલ પુરાવા એકત્રીત અને વિશ્લેષણ કરવા માટે ઘણા બધા સોફ્ટવેર ફ્રી-ટૂલ તરીકે ઇન્ટરનેટ થી ડાઉનલોડ કરી શકાય. પરંતુ અમુક હાર્ડવેર અને સોફ્ટવેર ખરીદવાની જરૂર પડે છે.

ગુજરાત પોલીસને ડિજિટલ પુરાવા એકત્રીત કરવા માટે વિવિધ સોફ્ટવેર અને હાર્ડવેરથી સજ્જ કરવામાં આવેલ છે. આ પ્રકરણના નીચેના ભાગમાં ગુજરાત પોલીસ પાસે ઉપલબ્ધ હાર્ડવેર અને સોફ્ટવેર અને તેના ઉપયોગ જણાવવામાં આવ્યા છે. <u>આ તમામ સોફ્ટવેર અને હાર્ડવેર રેન્જ-વડા અને પોલીસ-કમિશ્નર કચેરી ખાતે ફાળવેલ છે.</u> સદરહુ સાયબર-ક્રાઈમ ટૂલ્સનો ઉપયોગ પોલીસ અધિકારી અને કર્મચારી ડિજિટલ પુરાવા એકત્ર કરવા

માટે જરૂર પડે તો પ્રશિક્ષિત માણસ સાથે રાખીને કરી શકે. વધુમાં, ડાયરેક્ટરેટ ઑફ ફોરેંસિક સાયન્સ, ગાંધીનગર, પાસે એડવાન્સ(અધ્યતન) સાયબર-ક્રાઈમ ટૂલ્સ પણ ઉપલબ્ધ છે.ફોરેંસિક સાયન્સ યુનિવર્સિટી, ગાંધીનગર પાસે 'સાયબર ડિફેન્સ સેન્ટર' ની અતિ-આધુનિક સુવિધા વિકસાવવામાં આવી છે.

૨. રાઈટ બ્લોકર કિટ (Write Blocker Kit):

રાઈટ બ્લોકર કિટ નો ઉપયોગ ડેટા ડિસ્કની નકલ (Bit-Imaging) અને બેકઅપ (Logical Backup) તૈયાર કરવામાં થાય છે. પ્રકરણ-૨ માં નકલ અને બેકઅપની પ્રક્રિયાનું વિગતવાર વર્ણન કરવામાં આવ્યુ છે. રાઈટ બ્લોકર કિટ વડે નકલ/બેકઅપ તૈયાર કરવાથી ડેટાની હેશવેલ્યુ માં ફેરફાર નથી આવતો. હેશવેલ્યુમાં બદલાવ ન હોવાનું એ પ્રસ્થાપિત કરે છે કે ડેટામાં કોઈ છેડછાડ થયેલ નથી.

3. <u>ફોરેન્સિક વર્ક-સ્ટેશન:</u>

પુરાવા તરીકે શંકાસ્પદના ડેસ્કટોપના હેવી ગ્રાફિક્સને ઝડપથી પ્રોસેસ કરવા માટે આ ઇક્વીપમેન્ટનો ઉપયોગ થાય છે. પુરાવાઓની સાંકળ (chain of evidences custody) ને એવી રીતે જાળવવા અને સાચવવામા મદદ કરે છે કે જેથી તે કોર્ટમાં ટકી રહે અને તે શંકાસ્પદ ઉપકરણમાંથી મેળવેલ માહિતી સાથે કોઈપણ રીતે છેડછાડ થઇ ન હતી તે સાબીત કરવા માટે પણ જરૂરી છે. આ વર્કસ્ટેશનો ઉચ્ચસ્તરીય કોમ્પ્યુટર્સ છે જે જપ્ત ડિજિટલ ઉપકરણો માંથી ડેટા

મેળવવામાં અને પ્રોસેસ કરવામાં,તેને સાચવવામાં મદદરૂપ બને છે. વર્ક-સ્ટેશનના ઉપયોગ થી હાર્ડડિસ્કથી કોપી કરેલ ડેટાનુ વિશ્લેષણ ઝડપથી થઈ શકે.

<u>૪. ફાલ્કન ડિસ્ક-ડુપ્લીકેટર:</u>

ઘણી વખતે ગુન્હાના કામે પોલીસ દ્વારા ગુન્હા સ્થળેથી કોમ્પ્યુટર સિસ્ટમમાંથી હાર્ડ ડિસ્ક કબજે કરવામાં આવે છે. પરંતુ આ હાર્ડડિસ્કને FSL (ફોરેન્સીક સાયંન્સ લેબોરેટરી)ને સોંપતા પહેલા જો આ ડીસ્કની એક વર્કીંગ કોપી બનાવી લેવામાં આવે તો ઇન્વેસ્ટીગેટીંગ ઓફિસર આ ડેટા ઉપર જાતે

તપાસ કરી શકે છે. પણ આ કોપી બનાવવા માટે ફાલ્કન જેવા ડિસ્ક ડુપ્લીકેટરનો ઉપયોગ કરવો જોઈએ કે જેમાં રાઈટ બ્લોકરકિટ પહેલાથીજ ઇન્સ્ટોલ છે, અને ડેટાને કોપી કરવાના ઘણા ઓપ્શન છે, જેવા કે ડિસ્ક-ટુ-ડિસ્ક (ક્લોન) અને ડિસ્ક-ટુ-ફાઇલ (ઇમેજ). સાથો-સાથ, ડુપ્લિકેશન, ફોર્મેટ, વાઇપ, હેશ (એમડી-5 અથવા એસએચએ-1), એચપીએ / ડી.સી.ઓ. ડિટેક્શન અને તેને દૂર કરીને બ્લેન્ક ડિસ્ક ચેક, પુરાવા ડ્રાઈવોની વન ટુ વન (1: 1) અને વન ટુ ટુ (1: 2) નકલો બનાવવાના વિકલ્પો છે.

પ. UFED (Universal Forensic Extraction Device):

આ સાધન હાર્ડવેર અને સોફ્ટવેર બંને ભાગો ધરાવે છે. હાર્ડવેરમાં ફોનને સંપાદન મશીન સાથે જોડવા માટે સંખ્યાબંધ કેબલનો સમાવેશ થાય છે. જે સૉફ્ટવેર આ સાધનમાં અસ્તિત્વમાં છે તે પુરાવા કાઢવા અને એકત્ર કરવા માટે અને, જરૂર પડે તો વિશ્લેષણ કરવા માટે છે. મોબાઈલ ડિવાઈસમાં યથાવત, છુપાયેલા અને ડીલીટ કરી નાખેલ ડેટાનું ફોરેન્સીકલી અદ્યતન લોજીકલ, ફિજીકલ અને ફાઈલ સિસ્ટમથી નિષ્કર્ષણ કરવા માટે આ સાધનનો ઉપયોગ થાય છે. વિવિધ ઉપકરણો જેવા કે સ્માર્ટફોન, ફીચર-ફોન, ટેબ્લેટ્સ, જીપીએસ ડિવાઇસ, સ્માર્ટ ઘડિયાળો વિગેરે ઉપર કામ કરવામાં મદદરૂપ બને છે.

<u>૬. XRY:</u>

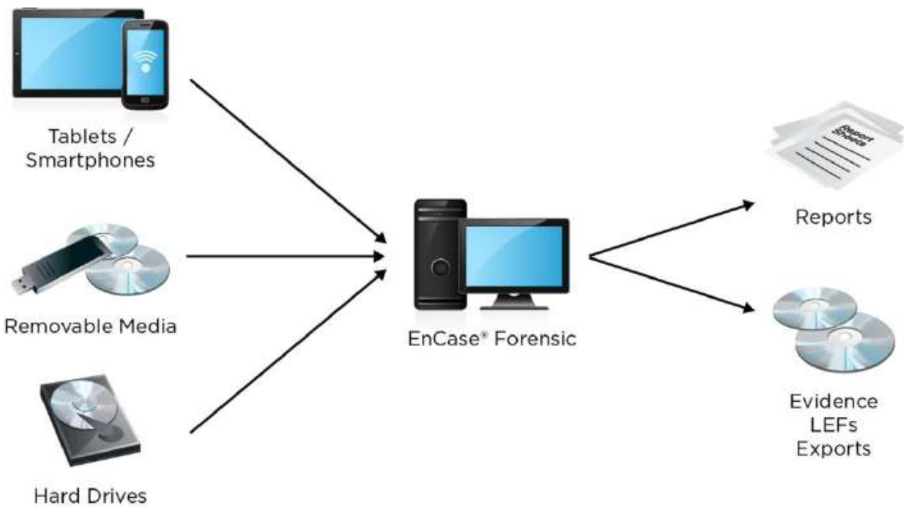
મોબાઇલ ઉપકરણ બજાર સતત વિસ્તરણ કરી રહ્યું છે અને ઘણા નવા ઉપકરણો નિયમીત ધોરણે ઉત્પાદિત કરવામાં આવી રહ્યાં છે, જેથી કોઈ પણ એક મોબાઈલ ડેટા એક્સ્ટ્રેક્શન ટૂલ તમામ મોબાઈલ ઓપરેટિંગ સિસ્ટમ અને મોડલ ઉપર અસરકારક નથી. જેથી એક થી વધુ ડિવાઈસ ની જરૂર પડે છે. UFED અને XRY નો સરખા હેતુ માટે ઉપયોગ થાય છે,

પરંતુ કયા મોબાઈલ હેંડસેટ સાથે કયુ ટૂલ સુસંગત છે, એ સ્થળ પર ચકાસવુ પડશે.

<u>૭. EnCase સોફ્ટવેર:</u>

ફોરેન્સીક્સમાં Encaseનો ઉપયોગ પરંપરાગત રીતે જપ્ત કરેલ હાર્ડ ડ્રાઈવો માંથી પુરાવા પુનઃસ્થાપિત કરવા માટે થાય છે. Encaseની મદદથી તપાસકર્તા સીસ્ટમ યુઝરની ફાઇલોનું ઊંડાણપૂર્વક વિશ્લેષણ કરી શકે છે. જેમકે દસ્તાવેજો, ચિત્રો, ઇન્ટરનેટ ઇતિહાસ અને વિન્ડોઝ રજીસ્ટ્રી માહિતી વિગેરે બાબતોની માહિતી મેળવવી.

- Encase ડિક્રીપ્શન સ્યુટ (ઇડીએસ) એ એનક્રિપ્ટ થયેલ ફાઇલો અને ફોલ્ડર્સને ડિક્રિપ્ટ કરવામાં સક્ષમ છે. ઇડીએસ ડિસ્ક અને વોલ્યુમ ડિક્રિપ્શન, ફાઇલ-આધારિત એન્ક્રિપ્શન અને માઉન્ટ થયેલ ફાઇલો પર વાપરી શકાય છે.
- વધુમાં Encase દ્વારા પુરાવા શોધવાની ત્રણ મુખ્ય પદ્ધતિઓ પુરી પાડવામાં આવે છે જ્યારે RAW ડેટા મારફતે ઈન્ડેક્સ સર્ચ, ટેગ સર્ચ અને કીવર્ડ સર્ચ.



<u>૮. i2 iBase:</u>

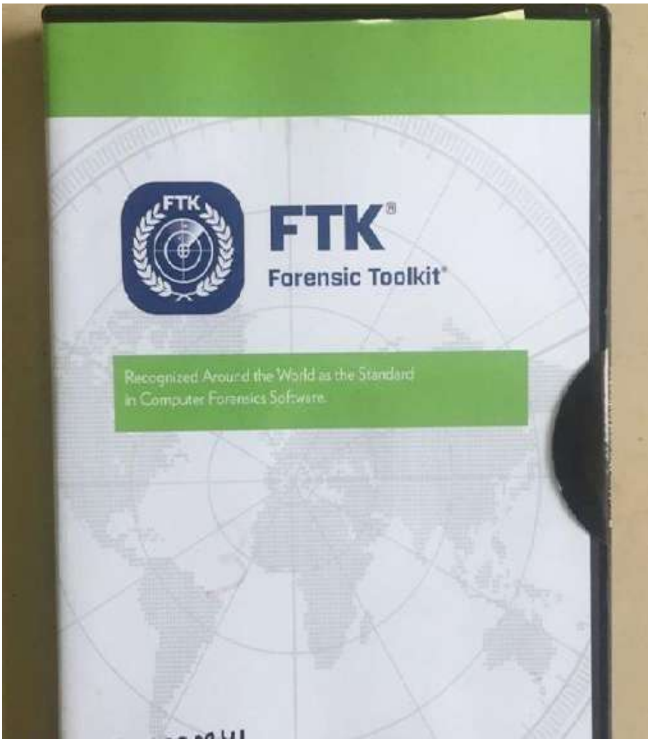
i2 iBase સુરક્ષિત વાતાવરણમાં વિવિધ સ્ત્રોતોમાંથી ડેટા હસ્તગત, નિયંત્રણ અને વિશ્લેષણ માટે વાપરી શકાય છે.

i2iBase ખાસ કરીને તપાસ વિશ્લેષણ માટે રચાયેલ છે. i2iBase ડેટાના છૂપા સંબંધોની ઓળખાણ અને વિશ્લેષણ માટે વાપરી શકાય.

