पुलिस आदेश 328 /2024

विषयः- **इलेक्ट्रानिक साक्ष्य की पहचान, संरक्षा और संग्रहण तथा भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4) के अंतर्गत] के अंतर्गत प्रमाण-पत्र के लिए अनुसंधानकर्त्ताओं हेतु मानक संचालन प्रक्रिया ।**

1. सूचना प्रौद्योगिकी के प्रसार के कारण अपराध करने के लिए इलेक्ट्रानिक /डिजिटल माध्यम का उपयोग बढ़ गया है । अन्वेषण के दौरान इलेक्ट्रानिक साक्ष्य को पेशेवर तरीके से संभालना, केस के उद्भेदन और अपराधियों के विरूद्ध सफल विचारण के लिए महत्वपूर्ण है। अतः अनुसंधानकर्त्ता के लिये इलेक्ट्रानिक साक्ष्य की प्रकृति और उन्हें संभालते समय अपनाई जाने वाली प्रक्रियाओं को समझना आवश्यक है । यह पुलिस आदेश अनुसंधानकर्त्ताओं द्वारा इलेक्ट्रानिक साक्ष्य की पहचान और संग्रह करने के साथ भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के अधीन प्रमाण पत्र प्राप्त करने हेतु अपनाई जाने वाली प्रक्रियाओं को निर्धारित करता है। 01-07-2024 से पंजीकृत मामलों के लिए भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) के तहत प्रमाण पत्र के स्थान पर भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4) के तहत प्रमाण पत्र का प्रावधान लागू होगा ।

2. इलेक्ट्रानिक साक्ष्य समय-संवेदी (time sensitive) प्रकृति के होते हैं, इन्हें आसानी से सीमाओं के पार भेजा जा सकता है, ये अस्थिर (volatile) एवं भंगुर (fragile) होते हैं और इन्हें आसानी से बदला, क्षतिग्रस्त या विनष्ट किया जा सकता है । इलेक्ट्रानिक साक्ष्य जिस अपराध स्थल/परिसर में स्थित है, वहां सबसे पहले पहुंचने वाला पुलिस अधिकारी उक्त परिसर को संरक्षित रखने के लिए जिम्मेदार होगा । अनुसंधानकर्त्ता द्वारा अधिकृत अधिकारी या भारतीय नागरिक सुरक्षा संहिता, 2023 की धारा 176(3) के तहत राज्य सरकार द्वारा अधिसूचित फोरेंसिक विशेषज्ञ इलेक्ट्रानिक साक्ष्य की पहचान करने और उसे जप्त करने के संबंध में कार्रवाई के लिए जिम्मेदार होगा । इस दौरान उसे यह ध्यान रखना चाहिए कि

उसकी कार्रवाई से साक्ष्य में कोई बदलाव/परिवर्तन नहीं होना चाहिए। जहां आवश्यक हो, इलेक्ट्रानिक साक्ष्य को संभालने के लिए एक प्रशिक्षित पुलिस अधिकारी/फोरेंसिक विशेषज्ञ को लगाया जाना चाहिए और अभिरक्षा की श्रृंखला (chain of custody) को बनाए रखने के लिए इलेक्ट्रानिक साक्ष्य की जप्ती, हस्तांतरण, भंडारण या जांच को ठीक से अभिलेखित किया जाना चाहिए । इलेक्ट्रानिक साक्ष्य को सुरक्षित रखने, संग्रह करने या संरक्षित करने के दौरान की गई किसी भी त्रुटि के परिणामस्वरूप इलेक्ट्रानिक साक्ष्य को नुकसान हो सकता है, जिससे न्यायालय के समक्ष साक्ष्य की प्रमाणिकता प्रभावित हो सकती है ।

3. भारतीय साक्ष्य अधिनियम, 1872 के अनुसार, **द्वितीयक** इलेक्ट्रानिक दस्तावेज के माध्यम से किसी तथ्य को साबित/खण्डित करने के लिए, यह आवश्यक है कि अनुसंधानकर्त्ता भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) के अनुसार प्रमाण पत्र प्रस्तुत करें। किसी तथ्य को प्राथमिक इलेक्ट्रानिक साक्ष्य के माध्यम से साबित/खण्डित करने हेतु भारतीय साक्ष्य अधिनियम के तहत प्रमाण पत्र प्रस्तुत करने की कोई आवश्यकता नहीं है । उदाहरण के लिए, जहां एक आपराधिक मामले में मोबाइल फोन जप्त किया जाता है और अगर जप्त किया गया मोबाइल फोन ही किसी तथ्य को साबित/खण्डित करने के लिए न्यायालय के समक्ष पेश किया जाता है, तो भारतीय साक्ष्य अधिनियम की धारा 65बी(4) के तहत प्रमाण पत्र प्रस्तुत करने की कोई आवश्यकता नहीं है । परन्तु यदि अनुसंधानकर्त्ता मोबाइल फोन से कोई फाइल आदि डाउनलोड करके किसी तथ्य को साबित/खण्डित करना हो तो भारतीय साक्ष्य अधिनियम के तहत प्रमाण पत्र अनिवार्य है। इसलिए, अनुसंधानकर्त्ता को भारतीय साक्ष्य अधिनियम के तहत प्रमाण पत्र की विषय-वस्तु तथा उन परिस्थितियों से अच्छी तरह परिचित होना आवश्यक है, जिनमें ऐसा प्रमाण पत्र न्यायालय के समक्ष प्रस्तुत किया जाना आवश्यक है।

4. अनुसंधानकर्त्ता को यह सुनिश्चित करना चाहिए कि जप्त की जाने वाली इलेक्ट्रानिक सामग्री अनुसंधान अन्तर्गत अपराध से सीधे संबंधित है और केवल उतना ही साक्ष्य जप्त किया जाना चाहिए जो अपराध/आरोपी की भूमिका को स्थापित करने के लिए पर्याप्त हो।

अनावश्यक/अंधाधुंध जप्ती से बचना चाहिए। संग्रह और जप्ती प्रक्रिया का उचित दस्तावेजी हर चरण में महत्वपूर्ण है । न्यायिक विचारण के दौरान साक्ष्य संग्रह के लिए अपनाई गई प्रक्रिया, तकनीक और वैज्ञानिक पद्धति सत्यापित हो जानी चाहिए । यह पुलिस आदेश इलेक्ट्रानिक साक्ष्य की पहचान, सुरक्षा और संग्रह करते समय अपनाए जाने वाले चरणों को निर्धारित करता है ताकि डिजिटल साक्ष्य की विश्वसनीयता और सटीकता बनी रहे और इसे न्यायिक विचारण के दौरान स्वीकार्य साक्ष्य के रूप में प्रस्तुत किया जा सके।

5. **सावधानियांः-** इलेक्ट्रानिक साक्ष्य की प्रमाणिकता अक्षुण्ण बनाये रखने हेतु अनुसंधानकर्त्ता द्वारा निम्नलिखित सावधानियां बरती जानी आावश्यक हैः-

i. वैसे परिसर जहां इलेक्ट्रानिक साक्ष्य अवस्थित है, को सुरक्षित करें ।

ii. परिसर में या उसके आसपास यदि कोई वायरलेस/वाई-फाई कनेक्शन हो तो उसकी पहचान करें।

iii. परिसर के सभी कमरों की जाँच करें और उपलब्ध इलेक्ट्रानिक उपकरणों की पहचान करें।?

iv. यदि आवश्यक हो, थानाध्यक्ष द्वारा अधिकृत प्रशिक्षित पुलिस कर्मियों की सहायता ली जाये और उपयोगकर्ताओं, इंटरनेट सुविधा, आईपी एड्रेस, भंडारण सुविधाओं, सर्वर, ई-मेल, वेबमेल, ब्लॉग, सोशल मीडिया खातों, इंटरनेट मैसेजिंग आदि के user name और पासवर्ड की पहचान करें।

v. केस के तथ्यों के आधार पर संभावित इलेक्ट्रानिक साक्ष्य की पहचान करें।

vi. इलेक्ट्रानिक साक्ष्यों की स्थिति का रेखाचित्र (sketch) बनाएं और उसका फोटोग्राफ लें।

vii. सम्पूर्ण साक्ष्य को जप्त करने साक्ष्य की फोरेंसिक प्रतिलिपि पर्याप्त ।

viii. इलेक्ट्रोनिक उपकरण की वर्तमान स्थिति में परिवर्तन न करें।

ix. यदि कोई इलेक्ट्रोनिक उपकरण बंद हो तो उसे चालू न करें।

x. यदि इलेक्ट्रोनिक उपकरण चालू है, तो उसे बंद करने या कुछ भी करने से पहले किसी प्रशिक्षित व्यक्ति को बुला लें।

xi. यदि इलेक्ट्रोनिक उपकरण चार्ज नहीं है, तो उसे चार्ज न करें।

xii. सुनिश्चित करें कि इलेक्ट्रोनिक उपकरण को खुले क्षेत्र या असुरक्षित स्थान पर न छोड़ा जाए।

xiii. इलेक्ट्रोनिक उपकरण जहाँ स्थित है, जिन व्यक्तियों की उस तक पहुंच है और उसे जब स्थानांतरित किया गया हैं, इसका दस्तावेजीकरण करें।

xiv. इलेक्ट्रोनिक उपकरण में कोई भी अन्य उपकरण जैसे मेमोरी कार्ड, यूएसबी थंब ड्राइव, या कोई अन्य स्टोरेज मीडिया न जोड़े क्योंकि इससे डेटा आसानी से नष्ट हो सकता है।

xv. इलेक्ट्रोनिक उपकरण पर कोई भी एप्लीकेशन, फाइल या चित्र न खोलें। इससे डेटा की आकस्मिक हानि या ओवरराइटिंग हो सकती है।

xvi. इलेक्ट्रोनिक उपकरण से या उसपर कुछ भी कॉपी न करें।

xvii. साक्ष्य की स्थिति को प्रमाणित करने के लिए उसकी तस्वीरें (सामने से, पीछे से, आदि) लें।

xviii. इलेक्ट्रोनिक उपकरण का पिन/पासवर्ड पैटर्न ज्ञात करना सुनिश्चित करें ।

xix. ऊपर बताए गई सावधानियां केवल उदाहरण के लिए हैं। इलेक्ट्रोनिक साक्ष्य के स्थान और प्रकृति के आधार पर अनुसंधानकर्त्ता को अतिरिक्त सावधानियां बरतनी पड़ सकती हैं। चूंकि इलेक्ट्रोनिक साक्ष्य की जप्ती बहुत सावधानी से की जानी चाहिए, इसलिए यह आवश्यक है कि अनुसंधानकर्त्ता अपराध के घटनास्थल की जांच करने के लिए जाते समय आईटी जांच किट साथ रखें ।

6. आईटी जांच किटः इलेक्ट्रोनिक साक्ष्य एकत्र करने के लिए जाते समय, अनुसंधानकर्त्ता को अपने साथ निम्नलिखित वस्तुएं आईटी जांच किट में रखनी चाहिएः-

i. तलाशी और जप्ती की रिकॉर्डिंग के लिए फोटो/वीडियो कैमरा या मोबाइल फोन

ii. साक्ष्य टेप

iii. अभिरक्षा की श्रृंखला प्रपत्र

iv. टूलकिट (स्क्रूड्राइवर सेट, आदि)

v. चिपकने वाला टेप
vi. स्टिकी नोट
vii. नई/खाली पेन ड्राइव और हार्ड ड्राइव
viii. दस्ताने और स्टैटिक कलाई बैंड
ix. राईट ब्लॉकर
x. इमेजिंग के लिए हार्डवेयर (TD2U, फाल्कन, ट्रू इमेजर)
xi. पेन ड्राइव, हार्ड डिस्क, आदि.
xii. FTK युक्त लैपटॉप (क्रासओवर परीक्षणित)
xiii. कार्ड रीडर
xiv. आवर्धक (magnifying) लेंस, फ्लैशलाइट, आदि.
xv. फैराडे बैगएल्युमिनियम फॉयल, बबल रैप्स, आदि।
xvi. गैर-चुंबकीय उपकरण
xvii. स्थायी मार्कर
xviii. एंटीस्टेटिक बैग
xix. गत्ते के बक्से
xx. पावर बैंक
xxi. अन्य सामग्री आवश्यकतानुसार।

