डीजी परिपत्र संख्याः- 17 /2016

जावीद अहमद
आई.पी.एस.

पुलिस महानिदेशक
उत्तरप्रदेश
1-तिलक मार्ग, लखनऊ।
दिनांकः लखनऊः मार्च 16 ,2016

प्रिय महोदय,

आप सभी अवगत है कि विगत वर्षो में प्रत्येक क्षेत्र में जिस तीव्रता के साथ कम्प्यूटर के प्रयोग में वृद्धि हो रही है उसी अनुपात मे कम्प्यूटर सम्बन्धी अपराधो मे भी निरन्तर वृद्धि हो रही है। इन अपराधो में कम्प्यूटर द्वारा होने वाले अपराध एवं कम्प्यूटर को लक्ष्य बनाकर किये जाने वाले अपराध आदि शामिल हैं।

साइबर अपराधो की विवेचना जटिल होती है, इन अपराधो से सम्बन्धित साक्ष्य अमूर्त होते हैं। साक्ष्यो का सकंलन एंव मूल्यांकन करने मे विवेचक को परम्परागत विवेचनाओ से अलग चुनौती पूर्ण कार्य करना पडता है। कम्प्यूटर नेटवर्क के बढते चलन से इसकी जटिलता में और भी वृद्धि हुयी है। तकनीकी रूप से यह सम्भव है कि भारत में बैठा कोई व्यक्ति किसी भी देश के कम्प्यूटर का प्रयोग कर किसी अन्य देश में स्थित डाटा चोरी कर सकता है। इस तरह एक ही साइबर अपराध का अलग-अलग देशों से सम्बन्ध होने के कारण इन अपराधो का न केवल तकनीकी रूप से अनावरण करना कठिन होता है, बल्कि इसमे वैधानिक कठिनाईयॉ भी आती है।

उपरोक्त के परिप्रेक्ष्य में यदि किसी विवेचना में संदिग्ध कम्प्यूटर नेटवर्क अथवा कम्प्यूटर से सम्बन्धित इलेक्ट्रानिक सामग्री को सीज किया जाना हो तो Search and Seizure हेतु आवश्यक निम्नाकित हार्डवेयर, कम्प्यूटर फोरेंसिक साफ्टवेयर एवं अन्य सामग्री को साथ में ले जाना चाहिये-

1. स्टोरेज डिवाइस **(Storage device)**:-यू0एस0बी (USB)हार्ड डिस्क (Hard Disk) , पेन ड्राइव (Pen Drive) इत्यादि):- इनका प्रयोग कम्प्यूटर से फाइलों की इमेंज तैयार करने हेतु किया जा सकता है।

2. लेबलिग मटेरियल(Labeling Material):- लेबल का प्रयोग केबल्स पर एवं कम्प्यूटर के सॉकिट पर लिखने के लिए किया जाता है ताकि यह जानकारी हो सके कि घटनास्थल पर कम्प्यूटर से सम्बन्धित पोर्ट किन-किन सॉकिट में लगे थे।

3. स्क्रूडाइवर(Screwdrivers) और अन्य आवश्यक औजारः- जिसकी मदद से कम्प्यूटर के पुर्जो को अलग करने में सहायता मिल सके।

4. दस्ताने (Gloves):- सर्च या सीज करते समय दस्ताने पहनकर ही कार्य किया जाना चाहिए।

5. पैकिंग सामाग्री (Packing Materials):- रबर बैण्ड (Rubber Bands), टेप (Tape), बक्से (Boxes), बबल रैप (Bubble wrap), एण्टी स्टैटिक बबल रैप (Anti-static Plastic Bubble wrap), फैराडे बैग (Faraday Bag) आदि। यदि एण्टी स्टैटिक बबल रैप उपलब्ध न हो तो कागज का लिफाफा प्रयोग किया जा सकता है।

6. कैमरा(Camera):- वीडियो रिकार्डिग तथा घटना स्थल की फोटो खीचने हेतू।

7. माल हिरासत मे लेने हेतु चेन, रिपोर्टशीट तथा अन्य प्रपत्र जो सीजर हेतु आवश्यक हो।

8. वॉलेटाइल डाटा(Volatile Data) कलेक्शन किट:- यदि कम्प्यूटर ऑन अवस्था में प्राप्त हो तो सम्बन्धित साफ्टवेयर एवं तकनीकी मदद से वॉलेटाइल डाटा एकत्र किया जाना चाहिये। उक्त के अतिरिक्त पोर्टेबल कम्प्यूटर फारेंसिक किट यदि उपलब्ध हो तो अवश्य साथ में ले जानी चाहिये।

