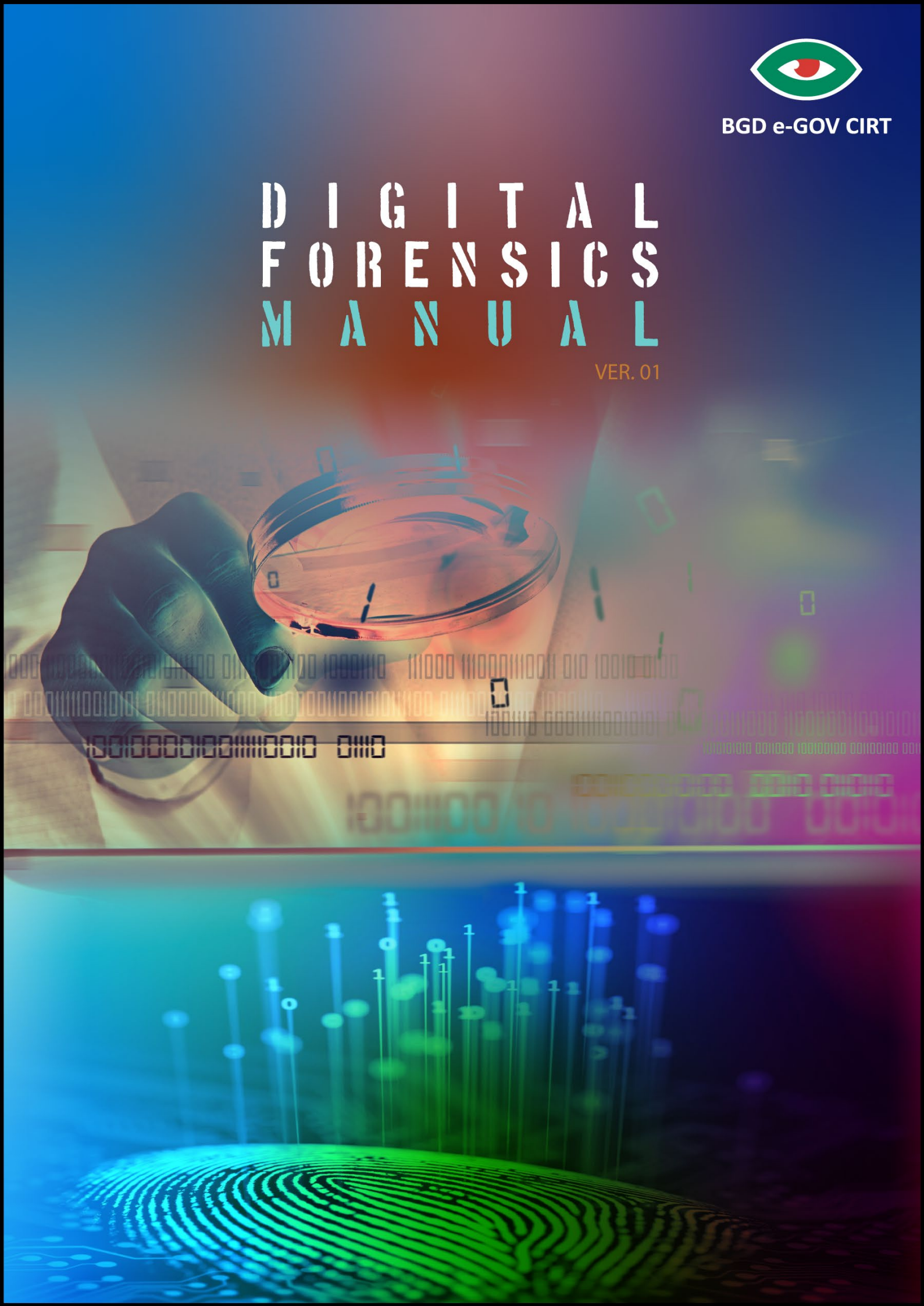
BGD e-GOV CIRT

DIGITAL FORENSICS MANUAL

VER. 01



পটভূমি

ফরেনসিক বিশ্লেষণের মাধ্যমে ফৌজদারী মামলায় তদন্তকারীরা বৈজ্ঞানিক পদ্ধতিতে অপরাধের চিহ্ন (ট্রেস) অনুসরণ করিয়া ঘটনার প্রমাণক খুঁজিয়া বাহির করে এবং দায়ীদের বিচারে সোপর্দ করে। একইরুপে ডিজিটাল পদ্ধতিতে অপরাধ সংঘটিত হইলে ডিজিটাল ফরেনসিক ব্যবহার করিয়া ডিজিটাল ফরেনসিক ল্যাবরেটরির বিশেষজ্ঞবৃন্দ ডিজিটাল পদ্ধতিতে সংঘটিত অপরাধের বিশ্বাসযোগ্য প্রমান আদালতে বা কর্তৃপক্ষের কাছে উপস্থাপন করিয়া থাকেন।