7. इलेक्ट्रानिक साक्ष्य की पहचानः- अनुसंधानकर्त्ता को इलेक्ट्रोनिक साक्ष्य की जानकारी उसके संभावित स्रोतों की तलाशी में सहायक होती है। इलेक्ट्रोनिक साक्ष्य की पहचान करते समय, अनुसंधानकर्त्ता को अपराध की प्रकृति, अपराध का स्थान, डेटाबेस सर्वर का स्थान, संरक्षक, साइट प्रशासक, उपयोगकर्ता, कंप्यूटर में संग्रहीत जानकारी का प्रकार, सूचना किसने और किस रूप में प्रेषित की, अपराध करने में शामिल उपकरणों की संख्या और प्रकार, उपलब्ध सूचना भंडारण सुविधाएँ, कंप्यूटर की दूरस्थ लॉगिन क्षमताएँ, उपलब्ध नेटवर्क कनेक्शन आदि को ध्यान में रखना चाहिए । इस दौरान, अनुसंधानकर्त्ता को इलेक्ट्रानिक साक्ष्य के हर संभावित स्रोत की पहचान करनी चाहिए। इलेक्ट्रानिक साक्ष्य के सामान्यतः निम्नलिखित स्रोत हैंः

i. सेंट्रल प्रोसेसिंग यूनिट
ii. डिस्प्ले मॉनिटर
iii. मोबाइल फोन की स्क्रीन

iv. स्मार्ट कार्ड

v. डोंगल, बायोमेट्रिक स्कैनर आदि।

vi. डिजिटल कैमरें

vii. सीसीटीवी कैमरे/ डीवीआर

viii. व्यक्तिगत डिजिटल सहायक ख्पीडीए,

ix. स्मार्टफोन

x. हार्ड ड्राइव

xi. लोकल एरिया नेटवर्क (स छ) कार्डध्नेटवर्क इंटरफेस कार्ड (छप्ब्)

xii. मॉडेम और राउटर

xiii. हब और स्विच

xiv. सर्वर

xv. नेटवर्क केबल और कनेक्टर

xvi. पेजर, प्रिंटर, आदि

xvii. हटाने योग्य भंडारण मीडिया जैसे हार्ड डिस्क, पेन ड्राइव आदि

xviii. स्कैनर

xix. कॉपियर

xx. सीडी और डीवीडी ड्राइव

xxi. क्रेडिट कार्ड स्किमर्स

xxii. डिजिटल घड़ियाँ

xxiii. फैक्स मशीन

xxiv. ग्लोबल पोजिशनिंग सिस्टम (जीपीएस)

xxv. कीबोर्ड और माउस

xxvi. कॉल रिकॉर्ड

xxvii. ईमेल

xxviii. मोबाइल फोन के माध्यम से भेजे गए एसएमएस (संक्षिप्त संदेश)

xxix. टेप रिकॉर्ड

xxx. डिजिटल फोटो, आदि

xxxi. अपराध की प्रकृति और तथ्य को साबित/खण्डित करने के लिए आवश्यक तद्नुसार अनुसंधानकर्त्ता इलेक्ट्रानिक साक्ष्य के अतिरिक्त स्रोतों की तलाश कर सकता है।

8. अनुसंधानकर्त्ता को यह ध्यान रखना चाहिए कि पहचान के दौरान एकत्र की गई जानकारी को बाद में न्यायालय द्वारा मांगा जा सकता है। इसलिए यह आवश्यक है कि पहचान के दौरान एकत्र जानकारी को अनुसंधानकर्त्ता सही ढंग से प्रलेखित और संरक्षित करें । अनुसंधानकर्त्ता द्वारा (अपनाई गई प्रक्रिया को) को तिथि और समय के साथ प्रलेखित किया जाना चाहिए। इलेक्ट्रोनिक साक्ष्य की पहचान हो जाने के बाद अनुसंधानकर्त्ता इलेक्ट्रॉनिक साक्ष्य को सुरक्षित करने हेतु अग्रतर कार्यवाही कर सकता है । इलेक्ट्रानिक साक्ष्य को सुरक्षित करने के लिए अनुसंधानकर्त्ता को घटनास्थल का निरीक्षण करना आवश्यक है।

9. **इलेक्ट्रानिक साक्ष्य सुरक्षित करनाः-** ऊपर बताई गई प्रक्रियाओं/सावधानियों का पालन करते हुए अनुसंधानकर्त्ता इलेक्ट्रानिक साक्ष्य सुरक्षित करने के लिए अग्रतर कार्रवाई कर सकता है। इलेक्ट्रानिक साक्ष्य सुरक्षित करने का मतलब है कि फॉरेंसिक जांच या भंडारण के लिए भौतिक रूप से साक्ष्य की जप्ती, लेबलिंग और पैकेजिंग करते हुये सुरक्षित करना। अनुसंधानकर्त्ता को यह ध्यान में रखना चाहिए कि इलेक्ट्रानिक साक्ष्य के कई स्रोत हैं और वे स्टैंड-अलोन इलेक्ट्रोनिक उपकरण, नेटवर्क इलेक्ट्रोनिक उपकरण, स्टोरेज इलेक्ट्रोनिक उपकरण, मोबाइल फोन आदि के रूप में हो सकते हैं, और विभिन्न प्रकार के इलेक्ट्रानिक साक्ष्य को सुरक्षित करने के लिए अलग-अलग तरीकों की आवश्यकता हो सकती है।

10. विभिन्न प्रकार के इलेक्ट्रानिक साक्ष्य सुरक्षित करते समय अपनाई जाने वाली प्रक्रियाएं निम्नानुसार हैंः

A. मोबाइल फोन

घटनास्थल से मोबाइल फोन इलेक्ट्रोनिक उपकरण बरामद करते समय दस्ताने या अन्य साफ, रोगाणुरहित सूती कपड़े का प्रयोग करें।

अगर फोन चालू है

i. फोन में फ्लाइट मोड विकल्प का चयन करके इलेक्ट्रोनिक उपकरण को isolate करें।

ii. यदि फ्लाइट मोड विकल्प उपलब्ध नहीं है, तो इलेक्ट्रोनिक उपकरण को isolate करने के लिए फैराडे बैग का उपयोग करें।

iii. यदि फैराडे बैग भी उपलब्ध न हो तो मोबाइल को एल्युमीनियम फॉयल में लपेट लें।

iv. मोबाइल फोन को पावर बैंक से जोड़े ताकि इलेक्ट्रोनिक उपकरण बंद न हो।

v. यदि मोबाइल इलेक्ट्रोनिक उपकरण कंप्यूटर/लैपटॉप से सिंक हो और डेटा स्थानांतरण हो रहा हो, तो फोन को कंप्यूटर/लैपटॉप से दूर न खींचें, क्योंकि इससे डेटा स्थानांतरण रुक जाएगा।

vi. इलेक्ट्रोनिक उपकरण से भौतिक साक्ष्य जैसे फिंगर प्रिंट, डीएनए आदि तथा डिजिटल साक्ष्य जैसे कॉल लॉग, एसएमएस आदि प्राप्त करने के लिए फोन को फोरेंसिक लैब में भेजें।

vii. सभी चरणों का दस्तावेजीकरण करें।

यदि मोबाइल फोन बंद हो

i. यदि बैटरी निकाली जा सकती है, तो उसे निकाल दें और सिम की स्थिति का फोटो लें।

ii. बैटरी, सिम और हैंडसेट को अलग-अलग पैक करें।

iii. सिम और हैंडसेट का विवरण जैसे मेक, मॉडल, IMEI, ICCID आदि नोट कर लें।

iv. यदि इलेक्ट्रोनिक उपकरण किसी तरल पदार्थ में डूबा हुआ है, तो इलेक्ट्रोनिक उपकरण को बाहर निकालें, बैटरी, सिम कार्ड आदि को हटा दें। इलेक्ट्रोनिक उपकरण की वर्तमान स्थिति पर तरल पदार्थ के प्रभाव को साबित करने के लिए उस तरल पदार्थ की थोड़ी मात्रा भी इकट्ठा करें जिसमें इलेक्ट्रोनिक उपकरण डूबा हुआ था।

v. भौतिक साक्ष्य जैसे फिंगरप्रिंट, डीएनए आदि तथा डिजिटल साक्ष्य जैसे कॉल लॉग, एसएमएस आदि प्राप्त करने के लिए इलेक्ट्रोनिक उपकरण को फोरेंसिक प्रयोगशाला में भेजें।

vi. सभी चरणों का दस्तावेजीकरण करें।

B. होम/ पर्सनल कंप्यूटर/ लैपटॉपः-

i. कंप्यूटर या लैपटॉप नेटवर्क के किसी से जुड़े रहने की जानकारी एकत्र करे, यदि किसी राउटर या मॉडेम से जुड़ाव है, तो सिस्टम से जुड़े ईथरनेट केबल को अलग करके या वाई-फाई कनेक्शन को अक्षम करके सिस्टम को नेटवर्क से अलग करें।

ii. कंप्यूटर का सीधे उपयोग न करें अथवा कंप्यूटर में सीधा साक्ष्य खोजने का प्रयास न करें। उचित प्रक्रिया का पालन करें ।

iii. कंप्यूटर के आगे और पीछे के भाग के साथ सभी तार और उससे जुड़े उपकरणों की तस्वीर लें।

iv. किसी भी साक्ष्य को हटाने से पहले आसपास के क्षेत्र की तस्वीरें लें।

यदि कंप्यूटर ''बंद'' स्थिति में है

i. यदि कंप्यूटर "बंद" स्थिति में है, तो उसे किसी भी परिस्थिति में "चालू" न करें।

ii. लैपटाप आदि में बैटरी हटायी जा सकती हो तो पहले बैटरी निकाल लें।

iii. ढक्कन बंद लैपटॉप को न खोलें क्योंकि ढक्कन खोलने पर कुछ लैपटॉप स्वतः ही चालू हो जाते हैं।

iv. बैटरी पैक निकालने से कंप्यूटर का आकस्मिक स्टार्ट-अप रोका जा सकेगा ।

v. पावर कॉर्ड को अनप्लग करें ।

vi. जुड़े हुए उपकरणों की पहचान के लिए सभी तार का रेखाचित्र बनाएं और लेबल लगाएं ।

vii. सभी तार और उपकरणों को अलग करें ।

viii. आजकल, ऑल-इन-वन कंप्यूटर मॉनिटर के अंदर एम्बेडेड हार्ड ड्राइव के साथ आते हैं। ऐसे मामलों में जहां हार्ड ड्राइव को इलेक्ट्रोनिक उपकरण से हटाया नहीं जा सकता है, तो साक्ष्य के तौर पर पूरे इलेक्ट्रोनिक उपकरण को जप्त करें ।

ix. सीपीयू या लैपटाप के बाहरी आवरण को ध्यानपूर्वक खोलें और हार्ड डिस्क की पहचान करें।

x. डेटा ट्रांसफर और पावर के केबल को अलग करके हार्ड डिस्क को मदरबोर्ड से अलग करें।

xi. स्टोरेज इलेक्ट्रोनिक उपकरण (हार्ड डिस्क) को सावधानी से बाहर निकालें और मेक, मॉडल और सीरियल नंबर जैसे विशिष्ट

पहचान को अभिलेखित करें। यदि पूरा CPU भी जप्त भी किया जाय तब भी विशिष्ट पहचान अवश्य अभिलेखित कर लें ।

xii. सभी जप्त सामग्री पर हस्ताक्षर के साथ पूर्ण लेबल लगावें ।

xiii. घटनास्थल पर केस से संबंधित गैर-डिजिटल साक्ष्य की तलाश करें, जैसे डायरी, नोटबुक, चालान, बैंक लेनदेन या पासवर्ड वाले कागज के टुकड़े।

xiv. उपकरण में एन्क्रिप्शन या पासवर्ड रहने की स्थिति में उपयोगकर्ता की सहायता लें। संदिग्ध सिस्टम में मौजूद ऑपरेटिंग सिस्टम, एप्लिकेशन पैकेज और अन्य कंप्यूटर उपयोगकर्ताओं के पासवर्ड की जाँच करें।

xv. उपकरण के सिस्टम की घड़ी की अशुद्धि से बचने के लिए, साक्ष्य की प्रमाणिकता में परिवर्तन किए बिना सिस्टम पर वास्तविक दिनांक और समय को नोट कर लें ।

xvi. राउटर और मॉडेम सहित सभी घटकों (components) को पैक करें ।

xvii. यदि अतिरिक्त भंडारण मीडिया पाया जाए तो उसे भी जप्त कर लें ।

xviii. सभी भंडारण/ अन्य मीडिया को चुम्बकों, रेडियो ट्रांसमीटरों और अन्य संभावित नुकसानदायक तत्वों से दूर रखें।

xix. कंप्यूटर से संबंधित अनुदेश पुस्तिकाएं, दस्तावेज और नोट्स एकत्र करें।

xx. सभी चरणों का दस्तावेजीकरण करें।

यदि कंप्यूटर ''चालू'' स्थिति में हैः-

i. यदि कंप्यूटर ''चालू'' है और मॉनिटर पर कुछ प्रदर्शित हो रहा है, तो स्क्रीन की तस्वीर लें।

ii. अगर कंप्यूटर "चालू" है और स्क्रीन Blank है, तो माउस को हिलायें या स्पेस बार दबाएँ क्योंकि इससे स्क्रीन पर सक्रिय छवि प्रदर्शित होगी। मॉनीटर पर छवि दिखाई देने के बाद स्क्रीन की तस्वीर लें।

iii. बाह्य USB ड्राइव (लाइव डाटा अधिग्रहण/ RAM अधिग्रहण टूल के साथ प्रीलोडेड) को संदिग्ध सिस्टम से कनेक्ट करें।