૯. FTK (Forensic Took Kit):

Forensic Tool Kit (FTK) એક્સેસ ડેટા દ્વારા બનાવવામાં આવેલ કોમ્પ્યુટર ફોરેન્સીક સૉફ્ટવેર છે. તે વિવિધ માહિતીની શોધમાં હાર્ડડ્રાઈવને સ્કેન કરે છે, ઉદાહરણ તરીકે, ડીલીટ કરી નાખેલ ઇમેઇલ્સ શોધી શકાય છે અને એન્ક્રિપ્શનને તોડવા માટે પાસવર્ડ શબ્દકોષ તરીકે ઉપયોગ કરવા માટે ટેક્સ્ટ

શબ્દમાળાઓ માટે ડિસ્ક સ્કેન કરી શકે છે. ટૂલકિટમાં FTK ઈમેજર નામનો ડિસ્ક ઇમેજિંગ પ્રોગ્રામનો સમાવેશ કરેલ છે. FTK ઈમેજર એક સરળ પણ સંક્ષિપ્ત સાધન છે. તે એક ફાઇલમાં અથવા સેગમેન્ટ્સમાં હાર્ડ ડિસ્કની કોપી સેવ કરી રાખે છે જેનુ પુનઃનિર્માણ થઈ શકે છે. તે MD5 હેશ મૂલ્યોની ગણતરી કરે છે અને ફાઇલોને બંધ કરતા પહેલા ડેટાની પ્રામાણિકતાની ખાતરી કરે છે.



૧૦. X1SD (Social E-Discovery Software):

X1SD એક વિશ્લેષણાત્મક ઉકેલ છે જે વિશેષ રૂપે ઈ-Discovery અને કોમ્પ્યુટર ફોરેન્સીક વ્યવસાયિકો માટે નું ટૂલ છે જેની મદદથી સોશિયલ મીડિયા સામગ્રી, વેબસાઇટ સંગ્રહ, વેબમેઇલ, અને YouTube વિડિયો કેપ્ચરને અસરકારક રીતે પ્રદર્શીત કરી શકે છે. X1SD મુખ્યત્વે ફેસબુક, ટ્વિટર અને લિન્ક્ડ-ઇન જેવા મુખ્ય સોશીયલ મીડિયા નેટવર્કિંગ સાઇટ્સમાંથી સોશીયલ મીડિયાની સામગ્રીનુ અસરકારક રીતે નિદાન કરવા માટે બનેલું છે. વધુમાં, તે વેબસાઇટસ, વેબમેઇલ અને YouTube માંથી સામગ્રીને ક્રોલ, કેપ્ચર અને ત્વરીત શોધ કરી શકે છે

<u>પ્રકરણ–૯</u>

<u>સાયબર અવેરનેસ (જાગૃતતા)</u>

<u>૧. OTP (One Time Password) સંબંધી જાગૃતિ :-</u>

(i) OTP સાથે

(ii) OTP વગર

(i) With OTP:-

- ડેબિટ કાર્ડ, ક્રેડિટ કાર્ડ, એપ્લિકેશન રજિસ્ટર્ડ કરવા, ઈમેલ ખાતું બનાવવાં, ઓનલાઈન ખરીદી કરવાં, ઇ-વોલેટમાં પૈસા રાખવાં/મુક્વાં, સોશિયલ મીડિયા ઉપર ફેસબુક, ટ્વિટર, વોટ્સએપ વિગેરેમાં રજિસ્ટર્ડ થવાં વિગેરે પ્રકારે OTP ની જરૂર પડે છે જે કોઈને આપવો નહીં.
- બેન્ક માંથી મેનેજર બોલું છું તમારૂ ATM કાર્ડ બંધ થઈ જવાનું છે તે ચાલું રાખવા માટે તેમજ તમારાં બેંકનાં ખાતામાં અમુક એન્ટ્રી ખોટી રીતે આવેલ છે જેના લીધે તમારું ખાતું સસ્પેન્ડ કરવામાં આવશે અને તમારું બેલેન્સ RBI માં જમા થઈ જશે, જો એવું ન કરાવવું હોય તે માટે, તેમજ તમારાં બેંકનાં ખાતા સાથે તમારું આધાર કાર્ડ લિન્ક કરેલ નથી, જો તમે આધાર કાર્ડ લિન્ક નહીં કરાવો તો

તમારું ખાતું બંધ થઈ જશે જેથી તમારે બેન્ક ચાલું રાખવું હોય તે માટે, વિગેરે પ્રકારે ફોન આવતાં હોય છે ત્યારે ચાર આકડાં વાળો OTP નંબર માંગવામાં આવે છે ત્યારે એ OTP નંબર આપવો નહીં કારણ કે કોઈ પણ બેન્ક ક્યારેય ફોન કરીને OTP નંબર માંગતી નથી.

- ઘણીવાર કોઈપણ જાણીતી કે અજાણી વ્યક્તી તમારાં મોબાઇલમાં આવેલો OTP નંબર તમારી પાસે થી મેળવીને પોતાના મોબાઈલમાં એપ્લિકેશન ડાઉનલોડ કરે છે (વ્હોટ્સએપ, ફેસબુક, ટ્વિટર વિગેરે) અને તમારી પાસે થી મેળવેલ OTP ને એપ્લિકેશનમાં નાખે છે જેનાથી તે એપ્લિકેશનમાં તમારો મોબાઈલ નંબર રજીસ્ટર્ડ થઈ જાય છે બાદ તે જાણીતી કે અજાણી વ્યક્તી છેતરપિંડી કરતાં હોય છે જેથી OTP નંબર આપવો નહીં.
- હું સાયબર ક્રાઇમ માંથી બોલું છું તમારું ફેસબુક પેજ (જે નામ થી બનાવેલ હોય) છે તે શંકાસ્પદ છે અને તે પેજ અમારાં સર્વર ઉપર બ્લોક થઈ જશે જો તમારે તમારું પેજ બ્લોક ન થવાં દેવું હોય તો તમારે માહિતી અપડેટ કરાવી પડશે અને ચાર આકડાં વાળો OTP નંબર જનરેટ થશે તે અમને આપવો પડશે જેનાથી તમારું ફેસબુક પેજ બ્લોક નહીં થાય તે પ્રકારે પણ ફોન આવે છે ત્યારે OTP આપવો નહીં. (જે નંબરથી ફોન આવે છે એને Truecaller માં નાખશો

તો પણ સાઇબર ક્રાઇમ લખેલું જોવા મળશે તો પણ OTP નહીં આપવો.)

- OTP મેળવીને કોઈપણ વ્યક્તિ ડુપ્લિકેટ ઈમેલ આઈડી બનાવી લે છે જેનાથી તે ડુપ્લિકેટ ઈમેલ આઈડીમાં તમારો મોબાઈલ નંબર રજિસ્ટર્ડ થઈ જાય છે જેથી ક્યારેય OTP કોઈ ને આપવો નહીં.
- ઘણીવાર કોઈપણ અજાણી વ્યક્તિ તમારી પાસેથી OTP મેળવીને ઓનલાઈન ખરીદી કરે છે અને તમારો મોબાઈલ નંબર તે ઓનલાઈન ખરીદી વાળી વેબસાઇટ ઉપર રજિસ્ટર્ડ થઈ જાય છે, જેથી કોઈપણ વ્યક્તિને OTP આપવો જોઈએ નહીં.
- OTP ક્યારેય કોઈપણ જાણીતી કે અજાણી વ્યક્તિને આપવો જોઈએ નહીં.

(ii) Without OTP:-

- ડેબિટ કાર્ડ અથવા ક્રેડિટ કાર્ડ નો આગળ અને પાછળના ભાગનો ફોટો પાડીને ક્યારેય મોબાઈલમાં રાખવો નહીં.
- ડેબિટ કાર્ડ અથવા ક્રેડિટ કાર્ડ નો પીન નંબર કોઈને આપવો નહીં.

- ડેબિટ કાર્ડ અથવા ક્રેડિટ કાર્ડ નો ૧૬ આકડાં વાળો નંબર અને કાર્ડની પાછળનાં ભાગે આવેલો ૩ આકડાં વાળો સીવીવી નંબર કોઈને આપવો નહીં.
- ડેબિટ કાર્ડ અથવા ક્રેડિટ કાર્ડ નો પીન નંબર કે ૩ આકડાં વાળો સીવીવી નંબર ને ક્યારેય મોબાઈલ ફોનનાં કોંટેક્ટ માં સેવ કરવો નહીં.
- જ્યારે કોઈપણ જગ્યાએ ક્રેડિટ કાર્ડ દ્વારા ખરીદી કરો ત્યારે પીન નંબર નાખતાં સમયે તે જગ્યાના CCTV કેમેરામાં પીન નંબર ટાઈપ કરો એ દેખાય નહીં એ રીતે પીન નંબર નાખવો.
- ખરીદી કરવાં કોઈપણ મોલ, દુકાન, પેટ્રોલ પંપ જેવી જગ્યાએ જવાનું થાય તે સમયે ખરીદી કર્યા બાદ જ્યારે વેપારીને તમારૂં ક્રેડિટ કાર્ડ/ડેબિટ કાર્ડ આપ્યાં પછી કાર્ડ સ્વાઈપ કરવાનું મશીન ચેક કરી લેવું તેમજ સ્વાઈપ કરનારના હાથમાં કોઈ સ્કિમર મશીન તો નથી ને તે ચકાસી લેવું.
- કોઈપણ ATM સેન્ટરમાં પૈસા ઉપાડવાં, બેલેન્સ જોવા અથવા પેમેન્ટ કરવાં જાવ ત્યારે તામારુ ATM કાર્ડ કોઈને આપવું નહીં તેમજ તમારી પાછળ જો કોઈ વ્યક્તિ ઉભી હોય તો તેમને સેન્ટરની બહાર ઉભા રહેવાં જણાવવું. જેથી તે વ્યક્તિ તમારો પીન નંબર જોઈ ન શકે.

- જ્યારે ATM સેન્ટરમાં પૈસા ઉપાડવાં, બેલેન્સ જોવા અથવા પેમેન્ટ કરવાં જાવ ત્યારે ATM મશીનમાં જે જગ્યાએ તમે ATM કાર્ડ સ્વાઈપ કે અંદર નાખશો તેને પકડીને ખેચીને કે હલાવીને ચેક કરી લેવું કે ત્યાં કોઈ કાર્ડ સ્કિમર ફિટ કરેલું છે કે નહીં.
- જ્યારે ATM સેન્ટરમાં પૈસા ઉપાડવાં, બેલેન્સ જોવા અથવા પેમેન્ટ કરવાં જાવ ત્યારે ATM મશીનમાં જે જગ્યાએ તમે પીન નંબરના બટન દબાવો છો તે કી પેડ ની ધાર ઉપર આંગળીના નખ વડે અથવા પાતળી વસ્તુ થી ચેક કરી લેવું કે કી પેડ સ્કિમર ફિટ કરેલું છે કે નહીં.
- ઓનલાઈન ખરીદી કરતાં સમયે કોઈપણ અજાણી વેબસાઇટ અથવા એપ્લિકેશન ઉપર થી ખરીદી કરવી નહીં, કેમ કે તેનાથી તમારાં ડેબિટ કાર્ડ અથવા ક્રેડિટ કાર્ડ ની માહિતી ચોરાઈ જવાની સંભાવના રહે છે.
- ઘણીવાર ઓનલાઈન વેબસાઇટ ઉપર વસ્તુઓમાં સારાં ડિસ્કાઉન્ટ વાળી લોભામણી જાહેરાતો આવતી હોય છે તેની ચકાસણી કર્યા વિના ખરીદી કરવી નહીં કે જેથી તમારાં ડેબિટ કાર્ડ અથવા ક્રેડિટ કાર્ડની માહિતીનો દુરુપયોગ ન થાય.
- જો તમે ડેબિટ કાર્ડ અથવા ક્રેડિટ કાર્ડ ખોવાઈ જાય ત્યારે તાત્કાલિક જે તે ડેબિટ કાર્ડ અથવા ક્રેડિટ કાર્ડની બેંકનાં

કસ્ટમર કેર માં ફોન કરીને ખોવાઈ ગયેલ કાર્ડને બંધ કરાવી દેવું તેમજ તે કાર્ડની બેન્કમાં જઈને કાર્ડ ખોવાઈ ગયેલ બાબતેની અરજી બેન્કના મેનેજરને આપી દેવી.

<u>૨. સિમ કાર્ડ બદલાવું (સિમ રિપ્લેસ):-</u>

- હું એરટેલ/વોડાફોન/આઈડિયા કોઈપણ કંપની માંથી બોલું છું તમારું સિમ કાર્ડ હમણાં થોડી વાર માં બંધ થઈ જવાનું છે, તમારું આધાર કાર્ડ લિન્ક નથી અથવા 4G સિમ કાર્ડ વાપરવું ફરજિયાત છે અથવાં કોઈપણ કારણ બતાવીને OTP માંગવામાં આવે છે તેવા સમયે OTP આપવો નહીં.
- જો OTP આપી દેવાય છે ત્યારે તમારું સિમ કાર્ડ બંધ થઈ જશે અને ફોન કરનારી વ્યક્તિ પહેલે થી જ તમારું સિમ કાર્ડ જે નેટવર્ક કંપનીનું હશે તે કંપનીનાં સ્ટોરમાં હાજર રહીને OTP દ્વારા તમારો નંબર ત્યાં ચાલુ કરી નાખશે અને તમારાં મોબાઈલ નંબર થી ઇન્ટરનેટ બેંકિંગ દ્વારા તમારાં બેન્ક ખાતા માંથી રૂપિયા ઉપાડી લેશે.
- જેથી આ પ્રકારે ફોન આવે ત્યારે તમારી નજીકનાં વિસ્તારમાં તમારું સિમ જે નેટવર્ક કંપનીનું છે તેના સ્ટોરમાં જઈને ચકાસણી કરાવી લેવી અથવા નેટવર્ક કંપનીનાં કસ્ટમર કેરમાં ટોલ ફ્રી નંબર ઉપર ફોન કરીને ચકાસણી કરી લેવી.