বাংলাদেশে ফৌজদারী ও ডিজিটাল অপরাধ তদন্ত ও বিচারে ডিজিটাল নিরাপত্তা আইন ২০১৮, ফৌজদারী কার্যবিধি ১৮৯৮ (সংক্ষেপে সিআরপিসি), পুলিশ রেগুলেশন ১৯৪৩ (সংক্ষেপে পিআরবি), দন্ডবিধি ১৮৬০, ও সাক্ষ্য আইন ১৮৭২ প্রয়োগ করা হয়। প্রযুক্তির প্রসারের কারণে সনাতন বা ডিজিটাল মাধ্যমে বা ডিজিটাল যন্ত্র ব্যবহার করিয়া সংঘটিত অপরাধ তদন্ত ও অপরাধ উৎঘাটন ও বিচারে ফরেনসিক বিজ্ঞান নতুন নতুন হাতিয়ার ও কৌশল সংযোজন করিতেছে। ইহার সর্বশেষ সংযোজন ডিজিটাল ফরেনসিক। ডিজিটাল মাধ্যমে সংঘটিত অপরাধে অতিরাষ্ট্রিক মাত্রা যুক্ত হওয়ায় দেশ-বিদেশের আদালতে অপরাধের সাক্ষ্য প্রমান গ্রহণযোগ্যভাবে উপস্থাপন করিবার নিমিত্তে আন্তর্জাতিক মান ও পদ্ধতি অনুসরণ আবশ্যক।

ডিজিটাল অপরাধগুলো সাধারণত দেশের সীমানা ছাড়িয়েও (Borderless) যাইতে পারে এবং এই অপরাধগুলো সেকেন্ডের ভগ্নাংশেও ঘটিতে পারে। এসব অপরাধের সহিত অনেক সময় শুধু দেশীয় আদালত যথেষ্ট নয়, আন্তর্জাতিক আদালতের শরণাপন্ন হইতে হয়। সুতরাং ডিজিটাল আলামত বিশ্লেষণ হইতে প্রাপ্ত ফলাফলসমূহ দেশীয় ও আন্তর্জাতিক উভয় আদালতে গ্রহণযোগ্য হওয়ার লক্ষ্যে নির্দিষ্ট স্ট্যান্ডার্ড অনুসরন পালন করা বাঞ্ছনীয়।

অত্র নির্দেশিকাটি ডিজিটাল নিরাপত্তা আইন ও বিধিমালার অনুসরণে জাতীয়ভাবে স্বীকৃত আন্তর্জাতিক আইনী কাঠামোর আলোকে ডিজিটাল ফরেনসিক ল্যাবরেটরির নিমিত্তে একটি প্রয়োজনীয় ও সহায়ক দলিল হিসাবে প্রণয়ন করা হইয়াছে।

প্রস্তাবনা

নং. .....। ডিজিটাল নিরাপত্তা এজেন্সী ডিজিটাল নিরাপত্তা আইন ২০১৮ এর ১০ ও ১১ ধারা এবং ডিজিটাল নিরাপত্তা বিধি ২০২০ এর ১৩-১৬ বিধিতে প্রদত্ত ক্ষমতাবলে সরকারের অনুমোদনক্রমে এতদ্বারা ডিজিটাল ফরেনসিক ল্যাব প্রতিষ্ঠা, ব্যবস্থাপনা এবং ইলেকট্রনিক যন্ত্রপাতি থেকে ডিজিটাল সাক্ষ্য উদ্ধার ও ফরেনসিক বিশ্লেষনের নিমিত্তে নিম্নরূপ গাইডলাইন প্রণয়ন ও জারি করিল:

সূচীপত্র

অংশ-১: প্রারম্ভিক ৮

১। শিরোনাম ও প্রবর্তন: ৮

২। সংজ্ঞা: ৮

অংশ-২: গাইডলাইন প্রণয়নের উদ্দেশ্য ও পরিধি ৮

৩। গাইডলাইন প্রণয়নের লক্ষ্য ও উদ্দেশ্য: ৮

৪। গাইডলাইনের প্রয়োগ ও পরিধি: ৮

অংশ-০৩: ডিজিটাল ফরেনসিক ৯

৫। ইলেকট্রনিক বা ডিজিটাল সাক্ষ্যের স্বীকৃতি: ৯

৬। ডিজিটাল সাক্ষ্য প্রক্রিয়াকরণ, ইত্যাদির চ্যালেঞ্জসমূহ: ৯

৭। ডিজিটাল সাক্ষ্যের গ্রহণযোগ্যতার বৈশিষ্ট্য: ৯

৮। ডিজিটাল সাক্ষ্য বিশ্লেষণের নীতি: ১০

অংশ-০৪: ডিজিটাল ফরেনসিক ল্যাব ব্যবস্থাপনা ১০

৯। ডিজিটাল ফরেনসিক ল্যাব এর অবস্থান: ১০

(ক) স্থান নির্বাচন: ১০

(খ) ভৌত নিরাপত্তা সংক্রান্ত বিষয়াদি: ১১

(গ) ফরেনসিক ল্যাব এর অবকাঠামোর অংশসমূহ: ১১

(ঘ) ফরেনসিক ল্যাব এর দর্শনার্থী প্রবেশ সংক্রান্ত নিয়মাবলী: ১২

১০। ডিজিটাল ফরেনসিক ল্যাব এর জনবল: ১২

অংশ-০৫: ডিজিটাল ফরেনসিক ল্যাব এর উপকরণ ১২

১১। যন্ত্রপাতি: ১২

১২। সফটওয়্যার সংক্রান্ত বিষয়াদি: ১৩

১৩। হার্ডওয়্যার সংক্রান্ত বিষয়াদি: ১৩

১৪। হার্ডওয়্যার ও সফটওয়্যার এর তালিকা: ১৩

১৫। টুলস এবং এক্সেসরিস: ১৪

অংশ-০৬ ডিজিটাল ফরেনসিক কেস ব্যবস্থাপনা ১৪

১৬। কেস ব্যবস্থাপনা পদ্ধতি: ১৪

১৭। ফরেনসিক পরীক্ষার অধিযাচন (Requisition): ১৫

১৮। ফরেনসিক কেস নিবন্ধন: ১৫

১৯। ফরেনসিক পরীক্ষার চাহিদা পর্যালোচনা:- ১৫

২০। ফরেনসিক পরীক্ষার তথ্য প্রমাণ নির্ধারণ (Evidence Assessment): ১৬

২১। ডিজিটাল নমুনা বা আলামত বিশ্লেষণ ১৬

২২। ডিজিটাল সাক্ষ্য-প্রমান প্রত্যর্পণ: ১৭

২৩। ফরেনসিক কেসের সমাপ্তি ও প্রতিবেদন: ১৭

অংশ-০৭: ফরেনসিক পরীক্ষার পর্যায় ১৭

২৪। ডিজিটাল ফরেনসিক পরীক্ষার পর্যায়সমূহ: ১৭

অংশ-০৮: ডিজিটাল নমুনা বা আলামত অধিগ্রহণ ও উপাত্ত আহরণ ১৮

২৫। উপাত্ত অধিগ্রহণ প্রক্রিয়া: ১৮
২৬। কম্পিউটার সিস্টেম হইতে উপাত্ত অধিগ্রহণ: ১৮
(৭) ফরেনসিক ইমেজ ফরম্যাট: ১৯
(৯) ডিজিটাল নমুনা বা আলামতের ইমেজ ফাইল যাচাইকরণ: ১৯
(১০) ফরেনসিক কপির ব্যাকআপ: ২০
২৭। মোবাইল ডিভাইস হইতে উপাত্ত আহরণ (Extraction): ২০
(৪) উপাত্ত আহরণের ফাইল ফরম্যাট: ২১
(৫) মোবাইল ডিভাইসের আলামত আহরণ প্রক্রিয়া: ২২
অংশ-০৯: ডিজিটাল ফরেনসিক নমুনা বা আলামত পরীক্ষণ ২৪
২৯। কম্পিউটার পরীক্ষণ পদ্ধতি: ২৪
৩০। মোবাইল ডিভাইস পরীক্ষণ পদ্ধতি: ২৬
অংশ-১০: ডিজিটাল ফরেনসিক নমুনা বা আলামত বিশ্লেষণ ২৭
৩১। ফরেনসিক নমুনা বা আলামত বিশ্লেষণ: ২৭
৩২। কম্পিউটার সিস্টেম বিশ্লেষণ: ২৭
৩৩। মোবাইল ডিভাইস এর উপাত্ত বিশ্লেষণ: ২৯
(২) মোবাইল ডিভাইসের ডিজিটাল চিহ্নের (Trace) শ্রেণিবিন্যাস: ২৯
(৩) মোবাইল ডিভাইসের বিভিন্ন প্রকার চিহ্ন আহরণ পদ্ধতি: ২৯
অংশ-১১: ফরেনসিক প্রতিবেদন প্রস্তুতকরণ ও উপস্থাপন ২৯
৩৫। ফরেনসিক ফলাফল উপস্থাপন: ৩০
৩৬। ডিজিটাল সাক্ষ্য প্রমাণাদির গ্রহণযোগ্যতা: ৩০
অংশ ১২: ডিজিটাল ফরেনসিক ল্যাবরেটরির অনুসরণীয় মানদণ্ড ৩০
অংশ-১৩: ফরেনসিক ল্যাব এর গুনগতমান নিশ্চিতকরণ (Quality Assurance) ৩১
৩৮। গুনগতমান নিশ্চিতকরণ: ৩১
৩৯। গুনগতমান নিশ্চিতকরণের উপাদান (Component) ৩১
অংশ-১৪: বিবিধ বিষয়াবলী ৩১
৪০। জরুরি পরিস্থিতিতে মহাপরিচালকের ক্ষমতা: ৩১
৪১। নমুনা বা আলামতের তথ্য-উপাত্ত সংরক্ষণ: ৩১
৪২। ফরেনসিক পরীক্ষা সম্পাদনের সময়সীমা: ৩২
৪৩। তথ্যে-উপাত্তের গোপনীয়তা: ৩২
৪৪। ডিজিটাল ফরেনসিক ল্যাব পরিচালনা: ৩২
৪৫। নির্দেশ প্রদানের ক্ষমতা: ৩২
৪৬। অব্যাহতি: ৩২
৪৭। গাইডলাইনের সীমাবদ্ধতা: ৩২
পরিশিষ্ট-০১: ডিজিটাল ফরেনসিক ল্যাব স্থাপন ও মাননিয়ন্ত্রণ ৩৩
পরিশিষ্ট-০২: ডিজিটাল ফরেনসিক ল্যাব এর জনবল ৩৪
পরিশিষ্ট-০৩: ডিজিটাল ফরেনসিক ল্যাব এর জনবলের দক্ষতা ৩৫
পরিশিষ্ট-০৪: ডিজিটাল ফরেনসিক পরীক্ষার কেস অধিযাচন ফরম ৩৭
পরিশিষ্ট-০৫: চেইন অফ কাস্টডি ৩৯