iv. यूएसबी ड्राइव को कनेक्ट करने की तारीख और समय के साथ ड्राईव के मेक, मॉडल, सीरियल नंबर रिकॉर्ड करें और उसे दस्तावेज में दर्ज करें ।

v. RAM मेमोरी अधिग्रहण उपकरणों (जैसे, डम्पिट, कैन, आदि) का उपयोग करके RAM प्राप्त करें।

vi. RAM प्राप्त करने के बाद, लाइव हैशिंग टूल (हैश माई फाइल्स, हैशकैल्क, आदि) का उपयोग करके फोरेंसिक इमेज फाइल का हैश मान उत्पन्न करें।

vii. उपयोग किए गए हैशिंग एल्गोरिदम के साथ हैश मान का चित्र लें या नोटपैड में कॉपी और पेस्ट करें और बाहरी यूएसबी ड्राइव में सहेजें।

viii. उचित उपकरणों (जैसे EDD) का उपयोग करके सिस्टम ड्राइव एन्क्रिप्टेड रहने की जानकारी एकत्र करें । विंडोज ऑपरेटिंग सिस्टम के साथ यदि एन्क्रिप्शन का पता चलता है, तो प्रत्येक वॉल्यूम की बिट-लॉकर रिकवरी कुंजियों की एक प्रति लें और इसे बाहरी स्टोरेज इलेक्ट्रोनिक उपकरण में स्टोर करें।

ix. सिस्टम में उपलब्ध Non-volatile (HDD/SSD) डेटा को लाइव फोरेंसिक टूल का उपयोग करके प्राप्त किया जा सकता है।

x. सक्षम और प्रशिक्षित व्यक्ति के द्वारा सिस्टम का लाइव अधिग्रहण करना चाहिए।

xi. कंप्यूटर ''चालू'' स्थिति में जप्त किया जा रहा हो तो साइट पर बाहरी भंडारण इलेक्ट्रोनिक उपकरण से इमेजिंग प्रक्रिया (फोरेंसिक प्रतिलिपि) की जानी चाहिए और प्रक्रिया के आउटपुट को यूएसबी स्टोरेज जैसे एक स्टेराइल डिजिटल स्टोरेज माध्यम पर संग्रहीत किया जाना चाहिए।

xii. यदि इलेक्ट्रोनिक उपकरण पर डेटा स्थिर है, तो सामान्य शटडाउन करें। यदि एंटी-फोरेंसिक शटडाउन विधियों का संदेह है, तो पावर केबल को हटा दें।

xiii. बंद मशीन से साक्ष्य एकत्र करने की प्रक्रिया में ऊपर बताई गई शेष प्रक्रिया का पालन करें।

C. नेटवर्क सर्वर/ बिजनेस नेटवर्क

i. सहायता के लिए प्रशिक्षित व्यक्ति/विशेषज्ञ से परामर्श लें ।
ii. घटनास्थल को सुरक्षित रखें और नेटवर्क सिस्टम को संभालने के लिए प्रशिक्षित कर्मियों को छोड़कर किसी को भी वहां स्पर्श न करने दें ।
iii. सिस्टम का प्लग न हटायें क्योंकि प्लग खींचने से :-
   - सिस्टम को गंभीर रूप से नुकसान पहुंचा सकता है ।
   - विधिसम्मत गतिविधि अव्यवस्थित हो सकती है ।

D. भंडारण मीडिया

i. भंडारण मीडिया से संबंधित अनुदेश पुस्तिकाएं, दस्तावेज और नोट्स एकत्र करें।
ii. भंडारण मीडिया को चुम्बकों, रेडियो ट्रांसमीटरों और अन्य संभावित रूप से नुकसान पहुंचाने वाले उपकरणों से दूर रखें।
iii. भंडारण मीडिया की जप्ती में शामिल सभी चरणों का दस्तावेजीकरण करें।

E. पर्सनल डिजिटल असिस्टेंट (पीडीए), डिजिटल कैमरा, आदि

i. यदि इलेक्ट्रोनिक उपकरण "बंद" है, तो उसे "चालू" न करें,
ii. अगर पीडीए चालू है, तो उसे चालू ही रहने दें । बंद करने के बाद चालू करने पर पासवर्ड आवश्यक हो सकता है, जिससे उसमें उपलब्ध साक्ष्य तक पहुँच नहीं हो पाएगी ।
iii. इलेक्ट्रोनिक उपकरण और डिस्प्ले स्क्रीन, यदि हो, तो उसकी फोटो लें ।
iv. बिजली के तारों सहित सभी केबल पर लेबल लगाएं और उन्हें एकत्रित करें तथा उपकरण के साथ जप्त करें ।
v. इलेक्ट्रोनिक उपकरण को चार्ज रखें ।
vi. यदि इलेक्ट्रोनिक उपकरण को चार्ज नहीं रखा जा सकता है, तो बैटरी डिस्चार्ज करने से पहले विशेषज्ञ द्वारा जांच पूरी करवा लेनी चाहिए, अन्यथा डेटा खो सकता है ।
vii. अतिरिक्त भंडारण मीडिया जैसे मेमोरी स्टिक, कॉम्पैक्ट फ्लैश आदि को जप्त कर लें।
viii. सभी चरणों का दस्तावेजीकरण करें।

F. क्लाउड आधारित डिजिटल साक्ष्य

क्लाउड-आधारित डेटा के संबंध में कार्यवाही के दौरान यह ध्यान रखना महत्वपूर्ण है कि इसमें तीसरे पक्ष के सेवा प्रदाताओं के स्वामित्व वालेधरखरखाव वाले दूरस्थ सर्वर पर डेटा का भंडारण और प्रसंस्करण रहता है । क्लाउड सेवा प्रदाताओं के उदाहरणों में अमेजॅन वेब सर्विसेज (ाँ), माइक्रोसॉफ्ट एज़्योर, गूगल क्लाउड प्लेटफॉर्म आदि शामिल हैं। अन्वेषण के दौरान क्लाउड-आधारित डेटा को संभालने के चरण नीचे दिए गए हैं:

i. प्रासंगिक क्लाउड सेवाओं की पहचान करें। सामान्य क्लाउड स्टोरेज सेवायें हैं: गूगल ड्राइव, ड्रॉपबॉक्स, ईमेल सेवाएँ आदि।
ii. संबंधित क्लाउड सेवाओं से जुड़े उपयोगकर्ता खातों के बारे में जानकारी इकट्ठा करें। इसमें username, ईमेल पते, खाता पहचानकर्ता आदि शामिल हो सकते हैं।
iii. क्लाउड सेवा प्रदाता को संरक्षण अनुरोध जारी करें। यह अनुरोध प्रदाता को निर्दिष्ट डेटा को संरक्षित करने में मदद करता है और इसके विलोपन या परिवर्तन को रोकता है।
iv. विभिन्न सेवा प्रदाताओं की प्रक्रियाएं और आवश्यकताएं अलग-अलग हो सकती हैं, इनकी जानकारी प्राप्त करें और उनके द्वारा निर्धारित प्रक्रिया का पालन करें ।
v. कुछ क्लाउड सेवा प्रदाता फोरेंसिक उपकरण या एपीआई (एप्लीकेशन प्रोग्रामिंग इंटरफेस) प्रदान करते हैं जिनका उपयोग सही फोरेंसिक तरीके से डेटा तक पहुंचने और एकत्र करने के लिए किया जा सकता है। ऐसी सुविधाओं का उपयोग किया जा सकता है।
vi. क्लाउड-आधारित डेटा से जुड़े प्रासंगिक मेटाडेटा को इकट्ठा करें, जैसे सृजन तिथियां, संशोधन तिथियां और एक्सेस लॉग। ये मेटाडेटा घटनाओं की समयरेखा स्थापित करने के लिए मूल्यवान हो सकते हैं।
vii. डेटा संग्रहण प्रक्रिया के प्रत्येक चरण का दस्तावेजीकरण करें और इसमें दिनांक, समय, प्रयुक्त विधियां और सामने आई चुनौतियों जैसे विवरण शामिल करें।

viii. साक्ष्य की अखंडता बनाए रखने के लिए अभिरक्षा की श्रृंखला हेतु प्रक्रियाओं का पालन करें।

ix. जिन मामलों में ईमेल-आईडी/पासवर्ड की पुनर्प्राप्ति संभव नहीं है, उनके संबंध में अनुसंधानकर्त्ता क्लाउड डेटा के संरक्षण के लिए क्लाउड सेवा प्रदाता को अनुरोध भेज सकता है।

x. यदि इलेक्ट्रोनिक उपकरण पासवर्ड से सुरक्षित नहीं है तो क्लाउड स्टोरेज तक पहुंच संभव है, अन्यथा पासवर्ड प्राप्त करने के लिए मालिक से पूछताछ की जा सकती है।

xi. यदि क्लाउड स्टोरेज तक पहुंच है, तो डेटा को राइट ब्लॉकर्स प्रक्रिया का उपयोग करके इमेज किया जा सकता है।

xii. डाउनलोड किए गए डेटा को एक नए स्टोरेज इलेक्ट्रोनिक उपकरण में संग्रहीत करते हुये डेटा का हैश मान प्राप्त किया जाए ।

xiii. क्लाउड डेटा के पासवर्ड को स्वतंत्र गवाहों की मौजूदगी में बदला जाना चाहिए ताकि मालिक द्वारा उसमें कोई परिवर्तन या विलोपन न किया जा सके। सफल लॉगिन परीक्षण के बाद नया पासवर्ड दर्ज किया जाना चाहिए और जप्ती ज्ञापन के साथ सीलबंद लिफाफे में संग्रहीत किया जाना चाहिए।

xiv. क्लाउड खाते के लिए सुरक्षा प्रश्न और सुरक्षा फोन नंबर भी बदला जाना चाहिए ताकि मालिक द्वारा पहुंच को रोका जा सके।

xv. सभी चरणों का दस्तावेजीकरण करें।

G. सीसीटीवी

स्मार्ट सिटी की अवधारणा तथा व्यक्तिगत और संस्थागत परिवेश में क्लोज्ड सर्किट टेलीविजन (ब्ब्ज्ट) निगरानी प्रणालियों के बढ़ते उपयोग से इन प्रणालियों में उपलब्ध रिकॉर्डिंग अपराध अन्वेषण का एक महत्वपूर्ण हिस्सा बन गई है। ब्ब्ज्ट फुटेज की जांच से अनुसंधानकर्त्ता को घटनाओं के क्रम, आरोपी व्यक्तियों के प्रवेश और निकास बिंदुओं आदि के बारे में जानकारी मिल सकती है । न्यायालय में साक्ष्य के रूप में ब्ब्ज्ट सिस्टम से फुटेज का उपयोग करने के लिए, इसे निम्नलिखित तरीके से सुरक्षित और एकत्र किया जाना चाहिएः-

सीसीटीवी/डीवीआर/एनवीआर निगरानी प्रणालियों को संभालते समय प्रक्रियाएंः

i. अनुसंधानकर्त्ता को उस स्थान का सर्वेक्षण करना चाहिए जहां सीसीटीवी प्रणाली स्थापित है और निम्नलिखित दस्तावेज तैयार करना चाहिएः
   - सीसीटीवी कैमरों और डीवीआर/एनवीआर के बीच अंतर्संबंधों को दर्शाता फोटोग्राफ/स्केच।
   - डीवीआर/एनवीआर प्रणाली से जुड़े कैमरों की संख्या।
   - जाँच करें कि सिस्टम स्टैंड-अलोन/पीसी-आधारित है या नेटवर्क आधारित है।
   - पहचान करें कि फुटेज ऑन-प्रिमाइस/रिमोट/क्लाउड कहाँ पर संग्रहीत हैं ।
   - निर्धारित करें कि अन्वेषण के लिए कौन से कैमरा दृश्य आवश्यक हैं।
   - अन्वेषण की आवश्यकता और घटनास्थल की स्थिति के आधार पर जप्ती की सर्वोत्तम विधि का निर्णय लें।
   - डीवीआर/एनवीआर प्रणाली में दर्शायें जा रहे दिनांक और समय तथा वास्तविक दिनांक और समय को लेखबद्ध करें ।

ii. अनुसंधानकर्त्ता द्वारा आवश्यकतानुसार डीवीआर/एनवीआर सिस्टम के साथ मूल हार्ड डिस्क को भी जप्त किया जा सकता है। यदि मूल की जप्ती की आवश्यकता नहीं है या संभव नहीं है, उदाहरण के लिए रेलवे स्टेशनों, सार्वजनिक स्थानों, यातायात पुलिस कैमरे आदि पर लगे सीसीटीवी के मामले में, तो अनुसंधानकर्त्ता को संबंधित फुटेज की प्रति प्राप्त करनी चाहिए।

iii. यदि संपूर्ण DVR/NVR सिस्टम को जप्त करना आवश्यक हो, तो सिस्टम में उपलब्ध पासवर्ड/पिन की जांच करें। यदि संभव हो, तो उसे भी प्राप्त कर लेखबद्ध कर लें ।

iv. सिस्टम की स्थापना के बारे में विवरण प्राप्त करें जैसे कि
   - सिस्टम को रिकॉर्ड करने के लिए कैसे कॉन्फिगर किया गया है?