3. ઓનલાઈન બેંકિંગ:-

- ઓનલાઈન બેંકિંગ માટે નો આઈડી અને પાસવર્ડ ક્યારેય કોઈપણ જાણીતી કે અજાણી વ્યક્તિને આપવો નહીં તેમજ ક્યાય નોટબુકમાં કે મોબાઈલમાં સેવ રાખવો નહીં.
- ઓનલાઈન બેંકિંગ માટે પોતાના જ મોબાઈલ અને કોમ્પ્યુટરનો ઉપયોગ કરવો.
- ઓનલાઈન બેંકિંગ માટે ૨ થી ૩ મહિને પાસવોર્ડ બદલી નાખવો જોઈએ.
- ઓનલાઈન બેંકિંગ કરવાં માટે કોમ્પ્યુટરમાં જે બ્રાઉઝરનો ઉપયોગ કરો છો તે અપડેટ હોવું જોઈએ અને પાસવર્ડ સેવ રાખવો નહીં.
- જે બેન્ક થી ઓનલાઈન બેંકિંગ કરવાનું હોય તે બેન્કની વેબસાઈટ વાળું પેજની ખાત્રી કરીને જ આઈડી અને પાસવર્ડ નાખવો.
- ઓનલાઈન બેંકિંગનો વ્યવહાર કરવા માટે મોબાઈલમાં એપ્લિકેશન ડાઉનલોડ કરતાં પહેલા ખાત્રી કરી લેવી જોઈએ કે તમારે જે બેન્ક ખાતા માંથી બેંકનાં વ્યવહાર કરવાનાં છે તે જ બેન્કની માન્યતા વાળી એપ્લિકેશન છે કે નહીં, જેનાથી ફેક એપ્લિકેશન ડાઉનલોડ ન થાય અને તમારી બેન્કની માહિતીની સુરક્ષા જળવાઈ રહે.

- ઓનલાઈન બેંકિંગમાં ઘણીવાર જાણીતી કે અજાણી વ્યક્તિ ફેક ઈમેલ કરીને બેન્કની માહિતી અલગ આપીને પેમેન્ટ મેળવી લેતા હોય છે તેવાં સમયે કોઈ કંપની, વ્યક્તિ, સંસ્થા વિગેરે ને ઓનલાઈન પેમેન્ટ કરવાનું હોય ત્યારે ઓનલાઈન પેમેન્ટ કરતાં પહેલા જે તે કંપની, વ્યક્તિ, સંસ્થા વિગેરેનો ઈમેલ આઈડી તેમજ તેમની બેન્કની માહિતીની ખાત્રી કર્યા બાદ જ પેમેન્ટ કરવું.

<u>૪. ફેસ્બુક:-</u>

- પોતાનો મોબાઈલ ફોન ક્યારેય કોઈપણ જાણીતી કે અજાણી વ્યક્તિને વાપરવાં આપવો નહીં કે જેનાથી તમારાં મોબાઇલમાં રહેલ ફેસબુકનો દુરુપયોગ થઈ શકે.
- ફેસબુકનો આઈડી અને પાસવર્ડ ક્યારેય કોઈપણ જાણીતી કે અજાણી વ્યક્તિને આપવો નહીં તેમજ ક્યાય નોટબુકમાં કે મોબાઈલમાં સેવ રાખવો નહીં.
- ફેસબુકમાં ક્યારેય કોઈપણ જાણીતી કે અજાણી વ્યક્તિનાં નામનું અથવા તેનાં ફોટો વાળું ખોટું આઈડી બનાવવું નહીં.
- ફેસબુક ઉપર જાહેરમાં કે અંગત રીતે કોઈપણ જાણીતી કે અજાણી વ્યક્તિ સાથે કોમેન્ટમાં જીભા જોડી અથવા ગંદા શબ્દોનો ઉપયોગ કરવો નહીં.

- ફેસબુક ઉપર જાહેરમાં કે અંગત રીતે કોઈપણ જાણીતી કે અજાણી વ્યક્તિને ગંદા ફોટો અથવા ગંદા વિડીયો મોકલવા નહીં.
- કોઈપણ જાણીતી કે અજાણી વ્યક્તિનાં ફોટા કે વિડ્યોમાં સુધારો વધારો કરીને જાહેરમાં કે અંગત રીતે ફેલાવવાં નહીં અથવા શેર કરવાં જોઈએ નહીં.
- ફેસબુક ઉપર જાહેરમાં કે અંગત રીતે ખોટાં સમાચારો, ફોટા, વિડીયો ફેલાવવાં નહીં અથવા શેર કરવાં નહીં.
- ફેસબુક ઉપર જાહેરમાં કે અંગત રીતે અફવાઓ ફેલાવવી નહીં અથવા શેર કરવી જોઈએ નહીં કે જેનાથી કાયદો અને વ્યવસ્થા ખોરવાય તેમજ કોઈપણ જાણીતી કે અજાણી વ્યક્તિની લાગણી દુભાય.
- ફેસબુક ઉપર જાહેરમાં કે અંગત રીતે કોઈપણ ધર્મ, દેશ, સમાજ, સંસ્થા, સરકાર, રાજકીય પક્ષ અથવા પ્રતિષ્ઠિત વ્યક્તિની લાગણી દુભાય તેવાં ખોટાં શબ્દો, અફવાઓ, ફોટો કે વિડીયો મોકલવા અથવા શેર કરવાં જોઈએ નહીં.
- જ્યારે પણ કોમ્પ્યુટરમાં ફેસબુક લૉગ ઇન હોવ ત્યારે કોમ્પ્યુટર છોડતાં પહેલાં ફેસબુક માંથી લૉગઆઉટ થઈ જવું. જેનાથી કોઈ વ્યક્તિ તમારાં ફેસબુકનો દુરુપયોગ ન કરી શકે.

<u>૫ વ્હોટ્સએપ: -</u>

- પોતાનો મોબાઈલ ફોન ક્યારેય કોઈપણ જાણીતી કે અજાણી વ્યક્તિને વાપરવાં આપવો નહીં કે જેનાથી તમારાં મોબાઇલમાં રહેલ વ્હોટ્સએપનો દુરુપયોગ થઈ શકે.
- વ્હોટ્સએપમાં ક્યારેય કોઈપણ જાણીતી કે અજાણી વ્યક્તિની સાથે ગ્રુપમાં કે અંગતમાં ગંદી વાતો કરવી નહીં.
- વ્હોટ્સએપનાં ગ્રુપમાં કે કોઈને અંગતમાં ગંદા ફોટા અથવા વિડીયો મોકલવા નહીં.
- વ્હોટ્સએપનાં ગ્રુપમાં કે કોઈને અંગતમાં અફવાઓ ફેલાવવી નહીં અથવા તે અફવાને સમર્થન આપવું જોઈએ નહીં જેનાથી કાયદો અને વ્યવસ્થા તૂટે તેમજ કોઈપણ જાણીતી કે અજાણી વ્યક્તિની લાગણી દુભાય.
- કોઈપણ જાણીતી કે અજાણી વ્યક્તિનાં ફોટા સાથે ચેડાં કરીને વ્હોટ્સએપનાં ગ્રુપમાં કે કોઈને અંગતમાં મોકલવા નહીં.
- વ્હોટ્સએપનાં પ્રોફાઇલમાં કોઈપણ જાણીતી કે અજાણી વ્યક્તિનો ફોટો મૂકવો જોઈએ નહીં.
- વ્હોટ્સએપનાં ગ્રુપમાં કે કોઈને અંગતમાં ખોટાં સમાચારો, ફોટા, વિડીયો ફેલાવવાં નહીં.
- વ્હોટ્સએપનાં ગ્રુપમાં કે કોઈને અંગતમાં કોઈપણ ધર્મ, દેશ, સમાજ, સંસ્થા, સરકાર, રાજકીય પક્ષ અથવા પ્રતિષ્ઠિત

વ્યક્તિની લાગણી દુભાય તેવાં ખોટાં શબ્દો, અફવાઓ, ફોટો કે વિડીયો મોકલવા જોઈએ નહીં.

- જ્યારે પણ કોમ્પ્યુટરમાં વ્હોટ્સએપ વેબ વાપરતાં હોવ ત્યારે કોમ્પ્યુટર છોડતાં પહેલાં વ્હોટ્સએપ વેબ માંથી લૉગઆઉટ થઈ જવું. જેનાથી કોઈ વ્યક્તિ તમારાં વ્હોટ્સએપનો દુરુપયોગ ન કરી શકે.

<u>ઙ. સોશિયલ મીડિયા:-</u>

- સોશિયલ મીડિયા ઉપર ઘણી એપ્લિકેશન છે જેથી બિન જરૂરી એપ્લિકેશનનો ઉપયોગ કરવો નહીં. જેથી મોબાઈલની સિક્યુરિટી જળવાઈ રહે.
- સોશિયલ મીડિયાનાં કોઈપણ પ્લેટફોર્મ ઉપર ક્યારેય પોતાની સાચી ઓળખ છુપાવીને ખોટી માહિતીનો અથવા બીજી વ્યક્તિનાં નામ, ફોટો, વિડીયોનો ફેલાવો કરવો નહીં તેમજ જાહેરમાં કે અંગત રીતે ક્યાય પણ આવા વિડીયો મોકલવા નહીં.
- સોશિયલ મીડિયાનાં કોઈપણ પ્લેટફોર્મ ઉપર કોઇપણ વ્યક્તિ, ધર્મ, દેશ, સમાજ, સંસ્થા, સરકાર, રાજકીય પક્ષ અથવા પ્રતિષ્ઠિત વ્યક્તિની લાગણી દુભાય તેવાં ખોટાં શબ્દો, અફવાઓ, ફેક ન્યૂઝ, ફોટો કે વિડીયો મોકલવા જોઈએ નહીં.

- સોશિયલ મીડિયા ઉપર ફેક સમાચાર ફેલાવવાંથી કોઇની પ્રતિષ્ઠા ખરડાઈ શકે અથવા જીવ જોખમમાં મુકાઈ શકે છે.
- સોશિયલ મીડિયાનાં કોઈપણ પ્લેટફોર્મ ઉપર ફેક ન્યૂઝ અથવા અફવાઓ ને લીધે દેશમાં કાયદો અને વ્યવસ્થા ખોરવાઈ શકે તેથી દેશની આંતરિક સુરક્ષા જોખમાય તેમજ ગરિમાને આંચ પહોચે તેવાં ફેક સમાચારો કે અફવાઓ ફેલાવવી જોઈએ નહીં.

<u>૭. ઓનલાઈન જોબ:-</u>

- ઓનલાઈન જોબ માટે એપ્લાય કરતાં સમયે અજાણી વેબસાઈટ ઉપર ક્યારેય પોતાની અંગત માહિતી મૂકવી નહીં.
- ઓનલાઈન જોબની ઘણી વેબસાઈટ છે અને તેના જેવી જ ડુપ્લિકેટ વેબસાઈટ હોય છે જ્યાં ફ્રોડ થતાં હોય છે ત્યારે વેબસાઈટનું એડ્રેસ ચેક કરીને જ અંગત માહિતી મૂકવી.
- જેમ કે :- www.timesjob.com
- ડુપ્લિકેટ :- www.timejob.com (time પછી s નથી)
- નોકરીમાં વધારે પગાર આપતી લોભામણી જાહેરાતોને ધ્યાને લેવી નહીં અને તેવી વેબસાઈટ સર્ચ કરવી નહીં.
- ઓનલાઈન જોબ માટે એપ્લાય કર્યા બાદ નોકરી માટે જ્યારે સામે થી ઈમેલ આવે અથવા ફોન આવે ત્યારે તે

ઈમેલ અને ફોન નંબરની ચકાસણી કરી લેવી તેમજ જે કંપનીમાં નોકરીની જગ્યા ખાલી છે તેવું જણાવતાં તે કંપનીનો સંપર્ક કરીને ખાત્રી કરી લેવી.

૮. ઓનલાઈન લગ્ન સંબંધી વેબસાઈટ:-

- ઓનલાઈન લગ્ન સંબંધી વેબસાઈટ ને મેટ્રિમોનિયલ વેબસાઈટ કહેવાય છે.
- કોઈપણ મેટ્રિમોનિયલ વેબસાઈટ ઉપર એપ્લાય કરતાં સમયે અજાણી વેબસાઈટ ઉપર ક્યારેય પોતાની અંગત માહિતી કે ફોટો મૂકવાં નહીં.
- મેટ્રિમોનિયલની ઘણી વેબસાઈટ છે અને તેના જેવી જ ડુપ્લિકેટ વેબસાઈટ હોય છે જ્યાં ફ્રોડ થતાં હોય છે ત્યારે વેબસાઈટનું એડ્રેસ ચેક કરીને જ અંગત માહિતી મૂકવી.
- જેમ કે :- www.shaadi.com
- ડુપ્લિકેટ :- www.shadi.com (shaadi માં a ઓછો છે.)
- મેટ્રિમોનિયલ વેબસાઈટ ઉપર ઘણીવાર જાણીતી કે અજાણી વ્યક્તિ ફેક આઈડી બનાવે છે અને સામે થી સંપર્ક કરીને લગ્નની લાલચ આપે છે તેવાં સમયે લગ્નની લાલચ આપનાર વ્યક્તિને કોઈપણ એપ્લીકેશન દ્વારા વિડીયો કોલિંગ કરાવીને ચકાસી લેવું કે પ્રોફાઇલ ફોટોમાં જે વ્યક્તિ છે તે જ વિડીયો કોલિંગમાં છે કે નહીં.