9. अन्य सामग्री(Other Materials):- स्केल, मेजरिंग टेप, नोट पैड, स्कैच पैड, पेन, पेन्सिल, परमानेन्ट मार्कर।

10. चेन आफ कस्टडी रिपोर्ट शीट(Chain Of custody Report Sheets) एवं अन्य आवश्यक प्रपत्र।

11. Electronic Evidence Container.

कम्प्यूटर या कम्प्यूटर नेटवर्क द्वारा कारित किये गये अपराध के सम्बन्ध में घटनास्थल पर पहुंचने के उपरान्त विवेचक को निम्न महत्वपूर्ण तथ्यों को ध्यान में रखा जाना चाहिये:-

1. यह अत्यन्त आवश्यक है कि घटना स्थल पर संदेही अथवा अभियुक्त को इस बात की अनुमति न दी जाए कि वह अपराध मे प्रयुक्त कम्प्यूटर के किसी भाग को किसी भी प्रकार से प्रयोग करे, क्योंकि अभियुक्त द्वारा एक KEY दबाने या माउस के एक Click मात्र से ही पूरा का पूरा डाटा नष्ट हो सकता है या Data Tamper हो सकता है, साथ ही कम्प्यूटर के डाटा को नेटवर्क के जरिये वायरलेस के माध्यम से नष्ट किया जाना अत्यन्त

आसान है, अतः संदिग्ध को कम्प्यूटर से तुरन्त दूर कर देना चाहिये तथा अन्य किसी अनधिकृत व्यक्ति द्वारा भी कम्प्यूटर को Operate नही किया जाना चाहिये।

2. यदि कोई कम्प्यूटर System किसी Physical Network (LAN, Fiber Optic, Cables, Telephones, Wi-Fi अथवा Wi-Max Wireless-Network यहॉ तक कि मोबाइल फोन जिसमें Wireless Communication Port हो) से जुडा हो तो ऐसी परिस्थितियों मे विवेचक को अत्यन्त सतर्क रहते हुए एक कम्प्यूटर विशेषज्ञ से मार्गदर्शन प्राप्त किया जाना चाहिए यदि विशेषज्ञ मौके पर उपलब्ध नही हो तो उससे दूरभाष के जरिये सम्पर्क कर मार्गदर्शन प्राप्त किया जा सकता है।

3. जब कम्प्यूटर On/Sleep Mode में हो तो ऐसी स्थिति में विशेषज्ञ की यथा सम्भव मदद ली जाए। विशेषज्ञ मौके पर मौजूद न हो तब दूरभाष के माध्यम से सम्पर्क स्थापित करते हुये दिशा-निर्देश प्राप्त किये जाए। कम्प्यूटर आन होने की स्थिति में Volatile Data Collection हेतु Computer Forensic Expert की मदद अवश्य प्राप्त करे।

4. ध्यान रहे कि यदि घटना स्थल पर कम्प्यूटर Off हो तो उसे On नही करना चाहिए क्योंकि हैकर अपने सिस्टम में ऐसा प्राविधान कर सकता है कि On करते ही सम्बन्धित समस्त डाटा नष्ट हो जाए और ऐसा करने से कम्प्यूटर का Log भी बदल जायेगा तथा साक्ष्य की सत्यनिष्ठा प्रभावित होगी। इसलिये यदि कम्प्यूटर Off अवस्था में है तो उसे On नही किया जाना चाहिए। ऐसी अवस्था में इलेक्ट्रानिक साक्ष्य को उसी Off अवस्था में ही सीज किया जाना चाहिए।

5. सीज करने से पहले डेक्सटॉप कम्प्यूटर के C.P.U. से Power Cable को हटाना चाहिये एवं सभी केबल को सम्बन्धित सॉकेट के साथ Labelling/Marking करते हुये फोटोग्राफी अवश्य करानी चाहिये।

6. **<u>लैपटॉप प्राप्त होने की दशा में</u>**:- यदि लैपटाप आन है तो Shutdown न करते हुये उसकी बैटरी निकालकर उसे Switch Off करना चाहिये और यदि Off अवस्था में है तो उसे उपरोक्त के भांति बिना On किये हुये सीज कर लेना चाहिये।

7. किसी भी प्रकार के स्टोरेज डिवाइस को सीज करने के लिये यथासम्भव Anti-static Packaging Bubble wrap का प्रयोग करना चाहिए।