- हार्ड डिस्क स्थान को अधिलेखित (overwrite) करने के लिए क्या नीति अपनाई जाती है?
- क्या कोई मोशन सेंसर तकनीक अपनाई गई है?
- क्या सिस्टम पासवर्ड/पिन से सुरक्षित है या नहीं?

v. यदि संभव हो तो डीवीआर/एनवीआर प्रणाली स्थापित करने वाले तकनीकी व्यक्ति की सहायता लें।

vi. यदि डीवीआर प्रणाली जप्त नहीं की गई है, तो निम्नलिखित कदम उठाए जाने चाहिएः-

- अनुसंधानकर्त्ता को मालिक/प्रभारी को सिस्टम में कोई भी बदलाव न करने के लिए संरक्षण नोटिस जारी करना चाहिए।
- भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के तहत उस व्यक्ति से प्रमाण-पत्र प्राप्त किया जाना चाहिए जो उस प्रणाली का स्वामी या प्रभारी है।
- अन्य बिंदुओं के अलावा, प्रमाणपत्र में निम्नलिखित तकनीकी विवरण का उल्लेख होना चाहिएः
    - डीवीआर प्रणाली का निर्माण
    - डीवीआर प्रणाली में प्रयुक्त हार्ड डिस्क
    - डीवीआर और हार्ड डिस्क का सीरियल नंबर/उत्पाद संख्या
    - घड़ी की अशुद्धि को रिकॉर्ड करने के लिए DVR प्रणाली में दर्शाया जा रहा दिनांक और समय ।
    - घटना के समय डीवीआर प्रणाली ठीक से काम कर रही थी।

vii. यदि अनुसंधानकर्त्ता प्रासंगिक फुटेज प्राप्त का निर्णय लेता है, तो इसकी विशिष्ट पहचान को रिकॉर्ड करने के बाद एक स्टेराइल पेन ड्राइव या बाहरी HDD को प्लग-इन किया जाय ।

viii. DVD/NVR सिस्टम और निर्यात (export) सुविधाओं का अध्ययन करें। प्रासंगिक कैमरा फ्रेम का प्रारंभ समय और समाप्ति समय दर्ज करें, समर्थित डाउनलोड प्रारूप का चयन करें और गवाहों के सामने डाउनलोड/निर्यात करें।

ix. प्रासंगिक फुटेज की प्रतिलिपि लेते समय यह सुनिश्चित करें कि रिकॉर्ड की गई और प्राप्त की गई प्रतिलिपि की फ्रेम दर में कोई अंतर न हो।

x. सामान्यतः DVR/NVR जानकारी को Proprietary प्रारूप में संग्रहीत करता है, इसलिए मूल Proprietary प्रारूप के साथ-साथ परिवर्तित प्रारूप (जैसे MP4) की प्रतिलिपि बनाना आवश्यक है।

xi. उपयोग किए गए हैशिंग एल्गोरिदम के साथ हैश मान की गणना करें और उन्हें लेखबद्ध करें। फुटेज का पूर्वावलोकन करें ताकि यह सुनिश्चित हो सके कि यह सुलभ प्रारूप में है।

xii. यदि आवश्यक हो तो संग्रहित वीडियो देखने के लिए आवश्यक वीडियो प्लेबैक सॉफ्टवेयर भी साथ में संग्रहित करना चाहिए ।

xiii. अनुसंधानकर्त्ता को वीडियोग्राफी/फोटोग्राफी और उचित अभिलेखों के माध्यम से पूरी जप्ती प्रक्रिया का दस्तावेजीकरण करना चाहिए।

xiv. अन्वेषण के दौरान प्राप्त सीसीटीवी क्लिपिंग को सीसीटीवी सिस्टम के मालिक/प्रभारी द्वारा दिये गये प्रमाण पत्र के साथ साक्ष्य के रूप में न्यायालय में प्रस्तुत किया जा सकता है।

xv. डीवीआर/एनवीआर प्रणाली को नीचे उल्लिखित स्थितियों में फोरेंसिक विज्ञान प्रयोगशालाओं को भेजा जा सकता हैः-

- ऐसे मामले जहां हटाए अथवा मिटाये गए फुटेज की पुनर्प्राप्ति आवश्यक है।
- फोटोग्राफ/फुटेज की तुलना आवश्यक है।
- किसी व्यक्ति या वाहन संख्या की पहचान करने के लिए छवि का संवर्धन।
- यह जांचने के लिए कि वीडियो फ्रेम में कोई गड़बड़ी तो नहीं है, ताकि छेड़छाड़ की संभावना को नकारा किया जा सके ।

xvi. सभी चरणों का दस्तावेजीकरण करें ।

H. IoT इलेक्ट्रोनिक उपकरण

i. परिसर/जप्ती के स्थान पर IoT उपकरणों की पहचान करें। IoT उपकरणों को कई वर्गों या उपकरणों के समूहों में

विभाजित किया जा सकता है, जिसमें पहनने योग्य (जैसे स्मार्ट घड़ियाँ, फिटनेस बैंड, स्मार्ट रिंग आदि), स्मार्ट स्पीकर, स्मार्ट डिस्प्ले, नियंत्रण प्रणाली (जैसे स्मार्ट डोर लॉक), वर्चुअल असिस्टेंट (जैसे एलेक्सा, सिरी, बिक्सबी आदि) आदि शामिल हैं।

ii. बाजार में विभिन्न IoT उपकरण उपलब्ध हैं और नियमित रूप से नए उपकरण जोड़े जाते हैं । इन उपकरणों के उपयोग और क्षमताओं को ऑनलाइन जानकारी देखकर या उपयोगकर्ता मैनुअल का संदर्भ लेकर निर्धारित किया जा सकता है।

iii. IoT इलेक्ट्रोनिक उपकरण और उससे जुड़े अन्य उपकरणों की तस्वीर लें।

iv. इलेक्ट्रोनिक उपकरण पर कार्रवाई से पहले उसकी स्क्रीन पर कुछ प्रदर्शित हो तो उसपर प्रदर्शित सामग्री/स्थिति को कैप्चर कर लें।

v. सिस्टम के किसी नेटवर्क से जुड़ा होने की जाँच करें। जुड़ा होने पर इलेक्ट्रोनिक उपकरणों को नेटवर्क से अलग करें।

vi. अलग करने की प्रक्रिया के दौरान अनुसंधानकर्त्ता को ट्रिगर घटनाओं से सावधान रहना चाहिए। इन घटनाओं के परिणामस्वरूप इलेक्ट्रोनिक उपकरण में ही हेरफेर हो सकता है। ऐसी घटनाओं में अनुसंधानकर्त्ता द्वारा की गई हरकत या उपकरण को हिलाना शामिल हो सकते हैं जिन्हें कनेक्टेड सेंसर द्वारा पता लगाया जा सकता है । वेक-वर्ड्स को मुखर करना जैसे कि यह कहना कि आपको ''एलेक्सा'' इलेक्ट्रोनिक उपकरण मिल गई है, और ''एलेक्सा'' वेक-वर्ड भी है अथवा एक पहचान योग्य सीमा से ऊपर की आवाजें निकालना, या ऐसी अन्य क्रियाएं या घटनाएँ ट्रिगर का काम कर सकती हैं ।

vii. ईथरनेट तार को डिस्कनेक्ट करने या वाई-फाई कनेक्शन को बंद करने से IoT इलेक्ट्रोनिक उपकरण नेटवर्क से अलग हो जायेंगे ।

viii. हब या राउटर की मौजूदगी है अथवा इलेक्ट्रोनिक उपकरण सीधे इंटरनेट से कनेक्ट है इसको निर्धारित करते हुए उसका दस्तावेजीकरण करें। यदि कोई हब या राउटर IoT इलेक्ट्रोनिक उपकरण से जुड़ा है, तो उनको भी जप्त कर लिया जाना चाहिए।

ix. इलेक्ट्रोनिक उपकरण को नेटवर्क से अलग करने के लिए उसकी पावर को अनप्लग करें या उसकी बैटरी निकाल लें। अगर ये तरीके इलेक्ट्रोनिक उपकरण को बंद करने में विफल रहते हैं, तो फैराडे बैग या अन्य नेटवर्क आइसोलेशन तकनीकों का उपयोग करें।

x. इलेक्ट्रोनिक उपकरण का फोटोग्राफ लें और उसका मेक, मॉडल, सीरियल, नंबर और मीडिया एक्सेस कंट्रोल (MAC) पता रिकॉर्ड करें। यह स्मार्ट फोन जैसे अन्य इलेक्ट्रोनिक उपकरण के लिए उपयुक्त कनेक्शन के मिलान में उपयोगी दस्तावेज के रूप में कार्य करता है। यह ध्यान दिया जा सकता है कि IoT मानक की पहचान में ऑब्जेक्ट पहचान, संचार पहचान और एप्लिकेशन पहचान शामिल हैं।

xi. अगर अस्थिर मेमोरी है, तो उसमें उपयोगी जानकारी हो सकती है जिसे अनदेखा नहीं किया जाना चाहिए । कुछ IoT इलेक्ट्रोनिक उपकरण में सीमित RAM/स्टोरेज के कारण, डेटा/फाइलें बार-बार ओवरराइट हो सकती हैं।

xii. यदि डेटा क्लाउड या तृतीय-पक्ष ऐप्स में संग्रहीत है, तो क्लाउड से डेटा एकत्रित करें ।

xiii. क्लाउड सेवा प्रदाताओं की पहचान करें और उनके द्वारा प्रदान की जाने वाली सेवाओं तथा उनके द्वारा एकत्रित की जाने वाली सूचनाओं के बारे में जानकारी प्राप्त करें ।

xiv. यदि किसी सेवा प्रदाता से डेटा लिंक किया गया हो तो सेवा प्रदाता से डेटा उपलब्ध कराने का अनुरोध करें । यदि डेटा स्वामित्व प्रारूप में मौजूद है, तो सेवा प्रदाता से डेटा को सामान्य फाइल प्रारूप में प्राप्त करें।

xv. IoT इलेक्ट्रोनिक उपकरण, या संबंधित ऐप्स, या कनेक्टेड इलेक्ट्रोनिक उपकरण या क्लाउड से डेटा निकालने के बाद, एकत्रित डेटा के हैश मान की गणना करें और उसे संग्रहित करें ।

xvi. प्राप्त डेटा का पूर्वावलोकन करें ताकि यह सुनिश्चित हो सके कि यह सुलभ प्रारूप में है।

xvii. यदि डेटा की प्राप्ति भौतिक मीडिया (जैसे, ऑप्टिकल डिस्क या हार्ड ड्राइव) में है, तो उसे दस्तावेजित करें।

xviii. क्लाउड, मोबाइल और अन्य जुड़े इलेक्ट्रोनिक उपकरणों तथा तृतीय पक्षों के पास डेटा जो संग्रहित किया गया है, उस संबंध में संबंधित क्लाउड सेवा प्रदाताओं को संरक्षण नोटिस भेजना सुनिश्चित करें।

xix. जप्त किए गए IoT उपकरणों को पैकेजिंग, परिवहन, परीक्षण पूर्व भंडारण, आदि के दौरान पावर-ऑफ मोड और नेटवर्क से अलग रखा जाना सुनिश्चित करें ।

xx. सभी चरणों का दस्तावेजीकरण करें।

I. सीडीआर/आईपीडीआर/आदि।

i. दूरसंचार/इंटरनेट सेवा प्रदाताओं से प्राप्त सीडीआर/आईपीडीआर इलेक्ट्रानिक दस्तावेजों की श्रेणी में आते हैं और उनकी स्वीकार्यता के संबंध में भारतीय साक्ष्य अधिनियम के प्रावधानों का अनुपालन करना आवश्यक है ।

ii. जहां अनुसंधानकर्त्ता इन्हें सीधे टीएसपी/आईएसपी के नोडल अधिकारी के माध्यम से प्राप्त करता है, हार्ड कॉपी या सॉफ्ट कॉपी में, उसे नोडल अधिकारी द्वारा जारी भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के तहत प्रमाण पत्र के साथ प्राप्त करें ।

iii. जहां अनुसंधानकर्त्ता इन्हें डीआईयू या किसी अन्य अधिकारी के माध्यम से प्राप्त करता है, जो अपने स्तर पर इन्हें टीएसपी/आईएसपी के नोडल अधिकारी के माध्यम से प्राप्त करते है, हार्ड कॉपी या सॉफ्ट कॉपी में, उस स्थिति में प्राप्त सीडीआर/आईपीडीआर के साथ भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के तहत टीएसपी/आईएसपी के नोडल अधिकारी द्वारा जारी प्रमाण पत्र के अलावा डीआईयू के सिस्टम प्रशासक द्वारा या संबंधित अधिकारी द्वारा जारी भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के तहत भी प्रमाण पत्र संलग्न करना अनिवार्य रहेगा ।