- મહિલાઓ/પુરુષ જ્યારે કોઈપણ મેટ્રિમોનિયલ વેબસાઈટ ઉપર લગ્ન માટે આઈડી બનાવે છે ત્યારે ઘણીવાર સામે થી રિકવેસ્ટ આવતી હોય છે ત્યાર બાદ તે રિકવેસ્ટ સ્વીકાર્યા બાદ મેસેજ દ્વારા સંપર્કમાં આવે છે બાદ એકબીજા સાથે લગ્ન કરવાં સંમત થાય છે અને સામે થી રિકવેસ્ટ આવેલ વ્યક્તિ ઈરાદાપૂર્વક મહિલા/પુરુષની સાથે ફ્રોડ કરવાં ખોટી વાર્તા બનાવીને પોતાની જાળમાં ફસાવવાં અમુક સમય પછી જણાવે છે કે હું એરપોર્ટ ઉપર આવેલ છું અને કસ્ટમનાં અધિકારીએ મને પકડ્યો છે મને છોડાવો નહીં તો મને જેલમાં પૂરી દેશે ત્યારે આ પ્રકારથી તે વ્યક્તિનો સંપર્કમાં રહેવું નહીં અને જે પ્રમાણે કહે તે મુજબ કરવું નહીં.

<u>૯. મોબાઇલમાં આવતાં લખાણવાળા અજાણ્યા SMS:-</u>

- મોબાઈલમાં જ્યારે કોઈ અજાણ્યો મેસેજ આવે તો તેને ડિલીટ કરી દેવો.
- મોબાઇલમાં ઘણીવાર લોભામણી જાહેરાત વાળા મેસેજમાં અજાણી લિન્ક મૂકેલી હોય છે તે લિન્કને ઉપર ક્યારેય ક્લિક કરવું નહીં.
- હાલમાં તાજેતરમાં મોબાઇલમાં લખાણ વાળો એક મેસેજ વાયરલ થઈ રહ્યો છે જેમાં તમારું સાચું નામ હોય છે અને જણાવે છે કે તમારું ઈન્કમટેક્ષ રિટર્ન ફાઇલ નહીં કરો તો

તમને પેનલ્ટી લાગશે જે માટે નીચેની લિન્ક ઉપર ક્લિક કરો પરંતુ તેવાં મેસેજને ધ્યાને લેવા નહીં અને ડિલીટ કરી દેવાં.

- ઘણીવાર મોબાઈલમાં લોભામણા મેસેજ આવતાં હોય છે જેવા કે ઈનામ લાગેલ, મફત SMS, મફતમાં કોલિંગ, વિગેરે પ્રકારનાં મેસેજને ધ્યાને લેવા નહીં.
- તમે કોઈ બેન્ક ટ્રાન્ઝેકસન કર્યું ન હોય અને તમારા બેન્કનાં ખાતાં માંથી ૫૦૦૦/- કપાઈ ગયેલ છે તેવો મેસેજ આવે બાદ જો કોઈ ફોન આવે અને એવું જણાવે કે હું બેન્ક માંથી બોલું છું અને તમારાં બેન્ક માંથી ૫૦૦૦/- રૂપિયા કપાઈ ગયા છે અને તમારું બેન્ક ખાતું RBI દ્વારા સસ્પેન્ડ થઈ જશે, તો તેવાં ફોનને ધ્યાને ન લેવો અને તુરત જ પોતાની નજીકમાં આવેલી જે બેન્કમાં ખાતું હોય ત્યાં જઈને અથવા નજીકનાં કોઈપણ બેન્કનાં ATM માં જઈને સ્ટેટમેન્ટ કાઢીને ચકાસણી કરી લેવી.

<u>૧૦. ઈમેલ:-</u>

- ઈમેલ આઈડી નો પાસવર્ડ મજબૂત હોવો જોઈએ.
- ઈમેલ આઈડી ને હંમેશા 2 સ્ટેપ વેરિફિકેશન વાળા ઓપ્શન વાળું હોવું જોઈએ.
- ડુપ્લિકેટ ઈમેલ આઇડી બનાવવું નહીં.

- બિન જરૂરી એક કરતાં વધારે ઈમેલ આઈડી બનાવાનું ટાળો.
- જ્યાં ઈમેલ આઈડી આપવું જરૂરી છે તે જગ્યા એ જ ઈમેલ આઈડી આપવું.
- જ્યારે કોઈ અજાણ્યો ઈમેલ આવે ત્યારે તેવાં મેલ ને ધ્યાને ન લેવાં.
- SPAM બોક્ષમાં આવતા ઈમેલ મોટેભાગે છેતરનારા મેલ હોય છે જેથી SPAM મેલ ને ખોલવા નહીં.
- ઇનબોક્ષમાં આવેલ ઈમેલમાં જ્યારે કોઈ લિન્ક આવે છે ત્યારે તે લિન્ક ઉપર ક્લિક કરતાં પહેલાં વિચાર કરીને ક્લિક કરવી. બિનજરૂરી મેલ અથવા લિન્ક ઉપર ક્લિક કરવી નહીં.
- જ્યારે કોઈપણ જાણીતી કે અજાણી વ્યક્તિનો ઈમેલ ઈનબોક્ષમાં આવે ત્યારે ઈમેલ ખોલી ને મેલ મોકલનારનું ઈમેલ આઈડી ચકાસીને ખરાઈ કરી ને જ મેલ નો જવાબ આપવો અથવા આગળ વધવું.
- ઈમેલ માં ઘણીવાર લોભામણી જાહેરાતો આવતી હોય છે, તેવી જાહેરાતો વાળાં મેલ ને જવાબ આપવો નહીં.
- તમે જ્યારે વિદેશમાં ધંધો કરતાં હોવ છો ત્યારે મોટે ભાગે ધંધાની વાતચીત અને રૂપિયાની લેતી દેતી ઈમેલ મારફતે કરવામાં આવે છે. તમે રેગ્યુલર તમારા વિદેશનાં વેપારી

સાથે ધંધો કરતાં હોવ છો. ક્યારેક એવો ઈમેલ આવે છે કે ‘હવે થી અમારી કંપનીનું બેન્ક ખાતું બદલાઈ ગયું છે તો હવે પછીનું પેમેન્ટ નીચે જણાવેલ બેન્ક ખાતાંમાં કરવું.” તે ઈમેલ આઈડી તમારા વિદેશના વેપારીની કંપનીના ઈમેલ આઇડી જેવુ જ હોય છે માત્ર તેમાં a,i,e જેવા spelling ઓછો અથવા વધારે હોય છે.

- જેમ કે...
- વિદેશની કંપનીનું સાચું ઈમેલ આઈડી = reckingspharmaceuticals@gmail.com
- ખોટું ઈમેલ આઈડી = reckingspharmaceutiicals@gmail.com (pharmaceutiicals માં i વધારે મૂકી દેવામાં આવેલો છે)
- જેથી બેન્ક ખાતું બદલાઈ ગયેલ બાબતેનો ઈમેલ આવે ત્યારે સૌથી પહેલાં ઈમેલ આઈડી ચકાસી લેવું અને બાદ એ વિદેશનાં વેપારીને ફોન કરીને બેન્કની વિગત બદલેલ બાબતે ચકાસણી કરી લેવી.

<u>૧૧. સંવેદનશીલ માહિતી:-</u>

- વપરાશકર્તાએ પોતાનાં બધાં સંવેદનશીલ ડેટા અને માહિતીને સુરક્ષિત રાખવી જોઈએ. (જો ડેટા, દસ્તાવેજો કે ફાઈલ સુરક્ષિત નહીં હોય તો કંપની, સંસ્થા અથવા કોઈપણ સરકારી વિભાગને પ્રતિકૂળ અસર થશે.)

- કોઈપણ સંવેદનશીલ ડેટા અને માહિતીને સુરક્ષિત ભૌતિક વાતાવરણમાં સંગ્રહિત હોવું આવશ્યક છે. (બધાં મીડિયા ફોર્મેટમાં જેવા કે, પેપર, CD, પેન ડ્રાઈવ, હાર્ડ ડ્રાઈવ, વિગેરે)
- કોઈપણ સંવેદનશીલ ડેટા અને માહિતીને પોતે કોઈપણ મીડિયા ફોર્મેટમાં ચકાસણી કરીને મૂકવી.
- જો શક્ય હોય તો સંવેદનશીલ ડેટા અને માહિતીને મોબાઈલ, લેપટોપ, કોમ્પ્યુટર, CD, DVD, USB ઉપકરણમાં પાસવર્ડથી સુરક્ષિત તેમજ એન્ક્રિપ્ટેડ હોવું આવશ્યક છે.
- સંવેદનશીલ ડેટા અને માહિતીનો બેક અપ સર્વર ઉપર અને CD, DVD માં દર મહિને મેળવી લેવો જોઈએ.
- સંવેદનશીલ ડેટા અને માહિતીનો યોગ્ય રીતે નિકાલ કરવો.

<u>૧૨. કોમ્પ્યુટર/લેપટોપ:-</u>

- વપરાશકર્તાએ જ્યારે કોમ્પ્યુટર/લેપટોપનો ઉપયોગ ન કરતાં હોવ ત્યારે તે મેન્યુલી પાસવર્ડથી લોક હોવું જોઈએ.
- જ્યારે કોમ્પ્યુટર/લેપટોપમાં કોઈ કામ ન કરતાં હોવ ત્યારે તે ઓટોમેટિક લોક થઈ જવું જોઈએ. જેમ કે, ૦૫ કે ૧૦ મિનિટ પછી

- જ્યારે તમે તમારું ટેબલ છોડી દો અથવા તમારું કોમ્પ્યુટર/લેપટોપ/મોબાઇલ ઉપકરણ અડ્યા વિના છોડી જાઓ ત્યારે તમારું વર્ક સ્ટેશન લૉક કરો.
- જેમ કે... Press the Windows Key and "L" (એ જ સમયે)

અથવા

Press Ctrl-Alt-Del and click on "Lock"

- કોમ્પ્યુટર/લેપટોપમાં અમુક સમય પછી વિન્ડો લોક અને સ્ક્રીન સેવર લોક નો પાસવર્ડ બદલી નાખવો.
- કોમ્પ્યુટર/લેપટોપનાં પાસવર્ડને નોટબુકમાં લખવો નહીં કે મોબાઇલમાં સેવ નહીં.
- કોઈપણ ફોર્મેટની ફાઇલને ડેસ્કટોપ ઉપર અથવા C:/ ડ્રાઈવમાં સેવ રાખવું નહીં.

<u>૧૩. પાસવર્ડ:-</u>

- વપરાશકર્તાએ પાસવર્ડ્સ સુરક્ષા ધોરણોનું પાલન કરવું આવશ્યક છે.
- પાસવર્ડ મજબૂત હોવો જોઈએ:
- જેમ કે... અપર કેસ આલ્ફા, લોઅર કેસ આલ્ફા, આંકડાકીય (૦-૯) બિન-આલ્ફાબેટીક અક્ષરો (~! # $% ^ અને ∗)
- વપરાશકર્તાએ સોશિયલ મીડિયામાં જ્યાં પણ આઈડી બનાવેલ હોય તેમજ ઈમેલ પોતાનાં તમામ પાસવર્ડને દર ૩ મહિને બદલી નાખવો જોઈએ.

- પાસવર્ડને નોટબુકમાં લખવો નહીં કે મોબાઇલમાં સેવ નહીં, જો વધારે પાસવર્ડ હોય અને તે અલગ અલગ પાસવર્ડને યાદ રાખી શકાતો ન હોય તેની ફાઇલ બનાવીને ઈમેલમાં રાખવી અને ઈમેલને પોતાનાં મોબાઈલમાં ૨ સ્ટેપ વેરિફિકેશન સાથે રાખવો.
- જ્યારે લૉગિન થવા પાસવર્ડ નાખતાં હોવ અને પાસવર્ડ ભૂલી ગયા હોવ ત્યારે અલગ અલગ પાસવર્ડ વધારે વખત નાખવો નહીં કે જેનાથી તમારું એકાઉન્ટ લોક થઈ જાય.
- વપરાશકર્તાએ પોતાનો પાસવર્ડ કોઈપણ કારણસર કોઈને આપવો નહીં.

<u>૧૪. ઓપરેટિંગ સિસ્ટમ અપડેટ:-</u>

- વપરાશકર્તાએ કોમ્પ્યુટર/લેપટોપ/મોબાઈલમાં સિક્યુરિટી અપડેટ્સ એપ્લાય કરીને ઑપરેટિંગ સિસ્ટમને સુરક્ષિત રાખવી જોઈએ.
- જેમ કે... Microsoft Office Word, Excel, PowerPoint, Adobe Reader/Acrobat
- કોમ્પ્યુટર/લેપટોપ/મોબાઈલમાં બધાં સોફ્ટવેર અપ ટુ ડેટ હોવા જોઈએ અને દરરોજ સ્કેન થવા જોઈએ
- જેમ કે... Windows Defender, McAfee, Norton, Kaspersky, વિગેરે પ્રકારનાં એન્ટિ વાઇરસ સોફ્ટવેરથી

અપડેટ ચેક તેમજ કોમ્પ્યુટર/લેપટોપ શરૂ અને બંધ થાય ત્યારે સ્કેન કરી લેવું જોઈએ.

- વપરાશકર્તાએ કોમ્પ્યુટર/લેપટોપમાં ઇન્ટરનેટ, બ્રાઉઝરના પેજ, ઈમેલ, જોડાણ કરેલી ફાઈલો અને ડાઉનલોડ માટે સિક્યુરિટી સોફ્ટવેર સેટ કરવું જોઈએ.