8. <u>मोबाईल को सीज किये जाने से पूर्वः-</u> यदि मोबाईल की बैटरी को निकाला जाना सम्भव है तो मोबाईल की बैटरी को निकाल देना चाहिए। अन्यथा बैटरी न निकल पाने की स्थिति में मोबाईल को सीज करने के लिये फैराडे बैग का प्रयोग करना चाहिए। फैराडे बैग (Faraday Bag) न होने की दशा में एल्यूमिनियम फॉइल (Aluminium foil)से मोबाईल को चार से पॉच बार चारो ओर से कवर कर लेना चाहिए, जिससे मोबाईल की Connectvity समाप्त हो जाए, या फिर मोबाईल फोन को फ्लाइट मोड में भी किया जा सकता है।

9. यदि अपराध कारित करने के लिये किसी बेवसाइट का प्रयोग किया गया है तो बेवसाइट के hosting server provider के बारे में विस्तृत जानकारी करें। बेवसाइट के Administrator को आवश्यक Log सुरक्षित रखने एवं उपलब्ध कराने हेतु धारा 91 द0प्र0स0 कें अन्तर्गत लिखित आदेश(Written Order) जारी करे। यदि वेब सर्वर अन्य देश में स्थित हो तो MLAT(Mutual Legal Assistance Treaty) के प्रावधानों का प्रयोग कर धारा 166 ए द0प्र0सं0 के तहत सूचना मॉगने हेतु मा0 न्यायालय द्वारा साक्ष्य के लिए पत्र (Letter Rogatory) जारी कराकर अग्रिम कार्यवाही करें।

10. किसी भी घटना स्थल पर सर्च करने से पहले विवेचक द्वारा यह भी निर्णय लिया जाना चाहिए कि सम्बन्धित हार्डवेयर/डाटा को कहॉ रखना है जिससे सीज किये जाने के उपरान्त सुरक्षित तरीके से कम्प्यूटर फारेंसिक लैब में परीक्षण हेतु भेजा जा सके। डाटा को मौके पर ही सीज किया जाना श्रेष्यकर रहता है क्योंकि इससे अनावश्यक हार्डवेयर को साथ मे नही ले जाना पडता है। अतः इस सम्बन्ध में डाटा को डाउनलोड तथा Analysis हेतु यथासम्भव Computer Forensic Expert की मदद ली जाए, जिसके द्वारा सम्बन्धित को मौके पर ही डाटा को मा0 न्यायालय मे प्रस्तुत करने हेतु संरक्षित किया जाए। यदि मौके पर Computer Forensic Expert न उपलब्ध हो तो विवेचक को सभी सम्बन्धित सामग्री को सीज कर लेना चाहिए।

11. घटना स्थल को सर्च करते समय प्रत्येक Digital Device जैसे- P.D.A., मोबाईल, MP3 Player, Camera, Flash Cards, Print Outs, Software /Data Disks, अन्य Missing Parts, स्टोरेज डिवाइसेस को भी आवश्यक साक्ष्य की दृष्टि से कब्जे में लिया जाना चाहिये। इसके अतिरिक्त की-बोर्ड/माउस से फिंगर प्रिन्ट भी ले लेना चाहिए।

12. यदि कोई प्रिन्टर घटनास्थल पर मौजूद हो तो उसको भी चेक कर लेना चाहिये, यह सम्भव है कि उसमें कोई प्रिन्ट कमान्ड दी गयी हो और पेपर न होने के कारण प्रिन्ट न निकल पाया हो तथा प्रिन्टर की इन्डीकेटर लाइट जल रही हो, ऐसी परिस्थिति में प्रिन्टर में पेपर लगाकर प्रिन्ट आउट ले लेना चाहिये (ध्यान रहे कि ऐसा करने के समय आपको कम्प्यूटर या लैपटाप इत्यादि को आपरेट नही करना है)।

13. सीज करते समय सभी उपकरणों के Item का नाम, Make, Model, Serial Number, सीज करने का समय इत्यादि अवश्य लिपिबद्ध करना चाहिए।

14. यदि Network अथवा Mainframe भी अपराध से सम्बन्धित है तो कम्प्यूटर को disconnect न करें, व ऐसे मामले में निश्चित रूप से कम्प्यूटर फोरेंसिक विशेषज्ञ की मदद से ही अग्रेतर कार्यवाही की जानी चाहिए।

15. घटनास्थल पर मुआयना करते समय उपकरण किस प्रकार एक-दूसरे से जुडे हैं, को भी लिपिबद्ध कराये। घटना स्थल से कम्प्यूटर सम्बन्धित सभी मैनुअल, उससे जुडे हुए सभी डिवाइस मुख्यतः साफ्टवेयर,ऑपरेटिंग सिस्टम एवं अन्य सम्बन्धित सामाग्रियों को भी सीज कर लिया जाना चाहिए।