iv. अनुसंधानकर्त्ता द्वारा मूल में प्राप्त किये गये CDR आदि पर सीधा या सॉफ्टवेयर से विश्लेषण में उपयोग नहीं करना चाहिए, बल्कि विश्लेषण के लिये उसकी एक प्रतिलिपि बनानी चाहिए। हार्डकॉपी की प्रतिलिपि सामान्य फोटोकॉपी प्रक्रिया के माध्यम से बनाई जा सकती है। सॉफ्टकॉपी के मामले में, राइट ब्लॉकर का उपयोग करके सॉफ्ट कॉपी वाले स्टोरेज इलेक्ट्रोनिक उपकरण से कॉपी किया जाना चाहिए ताकि मूल सुरक्षित रहे । आउटपुट एक स्टेराइल डिजिटल स्टोरेज माध्यम जैसे कि यूएसबी स्टोरेज, पेन ड्राइव आदि पर संग्रहीत किया जाना चाहिए जिसका उपयोग आगे के विश्लेषण के लिये करें ।

v. भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के अंतर्गत प्रमाण पत्र के साथ प्राप्त मूल सीडीआर/आईपीडीआर को न्यायालय में आरोप पत्र के साथ इलेक्ट्रानिक दस्तावेज/साक्ष्य के रूप में सीधे प्रस्तुत करें ।

vi. सभी चरणों का दस्तावेजीकरण करें।

J. अन्य स्रोतों से प्राप्त ऑडियो/ वीडियो क्लिप

i. खुले स्रोतों, इंटरनेट, मुखबिरों, वायरल क्लिप आदि जैसे स्रोतों से पुलिस को प्राप्त कोई भी ऑडियो/वीडियो क्लिप भी एक इलेक्ट्रानिक दस्तावेज है।

ii. स्वीकार्यता और प्रमाणिकता इसे अभिलेख पर लेने के तरीके पर निर्भर करेगा। ऐसी क्लिप को व्यक्तिगत मोबाइल फोन या किसी भी रेंडम कंप्यूटर सिस्टम से डाउनलोड नहीं किया जाना चाहिए। जिले में डीआईयू के पास ऐसी क्लिप, आदि प्राप्त करने के लिए एक समर्पित कंप्यूटर सिस्टम रखना चाहिए।

iii. इस तरह की क्लिप को इस समर्पित कंप्यूटर सिस्टम से डाउनलोड किया जाना चाहिए । साथ में भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के तहत उक्त सिस्टम के सिस्टम एडमिनिस्ट्रेटर द्वारा जारी किए गए प्रमाण पत्र प्राप्त करना चाहिए । प्राप्त मूल क्लिप को भविष्य में आवश्यकता पड़ने पर

पुनः प्राप्त करने के लिए सिस्टम में संग्रहीत किया जाना आवश्यक है । क्लिप की एक कार्यकारी प्रति को USB स्टोरेज, पेन ड्राइव आदि जैसे स्टेराइल डिजिटल स्टोरेज माध्यम पर भी डाउनलोड किया जाना चाहिए, जिसका उपयोग अनुसंधानकर्त्ता द्वारा अपने विश्लेषण के लिए किया जा सकता है ।

iv. अनुसंधानकर्त्ता डाउनलोड की गई क्लिप को तत्काल फोरेंसिक जांच के लिए भेजें ताकि क्लिप की प्रामाणिकता और छेड़छाड़/संपादन आदि की जाँच की जा सके।

v. ऐसे ऑडियो/वीडियो क्लिप में संदिग्धों की पहचान की पुष्टि करने के लिए वॉयस स्पेक्ट्रोग्राफी और/या छवि विश्लेषण भी करवाया जा सकता है।

vi. क्लिप की विषय-वस्तु का सावधानीपूर्वक अवलोकन/श्रवण/विश्लेषण करके उसके स्रोत का पता लगाने का प्रयास करें । यदि क्लिप के मूल स्रोत का पता लगा लिया जाता है उसकी प्रमाणिकता अधिक होगी ।

vii. जब स्रोत/उत्पत्ति का पता लग जाए, तो इलेक्ट्रानिक साक्ष्यों के संग्रहण के संबंध में ऊपर कंडिकाओं में दिए गए प्रक्रियाओं का पालन करें ।

viii. सभी चरणों का दस्तावेजीकरण करें।

K. विधिपूर्वक अंतरावरोधित सामग्री

i. भारतीय टेलीग्राफ अधिनियम, 1885 की धारा 5(2), भारतीय टेलीग्राफ नियम, 1951 के नियम 419ए और सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 69 में वैध अंतरावरोधन का प्रावधान है।

ii. इस तरह के वैध अंतरावरोधन के माध्यम से प्राप्त जानकारी इलेक्ट्रानिक साक्ष्य के दायरे में आती है।

iii. अंतरावरोधन वॉयस लॉगर मशीन के माध्यम से ही किया जाना चाहिए और नामित सिस्टम प्रशासक को निर्धारित मानक संचालन प्रक्रिया के अनुसार ही प्राप्त इनपुट को साझा करना चाहिए ।

iv. वैध अंतरावरोधन के माध्यम से प्राप्त किसी भी सामग्री को नोडल अधिकारी की स्वीकृती के बाद ही संबंधित अनुसंधानकर्त्ता के साथ साझा किया जाना चाहिए । सिस्टम प्रशासक को केवल

प्रासंगिक सामग्री को ही चिन्हित कर साझा करने हेतु निर्यात करना चाहिए और इसे संबंधित अनुसंधानकर्त्ता को भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के तहत प्रमाण पत्र के साथ एक स्टेराइल पेन ड्राइव या बाहरी एचडीडी में इसके विशिष्ट पहचान रिकॉर्ड करने के बाद प्रदान करना चाहिए।

v. संबंधित नंबर/आईपी या इकाई से जुड़ी सभी अंतरावरोधित सामग्री की मूल प्रति को ट्रायल के समापन तक वॉयस लॉगर मशीन में रखा जाना चाहिए। इस संबंध में गृह विभाग द्वारा जारी अंतरावरोधित सामग्री के प्रतिधारण/विनाश की मानक संचालन प्रक्रिया का दृढ़तापूर्वक पालन किया जाना चाहिए । वॉयस लॉगर मशीन के प्रतिस्थापन के मामले में भी, मूल हार्ड डिस्क को आवश्यकता समाप्त होने तक संरक्षित रखा जाना आवश्यक है ।

vi. नोडल अधिकारी को भारतीय टेलीग्राफ अधिनियम, 1885 की धारा 5(2), भारतीय टेलीग्राफ नियम, 1951 के नियम 419ए तथा सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 69 के अंतर्गत अंतरावरोधन को अधिकृत करने वाले सक्षम प्राधिकारी के आदेशों की एक प्रति भी अनुसंधानकर्त्ता को उपलब्ध करानी चाहिए।

vii. अनुसंधानकर्त्ता संबंधित फोन नंबर/आईपी का सीडीआर/आईपीडीआर भी प्राप्त करें, ताकि उसे अंतरावरोधित सामग्री से लिंक किया जा सके। सीडीआर/आईपीडीआर प्राप्त करने की लिए प्रक्रिया को ऊपर दिए गए पैराग्राफ में बताया गया है।

viii. सभी चरणों का दस्तावेजीकरण करें।

11. इलेक्ट्रोनिक साक्ष्य की पहचान एवं सरुक्षित करने के बाद संग्रहित करने के लिए निम्नलिखित अनुक्रम का पालन किया जा सकता हैः

A. लेखन अवरोधक का उपयोग करना.

B. फोरेंसिक छवि का निष्कर्षण, और

C. हैश मान उत्पन्न करना.

A. लेखन अवरोधक (राईट ब्लॉकर्स) का उपयोग करना

राइट ब्लॉकर्स हार्डवेयरध्सॉफ्टवेयर उपकरण हैं जो स्टोरेज मीडिया तक केवल पढ़ने के लिए पहुँच की अनुमति देते हैं। डिजिटल फोरेंसिक में राइट ब्लॉकर्स आवश्यक उपकरण हैं जो साक्ष्य संग्रह की प्रक्रिया के दौरान मूल स्टोरेज मीडिया पर डेटा के परिवर्तन या संशोधन को रोकते हैं। ये उपकरण अनुसंधानकर्त्ता को साक्ष्य में अनजाने में बदलाव किए बिना फाइलोंध्डेटा तक पहुँचने और उनका विश्लेषण करने में मदद करते हैं। इलेक्ट्रानिक साक्ष्य के संग्रह के दौरान राइट ब्लॉकर्स का उपयोग करने के तरीके पर सामान्य मार्गदर्शन नीचे दिया गया हैः-

i. एक ऐसा लेखन अवरोधक चुनें जो आपके द्वारा उपयोग किए जा रहे भंडारण मीडिया के प्रकार (जैसे, हार्ड ड्राइव, यूएसबी ड्राइव, एसएसडी) के लिए उपयुक्त हो।
ii. साक्ष्य भंडारण मीडिया को राइट ब्लॉकर से जोड़ने से पहले, उस सिस्टम को बंद कर दें जहाँ साक्ष्य स्थित है। इससे कनेक्शन प्रक्रिया के दौरान किसी भी आकस्मिक परिवर्तन को रोकने में मदद मिलेगी।
iii. राइट ब्लॉकर को मूल साक्ष्य स्टोरेज मीडिया से कनेक्ट करें। यदि हार्डवेयर राइट ब्लॉकर का उपयोग किया जाता है, तो सुनिश्चित करें कि हार्डवेयर स्टोरेज इलेक्ट्रोनिक उपकरण और फोरेंसिक वर्कस्टेशन के बीच ठीक से जुड़ा हुआ है।
iv. साक्ष्य भंडारण मीडिया को लेखन अवरोधक के माध्यम से फोरेंसिक वर्कस्टेशन/लैपटॉप से कनेक्ट करें।
v. फोरेंसिक वर्कस्टेशन/लैपटॉप को चालू करें और पुष्टि करें कि राइट ब्लॉकर सही ढंग से काम कर रहा है। अधिकांश राइट ब्लॉकर्स में उनकी स्थिति दिखाने के लिए इंडिकेटर लाइट या डिस्प्ले होते हैं।
vi. किसी भी फोरेंसिक जांच से पहले यह सुनिश्चित कर लें कि स्टोरेज मीडिया रीड-ओनली मोड में है। इससे यह सुनिश्चित होता है कि कोई भी डेटा मूल स्रोत पर वापस नहीं लिखा जा सकता।
vii. राइट ब्लॉकर के उपयोग का दस्तावेजीकरण करें और प्रयुक्त राइट ब्लॉकर का प्रकार, सीरियल नंबर, तथा हार्डवेयर या

सॉफ्टवेयर आदि के बारे में कोई भी प्रासंगिक जानकारी जैसे विवरण का उल्लेख करें।

viii. एक बार राइट ब्लॉकर लग जाने के बाद, अपने फोरेंसिक विश्लेषण के साथ आगे बढ़ें। साक्ष्य भंडारण मीडिया से डेटा की जांच और संग्रह करने के लिए विशेष फोरेंसिक उपकरणों का उपयोग करें।

ix. जब आपका विश्लेषण पूरा हो जाए, तो साक्ष्य भंडारण मीडिया को डिस्कनेक्ट करने से पहले फोरेंसिक वर्कस्टेशन को बंद कर दें।

x. लेखन अवरोधक से साक्ष्य भंडारण मीडिया को हटाने का दस्तावेजीकरण करें और हटाने की प्रक्रिया के बारे में समय, दिनांक और अन्य प्रासंगिक विवरण नोट करें।

B. फोरेंसिक छवि (image) का निष्कर्षण (extraction)

अगर अनुसंधानकर्त्ता अपराध स्थल पर इलेक्ट्रानिक इलेक्ट्रोनिक उपकरण की फोरेंसिक कॉपी आवश्यक पाते हो तो सबसे पहले उस इलेक्ट्रानिक इलेक्ट्रोनिक उपकरण की पहचान करनी चाहिए और उसका विवरण दर्ज करना चाहिए जिसकी फोरेंसिक छवि ली जानी है। मेक, मॉडल और किसी भी प्रासंगिक सीरियल नंबर जैसे विवरण सही ढंग से दर्ज करें। अनुसंधानकर्त्ता को यह भी सुनिश्चित करना चाहिए कि उसके पास फोरेंसिक छवि निकालने के लिए आवश्यक उपकरण हैं। इलेक्ट्रानिक इलेक्ट्रोनिक उपकरण की फोरेंसिक कॉपी निकालने के लिए निम्नलिखित कदम उठाए जा सकते हैंः-

i. छेड़छाड़ या डेटा विनष्टीकरण को रोकने के लिए इलेक्ट्रानिक इलेक्ट्रोनिक उपकरण को किसी भी नेटवर्क या बाहरी कनेक्शन से अलग रखें ।

ii. इलेक्ट्रोनिक उपकरण को बंद करें और इसकी मूल स्थिति को बनाए रखने के लिए कदम उठाएँ। इसके लिए इलेक्ट्रोमैग्नेटिक सिग्नल को ब्लॉक करने के लिए इलेक्ट्रोनिक उपकरण को फैराडे बैग में रखना भी पड़ सकता है।

iii. उस भौतिक वातावरण का दस्तावेजीकरण करें जहाँ निष्कर्षण हो रहा है। इलेक्ट्रोनिक उपकरण की स्थिति, किसी भी बाहरी