મૂળભૂત ખ્યાલ

: તમે જે ક્લિક કરવાનું પસંદ કરો છો તે તમને નિયંત્રિત કરે છે :

તમારે શું કરવું જોઈએ

: **ક્લિક** કરતાં પહેલાં **થોભો** અને **વિચારો** :

પરિશિષ્ટ-૧

DRAFT MUTUAL LEGAL ASSISTANCE TREATY REQUEST

(FOR UNITED STATES OF AMERICA)

TO : The Central Authority of the United States of America

FROM : The Central Authority of Republic of India

SUBJECT: Request for assistance in the investigation of Case No. _____________ related to *(short case outline)*

FILE NO : _________________________

1. The Ministry of Home Affairs, Government of India, Central Authority of the Republic of India avails this opportunity to pay its compliments to the Central Authority of the United States of America.

2. The Ministry of Home Affairs which is the Central Authority of the Republic of India, pursuant to the treaty between the Government of Republic of India and Government of the United States of Americaon Mutual Legal Assistance in Criminal Matters, which came into force since October 3, 2005, hereby requests assistance from the Central Authority of United States of Americato obtain evidence for use in a criminal investigation and any other related criminal proceedings. This request is also in consonance with the Resolution 1373 of the United Nations Security Council.

BACKGROUND AND PURPOSE

3. The *(Institution/ Police Station/ Branch),* Gujarat Police is investigating Case ____________________ under sections ________________ of IPC and _________________________ of the Unlawful Activities (Prevention) Act, 1967 of Unlawful Activities (Prevention) Act. *(relevant provisions of Acts/ Laws etc..),* pertaining to *(case brief).* In order to complete the on-going investigation, evidence as detailed below is necessary to be collected to prosecute the accused in court of law.

4. This request is being made under Article 1 and 7 of the MLAT and United Nations Security Council Resolution No. 1373 (2001).

TIMING

5. The Central Authority of the Republic of India requests that the evidence noted below be provided as soon as possible, (*reason for urgency/ timing for obtaining evidences)*

CONFIDENTIALITY

6. The details of this criminal investigation are considered sensitive in India. Therefore, in accordance with Article 5 (6) of the MLAT this document, its contents, and the fact that, this request has been made, be kept confidential and that it is not to be publicly disclosed.

DESCRIPTION OF SUBJECT MATTER OF INVESTIGATION

7. *(Brief Background)*The main objective of Islamic State (IS) or the Islamic State of Iraq (ISI) or the Islamic State of Iraq and AI Sham / Islamic State of Iraq and Syria (ISIS) or the Islamic State of Iraq and Levant (ISIL) or the ad-Dawlah-al Islamiyah fiI-Iraq wa-sh Sham (DAISH), an international Jihadi terrorist organization is to establish *Caliphate* by indulging in terrorist activities across different countries in the world including India. In furtherance of its larger conspiracy under its leadership, members of the above named organization in connivance with few residents and non-resident Indians have been indulging in identification, radicalization, recruitment, training and finally transfer of Indian youths to countries including but not limited to Syria, Libya, Iraq, etc. for indulging in terrorist activities as defined in Section 15 of UA (P) Act, 1967.

8. The *(Institution/ Police Station/ Branch)*, Gujarat, one of India's ______law investigation agency initiated an investigation into the matter vide case ______________________ [Copy of the First Information Report of *(Institution/ Police Station/ Branch)* is annexed as **Annexure 'A'**].

9. During investigation it was revealed that **(Name of the accused)**son of (Father's name) and resident of (Residential address), Gujarat State, India and other unknown persons had conspired with (Handler), based in Syria and purportedly the media chief of ISIS (facts which are relevant to the P.S. case) and *others to motivate and radicalize various persons from that locality to join*

Islamic State of Iraq and Syria (ISIS) and instigating them to travel abroad to become member of ISIS and contribute to the said terrorist organization in its terrorist acts and waging of war against allied nations of India.

10. Investigation has established that in pursuance of the above conspiracy, *(Give facts related to the case)*. However, it was revealed that *(Name of accused)* had *(give facts related to the accused)*. It is further learnt that ___________________ had ________________and suspected to have joined ISIS and involved in terror acts. He was purported to be in contact with ISIS members/ propagators and was motivated in joining ISIS. *He is accordingly shown as a wanted accused in this case*.

11. Investigation has also revealed that on the instruction *of (Handler) (who is declared as wanted accused in this case),* one *(Name of the Indian accused) (resident of ________________)* had *(facts of the case)* in *(year involved)and met with such likeminded people and organized meetings in which it was decided to form jihadi organization in India known as "_____________" which would be affiliated to ISIS and whose sole objective would be to spread the ideology of ISIS by violent means (facts of the case)*. In pursuance of the said conspiracy, *(Accused ____)* had visited ______________________. In the process, *(facts related to the accused ____ and his associates in the crime). (Accused ________)* was thereafter arrested in this case on __________

12. From the interview/ questioning of (Accused) and other evidence, it has come to light that he alongwith one (Handler) have been involved in radicalizing Indian youths and instigating them to join ISIS to travel abroad to become member of ISIS and contribute to the said terrorist organization in its terror acts. (Handler) has

purportedly travelled to ________ and joined ISIS and has become active member of ISIS and involved in instigating Indian Muslim youth in joining ISIS through (accused/ suspects/ associates). (Handler) is still suspected to be in ______ and with the ISIS members and propagators he is trying to establish a jihadi organization in India having affiliation and working under the umbrella of ISIS with the primary objective of spreading the ideology of ISIS and its path of Jihad through violence means in India.

13. *(Facts of the case).*

14. To evade detection by intelligence and investigation agencies, the arrested accused person and the wanted accused person/suspect used various social media platforms i.e. chat and messenger services etc. The interaction over the web based social media services resulted in strengthening the group, transmission of jihadi materials to influence and instigate young Muslim Indian to travel to the conflicted zone of Iraq and Syria. (Facts related to this case)

15. The execution of request under MLAT will help unearth the conspiracy through which the above mentioned persons were recruited to the ISIS and the details of the terrorist acts they have committed in Syria or were planning to commit such act in India. It will also help reveal their future plans for terrorist activities in Iraq, Syria and other countries, including India. Besides, the assistance provided may help establish the identities of the recruiters and facilitators who assisted the recruitment of the above mentioned persons to the ISIS, their Indian colleagues in ISIS affiliated organization "__________" and potential Indian recruits to the ISIS/ ___________.

16. The investigation in this case is in progress. These evidences needs to be placed before the Court on or before (_________ period of last date of charge-sheet) for the Court to take cognizance of the offences purported to have been committed by them. The evidence to be collected from central authority of United State of America shall be adduced as evidence against the said arrested accused as well as wanted accused amongst others.

17. This request is also in consonance with the express understanding of both the countries that to extend all cooperation in the investigation, prosecution, and proceedings in criminal matters including those relating to terrorism, and in line with the letter and spirit of the binding resolutions of the United Nation Security Council Resolutions Nos. 1267(1999), 1373 (2001) and 1566 (2004), as well as the International Convention for the Suppression of the Financing of Terrorism, 1999.

SUMMARY OF PERTINENT FACTS

18. The instant case was registered on the allegation that certain unknown persons have radicalized in conspiracy with other terrorist groups are recruiting Indian nationals to commit terrorist acts and waging of war against allied nations of India.

19. (Accused) who was one such person recruited through this conspiracy, went to (facts of the case). He is presently learnt to be waging war against allied nations of India.

20. In the meantime, (other accused) who is learnt to be a motivator for ISIS was arrested on (date of arrest) in this case and during his interviews (arrested accused) revealed that he communicated with his recruiters/propagators of

ISIS and other likeminded colleagues using various electronic and social media platforms.

21. (Arrested accused) has revealed during investigation that for communication he used the following email ids provided by US based **Google/ Yahoo** domain

(a) ____________@gmail.com,

(b) ______________@gmail.com

(c) ___________@yahoo.com

These email ids are linked to social media accounts like facebook accounts, twitter, Trillian, Telegram, accountsetc having US based domain.

22. Investigation has revealed that during the period between ________ to _________, (arrested accused) had communicated with ISIS handler like (Name of the handler) or other likeminded people using different social media platform like **FACEBOOK; TWITTER; TRILLIAN; TELEGRAM;** ; (OTHER SOCIAL MEDIA PLATFORMS) etc for sharing thought and spreading the ideology of ISIS in India with the basic objective of influencing one another. Through this medium, lot of material was shared by them amongst themselves. (Arrested accused) had used the following social media accounts which were connected with his above mentioned email ids viz.

(A) FACEBOOK

(i)

(B) TWITTER

(i)

(C) TELEGRAM

(i)

(D) TRILLIAN

(i)

(E) Others Social media

(i)

23. Investigation has also revealed that (Other arrested accused) was using following email ids provided by US based **Google** and **Yahoo** domain for communication

(a) __________@gmail.com;

(b) _________@yahoo.com;

These email ids were linked to various social media accounts.

24. Investigation has revealed that during the period between ______ to _______, **(Other arrested accused)** was using the social media platform like **FACEBOOK**; **TELEGRAM; TWITTER** __________ from time to time for influencing young Indian Muslim youth. Through this medium, lot of material was shared by him. During this period, **(other arrested accused)** had used the following social media accounts which were connected with his above mentioned email ids viz.

(A) FACEBOOK

(i)

(B) TWITTER

(i)

(C) TELEGRAM

(i)

25. Investigation has revealed that during the period between _____ to ______, (Handler) was using different social media platform like **FACEBOOK; TWITTER, TELEGRAM, TRILLIAN;SURESPOT**etc from time to time for posting anti-national messages against India as well as spreading inflammatory posts and links regarding ISIS for spreading the ideology of ISIS with the basic objective of influencing young Indian Muslim youth. Through this medium, lot of material was shared by him with arrested accused persons. During this period, (handler) had used the following social media accounts

(A) FACEBOOK

(i)

(B) **<u>TWITTER</u>**
(i)
(C) **<u>TELEGRAM</u>**
<u>(i)</u>
(D) **<u>TRILLIAN</u>**
(i)
(E) **<u>SURESPOT</u>**
(i)

26. Investigation has also revealed that (OTHERS if required) was usingthefollowing email ids provided by US based **Google** domain for communicating with various persons.

(a) ____________@gmail.com;
(b) __________@gmail.com;

These email ids were linked to various social media accounts.

27. Investigation has revealed that during the period _______, (Others if required) had created various social media platform to communicate with his associates viz. ________, ______ etc. He has also tried to communicate with the arrested accused persons. For the said purpose, (Others) had created accounts like **FACEBOOK; TWITTER; TELEGRAM; TRILLIAN; SURESPOT** from time to time for chatting with his handlers. Through these medium, lot of material was shared with him. During this period, Mohsin Ibrahim Sayyed had used the following social media accounts

(A) **<u>FACEBOOK</u>**
(i)
(B) **<u>TWITTER</u>**
(i)
(C) **<u>TELEGRAM</u>**
<u>(i)</u>
(D) **<u>TRILLIAN</u>**
(i)

(E) **SUREPSPOT**

(i)

28. Investigation has further revealed that that during the period between ____ to _____, the arrested accused persons like _________ and ___________ have communicated with various likeminded people in different parts of India on the social media platform like **FACEBOOK**; **TWITTER**, **TELEGRAM,TRILLIAN**etc from time to time for sharing their thought and liking for ISIS and its ideology. The above named accused person or their associates have communicated with the following persons using the following ids in the social networking platforms as detailed below :

Sr. No.	**Accounts & User Ids**	**Used by**	**Relation**
A	**FACEBOOK ACCOUNT**		
1	_____________	___ from (Place)	Associates
2	_____________	___ from (Place)	Associates
B	**TWITTER ACCOUNT**		
1	_____________	___ from (Place)	Associates
2	_____________	___ from (Place)	Associates
C	**TELEGRAM**		
1	_____________	___ from (Place)	Associates
2	_____________	___ from (Place)	Associates

29. Investigation of the case so far suggests that there is a real and major risk of more Indians Muslim youth getting radicalized through the use of the social networking platforms and being influenced to join ISIS in near future. Besides, already recruited Indian in the ISIS, may return to India and pose a major security risk to the country. Both these factors suggest that the threat posed by the ISIS recruitment in India is ongoing and calls for an early response to this request.

OFFENCES CHARGED

30. The accused persons are being investigated for offences under sections _______ of IPC and ______ of the Unlawful Activities (Prevention) Act 1967 as amended. *(relevant provisions of Acts/ Laws etc..)*, [**Extract of relevant sections enclosed as Annexure B**]

DESCRIPTION OF EVIDENCE/INFORMATION REQUIRED

31. The Central Authority of the Republic of India requests that the Central Authority of the United States of America may please provide all the relevant information on points listed below in respect of the aforementioned email IDs and all social networking accounts since their inception and specifically for the period ________. The details of all the communications made on all the aforementioned email accounts and all social networking accounts by the subscribers are crucial and may help to identify and arrest the accused persons involved in the commission of crime and to unravel the greater criminal conspiracy hatched by them to prevent any future terror plots.

(A) **Assistance/ Information Required Pertaining to GOOGLE/ YAHOO accounts :**

(I) Complete Subscriber information including registration information, user names, screen names or any other identities of the above listed email IDs mentioned above in para(s) 21; 23 and 26.

(II) Login history (Login and Logout session details) of the account containing MAC ids, Internet Protocol (IP) addresses / Details and the associated time stamps as available.