16. घटनास्थल से अपराध से सम्बन्धित कम्प्यूटर के सभी पार्ट को अलग-थलग करने की समस्त कार्यवाही कर लेनी चाहिए तत्पश्चात उसे फॉरेसिंक लैब भेजे जाने हेतु अत्यन्त सावधानीपूर्वक एण्टी स्टैटिक प्लास्टिक बबल (Anti-static Plastic Bubble) का प्रयोगकर पैकिंग कर लेनी चाहिए ताकि परिवहन करते समय कम्प्यूटर के किसी Part को कोई नुकसान न पहुँचे।

17. कम्प्यूटर से सम्बन्धित समस्त Parts को उसी कम्प्यूटर के साथ रखना चाहिए ताकि उसे पुनः संरचना (Reconstruct) करने मे आसानी रहे।

18. घटना स्थल से सीज किये गये कम्प्यूटर उपकरणो को ऐसे बक्सों/वाहनो मे नहीं ले जाना चाहिए जिनमें झटके लगने की सम्भावना हो। इस प्रकार सीज किये गये कम्प्यूटर को सुरक्षित,ठण्डे,शुष्क स्थान पर रखना चाहिए तथा जेनरेटर से दूर रखना चाहिए क्योंकि जेनरेटर से निकलने वाले इलैक्ट्रोमैग्नेटिक सिग्नल्स कम्प्यूटर के डाटा को नष्ट कर सकता है।

19. विवेचक को इस बात का भी ध्यान रहे कि घटना स्थल पर जब्तीकरण की कार्यवाही के दौरान दो स्वतन्त्र गवाह होना आवश्यक है क्योकि ऐसा करने से न्यायालय में साक्ष्य देते समय किसी दुविधा की स्थिति उत्पन्न नही होगी।

20. इलेक्ट्रानिक साक्ष्यों को संकलित करते समय विवेचक को सम्बन्धित Administrator से भारतीय साक्ष्य अधिनियम, 1872 की धारा 65ए एवं 65बी के प्राविधानों के तहत आवश्यक प्रोफार्मा सर्टिफिकेट प्राप्त कर न्यायालय मे प्रस्तुत करना चाहिए, क्योकि बिना उपरोक्त प्रोफार्मा सर्टिफिकेट के आपके द्वारा संकलित किये गये साक्ष्य मा0 न्यायालय में ग्राह्य नही होगें।

21. सूचना प्रौद्योगिकी अधिनियम (I.T Act) के अध्याय 11 की सुसंगत धाराओ में अपराधों को वर्णित किया गया है एवं अध्याय 13 की धारा 80 में प्रवेश करने,तलाशी लेने आदि की पुलिस अधिकारी एवं अन्य अधिकारियों की शक्ति का उपबन्ध करती है, द0प्र0स0 1973 (1974 का 2) में किसी बात के होते हुए भी कोई पुलिस अधिकारी जो निरीक्षक की पंक्ति से नीचे का न हो किसी सार्वजनिक स्थान में प्रवेश कर सकेगा और तलाशी ले सकेगा तथा वहॉ पाये गये किसी ऐसे व्यक्ति को बिना वारण्ट गिरफ्तार कर सकेगा जो युक्ति-युक्त रूप से संदिग्ध व्यक्ति है या जिसने इस अधिनियम के अधीन कोई अपराध किया है या कर रहा है या करने वाला है।

मै अपेक्षा करता हूँ कि आप उक्त निर्देशों का भली-भॉति अध्ययन कर कार्यशाला आयोजित कर अपने अधीनस्थो को अवगत करायें तथा यह सुनिश्चित करें कि साइबर अपराध घटित होने के उपरान्त सम्बन्धित विवेचक साइबर फोरेन्सिक पद्धतियों का प्रयोग करते हुए घटना का सफल अनावरण कराते हुए दोषियों को दण्ड दिलाने मे सार्थक प्रयास करें।

भवदीय,

16.3.16

(जावीद अहमद)

समस्त जोनल पुलिस महानिरीक्षक,
उत्तर प्रदेश।
समस्त परिक्षेत्रीय पुलिस उपमहानिरीक्षक,
उत्तर प्रदेश।
समस्त वरिष्ठ पुलिस अधीक्षक/पुलिस अधीक्षक(नाम से)
जनपद/रेलवेज, उत्तर प्रदेश।

प्रतिलिपि - निम्न को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषितः-

1. पुलिस महानिदेशक, रेलवेज, उ0प्र0।
2. अपर पुलिस महानिदेशक, तकनीकी सेवाएं उ0प्र0।
3. पुलिस महानिरीक्षक, ए0टी0एस0, उ0प्र0।
4. समस्त राजपत्रित अधिकारी मुख्यालय पुलिस महानिदेशक,उ0प्र0।