পরিশিষ্ট-০৬: ডিজিটাল নমুনা বা আলামত বিশ্লেষণ প্রক্রিয়া..... ৪১
পরিশিষ্ট-০৭: নমুনা বা আলামত অধিগ্রহণ প্রক্রিয়া..... ৪২
পরিশিষ্ট-০৮: ডিজিটাল নমুনা বা আলামত অধিগ্রহণ প্রক্রিয়ার ফ্লো-চার্ট..... ৪৫
পরিশিষ্ট-০৯: কম্পিউটার পরীক্ষণ প্রক্রিয়ার ফ্লো-চার্ট..... ৪৬
পরিশিষ্ট-১০: ফরেনসিক নমুনা বা আলামত বিশ্লেষণ..... ৪৭
পরিশিষ্ট-১১: নথিভূক্তকরণ ও প্রতিবেদন প্রস্তুতকরণ..... ৪৯
পরিশিষ্ট-১২ক: ISO/IEC/BDS 17025 টেষ্টিং ও ক্যালিব্রেশন পরীক্ষাগারের যোগ্যতার সাধারণ মাপকাঠি..... ৫১
পরিশিষ্ট-১২খ: ISO/IEC/BDS 15489 রেকর্ডস ব্যবস্থাপনা..... ৫১
পরিশিষ্ট-১২গ: ISO/IEC/BDS 27037 ডিজিটাল সাক্ষ্য সনাক্তকরণ, সংগ্রহ, অধিগ্রহণ এবং সংরক্ষণ নির্দেশিকা..... ৫১
পরিশিষ্ট-১২ঘ: ISO/IEC/BDS 27041 ঘটনা তদন্ত পদ্ধতির গ্রহণযোগ্যতা ও উপযুক্ততা নিরুপণের মাপকাঠি/নির্দেশিকা..... ৫১
পরিশিষ্ট-১২ঙ: ISO/IEC/BDS 27042 ডিজিটাল সাক্ষ্য বিশ্লেষণ ও স্পষ্টিকরণ নির্দেশিকা..... ৫১
পরিশিষ্ট-১২চ: ISO/IEC/BDS 27043 ঘটনা তদন্তের পদ্ধতি ও নীতিমালা..... ৫১
পরিশিষ্ট-১২ছ: ISO/IEC/BDS 27050 ইলেকট্রনিক ডিসকভারি..... ৫১
পরিশিষ্ট-১৩: গুনগতমান নিশ্চিতকরণ চেকলিস্ট..... ৫২

অংশ-১: প্রারম্ভিক

১। শিরোনাম ও প্রবর্তন:

(১) এই গাইডলাইন ডিজিটাল ফরেনসিক ল্যাব গাইডলাইন, ২০২২ নামে অভিহিত হইবে।

(২) ডিজিটাল নিরাপত্তা এজেন্সি, আদেশ দ্বারা, যে তারিখ নির্ধারণ করিবে সেই তারিখে এই গাইডলাইন কার্যকর হইবে।

২। সংজ্ঞা:

এই গাইডলাইনে ব্যবহৃত যে সকল শব্দ বা অভিব্যক্তির সংজ্ঞা এই গাইডলাইনে প্রদান করা হয় নাই, সেই সকল শব্দ বা অভিব্যক্তি তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬, ডিজিটাল নিরাপত্তা আইন, ২০১৮ বা ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি ১৪ এ বর্ণিত ISO/IEC/BDS 17025, ISO/IEC/BDS 15489, ISO/IEC/BDS 27037, ISO/IEC/BDS 27041, ISO/IEC/BDS 27042, ISO/IEC/BDS 27043, ISO/IEC/BDS 27050 এ যে অর্থে ব্যবহৃত হইয়াছে সেই অর্থে ব্যবহৃত হইবে।

অংশ-২: গাইডলাইন প্রণয়নের উদ্দেশ্য ও পরিধি

৩। গাইডলাইন প্রণয়নের লক্ষ্য ও উদ্দেশ্য:

ডিজিটাল ফরেনসিক হইল ফরেনসিক বিজ্ঞানের একটি শাখা যাহা কোনো কম্পিউটার, ডিজিটাল ডিভাইস বা অন্যান্য ডিজিটাল স্টোরেজ মিডিয়াতে ধারণকৃত উপাত্ত সনাক্তকরণ, অধিগ্রহণ, প্রক্রিয়াকরণ, বিশ্লেষণ, ইত্যাদির উপর আলোকপাত করে।[১]