(III) All mails with email contents and attachments including but not limited to Inbox, Sent, Drafts, Bulk, Trash, Contacts and also all deleted information pertaining to the questioned email accounts since their inception.

(IV) All the contents, including but not limited to Profile information, Messages, Images, Audio, Videos, Friends List, Chats, Log-in Session details and also all deleted information pertaining to the above mentioned accounts.

(V) Information on any other email account linked to the tool bar with subscription details and other information related to services subscribed to.

(VI) Information, as to whether the mail id in question was used for logging in or registration of user accounts in in , Facebook, Telegram, , Trillian, Twitter, Orkut, Surespot, Hush Mail, Nimbuzz, Yahoo messenger any chat rooms, etc. or other accounts in the internet.

(VII) Information, as to whether the mail ids were used for any other transactions (including financial) on the internet.

(VIII) All data submitted for transliteration and Internet Protocol (IP) details.

(IX) All search history related to the accounts, via toolbar and website

(X) Any other information or mode of transmission of any data in any format other than what is mentioned above which may be relevant.

(XI) All archived records (including deleted data) for the period of __________ to ___________, pertaining to the above mentioned **Google** and **Yahoo and (others)**

accounts are crucial and important for taking the investigation to a logical conclusion and prosecution.

In this connection, the concerned authorities are required to be examined by the officers deputed pertaining to

(1) Google Inc hosting the server at Google Inc., 1600, Amphitheatre, Parkway, Mountain View, CA 94043, United States.

(2) Yahoo! Inc. 701 First Avenue Sunnyvale, California 94089, United States

(3) Others if any

(B) <u>Assistance/ Information Required Pertaining to FACEBOOK account:</u>

(I) Basic Subscriber Information-User Identification Number E-mail addresses Date and Time Stamp of account creation date displayed in Coordinated Universal Time Most Recent Logins in Coordinated Universal Time Registered Mobile Number Expanded Subscriber Content.

(II) Profile Contact Information Mini-Feed Status Update History Shares Notes Wall Postings Friend Listing, with Friends Facebook ID's Groups Listing, with Facebook Group.

(III) Future and Past Events Video Listing, with filename.

(IV) User Photos and photos uploaded by the user and photos uploaded by other users that have the requested user tagged in them.

(V) Group Information will include the BSI of the group creator/administrator and the current status of the group.

(VI) Private Messages if retained.

(VII) IP Logs if available may be provided in a tab delimited text file and may include:

a) View time - Date of execution.
b) Script - Script executed.
c) Scripts get - Additional information passed to the script.

d) Session Cookie - HTIP cookie set by user session.

e) Any other information or mode of transmission of any data in any format other than what is mentioned above which may be relevant.

(VIII) All archived records (including deleted data) for the period of ______ to __________, pertaining to the above mentioned **Facebook** accounts are crucial and important for taking the investigation to a logical conclusion and prosecution.

In this connection, the concerned authorities of **Facebook** hosting the server at-Facebook, Ireland Ltd., 4 Grand Canal Square, Dublin 2, Ireland are required to be examined by the officers deputed.

(C) <u>Assistance/ Information Required Pertaining to TWITTER IDS :</u>

(I) Registration information including full name provided at the time of account registration including details of IP, valid email ID, phone number, IMEI number, or MAC number of mobile handset and any other information required to complete signup process.

(II) Tweets/ Retweets.

(III) Follower/Followings/Likes.

(IV) Login history.

(V) Contents and logs of the said accounts.

(VI) Any video shared with someone.

(VII) Any other information or mode of transmission of any data in any format other than what is mentioned above which may be relevant to the said case.

(VIII) All archived records (including deleted data) for the period from ------------ to --------------, pertaining to the above mentioned **Twitter** accounts are crucial and important for taking the investigation to a logical conclusion and prosecution.

In this connection, the concerned authorities of **Twitter** hosting the server at- Twitter Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, United States are required to be examined by the officers deputed.

(D) <u>Assistance/ Information Required Pertaining to TRILLIAN IDS :</u>

(I) Registration information including full name provided at the time of account registration including details of IP, valid email ID, phone number, IMEI number, or MAC number of mobile handset and any other information required to complete signup process.

(II) General Account details like
- (i) Trillian Credential
- (ii) Billing Information
- (iii) Instant Messenger Usernames And Password
- (iv) Instant Messenger Contact List
- (v) Instant Messenger Conversations
- (vi) Shared Images
- (vii) Web Cookie(s)
- (viii) Chat History/ Group Chats

(III) All archived records (including deleted data) for the period from ----------- to -------------, pertaining to the above mentioned **Trillian** accounts are crucial and important for taking the investigation to a logical conclusion and prosecution.

(IV) Financial transactions, if any, conducted through **Trillian** ids with billing addresses and the mode of payment.

(V) Destination telephone/mobile numbers for any chats/messages placed to the Public Switch Telephone Networks (PSTN) within India.

(VI) All archived data including deleted data pertaining to video messaging, instant messaging, text (SMS), voice messages, chats contents, all type of files, all media files including photos, videos etc. transmitted or shared during each session.

(VII) Any other information or mode of transmission of any data in any format other than what is mentioned above which may be relevant.

In this connection, the concerned authorities of **Trillian** hosting the server at 59, Bassant Avenue, Pen Rose Auckland 1061, New Zealand are required to be examined by the officers deputed.

(E) <u>Assistance/ Information Required Pertaining to TELEGRAM IDS :</u>

(I) Registration information including full name provided at the time of account registration including details of IP, valid email ID, phone number, IMEI number, or MAC number of mobile handset and any other information required to complete signup process.

(II) The contact list (stored and deleted) of the persons with whom communication was made including E-mail addresses/ **Telegram** ID, the Phone numbers and IMEI number or MAC number of mobile handsets used for accessing these IDs.

(III) Archived log including deleted logs of each session with IP addresses, E-mail addresses/ **Telegram** ID, the Phone numbers and IMEI number or MAC number of mobile handsets of all the contacts with whom communication was made.

(IV) Financial transactions, if any, conducted through **Telegram** ids with billing addresses and the mode of payment.

(V) Destination telephone/mobile numbers for any chats/messages placed to the Public Switch Telephone Networks (PSTN) within India.

(VI) All archived data including deleted data pertaining to video messaging, instant messaging, text (SMS), voice messages, chats contents, all type of files, all media files

including photos, videos etc. transmitted or shared during each session.

(VII) Groups, Super groups, and Channels used.

(VIII) Any other information or mode of transmission of any data in any format other than what is mentioned above which may be relevant.

In this connection, the concerned authorities of **Trillian** hosting the server at 3739 Balboa St.San Francisco, CA 94121, USA are required to be examined by the officers deputed.

(F) <u>Assistance/ Information Required Pertaining to SURESPOT IDS :</u>

(I) Registration information including full name provided at the time of account registration including details of IP, valid email ID, phone number, IMEI number, or MAC number of mobile handset and any other information required to complete signup process.

(II) Details on the following issues are required -

- (i) Usernames.
- (ii) Friend relationships (who is friends with who, blocked who, ignored who, deleted who)
- (iii) Conversation relationships (how many friends currently you have a "conversation" with - meaning have a sent or received a message with)
- (iv) Messages which each have a server timestamp, to username, from username, and encrypted content, or link to encrypted content (image or file)
- (v) Encrypted message file data (image or other - anything but encrypted message content) is stored (encrypted in the same way text messages are) on rack space cloud files.
- (vi) Total messages sent per user.
- (vii) Total images sent per user.
- (viii) Current message count per user.

(ix) Signing (DSA) public keys and versions.
(x) Encryption (DH) public keys and versions.
(xi) Encrypted "friend images" or avatars and friend aliases that are assigned to certain usernames. These are encrypted with a key generated from ECDH key derivation of assigning identity's private/public key-pair.
(xii) Google GCM id (used for push messaging) which is related to the username in the surespot database.
(xiii) Apple APN token (used for push messaging) which is related to the username in the surespot database.
(xiv) If voice messaging is purchased, a purchase token given to by Google or Apple which is related to the username in the surespot database.

(III) Any other information or mode of transmission of any data in any format other than what is mentioned above which may be relevant.

In this connection, the concerned authorities of **Surespot** hosting the server at Surespotllc., 2995, 55th Street # 18034 Boulder, CO 80308 USA are required to be examined by the officers deputed.

CERTIFICATION

32. To ensure that the requested business and electronic records are admissible at trial, the Central Authority of the Republic of India requests that, in terms of Article 8 (5) of the MLAT and the provisions of 65-B and Section 78 (6) of the Indian Evidence Act, 1872 (**Annexure C**), a certificate as mandated under Section 65-B of the Indian Evidence Act, 1872 be issued in respect of electronic records provided by the custodian of the business and electronic records in soft form and the copies of the documents in hard forms, if any, be authenticated by the custodians of the records at the businesses, or such other person authorised by law providing such documents or records may execute the relevant Formas provided in the treaty and attach it to the documents/items. The

documents/items along with appended 'Form' should then be sent to the Central Authority of the Republic of India.

33. The Central Authority of the Republic of India also urges that the executing authority whether the custodian would, if necessary, be willing to travel to the Republic of India, at the expense of the Central Authority of the Republic of India, to testify during the trial. The Republic of India undertakes to bear any costs which may be incurred in execution of this request in terms of Article 6 of the Mutual Legal Assistance Treaty.

CONFIDENTIALITY

34. The details of this criminal investigation are considered sensitive in India. Therefore, in accordance with Article 5(6) of the Treaty, it is requested that the document, its contents, and the fact that this request has been made, be kept confidential and that it should not be publicly disclosed.

CONTACT INFORMATION

35. Further information regarding this request, if any, may please be obtained from *(Name of Head), (Designation)(Institution/ Police Station/ Branch)*, Gujarat Police, Gujarat Government, Government of India, at +91_______ and +_______, or by email at _________ .

CONCLUSION

36. Please accept the assurance of our highest esteem and regard for the Central Authority of the United States of America. We look forward for assisting the Central Authority of the United States in response to requests under the Treaty

.

37. The Ministry of Home Affairs, Government of India, once again avails of this opportunity to pay its highest compliments and considerations to the Central Authority of the United States of America.

List of Enclosures: –

1. **Annexure-A** (Copy of the FIR)
2. **Annexure-B** (Description of offences)
3. **Annexure-C** (Description of Section 65-B and Section 78 of the Indian Evidence Act,1872)

UNDER SECRETARY TO
GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS
(The Central Authority of the Republic of India)

પરિશિષ્ટ-૨

FORMAT FOR CERTIFICATE UNDER SECTION 65B OF INDIAN EVIDENCE ACT, 1872

(Authenticity of Electronic Records)

I ....(name) state that I am employed in ....(organization) as ....(designation).

2. I state that being employed in _______, I have personally supervised in preparation on the following electronic records as noted below, through computer terminals in my / our office, by me / our staff under my direct supervision.

a. A DVD-R bearing no...............................containing true copy of all electronic records pertaining to ....email account, original of which are available in our computers. The hash value of the contents of the DVD-R is ....

b. A DVD-R bearing no..containing true copy of all electronic records pertaining to ....email account, original of which are available in our computers.

c. A computer printout numbering from page.......... to ....marked as ....containing true copy of ......electronic records pertaining to ....original of which are available in our computers.

(Please note that print out of an electronic records stored in a computer is also an electronic record)

(a,b,c,......... is the list all the electronic documents which are being certified and sent under this certificate. It should be clearly identifiable and therefore the DVD-R or the printout should bear a seal / handwritten note/printed note/ signature, and which should be made note of in the certificate)

(Each page of printout should be carrying a seal of the office / officer sending it)

(Furnishing the hash value of the contents of the record furnished is not compulsory but desirable in the certificate)

3. I further state that all the electronic records contained in digital media / print outs as noted in para 2 above are true copies made of the original electronic records maintained in our computers, in our establishment and the same have been produced using the computers in our establishment under my command identifiable as noted below:-

a. Computer no./Computer Series/ Server no...

b. Printer...

c. ....

4. (Section 65B (4b) requires that the certificate should "give such particular of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by the computer" and also "describing the manner in which the electronic records were produced")

5. In respect of the records provided above and the Information contained therein, it is further certified that:-

a. The computer output containing the information was produced by our computers during the period over which computer was used regularly to store and/ or process information for the purposes of any activities regularly carried on over that period by our authorized employees.

b. During the said period the information of the kind contained in the electronic record or of the kind form which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities.

c. Throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation for that part of the period, was not such as to affect the electronic record or the accuracy of its contents.

d. The information contained in the electronic record reproduces or is derived from such information fed into computer in ordinary course of said activities.

6. This is stated to the best of my knowledge and belief.

Place	Signature
Date	Name & Designation
	(with seal preferably)

*(The marked text is only for guidance in making the certificate)

પરિશિષ્ટ-૩

LETTER ROGATORY (LETTER OF REQUEST) FOR EVIDENCE FROM SKYPE

TO : The Under Secretary (Legal), Internal Security Division,Ministry of Home Affairs, LokNayak Bhawan, New Delhi – 110003

FROM : *(Institution/ Police Station/ Branch)*, Gujarat Police,Gujarat

SUBJECT : Request for obtaining concurrence regarding issuance of Letter Rogatory in the investigation of Case No. ________ registered at *(Institution/ Police Station/ Branch)*, Gujarat Police Station related to *(short case outline)* .