भंडारण मीडिया और किसी भी परिधीय की उपस्थिति पर ध्यान दें ।

iv. निष्कर्षण प्रक्रिया के लिए उचित फोरेंसिक उपकरण चुनें। सामान्य उपकरणों में FTK इमेजर, एनकेस, या dd (बिट-फॉर-बिट कॉपी बनाने के लिए एक कमांड-लाइन टूल) जैसे सॉफ्टवेयर शामिल हैं ।

v. निष्कर्षण प्रक्रिया केवल पढ़ने के लिए है और मूल डेटा को संशोधित नहीं करती है । इसे सुनिश्चित करने के लिए इलेक्ट्रोनिक उपकरण को लेखन-अवरोधक हार्डवेयर या सॉफ्टवेयर का उपयोग करके फोरेंसिक वर्कस्टेशन से कनेक्ट करें।

vi. संपूर्ण स्टोरेज मीडिया (हार्ड ड्राइव, एसएसडी, आदि) की बिट-टू-बिट फोरेंसिक छवि बनाने के लिए चयनित फोरेंसिक टूल का उपयोग करें। सुनिश्चित करें कि उपयोग किया गया टूल फोरेंसिक रूप से सही छवि बनाने में सक्षम है,

vii. फोरेंसिक इमेज के लिए हैश मान (MD5, SHA-1, SHA-256, आदि) जेनरेट करें। निकाले गए इमेज की अखंडता को सत्यापित करने के लिए इस हैश मान की तुलना मूल इलेक्ट्रोनिक उपकरण के हैश मान से करें।

viii. निष्कर्षण प्रक्रिया का विवरण रिकॉर्ड करें, जिसमें प्रारंभ और समाप्ति समय, प्रयुक्त उपकरण, तथा प्रक्रिया के दौरान आई कोई समस्या भी शामिल है।

ix. फोरेंसिक छवि को सुरक्षित तरीके से संग्रहीत करें । यह सुनिश्चित करें कि यह अनधिकृत पहुंच, छेड़छाड़ या नुकसान से सुरक्षित है। साक्ष्य प्रबंधन और भंडारण के लिए सर्वोत्तम प्रथाओं का पालन करें ।

x. यदि इलेक्ट्रोनिक उपकरण में एकाधिक संग्रहण मीडिया (जैसे, एकाधिक हार्ड ड्राइव, USB ड्राइव) हैं, तो प्रत्येक संग्रहण इलेक्ट्रोनिक उपकरण के लिए निष्कर्षण प्रक्रिया को दोहराएं ।

C. हैश मान जेनरेट करना

इलेक्ट्रानिक साक्ष्य के संग्रह के दौरान हैश मानों को जनरेट करना और रिकॉर्ड करना डेटा अखंडता स्थापित करने और अभिरक्षा की श्रृंखला को बनाए रखने के लिए एक महत्वपूर्ण कदम है। हैश मान

क्रिप्टोग्राफिक एल्गोरिदम (जैसे MD5, SHA-1, या SHA-256) द्वारा उत्पन्न अद्वितीय पहचान हैं और इनका उपयोग इलेक्ट्रानिक फाइलों की अखंडता को सत्यापित करने के लिए किया जा सकता है। साक्ष्य संग्रह प्रक्रिया के दौरान हैश मानों को एकत्रित करने हेतु सामान्य मार्गदर्शन निम्नवत है :-

i. साक्ष्य संग्रहण प्रक्रिया का दस्तावेजीकरण करें, जिसमें दिनांक, समय, स्थान, शामिल व्यक्ति और संग्रहण का उद्देश्य जैसे विवरण शामिल हों।
ii. साक्ष्य संग्रह के लिए हमेशा विशेष फोरेंसिक उपकरणों का उपयोग करें। इन उपकरणों में अक्सर हैश गणना सुविधाएँ शामिल होती हैं। उदाहरणः एनकेस, एफटीके (फोरेंसिक टूलकिट), ऑटोप्सी, स्लीथ किट आदि।
iii. सुविधा के लिए ऐसे फोरेंसिक उपकरण का उपयोग किया जा सकता है जो फाइल निष्कर्षण या इमेजिंग प्रक्रियाओं के दौरान स्वचालित रूप से हैश मान उत्पन्न कर सकते हैं।
iv. एक सुरक्षित हैश फंक्शन चुनें (जैसे, MD5, SHA-1, SHA-256) ।
v. संपूर्ण भंडारण मीडिया की बिट-टू-बिट प्रतिलिपि या फोरेंसिक छवि बनाएं । मूल साक्ष्य को संरक्षित रखें ।
vi. फोरेंसिक छवि के लिए हैश मान की गणना करें ।
vii. व्यक्तिगत फाइलों और निर्देशिकाओं के लिए हैश मान की गणना करें और उत्पन्न/गणना किए गए हैश मानों का उचित दस्तावेजीकरण करें ।
viii. संग्रह के बाद मूल साक्ष्य के हैश मानों को फोरेंसिक छवि या एकत्रित फाइलों के हैश मानों के विरुद्ध सत्यापित करें। यदि कोई बेमेल है, तो डेटा से छेड़छाड़ का संकेत मिलता है ।
ix. मूल मीडिया में किसी भी आकस्मिक परिवर्तन को रोकने के लिए लेखन अवरोधकों का उपयोग करें ।
x. हैश मान का उल्लेख करते हुए अभिरक्षा अभिलेखों की श्रृंखला बनाए रखें ।
xi. मूल मीडिया की अखंडता बनाए रखने के लिए उसे सुरक्षित स्थान पर सुरक्षित रूप से संग्रहित करें ।

12. इलेक्ट्रानिक साक्ष्य की लेबलिंग, जप्ती, पैकेजिंग, परिवहन और भंडारणः

A. लेबलिंगः-

इलेक्ट्रानिक साक्ष्य को सुरक्षित करने के बाद, अनुसंधानकर्त्ता को दस्तावेजीकरण और पहचान उद्देश्यों के लिए साक्ष्य को उचित रूप से लेबल करना चाहिए। इलेक्ट्रानिक साक्ष्य को लेबल करते समय निम्नलिखित दिशा-निर्देशों का पालन किया जा सकता हैः-

i. वस्तुओं पर विशिष्ट संख्या/अक्षर/संयुक्त क्रामंक का लेबल लगाएं तथा जप्ती सूची में उक्त का उचित दस्तावेजीकरण करें।
ii. साक्ष्य पर उचित स्थान पर लेबल लगाएं।
iii. मुख्य इलेक्ट्रोनिक उपकरण के साथ-साथ उससे जुड़े सभी इलेक्ट्रोनिक उपकरणों पर लेबल लगाएं।
iv. यदि तार भी जप्त की गई है, तो भविष्य में पुनर्निर्माण के लिए इन तारों पर भी उचित लेबल लगा दें ।

अनुसंधानकर्त्ता को यह सुनिश्चित करना चाहिए कि जिस स्थिति में कंप्यूटर सिस्टम घटनास्थल पर मिला था उसकी तस्वीर ली जाए । मॉनिटर पर दिखाई गई छवि भी इसमें शामिल रहे, अगर कंप्यूटर सिस्टम उस समय चालू हालत में था । इसके अलावा, अनुसंधानकर्त्ता द्वारा तैयार की गई रिपोर्ट में मौके पर पहचाने गए लेकिन जप्त नहीं किए गए अन्य कंप्यूटर सिस्टम/डेटा और डिजिटल इलेक्ट्रोनिक उपकरण की सूचना भी तस्वीर में रहनी चाहिए ।

B. इलेक्ट्रानिक साक्ष्य की जप्ती, पैकेजिंग, परिवहन और भंडारणः-

साक्ष्य पर उचित लेबल लगाने के बाद यह कार्य शुरू होगा । इलेक्ट्रानिक साक्ष्य को जप्त करते समय साक्ष्य जप्त करने के लिए दी गई प्रक्रिया का सख्ती से पालन करें । जप्त साक्ष्य को एंटी-स्टेटिक बैग या बबल रैपर या प्लास्टिक बैग जैसी अन्य सामग्री से पैक किया जाना चाहिए क्योंकि चुंबकीय/रेडियोधर्मी बलों द्वारा इलेक्ट्रानिक साक्ष्य को बदला/नष्ट किया जा सकता है। साक्ष्य को पैक करते समय, अनुसंधानकर्त्ता को यह सुनिश्चित करना चाहिए कि पैकेजिंग से साक्ष्य को नुकसान न पहुंचे। परिवहन के दौरान अभिरक्षा की श्रृंखला का सख्ती से पालन करें । इलेक्ट्रानिक साक्ष्य को जप्त करने, पैक

करने, परिवहन करने और संग्रहीत करने के दौरान अनुसंधानकर्त्ता को निम्नलिखित सामान्य सावधानियां बरतनी चाहिए :-

i. कंप्यूटर सिस्टम, कंप्यूटर डेटा और डिजिटल उपकरणों को चुंबकीय स्रोतों या रेडियो ट्रांसमीटरों के पास न रखें।
ii. कंप्यूटर सिस्टम, कंप्यूटर डेटा और डिजिटल उपकरणों को नमी वाले स्थानों पर न रखें।
iii. कंप्यूटर सिस्टम, कंप्यूटर डेटा और डिजिटल उपकरणों को किसी झटके या अत्यधिक या लंबे कंपन के बिना परिवहन करें ।
iv. डिजिटल साक्ष्य को सिग्नल-ब्लॉकिंग बैग जैसे फैराडे आइसोलेशन बैग और रेडियो फ्रीक्वेंसी-शील्डिंग सामग्री में पैक करें ताकि इलेक्ट्रोनिक उपकरण द्वारा डेटा/संदेश भेजे या प्राप्त किए जाने से रोका जा सके। यह ध्यान रखें कि इलेक्ट्रोनिक उपकरण को सिग्नल-ब्लॉकिंग पैकेजिंग में रखने से बैटरी की लाइफ काफी कम हो सकती है। कम बैटरी पावर रहने पर संभव हो तो इलेक्ट्रोनिक उपकरण को ''फ्लाइट-मोड'' में रखें ।
v. इलेक्ट्रानिक साक्ष्य को ऐसी सामग्री के साथ पैक करने से बचें जो स्थैतिक बिजली उत्पन्न कर सकती है (जैसे स्टायरोफोम) ।
vi. परिवहन के दौरान साक्ष्य को चुंबकीय स्रोतों, नमी, धूल और अन्य हानिकारक कणों या संदूषकों से बचाएं ।
vii. विभिन्न प्रकार के साक्ष्यों के लिए विशेष पैकेजिंग की आवश्यकता होती है, इसलिए अनुसंधानकर्त्ता के पास विभिन्न प्रकार के साक्ष्य लिफाफे, बैग और कंटेनर होने चाहिए ।
viii. संदूषण (contamination) से बचने के लिए पैकेजिंग साफ होनी चाहिए । यथासंभव नई पैकिंग सामग्री रखें ।
ix. प्रत्येक साक्ष्य को पृथक पैक करके उसका दस्तावेजीकरण करें ।
x. इलेक्ट्रानिक साक्ष्य को मालखाना में संग्रहीत करने से पहले पुलिस हस्तक के प्रावधान अनुसार मालखाना बही में उचित प्रविष्टि करें ।

13. अभिरक्षा की श्रृंखला (chain of custody)

इलेक्ट्रानिक साक्ष्य की अखंडता को साबित करने के लिए अभिरक्षा की श्रृंखला महत्वपूर्ण है। कानूनी कार्यवाही में साक्ष्य की अखंडता और स्वीकार्यता को बनाए रखने के लिए इलेक्ट्रानिक साक्ष्य के लिए

अभिरक्षा की श्रृंखला (chain of custody) महत्वपूर्ण है। भारतीय नागरिक सुरक्षा संहिता, 2023 की धारा 193(3)(प) के अनुसार पुलिस रिपोर्ट में इलेक्ट्रानिक साक्ष्य के मामले में अभिरक्षा के अनुक्रम का उल्लेख करना अनिवार्य है। एक अच्छी तरह से प्रलेखित और सुरक्षित अभिरक्षा की श्रृंखला यह सुनिश्चित करती है कि इलेक्ट्रानिक साक्ष्य के साथ छेड़छाड़, परिवर्तन या उसके संग्रह, संरक्षण और विश्लेषण के दौरान समझौता नहीं किया गया है । अभिरक्षा की श्रृंखला (chain of custody) में उन सभी व्यक्तियों का दस्तावेजीकरण शामिल होता है जिन्होंने साक्ष्य को संभाला तथ जिस तारीख और समय पर ऐसे साक्ष्य एकत्र किए गए थे और मामले में ऐसे साक्ष्य एकत्र करने के उद्देश्य का भी उल्लेख रहता है ।