এই গাইডলাইন প্রণয়নের মুখ্য উদ্দেশ্য হইতেছে ডিজিটাল ফরেনসিক ল্যাবরেটরি প্রতিষ্ঠা, ব্যবস্থাপনা এবং ইলেকট্রনিক যন্ত্রপাতি হইতে ডিজিটাল সাক্ষ্য উদ্ধার ও ফরেনসিক বিশ্লেষণ করিয়া ঘটনার সত্যতা যাচাই ও অপরাধ বা দূর্ঘটনার দায়দায়িত্ব নিরুপণের নিমিত্তে জাতীয় ও আন্তর্জাতিকভাবে স্বীকৃত নীতি-নির্দেশনা বাস্তবায়নে সহায়তা করাসহ ডিজিটাল ফরেনসিক ল্যাব হইতে প্রাপ্ত ডিজিটাল আলামতসমূহ দেশীয় ও আন্তর্জাতিক আদালতসমুহে অপরাধ বিচার ব্যবস্থায় উপস্থাপনের যোগ্য করে তোলা।

এই গাইডলাইন ডিজিটাল ফরেনসিক ল্যাব এর পরিচালনা ও, ক্ষেত্রমত, ব্যবস্থাপনার মৌলিক নির্দেশনা হিসেবে ভূমিকা পালন করিবে।

৪। গাইডলাইনের প্রয়োগ ও পরিধি:

এই গাইডলাইন ডিজিটাল নিরাপত্তা আইন, ২০১৮ ধারা ১০ এর অধীন স্থাপিত বা প্রত্যায়িত বা স্বীকৃত এবং ধারা ১১ এ বিধৃত মানদন্ডের উদ্দেশ্য পূরণকল্পে, সকল ডিজিটাল ফরেনসিক ল্যাব এর ক্ষেত্রে প্রযোজ্য হইবে (*পরিশিষ্ট ০১: ডিজিটাল ফরেনসিক ল্যাব স্থাপন ও মাননিয়ন্ত্রণ দ্রষ্টব্য*)।

[1] INTERPOL Global guidelines for digital forensic laboratories, 2.1 Digital Forensics

অংশ-০৩: ডিজিটাল ফরেনসিক

৫। ইলেকট্রনিক বা ডিজিটাল সাক্ষ্যের স্বীকৃতি:

(১) কম্পিউটার, ডিজিটাল ডিভাইস বা অন্যান্য ডিজিটাল স্টোরেজ সিস্টেমে (যেমন-ল্যাপটপ, স্মার্টফোন, সার্ভার, ডিজিটাল ভিডিও রেকর্ডার, সিসিটিভি সিস্টেম, ড্রোন, জিপিএস সিস্টেম, গেম কনসোল, ইত্যাদি) রক্ষিত মূল্যবান কোনো তথ্য বা উপাত্ত যাহা সাধারণভাবে কোনো মামলা বা মামলার তদন্তের প্রয়োজনে ইলেকট্রনিক বা ডিজিটাল সাক্ষ্য হিসেবে গ্রহণযোগ্য ও স্বীকৃত হয়।

(২) ডিজিটাল ফরেনসিকের প্রধান লক্ষ্য হইতেছে ইলেকট্রনিক সাক্ষ্য-প্রমাণ হইতে যথাযথ ফরেনসিক প্রক্রিয়ার মাধ্যমে-

(ক) কোনো তথ্য বা উপাত্ত আহরণ করা;
(খ) উক্ত উপাত্তকে কার্যকর তথ্যে পরিনত করা; এবং
(গ) কোনো আইনগত কার্যধারায় উহার ফলাফল উপস্থাপন করা।

৬। ডিজিটাল সাক্ষ্য প্রক্রিয়াকরণ, ইত্যাদির চ্যালেঞ্জসমূহ:

ডিজিটাল সাক্ষ্য প্রক্রিয়াকরণ ও বিশ্লেষণের ক্ষেত্রে, এতদসংক্রান্ত অন্যান্য বিষয়ের মধ্যে, নিম্নবর্ণিত বিষয়াদি বিবেচনা করিতে হইবে, কেননা-

(ক) ইলেকট্রনিক উপাত্ত দেশের গণ্ডি ছাড়িয়ে বিভিন্ন ভৌত অবস্থানে বিক্ষিপ্ত বা, ক্ষেত্রমত, বিস্তৃত অবস্থায় থাকিতে পারে;

(খ) ইলেকট্রনিক উপাত্ত অনায়াসে এবং মুহূর্তের মধ্যে এক দেশ হইতে অন্য দেশে স্থানান্তর করা যায়;

(গ) ইলেকট্রনিক উপাত্ত সহজেই পরিবর্তনযোগ্য, কেননা একটি কীবোর্ড বাটন প্রেস করেই ইহাকে পরিবর্তিত, ওভাররাইট, ক্ষতিগ্রস্ত বা ধ্বংস করা যায়;

(ঘ) মূল ইলেকট্রনিক উপাত্তের কোনো ক্ষতি সাধন ছাড়াই মৌলিকত্ব বজায় রাখিয়া এবং উহার অভেদ্যতা বা শুদ্ধতা (Integrity) অক্ষুণ্ণ রাখিয়া অনুলিপি করা যায়;