FILE NO: _________________________

BACKGROUND AND PURPOSE

5. The *(Institution/ Police Station/ Branch)*, Gujarat Police is investigating Case ___________________ under sections _______________ of IPC and _______________________ of the Unlawful Activities (Prevention) Act, 1967 of Unlawful Activities (Prevention) Act. *(relevant provisions of Acts/ Laws etc..)*, pertaining to *(case brief)*. In order to complete the on-going investigation, evidence as detailed below is necessary to be collected to prosecute the accused in court of law.

6. This request is being made as per the guidelines issued by Internal Security Division, Ministry of Home

Affairs, vide its letter no. 25016/14/2007-Legal Cell, dated: 31/12/2007.

DESCRIPTION OF SUBJECT MATTER OF INVESTIGATION

7. *(Brief Background)*The main objective of Islamic State (IS) or the Islamic State of Iraq (ISI) or the Islamic State of Iraq and AI Sham / Islamic State of Iraq and Syria (ISIS) or the Islamic State of Iraq and Levant (ISIL) or the ad-Dawlah-al Islamiyah fiI-Iraq wa-sh Sham (DAISH), an international Jihadi terrorist organization is to establish *Caliphate* by indulging in terrorist activities across different countries in the world including India. In furtherance of its larger conspiracy under its leadership, members of the above named organization in connivance with few residents and non-resident Indians have been indulging in identification, radicalization, recruitment, training and finally transfer of Indian youths to countries including but not limited to Syria, Libya, Iraq, etc. for indulging in terrorist activities as defined in Section 15 of UA (P) Act, 1967.

8. The *(Institution/ Police Station/ Branch)*, Gujarat, one of India's ______law investigation agency initiated an investigation into the matter vide case _____________________ [Copy of the First Information Report of *(Institution/ Police Station/ Branch)* is annexed as **Annexure 'A'**].

9. During investigation it was revealed that **(Name of the accused)**son of (Father's name) and resident of (Residential address), Gujarat State, India and other unknown persons had conspired with (Handler), based in Syria and purportedly the media chief of ISIS (facts which are relevant to the P.S. case) and *others to motivate and radicalize various persons from that*

locality to join Islamic State of Iraq and Syria (ISIS) and instigating them to travel abroad to become member of ISIS and contribute to the said terrorist organization in its terrorist acts and waging of war against allied nations of India.

10. Investigation has established that in pursuance of the above conspiracy, **(Name of the accused)**extensively used Skype messenger sevices, for provoking youths to undertake terror acts like murdering jews, destabilize the law and order situation in India, especially Kashmir.

11. Investigation so far has also revealed that **(Name of the accused)** and**(Name of the co-accused)**came in contact with each **(Handler)**and (**Handler)** through Skype. Thereafter *(other details)* and other associates and used to communicate through various electronic chat and messenger platforms including **Skype**.

12. The execution of Letter Rogatory on basis of Assurance of Reciprocity will help unearth the conspiracy through which the above mentioned persons were recruited to the ISIS and the details of the terrorist acts they have committed in Syria or were planning to commit such act in India.

13. *(Brief Conclusion)* These evidences needs to be placed before the Court on or before ______i.e. last date of charge-sheet for the Court to take cognizance of the offences purported to have been committed by them. The evidence to be collected from Central Authority of The Grand Duchy of Luxembourg shall be adduced as evidence against the said arrested accused as well as wanted accused amongst others.

SUMMARY OF PERTINENT FACTS

14. The instant case was registered on the allegation that certain unknown persons have radicalized in conspiracy with other terrorist groups are recruiting Indian nationals to commit terrorist acts and waging of war against allied nations of India.

15. **(Name of the accused)**who was one such person recruited through this conspiracy, went to indulge in terror acts. He is presently arrested for waging war against allied nations of India. He was arrested on ______in this case and during his interviews **(Name of the accused)**revealed that he communicated with his recruiters/propagators of ISIS and other likeminded colleagues using various electronic and social media platforms.

16. **(Name of the accused)**has revealed during investigation that for communication he used the following id(s) linked/ provided by Luxembourg based **Skype Communications Sarl.**
(a) ______
(b) _________
(c) _________
(d) _______@yahoo.com
(e) __________
(f) ___________@gmail.com
(g) 94xxxxxxxx

17. Investigation has also revealed that one other arrested accused **(Name of the co-accused)**was using following id(s) linked/ provided by Luxembourg based **Skype Communications Sarl.**
(a) ________
(b) ________@yahoo.com
(c) ________@gmail.com

(d) 99xxxxxxxx

18. Investigation has revealed that during the period between 20xx to 20xx, various persons were in contact of both accused **(Name of the accused)** and**(Name of the co-accused)**using messenger platform **SKYPE,** from time to time for spreading anti-national messages against India as well as spreading the ideology of ISIS with the basic objective of influencing young Indian Muslim youth. Through this medium, lot of material was shared with arrested accused persons. During this period, the following **SKYPE** accounts were used for this purpose.

i) ________

ii) __________

19. Investigation of the case so far suggests that there is a real and major risk of more Indian Muslim youth getting radicalized through the use of the social networking platforms and being influenced to join ISIS in near future. Besides, already recruited Indian in the ISIS, may return to India and pose a major security risk to the country. Both these factors suggest that the threat posed by the ISIS recruitment in India is ongoing and calls for an early response to this request.

OFFENCES CHARGED

20. The accused persons are being investigated for offences under sections _______ of IPC and ______ of the Unlawful Activities (Prevention) Act 1967 as amended. *(relevant provisions of Acts/ Laws etc..)*.

CONTACT INFORMATION

21. Further information regarding this request, if any, may please be obtained from *(Name of Head)*, *(Designation)(Institution/ Police Station/ Branch)*, Gujarat Police, Gujarat Government, Government of India, at +91___________ and +____________, or by email at _________________.

CONCLUSION

22. The issuance of Letter Rogatory from a Competent Court is absolute necessary in order to obtain the required electronic evidence for taking the case to a logical conclusion.

23. Moreover it is necessary that the Letter Rogatory be issued on basis of Assurance of Reciprocity as there has been no Mutual Legal Assistant Treaty (MLAT) between The Government of The Republic of India and The Grand Duchy of Luxembourg in Criminal Matters.

List of Enclosures: –

4. **Annexure-A** (Copy of the FIR)
5. **Annexure-B** (Draft application to be filed in Competent Court for issue of Letter Rogatory)

(Name of Head)
(Designation)
(Institution/ Police Station/ Branch)
GUJARAT

Annexure-B

[DRAFT APPLICATION TO BE FILED IN THE COMPETENT COURT FOR ISSUE OF A LETTER ROGATORY]

IN THE HON'BLE COURT OF ____AT (PLACE), GUJARAT

(Institution/ Police Station/ Branch), Gujarat Case CR. No. ____/2017

Exh. __________

State represented by
(Institution/ Police Station/ Branch), Gujarat
… Applicant

Vs.

Name of Accused& Others
… Accused

Application under section 166-A of the Code of Criminal Procedure 1973 for Issuance of a Letters Rogatory to the Competent Authority in The Grand Duchy of Luxembourg for Judicial Assistance in the collection and transfer of evidence.

MAY IT PLEASE YOUR HONOUR

It is submitted on behalf of the P.S., Ahmedabad that:

1.1 A case with CR No. __________ was registered on ________ under sections _________ of IPC and under sections ___________ of Unlawful Activities (Prevention)

Act, 1967 as amended in 2008. *(relevant provisions of Acts/ Laws etc..),*; by the *(Institution/ Police Station/ Branch),* Gujarat against one (Name of accused) son of (Father's name) and (Name of co-accused), son of (Father's name), about the acts done by certain unknown persons to motivate and radicalize certain Indian youths to join the Islamic State of Iraq and Syria (ISIS), proscribed by the Government of India as a terrorist organization and to instigate him to travel abroad to become a member of ISIS and to contribute to the commission of terrorist acts and waging of war against the nations at peace with India. A copy of the First Information Report of the P.S. marked as **ANNEXURE - A** is enclosed for ready reference.

1.2 The P.S. has taken up the investigation and presently the investigation is in progress.

1.3 *(Basis of Letters Rogatory)*It is submitted that the Islamic State of Iraq and Syria (ISIS) is a terrorist organization having its base in Iraq and Syria with the principal objective of engaging in acts of terrorism. Al-Qaida in Iraq, subsequently renamed as Islamic State of Iraq and Syria (ISIS) in 2013, is listed in the Schedule to the U.N. Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007 made under section 2 of the United Nations (Security Council) Act, 1947 which is included at serial no. 38 in the first Schedule to the Unlawful Activities (Prevention) Act, 1967.

2. *(Basis of Letters Rogatory)*Para No. 2 (f) of United Nations Security Council Resolution No. 1373/2001 (passed in the 4385th meeting of the United Nations Security Council on September 28, 2001), specifically requires that all States shall provide the greatest measure of assistance in connection with criminal investigations and criminal proceedings relating to terrorist acts, including the obtainment or/ and collection of evidence within their

possession, and therefore in a positive sense, casts an international mutual obligation of cooperation in the matters of criminal investigations, including the collection and transfer of evidence particularly in terms of the provisions of Article 25 of the United Nations Charter, that reads as :

"The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter".

As per this resolution every member countries of UN are under obligation to exchange the information and evidences under their possessions to other countries which are in need of such information. Since the Federal Republic of Germany is a member state of UN, it will have a liability to exchange such information pertaining to terrorist acts.

3. <u>Facts established during Investigation</u>:

3.1 Investigation has established through witnesses that (Name of accused) is the son of (Father's Name)is the resident of *(Family Background)* The accused, (Name of accused)is the eldest son of them all. Documents collected during the course of investigation have established that the accused persons is holding an Indian Passport No. ______issued on _______ by the Regional Passport Officer, ______.

3.2 Investigation has brought on records through witnesses that the initial journey of the accused (Name of accused)towards radicalization started in or around 2013-2014 when he came in contact with (Name of handler). He was thoroughly monitoring the development of the ISIS activities on social media platforms. He started watching video clips as well as photos of the ISIS organisation. He also started listening to speeches related to the ISIS on his mobile phones. This had

great bearing and impact on the accused (Name of accused) in developing a violent Jihadi mind set. A radical change was also noticed in the attitude and behaviour of the accused (Name of accused).

3.3 During the course of investigation, it was brought on records through various witnesses as well as close associates that the accused (Name of accused)entered into a criminal conspiracy with his handler (Name of handler), a wanted accused in various cases of serial blasts by Indian Mujahideen and the accused (Name of co-accused)during the period between 20xx to 20xx in propagating the Jihadi activities of ISIS with the common objective and intention to join ISIS, a banned International Terrorist Organization and participate in its terrorist acts.

3.4 Investigation has further brought on records through witnesses and close associate that the accused (Name of accused)was having great influence over the Muslim youths of the (Address/ locality), Gujarat. He would constantly convene closed group meetings with gullible youths of Surat and radicalising them with ideology of Islamic State. In various conversations with these youths, (Name of accused) would call these youths for one-to-one meetings, and avoid discussing things on phone.

3.5 **Similar for co-accused.**

3.6 Interrogation/ interview of the arrested accused (Name of accused)has established that in pursuance of the above conspiracy, he created account ids/ ids associated with:

(i) __________;
(ii) ____________;
(iii) ________;
(iv) _________@yahoo.com;

in the social media platform "**Skype**" for communicating with his handler as well as his co-accused.

3.7 Investigation has established through independent witnesses and documents collected during investigation that during year 2013-2017 the accused (Name of accused)was using the mobile number 94xxxxxxxx. It needs to be ascertained with what other credentials, the **Skype** accounts were registered at the time of opening of the **Skype** accounts.

3.8 Similar for co-accused.

3.9 Similar for handler.

3.10 During the course of investigation preservation request was sent to the Nodal Officer of Skype Communications, Luxembourg at *(Time)* on *(Date)* for the preservation of the contents and data stored in the Skype accounts ids.

4 Investigation suggests that ISIS is continuously engaged in the acts to recruit more and more Indians. Besides Indians who have already been recruited to the ISIS, may return to India and pose a major security risk to the country. Both these factors suggest that the threat posed by the ISIS recruitment in India is ongoing and specific and calls for an early response to this request..

5 The records related to the above mentioned Skype accounts ids are available in the Skype server hosted at **Sarl, 22/24 Boulevard Royal, L-2249,** Luxembourg. The server of the Skype based in the Grand Duchy of Luxembourg will provide the details of the chats contents/ messages/ any conversations that had taken place between the Skype account ids of the accused (Name of accused) and (Name of co-accused)with the account ids of ISIS propagators/

sympathizer amongst others. It will also provide the details about the IP addresses, the date and time stamps and Internet Service Providers (ISPs) etc accessed through this account. As the evidence are required to be obtained from the Service Provider, Skype which is available in the Grand Duchy of Luxembourg, it is absolute necessary to get investigation conducted in the Grand Duchy of Luxembourgfor taking the case to its logical conclusion.

6 This Hon'ble Court may request the Competent Authority in the Grand Duchy of Luxembourg that any documents as may be necessary to prove a fact and its link with any of the witnesses or suspects or accused may be collected when they are examined by the officers deputed/ commissioned by the Competent Authority of the Grand Duchy of Luxembourg while executing the Letters Rogatory. The details pertaining to the assistance to be sought from the competent authorities of the Grand Duchy of Luxembourg is detailed in **ANNEXURE - H.**

7 This Hon'ble Court is requested to move the competent authority of the Grand Duchy of Luxembourg to order/direct competent investigation agency/officers in the Grand Duchy of Luxembourgfor collection of evidence and material for the purpose of transfer of such evidence to this court.