साक्ष्य जब एक बार एकत्र हो जाता है और उसके बाद जब भी साक्ष्य को स्थानांतरित किया जाता है, तो उसका दस्तावेजीकरण किया जाना चाहिए और जिस व्यक्ति को साक्ष्य सौंपे गए हैं, उसके अलावा किसी और को साक्ष्य तक पहुंच नहीं होनी चाहिए । इलेक्ट्रानिक साक्ष्य की अखंडता स्थापित करने और साक्ष्य को दूषित होने से बचाने के लिए साक्ष्य की अभिरक्षा की श्रृंखला (Chain of custody) को बनाए रखना महत्वपूर्ण है। यदि अभिरक्षा की श्रृंखला (Chain of custody) स्थापित नहीं हो पाती है, तो न्यायालय में प्रस्तुत साक्ष्य को चुनौती दी जा सकती है। एक व्यक्ति/स्थान/एजेंसी से दूसरे व्यक्ति/स्थान ऐजेंसी को इलेक्ट्रानिक साक्ष्य के हस्तांतरण को अभिरक्षा की श्रृंखला प्रपत्र में उचित रूप से दर्ज किया जाना चाहिए । प्रपत्र को इस पुलिस आदेश के **अनुलग्नक-1** के रूप में संलग्न किया गया है ।

14. इलेक्ट्रानिक साक्ष्य को फोरेंसिक विज्ञान प्रयोगशाला को अग्रेषित करना

यदि जप्त किए गए इलेक्ट्रानिक साक्ष्य के फोरेंसिक जांच की आवश्यकता है, तो अनुसंधानकर्त्ता को जांच के लिए प्रदर्श को फोरेंसिक विज्ञान प्रयोगशाला में भेजना चाहिए। फोरेंसिक विज्ञान प्रयोगशाला (FSL) को इलेक्ट्रानिक प्रदर्श भेजते समय, साक्ष्य की अखंडता, सुरक्षा और स्वीकार्यता सुनिश्चित करने के लिए विशिष्ट चरणों का पालन करना आवश्यक है। फोरेंसिक जांच के लिए

इलेक्ट्रानिक साक्ष्य भेजते समय अनुसंधानकर्त्ता द्वारा पालन किए जाने वाले दिशा-निर्देश निम्नवत है :-

i. अनुसंधानकर्त्ता अनुरोध प्रपत्र में मामले से संबंधित जानकारी का उल्लेख करें, जिसमें प्रदर्श का विवरण, केस संख्या, संग्रहण की तिथि और समय, तथा अन्य प्रासंगिक विवरण शामिल हों।
ii. न्यायालय से आवश्यक प्राधिकरण/आदेश प्राप्त करें।
iii. प्रदर्श के लिए अभिरक्षा की एक स्पष्ट श्रृंखला स्थापित करें और उसे बनाए रखें। दस्तावेज बनाएं कि साक्ष्य किसके पास और कब से हैं । अभिरक्षा की निरंतरता सुनिश्चित करें।
iv. परिवहन के दौरान भौतिक क्षति को रोकने के लिए इलेक्ट्रानिक प्रदर्श को सुरक्षित रूप से पैक करें। इलेक्ट्रानिक उपकरणों के लिए डिजाइन किए गए एंटी-स्टेटिक बैग या कंटेनर का उपयोग करें।
v. मामले की जानकारी, प्रदर्श विवरण और हैंडलिंग निर्देशों के साथ पैक पर स्पष्ट रूप से लेबल लगाएं। उन सभी विशेष सावधानियों को शामिल करें जिनके बारे में एफएसएल को सबूतों को संभालते समय पता होना चाहिए ।
vi. परिवहन के दौरान छेड़छाड़ को रोकने के लिए पैकेज को सुरक्षित रूप से सील करें। छेड़छाड़-रोधी सील का उपयोग करें।
vii. एफएसएल को दिए जाने वाले प्रदर्श के साथ मामले और किसी भी विशिष्ट निर्देश/आवश्यकताओं के बारे में विस्तृत जानकारी दें । किए जाने वाले परीक्षण, आवश्यक साक्ष्य खोज करने के लिए मुख्य शब्द, आदि का विवरण भी प्रदान किया जा सकता है।
viii. FSL के पास इलेक्ट्रानिक प्रदर्श प्राप्त करने का अपना प्रोटोकॉल हो सकता है। FSL का चयन करते समय उनके द्वारा पालन किए जाने वाले विशिष्ट प्रोटोकॉल को भी समझें।
ix. एफएसएल से पुष्टि रिपोर्ट/रसीद/पावती लें कि उन्हें प्रदर्श प्राप्त हो गये है ।
x. जमा किये प्रदर्श के बारे में जानकारी के साथ केस फाइल को अद्यतन करें, जिसमें जमा करने की तारीख और समय तथा अन्य प्रासंगिक विवरण शामिल करें ।

xi. एफएसएल के साथ नियमित संपर्क में रहें । कोई भी अतिरिक्त जानकारी जो जांच में उनकी सहायता कर सकती है, उन्हें उपलब्ध करावें ।

xii. इलेक्ट्रानिक साक्ष्य की जांच के लिए भारत में वर्तमान में उपलब्ध कुछ फोरेंसिक विज्ञान प्रयोगशालाओं की सांकेतिक सूची इस आदेश के **अनुलग्नक-2** में दी गई है।

15. **भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4)/ भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4) के तहत प्रमाण-पत्र**

भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] इलेक्ट्रानिक साक्ष्य की स्वीकार्यता को नियंत्रित करती है, और इलेक्ट्रानिक दस्तावेज के साथ प्रमाण पत्र की आवश्यकता को निर्दिष्ट करती है।

A. भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4) के अंतर्गत] प्रमाण पत्र की आवश्यकता कब होती है ?

जब मूल उपकरण को ही साक्ष्य के रूप में न्यायालय के समक्ष प्रस्तुत किया जाता है, तो भारतीय साक्ष्य अधिनियम की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के तहत किसी प्रमाण-पत्र की आवश्यकता नहीं होती है। केवल उन मामलों में जहां किसी तथ्य को द्वितीयक इलेक्ट्रानिक साक्ष्य के माध्यम से सिद्ध/खण्डित करना प्रस्तावित है, उनमें भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के तहत प्रमाण पत्र की अनिवार्यता होती है।

B. भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के अंतर्गत प्रमाण पत्र जारी करने के लिए सक्षम प्राधिकार ।

इलेक्ट्रोनिक उपकरण का मालिक अथवा उसके संचालन या संबंधित गतिविधियों के प्रबंधन हेतु जिम्मेदार कोई व्यक्ति यह प्रमाण पत्र जारी कर सकता है। उदाहरण के लिए, इलेक्ट्रोनिक उपकरण/कंप्यूटर का ऑपरेटर, कंप्यूटर का मालिक, सेवा प्रदाता का अधिकारी,

कंप्यूटर/इलेक्ट्रोनिक उपकरण का उपयोगकर्ता, विभागाध्यक्ष जिसमें कंप्यूटर इलेक्ट्रोनिक उपकरण का उपयोग किया जा रहा है, आदि भारतीय साक्ष्य अधिनियम के तहत उक्त प्रमाण पत्र जारी करने के लिए सक्षम हैं। उल्लेखनीय है कि भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4) के तहत प्रमाण पत्र का ''भाग-ए'' इलेक्ट्रानिक साक्ष्य प्रस्तुत करने वाले व्यक्ति द्वारा निर्गत किया जाएगा और ''भाग-बी'' इलेक्ट्रानिक साक्ष्य की जांच करने वाले विशेषज्ञ द्वारा निर्गत किया जाएगा । यह भी उल्लेखनीय है कि भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4) के तहत प्रमाण-पत्रों में हैश मान का उल्लेख करना अनिवार्य किया गया है ।

C. भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4) के अंतर्गत] के अंतर्गत प्रमाण पत्र की आवश्यकताएं/ अवयव ।

द्वितीयक इलेक्ट्रोनिक दस्तावेज की स्वीकार्यता/ग्राह्यता के लिए निम्नलिखित को स्थापित करने की आवश्यकता हैः-

- डेटा की अखंडता (integrity)
- हार्डवेयर/सॉफ्टवेयर और सिस्टम की अखंडता ।
- प्रणाली की सुरक्षा ।

उपर्युक्त आवश्यकताओं को भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] द्वारा द्वितीयक इलेक्ट्रानिक साक्ष्य साबित करने के लिए ध्यान में रखा जाना है। भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के तहत प्रमाण पत्र स्वीकार्यता/ग्राह्यता के बारे में है न कि दस्तावेज की प्रामाणिकता के बारे में । भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) और भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4) के तहत प्रमाण पत्र का प्रारूप इस पुलिस आदेश के अनुलग्नक-**3, 4 और 4ए** के रूप में संलग्न हैं।

D. चूंकि 65बी(4)/63(4) प्रमाणपत्र इनपुट की शुद्धता (correctness) के बजाय इनपुट की नियमितता (regularity) पर केंद्रित है, इसलिए इलेक्ट्रानिक दस्तावेज को साक्ष्य में

स्वीकार्य बनाने के लिए संबंधित प्रमाणपत्रों में उल्लिखित सभी शर्तों को पूरा किया जाना अनिवार्य है । वस्तुतः 65बी(4)/63(4) के अधीन प्रमाणपत्र को यह अनिवार्य रूप से स्थापित करना है कि संबंधित कंप्यूटर/संचार उपकरण का :-

- ठीक से संचालन ।
- वैध नियंत्रण रखने वाले व्यक्ति द्वारा डेटा के प्रसंस्करण/भंडारण के लिए नियमित रूप से उपयोग किया जाता है ।
- इलेक्ट्रानिक आउटपुट, कंप्यूटर/ संचार उपकरण के सामान्य उपयोग के दौरान प्राप्त सूचना से निकालकर प्राप्त किया गया है ।

E. 65बी(4)/63(4) प्रमाण पत्र में निम्नलिखित का भी उल्लेख रहना चाहिएः-

i. सीडी, डीवीडी, मेमोरी कार्ड जैसे रिकार्ड की पहचान, इन्हें कैसे सुरक्षित रखा गया था, आदि ।
ii. इलेक्ट्रानिक दस्तावेज के उत्पादन में शामिल उपकरणों के विवरण/पहचान ।
iii. प्रमाणपत्र जारी करने वाला व्यक्ति संबंधित उपकरण के संचालन या संबंधित गतिविधियों के प्रबंधन के संबंध में जिम्मेदार है,
iv. यदि उपकरण पर प्रमाणित करने वाले व्यक्ति का नियंत्रण है तो ''मेरे सर्वोत्तम ज्ञान के अनुसार'' लिखें, तथा यदि उपकरण पर नियंत्रण नहीं है तो ''मेरे सर्वोत्तम विश्वास के अनुसार'' स्पष्ट लिखा हो ।

ध्यातव्य है कि द्वितीयक इलेक्ट्रानिक साक्ष्य को तब तक साक्ष्य के रूप में पेश नहीं किया जा सकता जब तक कि वह भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के तहत प्रमाण पत्र द्वारा समर्थित न हो । अतः अनुसंधानकर्त्ता आरोप पत्र प्रस्तुत करते समय भारतीय साक्ष्य अधिनियम, 1872 की धारा 65बी(4) [भारतीय साक्ष्य अधिनियम, 2023 की धारा 63(4)] के तहत प्रमाण पत्र प्रस्तुत करने के लिए सभी प्रयास करें ।

16. सूचना प्रौद्योगिकी निरंतर विकसित हो रही है इसलिए यह आवश्यक है कि प्रशिक्षण और प्रौद्योगिकी आवश्यकताओं की निरंतर समीक्षा की जाए और उन्हें लगातार अद्यतन किया जाए। आर्थिक अपराध इकाई, बिहार अनुसंधानकर्त्ता तथा पर्यवेक्षी पदाधिकारी के प्रशिक्षण तथा उन सभी पहलुओं पर शोध के लिये नोडल इकाई होगी जिनमें अपराध कारित करने हेतु साइबर माध्यम का प्रयोग किया गया है । आर्थिक अपराध इकाई, बिहार ईलोक्ट्रोनिक उपकरणों/माध्यमों से जुड़े घटनास्थल की जाँच के लिये पुलिस थानों में उपयोग हेतु आवश्यकत उपकरणों/जाँच किट का मानकीकरण करेगी और संबंधित पुलिस अधीक्षक उन आवश्यक उपकरणों को सभी थाना में उपलब्ध कराएंगे।

17. यह आदेश तत्काल प्रभाव से लागू होगा । अपर पुलिस महानिदेशक, अपराध अनुसंधान विभाग/आर्थिक अपराध इकाई/रेलवे/आतंकवाद निरोधक दस्ता/ सभी क्षेत्रीय पुलिस महानिरीक्षक/पुलिस उप-महानिरीक्षक/वरीय पुलिस अधीक्षक/पुलिस अधीक्षक(रेलवे सहित) अनुपालन सुनिश्चित करेंगे ।