(ঙ) ভৌত অন্যান্য ফরেনসিক প্রমাণের (যেমন- গুলির খোসা, ফাইবার, ইত্যাদি) বিপরীতে ডিজিটাল সাক্ষ্য প্রমাণের আয়ুষ্কাল (Life Span) সীমিত কেননা উহা যেকোনো সময় অকেজো বা অব্যবহারযোগ্য হইতে পারে (যেমন- একটি স্মার্ট ফোন, যাহা পাঁচ বৎসর পর নাও চালু করা যাইতে পারে) ।

৭। ডিজিটাল সাক্ষ্যের গ্রহণযোগ্যতার বৈশিষ্ট্য:

ডিজিটাল সাক্ষ্য-প্রমাণ গ্রহণযোগ্যতার বৈশিষ্ট্যসমূহ নিম্নরূপ, যথা: -

(ক) নিরীক্ষাযোগ্যতা (Auditability): ল্যাবে নিযুক্ত সুপারভাইজার ও বিশেষজ্ঞ কর্তৃক সম্পন্নকৃত কার্যক্রম আবশ্যিকভাবে একজন নিরপেক্ষ মূল্যায়নকারী বা একটি মূল্যায়নকারী টিম কর্তৃক নিরীক্ষাযোগ্য হইতে হইবে;

(খ) পুনরাবৃত্তিযোগ্যতা (Repeatability): যে যন্ত্রপাতি ও পদ্ধতি ব্যবহার করিয়া ডিজিটাল সাক্ষ্য-প্রমাণাদির বিশ্লেষণ বা পরীক্ষা করিয়া যে ফলাফল পাওয়া যায়, পরবর্তীতে একই যন্ত্রপাতি ও পদ্ধতি ব্যবহার করিয়া বিশ্লেষণ বা পরীক্ষা করা হইলে একই ফলাফল প্রাপ্ত হইতে হইবে;

(গ) পুনরুৎপাদনযোগ্যতা (Reproductability): যে যন্ত্রপাতি ও পদ্ধতি ব্যবহার করিয়া ডিজিটাল সাক্ষ্য-প্রমাণাদির বিশ্লেষণ বা পরীক্ষা করিয়া যে ফলাফল পাওয়া যায়, পরবর্তীতে ভিন্ন যন্ত্রপাতি ও পদ্ধতি ব্যবহার করিয়া বিশ্লেষণ বা পরীক্ষা করা হইলে একই ফলাফল প্রাপ্ত হইতে হইবে; এবং

(ঘ) ন্যায্যতা (Justifiability): ডিজিটাল সাক্ষ্য-প্রমাণাদির সকল বিশ্লেষণ বা পরীক্ষা ন্যায্যতার ভিত্তিতে সম্পন্ন করিতে হইবে যাহাতে উহা ভিন্ন ভিন্ন বিচারিক ব্যবস্থায় একইরূপ ডিজিটাল সাক্ষ্যের বিনিময় সহজসাধ্য হয়।

৮। ডিজিটাল সাক্ষ্য বিশ্লেষণের নীতি:

ডিজিটাল সাক্ষ্য বিশ্লেষণের ক্ষেত্রে নিম্নবর্ণিত নীতিসমুহ পরিপালন করিতে হইবে-

(ক) আইনগত পদ্ধতি অনুসরণ ব্যতীত কোনো ডিজিটাল সাক্ষ্য-প্রমাণ সংগ্রহ করা যাইবে না;

(খ) ডিজিটাল সাক্ষ্য-প্রমাণ বিশ্লেষণকারী বা পরীক্ষাকারী সুপারভাইজার ও বিশেষজ্ঞকে ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধান অনুসারে উপযুক্ত প্রশিক্ষণ, দক্ষতা ও যোগ্যতা থাকিতে হইবে;

(গ) ডিজিটাল সাক্ষ্য-প্রমাণাদির বিশ্লেষণ বা পরীক্ষা কার্যক্রম পরিচালনাকালে কোন অবস্থাতেই ডিজিটাল সাক্ষ্য-প্রমাণাদির উপাত্তে কোনোরূপ পরিবর্তন করা যাইবে না; উক্ত মূল উপাত্তে প্রবেশ করিতে হইলে বা ডিজিটাল সিস্টেমের সেটিং পরিবর্তন করিবার প্রয়োজন হইলে কেবল উহার যৌক্তিকতা (Justification) নিশ্চিত করিয়া উক্ত কার্য সম্পন্ন করিতে হইবে;

(ঘ) ডিজিটাল সাক্ষ্য-প্রমাণাদির বিশ্লেষণ বা পরীক্ষার সকল পর্যায়ে ধারাবাহিকভাবে রেকর্ড লগ সংরক্ষণ করিতে হইবে যাহাতে উহা পরবর্তীতে নিরপেক্ষভাবে নিরীক্ষাযোগ্য ও পুনরাবৃত্তিযোগ্য হয়।

অংশ-০৪: ডিজিটাল ফরেনসিক ল্যাব ব্যবস্থাপনা

এই অংশ একটি ডিজিটাল ফরেনসিক ল্যাব প্রতিষ্ঠার জন্য প্রয়োজনীয় প্রক্রিয়াসমূহ- ল্যাব প্রাঙ্গন পরিকল্পনা গ্রহণ, প্রয়োজনীয় সম্পদ সংগ্রহ এবং ল্যাব এর দৈনন্দিন কার্যকলাপ ও এর রক্ষণাবেক্ষণ ব্যাখ্যা করে।