8 This Hon'bleCourt may request the competent authority in the Grand Duchy of Luxembourg that while getting investigation conducted the statement of witnesses may be recorded as per the requirement of law and procedure prevalent in the Grand Duchy of Luxembourg.

9 The documents/ records and material objects that may be collected by law enforcement officers in the Grand Duchy of Luxembourg at the behest of the Competent Authority in the Grand Duchy of Luxembourg as far as possible, should

be in original. In case xerox copies of the documents are to be collected each sheet may be certified to be a true copy of the original in manner of certification provided in law ordinarily followed in the Grand Duchy of Luxembourg and the original may be kept in the safe custody. It would be enough if such documents/ records are certified to be true copies of their respective originals by their respective legal custodians upon proof of the character of such documents in accordance with the prevalent law and procedure in force in the Grand Duchy of Luxembourg with a certificate under the seal and signature of a Notary Public/ Competent Authority, or an Indian Consul or a diplomatic agent as admissible under section 78 (6) of the Indian Evidence Act 1872.

10 In case of electronic evidence the certificate as envisaged under section 65 (B) of the Indian Evidence Act may be got issued by the custodian of electronic evidence. A specimen certificate under section 65 B of the Indian Evidence Act is annexed as **ANNEXURE - G**.

11 It is submitted that this Hon'ble Court may request the Competent Authority in the Grand Duchy of Luxembourg that if the documents so collected are in Luxembourgish/ French/ German or any other language which is not the official languages of India, the same is required to be translated into English language duly certified by official translator bearing the seal and signature on each and every page so translated.

12 It is submitted that in the interest of investigation, this Hon'ble Court may request that the officers of P.S. may be permitted to remain present during the execution of the Letters Rogatory by the authorities concerned in the Grand Duchy of Luxembourg.

13 It is submitted that any information or material obtained from the Grand Duchy of Luxembourg in pursuance of this Letters Rogatory shall be specifically used only for the purpose of the investigation of this case and the criminal proceedings arising out of this criminal case and shall not be disclosed directly or indirectly to any other agency or person without the consent of the competent authority of the Grand Duchy of Luxembourg. The case under investigation is not of political, military, racial or religious character.

14 The extract of the sections of laws viz. the Unlawful Activities (Prevention) Act 1967, the Indian Penal Code, 1860, the Indian Evidence Act, 1872 and the Code of Criminal Procedure, 1973 under which the case is being investigated and prosecuted is enclosed as **ANNEXURE – C; ANNEXURE – D; ANNEXURE – E and ANNEXURE –F*(These Annexures may be as per relevant Acts/Laws)*.**

15 A letter of "**Assurance of Reciprocity**" from Ministry of Home Affairs addressed to the Grand Duchy of Luxembourg is enclosed.

16 As per Indian law, it is not necessary to give any notice to the accused person(s) before executing the Letters Rogatory.

<u>PRAYER</u>

Therefore, it is prayed that this Hon'ble Court may issue a Letters Rogatory to the Competent Authority in the Grand Duchy of Luxembourg in accordance with the provisions of Section 166-A of the Code of Criminal Procedure for collection of relevant evidence in connection with the investigation in this case pursuant to transferring the same

to this Hon'ble Court at the earliest opportunity to enable it to be used/relied upon in the relevant criminal proceedings that may arise out of this investigation in the instant criminal case in the interest of justice.

( )
P.P. / *(Institution/ Police Station/ Branch),*
Gujarat

( )
(Designation)/ IO
(Institution/ PoliceStation/ Branch), Gujarat.

Date: __/__/2018

Place: *(Place)*

[Annexure – A: Copy of FIR
Annexure – B: English Translation of FIR
Annexure – C,D,E,F: Extracts of relevant Acts/Laws
Annexure – G: Sample copy of Certificate u/s 65 (B) of the Indian Evidence Act
Annexure – H: Assistance Required under Letters Rogatory]

Annexure - H

Assistance Required

In order to complete the investigation of the conspiracy to commit terrorist act of joining terrorist organization, ISIS, the following records /investigative steps are required to be taken at the Grand Duchy of Luxembourg.

List of Documents which are required to be collected or seized and List of Witnesses whose statements are to be recorded are as under :

1. The below mentioned data and all archived records (including deleted data) from the date of creation of the account id to till date, pertaining to the following Skype accounts ids viz.

(a) _______
(b) __________
(c) ______________

and any related accounts amongst others are crucial and important for taking the investigation to a logical conclusion.

(i) Registration information provided at the time of account registration including details of IP, email IDs, phone number, IMEI number, or MAC number of mobile handset used for registration.

(ii) The contact list (stored and deleted) of the persons with whom communication was made including E-mail addresses/Skype Ids, the Phone numbers and IMEI number or MAC number of mobile handsets used for accessing these IDs.

(iii) Archived log including deleted logs of each session with IP addresses, E-mail addresses/ Skype Ids, the

Phone numbers and IMEI number or MAC number of mobile handsets of all the contacts with whom communication was made.

(iv) Financial transactions, if any, conducted through Skype Ids with billing addresses and the mode of payment.

(v) Destination telephone/mobile numbers for any chats/messages placed to the Public Switch Telephone Networks (PSTN) within India.

(vi) All archived data including deleted data pertaining to video messaging, instant messaging, text (SMS), voice messages, chats contents, all type of files, all media files including photos, videos etc. transmitted or shared during each session.

(vii) Any other information or mode of transmission of any data in any format other than what is mentioned above which may be relevant.

2. The above mentioned records are available in the Skype servers located at Skype Communications Sarl, 22/24 Boulevard Royal, L-2249 Luxembourg.

3. It needs to be ascertained with which mobile number was the Skype account id

(a) __________

(b) _____________

(c) ________

purportedly used by the accused (Name of accused), registered at the time of opening of the said accounts.

4. Similar for co-accused

5. Authorities of Skype hosting the server at Skype Communications Sarl, 22/24 Boulevard Royal, L-2249 Luxembourg needs to be examined by the officers deputed/ commissioned by the Competent Authority of **the**Grand Duchy of Luxembourg while executing Letters

Rogatory. Their detailed statement needs to be recorded covering the below mentioned points.

(i) The details pertaining to the Registration information including full name provided by the account holders at the time of registration of account including details of IP addresses, valid email IDs, phone number, IMEI number, or MAC number of mobile handset used or any other information required to complete signup process for registration by the persons in whose name the following Skype accounts have been opened viz.

(a) ________

(b) ___________

(c) _____________

(ii) The details about the contact list (stored and deleted) of the persons with whom communication was made including E-mail addresses/ Skype accounts IDs, the Phone numbers and IMEI number or MAC number of mobile handsets used for accessing these IDs.

(iii) The details about the Archived log including deleted logs of each session with IP addresses, E-mail addresses/ Skype accounts ID, the Phone numbers and IMEI number or MAC number of mobile handsets of all the contacts with whom communication was made.

(iv) The details about any financial transactions conducted through Skype ids, if any, with billing addresses and the mode of payment.

(v) The details pertaining to all archived data including deleted data pertaining to video messaging, instant messaging, text (SMS), voice messages, chats contents, all type of files, all media files including photos, videos etc. transmitted or shared during each session related to above accounts as available in the server of the company, Skype at Skype Communications Sarl, 22/24 Boulevard Royal, L-2249 Luxembourg.

(vi) Any other relevant document/s as may be necessary to prove a relevant fact based upon information provided by Skype at Skype Communications Sarl, 22/24 Boulevard Royal, L-2249 Luxembourg when they are examined by the officers

deputed/ commissioned by the Competent Authority of the Grand Duchy of Luxembourg.

****

પરિશિષ્ટ-૪

DoT MANDATE REGARDING IPDR PARAMETERS

Goverment of India
Ministry of Communications & IT
Department of Telecommunications
Sanchar Bhawan, 20 - Ashoka Road, New Delhi-110001
(Data Service Cell)

No. 820-01/98-LR/Vol.(IX) Pt.....I

Date : 01.10.2013

To
All Internet Service Providers
All UASL/CMTS/UL(AS)/UL Licensees

Subject : Parameters for Internet Protocol Details Record (IPDR) and SYS LOG of Network Address Translation (NAT)

The Internet Protocol Details Record (IPDR) format for Internet and GPRS Services and Parameters to be stored for SYS Log of Network Address Translation (NAT) have been Finalized.

2. The Internet Service Providers and the UASL/CMTS/UL(AS)/UL Licensees are hereby Directed to maintain log for the following parameteres with immediate effect.

(i) IPDR Parameters to be stored in respect of Internet and GPRS services,

Sr. No.	Paremeters
1*	Name of Person / Organization
2*	Address
3	Contact No.
4**	Alternate Contact No.
5**	E-mail Address
6	Landline / MSISDN / MDN / Leased circuit ID for Internet Access
7	User ID for Internet Access on authentication
8	IP address assigned
9	Static / Dynamic IP Address Allocation
10	Source port of the public IP Address in case of NATING
11	IST Start Time of IP address allocation (hh:mm:ss)
12	IST End Time of IP address allocation (hh:mm:ss)
13	Start Date of IP address allocation (dd/mm/yyyy)
14	End Date of IP address allocation (dd/mm/yyyy)
15***	Source MAC Address / Other device Identification number

(Sr. 1 to 5 above may be stored from Customer Acquisition From (CAF))
(* - Photo ID & Address Proof are required to be maintained seprately by the Service Providers)

("- Optional)
("'-In Place of Customer Device MAC address, virtual MAC Address of DSLAM/routing device is captured in some of the systems.)

(ii) Paraments to be stored in SYS LOG of Network Address Translation (NAT) for Internet Access.

Sr. No.	Parameters
1	State Date (mm:dd:yyyy) & Time (hh:mm:ss)
2	End Date (mm:dd:yyyy) & Time (hh:mm:ss)
3	Source IP Address
4	Source Port
5	Translated IP Address
6	Translated Port
7	Destination IP Address
8	Destination Port

• Term SYSLOG here reers to Logs for Network Address Translation.

3. Internet Service Providers and UASL/CMTS/UL(AS)/UL Licensees shall communicate to their subscriber, other than individual subscribers for recording and maintaining of NAT SYS Log Parameteres as mentioned in Para 2 (ii) above for and NAT mechanism deplayed by them for access of internet over the Internet connectivity. The Service Provides shall also obtain the compliance from them in this regard.

Compliance may kindly communicated immediately.

01-10-2013
(S.T. Abbas)
Director (DS-II), DoT

પરિશિષ્ટ-૫

PRESERVATION REQUEST

No. DYSP/P.S./___/____
Office of The Addl. Director
General Of Police,
Gujarat State, Ahmedabad.
Tel. No.02717-241035
Fax No.02717-241150
Email Id:-xxxx@gujarat.gov.in
DATE:- __/__/____

To,
Nodal Officer
Google Inc. Montain View,
California, USA
Email: gitanjli@google.com, lis-apac@google.com

Subject: - Request to Preserve all such data in respect of E-Mail Ids.

Whereas, P.S., Gujarat, India, is investigating a case with C.R. No.______ u/secs 120-B, 121-A and 125 of IPC and 13, 17, 18, 38 and 39 of the Unlawful Activities (Prevention) Act 1967 as amended 2013; and is a terrorism related offence, which involves actions by certain unknown persons who have motivated and radicalized certain Indian youths including (name of accused) and (name of co-accused), to join the terrorist organization ISIS (Islamic State of Iraq and Syria) proscribed by Government of India and to instigate him to travel abroad to become participant

of ISIS and contribute to the commission of terrorist acts and waging war against allied nations of India.

And whereas it is likely that the object of the conspiracy will be furthered and the likelihood of terrorist attacks will increase, if the accused are not detected in time, and the same needs to be prevented;

And whereas, from the information available from the investigation of the case, it appears that the following Google account(s) is/are owned and operated by accused and some of the conspirators.

Sr. No.	Email /Account ID
	Accused Name: ________
1	mirXXXX@gmail.com
2	y2xxxxxx@gmail.com
Sr. No.	Email /Account ID
	Accused Name: ___________
1	qu89xxxxx@gmail.com
2	khxxxxxx@gmail.com

Therefore, you are requested to preserve all such data in respect each E-mail Ids and Emergency Disclosure request, will be made in accordance with procedure to secure the content information of these emails and this may be taken as request for

preserving the contents.

(……………)
Dy. Superintendent of Police,
P.S., Ahmedabad, Gujarat,
India

પરિશિષ્ટ-૬

PERFORMA TO PRODUCE DOCUMENT OR OTHER THING (CDR/IPDR etc.) REQUEST u/s 91 and/or 92 of C.R.P.C. 1973

No.: P.S./ Techcell/ /2018
P.S., Ahmedabad
Phone No.: (O) 02717-241036
FAX NO:02717-241150
E-mail: xxxxxxxx@gujarat.gov.in

To,
The Nodal Officer,
Concerned TSPs,
Gujarat State.

Sub: Please provide the Call Detail Records (CDR) SDR, CAF of the following numbers (Search in Pan India Circle) :-

Sir,

Sr. No	Phone /Mobile /IPDR/ IMEI/ ILD No	TSP	Period		FIR / Case No
			From	To	
1					
2					
3					
4					

(1) The subscriber identity has been ascertained and it is ensured that the person in question is not someone whose call details are of a sensitive nature.

(2) The number is not subscribed in the name of a sitting MP/MLA

(xxxxxxxx)
Nodal Officer
Dy. Superintendent of Police
P.S., Gujarat state.

(xxxxxxxxx)
Investigating Officer
Police Inspector
P.S., Gujarat state.
Contact Details. –
[MO No.]

GUJARAT POLICE

સેવા સુરક્ષા શાંતિ

ગુજરાત પોલીસ