अनुलग्नकः- यथोपरि ।

3/6/2024

पुलिस महानिदेशक,
बिहार, पटना

ज्ञापांक 19 (B) /एल०-2

बिहार पुलिस मुख्यालय
(स्थापना एवं विधि प्रभाग)

पटना, दिनांकः- 03/06/24

प्रतिलिपिः-

1. महानिदेशक, निगरानी अन्वेषण ब्यूरो/बिहार गृह रक्षा वाहिनी एवं अग्निशमन सेवाएं/प्रशिक्षण/बिहार विशेष सशस्त्र पुलिस को सूचनार्थ एवं आवश्यक क्रियार्थ प्रेषित ।

2. अपर पुलिस महानिदेशक, बिहार पुलिस अकादमी/ मुख्यालय/आधुनिकीकरण एवं एस०सी०आर०बी०/वितंतु एवं तकनीकी सेवायें/मद्यिषेध/कमजोर वर्ग/यातायात/आर्थिक अपराध इकाई/ विशेष निगरानी इकाई/ अपराध अनुसंधान विभाग/विशेष शाखा/बजट, अपील एवं कल्याण/ रेलवे/प्रोविजन/

विधि-व्यवस्था/अभियान तथा आतंकवाद निरोधक दस्ता बिहार, पटना को सूचनार्थ एवं आवश्यक क्रियार्थ प्रेषित ।

3. सभी पुलिस महानिरीक्षक/उप-महानिरीक्षक (इकाई/रेलवे सहित), बिहार को सूचनार्थ एवं आवश्यक क्रियार्थ प्रेषित ।

4. सभी वरीय पुलिस अधीक्षक/पुलिस अधीक्षक (इकाई/रेलवे सहित), बिहार को सूचनार्थ एवं आवश्यक क्रियार्थ प्रेषित ।

3/6/2024

पुलिस महानिदेशक,
बिहार, पटना

अनुलग्नक–1

अभिरक्षा की श्रृंखला का प्रपत्र

इलेक्ट्रॉनिक साक्ष्य का विवरण	
थाना/केस नंबर	
अनुसंधानकर्त्ता का नाम, पहचान और ई–मेल/मोबाइल नंबर	
जप्ती की तिथि	
जप्ती का समय	
जप्त ईलक्ट्रॉनिक वस्तुओं/प्रदर्श का विवरण :–	

जप्त प्रत्येक इलेक्ट्रॉनिक प्रदर्श की तकनीकी सूचना

मद क्रमांक	उत्पादक/निर्माता	नमूना/मॉडल	क्रम संख्या	जप्ती की तिथि और समय

अभिरक्षा की श्रृंखला (उक्त प्रत्येक जप्त इलेक्ट्रॉनिक प्रदर्श के लिए)

मद क्रमांक	इलेक्ट्रॉनिक प्रदर्श के मूवमेंट का कारण	किससे प्राप्त किया गया	किसके द्वारा प्राप्त किया गया	तिथि	समय

अनुलग्नक – 2

भारत में उपलब्ध साइबर फॉरेंसिक लैब की संकेतक सूची

(i) विधि विज्ञान प्रयोगशाला, बिहार, पटना

(ii) राष्ट्रीय साइबर फॉरेंसिक विज्ञान प्रयोगशाला: https://ncfl&i4c-mha-gov-in/

(iii) सीएफएसएल (सीबीआई), सीजीओ कॉम्प्लेक्स, नई दिल्ली, ईमेल: dcfsl@cbi-gov-in

(iv) सीएफएसएल, चंडीगढ़, ईमेल: dircfl_chd@dfs-gov-in

(v) सीएफएसएल, हैदराबाद, ईमेल: dircfl_hyd@dfs-gov-in

(vi) सीएफएसएल, कोलकाता, ईमेल: dircfl_kol@dfs-gov-in

(vii) एसीडी, बाबा परमाणु अनुसंधान केंद्र, मुंबई

(viii) राज्य फॉरेंसिक विज्ञान प्रयोगशाला, रेड हिल्स, हैदराबाद, तेलंगाना

(ix) राज्य फॉरेंसिक विज्ञान प्रयोगशाला, गांधी नगर, गुजरात

(x) राज्य फॉरेंसिक विज्ञान प्रयोगशाला, केरल

(xi) राज्य फॉरेंसिक विज्ञान प्रयोगशाला, कर्नाटक।

अनुलग्नक – 3

प्रमाण–पत्र (भारतीय साक्ष्य अधिनियम की धारा 65 (बी)के अधीन)

कांड संख्या .....,थाना....., जिला.....

मैं,.....,पिता/पति....., उम्र (करीब).....वर्ष, पता.....
.....सत्यनिष्ठा से
प्रतिज्ञान करते हुए निम्नांकित घोषणा करता/करती हूँ कि–

1. मैं घोषणा करता/करती हूँ कि मैंने **(दस्तावेजों का विवरण दिया जाय)** का प्रिंट आउट प्रस्तुत किया है।
2. प्रिंट आउट तथा अन्य डिजिटल मेरे स्वामित्व में, मेरे द्वारा रख–रखाव तथा परिचालित किये जाने वाले कंप्यूटर से निकाले/लिए गए हैं तथा उपरोक्त कंप्यूटर डिवाईस और प्रिंटर का विवरण निम्नलिखित हैः–

   ओ0एस0 का नाम.....

   वर्जन.....

   ओ0एस0 के निर्माता.....

   सिस्टम का नाम.....

   सिस्टम के निर्माता.....

   सिस्टम का मॉडल.....

   स्टार्ट अप डिस्क.....

   इंस्टॉल्ड फिजिकल मेमोरी..... (RAM)
3. मैं यह दावा करता/करती हूँ कि कंप्यूटर द्वारा प्रस्तुत किए गए आउटपुट में विहित सूचना कंप्यूटर द्वारा उस समय उत्पन्न/जनित की गई थी जब कंप्यूटर को नियमित रूप से सूचना को संग्रहित या प्रसंस्कृत करने के लिए उपयोग किया जा रहा था, जो साक्ष्य में उल्लेखित कार्यों के उद्देश्य के लिए मेरे द्वारा उस समय नियमित रूप से किए गए कार्यों के अवधि के दौरान किया गया था और इस कंप्यूटर के उपयोग पर मेरा विधिक नियंत्रण है।
4. मैं यह दावा करता/करती हूँ कि उक्त अवधि के दौरान सूचना का प्रकार, जो इलेक्ट्रॉनिक रिकॉर्ड में शामिल है या जिससे ऐसी सूचना का प्रकार शामिल है, नियमित रूप से कंप्यूटर में दर्ज की गई थी जो मेरे और उत्तरदाता (respondent) के साथ मेरे आम संवाद से संबंधित थी।
5. मैं यह दावा करता/करती हूँ कि उक्त अवधि में संचालन के दौरान, कंप्यूटर इलेक्ट्रॉनिक रिकॉर्ड अथवा इसकी सटीकता को प्रभावित किये बिना सही ढंग से कार्य कर रहा था
6. मैं यह दावा करता/करती हूँ कि इलेक्ट्रॉनिक रिकॉर्ड में निहित सूचना उन सूचनाओं से प्राप्त की गई है जिन्हें सामान्य दिनचर्या में कंप्यूटर में दर्ज की गई थी।

स्थानः
दिनांकः–

उद्घोषक

सत्यापनः दिनांक.....को समय.....बजे सत्यापित करता/करती हूँ कि उक्त विषय–वस्तु से संबंधित शपथ–पत्र मेरी जानकारी/विश्वास में सही है।

उद्घोषक

भारतीय साक्ष्य अधिनियम, 2023 की धारा–63(4)(ग) के अधीन प्रमाण–पत्र

भाग–क

(पार्टी द्वारा भरा जाने वाला)

मैं,.....पिता / पति....., पता.....

.....

सत्यनिष्ठा से प्रतिज्ञान करते हुए निम्नांकित घोषणा करता / करती हूँ–

मैं निम्नांकित उपकरण / डिजिटल अभिलेख से इलेक्ट्रॉनिक रिकॉर्ड / डिजिटल रिकॉर्ड के आउटपुट को निकाल कर प्रस्तुत कर रहा / रही हूँ (बॉक्स को टिक किया जाय):–

कंप्यूटर / स्टोरेज मीडिया ☐ डी0वी0आर0 ☐ मोबाईल ☐ फ्लैश ड्राइव ☐ सीडी ☐ डी0वी0डी0 ☐ सर्वर क्लाउड ☐ अन्य ☐

अन्य .....

मेक एवं मॉडल.....रंग: .....

क्रम संख्या.....

आई0एम0ई0आई0 / यू0आई0एन0 / यू0आई0डी0 / एम0ए0सी0 / क्लाउड आई0डी0.....

(जो लागू हो)

तथा उपकरण / डिजिटल रिकॉर्ड से संबंधित अन्य कोई सुसंगत जानकारी, यदि कोई हो..... ..... (विशेष रूप से उल्लेख किया जाय)

डिजिटल उपकरण या डिजिटल रिकॉर्ड स्रोत रिकॉर्ड के सृजन, भंडारण अथवा सूचनाओं के नियमित प्रसंस्करण हेतु मेरे विधिक नियंत्रण में रोजमर्रा के दौरान की गई गतिविधियों हेतु था तथा इस अवधि में कंप्यूटर अथवा संचार उपकरण सही ढंग से काम कर रहा था तथा सामान्य कार्यों के दौरान इसमें नियमित रूप से सुसंगत सूचनाएं दर्ज की जा रही थी। यदि समय के किसी चरण मे कंप्यूटर / डिजिटल उपकरण सही ढंग से कार्य नहीं कर रहा था अथवा कार्यरत नहीं था वैसी परिस्थिति में भी इलेक्ट्रॉनिक / डिजिटल रिकॉर्ड की सटीकता (accuracy) प्रभावित नहीं हुई है। डिजिटल उपकरण अथवा डिजिटल रिकॉर्ड के स्रोत मेरे

स्वामित्व ☐ रख–रखाव ☐ प्रबंधन ☐ परिचालन ☐ में है।

(लागू होने वाले बॉक्स को टिक करें)

मैं घोषणा करता / करती हूँ कि इलेक्ट्रॉनिक / डिजिटल रिकॉर्ड का हैश वैल्यू ..... है जिसे निम्न एल्गोरिद्म (algorithm) से प्राप्त किया गया है –

एस0एच0–1 ☐

एस0एच0ए0–256 ☐

एम0डी0–5 ☐

अन्य– ☐ (विधिक रूप से मानक)

(प्रमाण–पत्र के साथ हैश रिपोर्ट संलग्न करें)

(नाम तथा हस्ताक्षर)

तिथि(DD/MM/YYYY):–.....

समय (IST):–.....बजे (24 घंटों के फॉर्मेट में)

स्थान:–.....

भारतीय साक्ष्य अधिनियम, 2023 की धारा–63(4)(ग) के अधीन प्रमाण–पत्र

भाग–ख

(विशेषज्ञ द्वारा भरा जाने वाला)

मैं,.....पिता / पति....., पता.....

.....

सत्यनिष्ठा से प्रतिज्ञान करते हुए निम्नांकित घोषणा करता / करती हूँ–

प्राप्त इलेक्ट्रॉनिक रिकॉर्ड / डिजिटल रिकॉर्ड के आउटपुट निम्नांकित उपकरण / डिजिटल अभिलेख से निकाले गये हैं (बॉक्स को टिक किया जाय):–

कंप्यूटर / स्टोरेज मीडिया ☐ डी0वी0आर0 ☐ मोबाईल ☐ फ्लैश ड्राइव ☐ सीडी ☐ डी0वी0डी0 ☐ सर्वर क्लाउड ☐ अन्य ☐

अन्य .....

मेक एवं मॉडल.....रंग:.....

क्रम संख्या.....

आई0एम0ई0आई0 / यू0आई0एन0 / यू0आई0डी0 / एम0ए0सी0 / क्लाउड आई0डी0.....

(जो लागू हो)

तथा उपकरण / डिजिटल रिकॉर्ड से संबंधित अन्य कोई सुसंगत जानकारी, यदि कोई हो.....

..... (विशेष रूप से उल्लेख किया जाय)

मैं घोषणा करता / करती हूँ कि इलेक्ट्रॉनिक / डिजिटल रिकॉर्ड का हैश वैल्यू ..... है जिसे निम्न एल्गोरिद्म (algorithm) से प्राप्त किया गया है–

एस0एच0–1 ☐

एस0एच0ए0–256 ☐

एम0डी0–5 ☐

अन्य– ☐ (विधिक रूप से मानक)

(प्रमाण–पत्र के साथ हैश रिपोर्ट संलग्न करें)

(नाम तथा हस्ताक्षर)

तिथि(DD/MM/YYYY):–.....

समय (IST):–.....बजे (24 घंटों के फॉर्मेट में)

स्थान:–.....