৯। ডিজিটাল ফরেনসিক ল্যাব এর অবস্থান:

ডিজিটাল ফরেনসিক ল্যাব এর অবস্থান নির্ধারণের ক্ষেত্রে বা, ক্ষেত্রমত, উহা স্থাপনকল্পে, পরিবেশ ও প্রতিবেশ ব্যবস্থাপনা গুরুত্বপূর্ণ বিধায় নিম্নবর্ণিত বিষয়াদি বিবেচনা করিতে হইবে, যথা:-

(ক) স্থান নির্বাচন:

নিম্নবর্ণিত বিষয়াদি বিবেচনাক্রমে ডিজিটাল ফরনেসিক ল্যাব এর স্থান নির্বাচন করিতে হইবে, যথা:-

(অ) ফরনেসিক ল্যাব এর যন্ত্রপাতি পরিচালনের ক্ষেত্রে পর্যাপ্ত ও নিরাপদ বিদ্যুৎ সরবরাহের ব্যবস্থা থাকিতে হইবে এবং এতৎপ্রয়োজনে বিদ্যুৎ সরবরাহের ব্যাকআপ (যেমন, জেনারেটর, ইউপিএস ইত্যাদি) এর ব্যবস্থা থাকিতে হইবে;

(আ) ফরেনসিক ল্যাব এর স্থান ভবনের উপরের দিকে অবস্থিত হইলে ইলেকট্রনিক সাক্ষ্য-প্রমাণাদি স্থানান্তরের জন্য পর্যাপ্ত লিফট এর ব্যবস্থা থাকিতে হইবে;

(ই) ফরেনসিক ল্যাব এর ভৌত কাঠামোগত পরিবেশ যাহাতে বিঘ্নিত না হয়, সেইজন্য ডিজিটাল ফরেনসিক এর স্থান পরিবেশগত ক্ষতি, প্রাকৃতিক দুর্যোগ ও মানবসৃষ্ট ক্ষতি থেকে সুরক্ষিত হইতে হইবে;

(ঈ) হার্ডওয়্যার ও অন্যান্য যন্ত্রপাতি রক্ষার জন্য পর্যাপ্ত শীতাতপ নিয়ন্ত্রণের ব্যবস্থা থাকিতে হইবে;

(উ) ফরনেসিক ল্যাব বাইরের যে কোনো আক্রমণ হইতে রক্ষার জন্য যথাযথ নিরাপত্তা ব্যবস্থা থাকিতে হইবে।

(খ) ভৌত নিরাপত্তা সংক্রান্ত বিষয়াদি:

ফরনেসিক ল্যাবে রক্ষিত ইলেকট্রনিক সাক্ষ্য-প্রমাণাদির ভৌত নিরাপত্তা প্রদানসহ উহার জনবল,সফটওয়্যার ও হার্ডওয়্যার এর নিরাপত্তা বিধানের সক্ষমতা থাকিতে হইবে। সে উদ্দেশ্যে নিম্নোক্ত ব্যবস্থাদি নিশ্চিত করা আবশ্যক:

(অ) ফরেনসিক ল্যাবে অবৈধ, অননুমোদিত প্রবেশ প্রতিরোধের জন্য নিবিড় নজরদারির ব্যবস্থা থাকিতে হইবে এবং এতদুদ্দেশ্যে ফরনেসিক ল্যাবে সিসি ক্যামেরাসহ অন্যান্য নিরাপত্তামূলক ব্যবস্থা স্থাপন করিতে হইবে;

(আ) সিস্টেমে অনুপ্রবেশ প্রতিরোধের জন্য ইলেকট্রনিক কি-প্যাড, সোয়াইপ কার্ড, বায়োমেট্রিক আক্সেস, ইত্যাদি স্থাপন করিতে হইবে;

(ই) অগ্নিদুর্ঘটনা জনিত নিরাপত্তা নিশ্চিতের জন্য প্রয়োজনীয় সনাক্তকরণ ও অগ্নি-নির্বাপণ যন্ত্রপাতির মজুদ থাকিতে হইবে;

(ঈ) নিরবিচ্ছিন্ন বিদ্যুৎ সরবরাহ নিশ্চিতের জন্য পর্যাপ্ত পাওয়ার সকেট, ফিউজ, সার্কিট ব্রেকার, ইত্যাদি যন্ত্রপাতি স্থাপন করিতে হইবে;

(উ) ক্ষতিকর ইলেক্ট্রো-স্ট্যাটিক ডিসচার্জ প্রতিরোধের জন্য ল্যাব এর মেঝেতে এন্টি স্ট্যাটিক (Anti Static) ব্যবস্থা থাকিতে হইবে;

(ঊ) ল্যাব এর নিজস্ব ইন্টারনেট ব্যবস্থায় বাইরের অনুপ্রবেশ প্রতিরোধের জন্য প্রযোজ্য ক্ষেত্রে সিগনাল জ্যামিং (Signal Jamming) সিস্টেম থাকিতে হইবে;

(ঋ) ডিজিটাল নমুনা বা আলামত সংরক্ষণ ও সার্ভার কক্ষ পর্যাপ্ত শীতাতপ নিয়ন্ত্রনের আওতায় থাকিতে হইবে;

(এ) ডিজিটাল নমুনা বা আলামতের অফসাইট সংরক্ষণের পর্যাপ্ত ব্যবস্থা থাকিতে হইবে;

(ঐ) ডিজিটাল নমুনা বা আলামত আইনগত বিধি-বিধান অনুসারে সংরক্ষণের ব্যবস্থা থাকিতে হইবে।

(গ) ফরেনসিক ল্যাব এর অবকাঠামোর অংশসমূহ:

(অ) **অভ্যর্থনা কক্ষ:** অভ্যর্থনা কক্ষে ইলেক্ট্রনিক নমুনা বা আলামত সংগ্রহ বা সরবরাহ করা যাইতে পারে, তবে ফরেনসিক ল্যাবে অবৈধ অনুপ্রবেশ রোধকল্পে, উক্ত স্থান মূল ল্যাব প্রবেশ দরজা দ্বারা পৃথক থাকিতে হইবে;

(আ) **ইলেক্ট্রনিক নমুনা বা আলামত সংরক্ষণাগার:** এই স্থানটি কেবল ইলেক্ট্রনিক নমুনা বা আলামত সংরক্ষনের স্থান হিসেবে নিবেদিত হইতে হইবে, তবে উক্ত কক্ষে সার্ভারও রাখা যাইবে;

(ই) **ইলেক্ট্রনিক নমুনা বা আলামত প্রক্রিয়ার স্থান:** ইলেকট্রনিক নমুনা বা আলামতের প্রক্রিয়াকরণ স্থান ফরেনসিক বিশেষজ্ঞের ডেস্ক হইতে পৃথক হইতে হইবে এবং উক্ত স্থান ইলেকট্রনিক নমুনা বা আলামত পৃথকীকরণ, একত্রীকরণ, তালিকাকরণ ও ইমেজ গ্রহণের নির্ধারিত স্থান হিসেবে ব্যবহৃত হইবে;

(ঈ) **ল্যাবরেটরি:** ইলেকট্রনিক নমুনা বা আলামতের ধরন অনুযায়ী ফরেনসিক ল্যাব এর এক বা একাধিক কক্ষ থাকিতে পারে (যেমন, কম্পিউটার ফরেনসিক ল্যাব, মোবাইল ফরেনসিক ল্যাব, ড্রোন ফরেনসিক ল্যাব, ইত্যাদি);

(উ) **কর্মকর্তাদের দাপ্তরিক ডেস্ক:** কর্মকর্তাদের অফিসের দাপ্তরিক কাজের ডেস্ক ফরনেসিক বিশ্লেষণের

কর্মসম্পাদন স্থান হইতে পৃথক হইতে হইবে;

(ঊ) **নিজস্ব ইন্টারনেট সুবিধা:** ফরনেসিক ল্যাবে ম্যালওয়্যার ও ভাইরাসের আক্রমণ হইতে সুরক্ষিত ইন্টারনেট সুবিধা থাকিতে হইবে। এই ইন্টারনেট হইতে ডার্ক ওয়েব ও ডিপ ওয়েবে প্রবেশের সুবিধা থাকিতে হইবে।

(ঘ) ফরেনসিক ল্যাব এর দর্শনার্থী প্রবেশ সংক্রান্ত নিয়মাবলী:

(অ) ডিজিটাল ফরনেসিক ল্যাবে সুপারভাইজার, ফরেনসিক বিশেষজ্ঞ ও দায়িত্বপ্রাপ্ত কর্মচারীর অনুমোদিত প্রবেশাধিকার সংরক্ষিত থাকিবে; অন্য কোনো ব্যক্তির উক্ত ল্যাবে প্রবেশ করিতে হইলে ল্যাব কর্তৃপক্ষের অনুমোদন থাকিতে হইবে;

(আ) ল্যাব এ প্রবেশাধিকার সীমিত ও নির্দিষ্ট সময়ের জন্য হইতে হইবে এবং ল্যাব কর্তৃপক্ষ অনুমোদিত নয় এমন কোনো কর্মকান্ড পরিচালনা করা যাইবে না;

(ই) ফরেনসিক ল্যাব এর দর্শনার্থীগণ প্রবেশকালে আবশ্যিকভাবে নিবন্ধন করিতে হইবে;

(ঈ) ল্যাব এ প্রবেশের ক্ষেত্রে দর্শনার্থীকে একটি সাময়িক আইডি কার্ড ইস্যু করা যাইতে পারে;

(এ) ডিজিটাল ফরেনসিক ল্যাব এর একজন কর্মকর্তা সার্বক্ষণিকভাবে দর্শনার্থীর সহিত গাইড (Escort) হিসেবে থাকিবেন;

(ঐ) ফরেনসিক ল্যাবে অবশ্যই ল্যাব পরিদর্শনের নিয়মাবলী লিখিত ও দৃশ্যমান থাকিতে হইবে;

(ও) ল্যাব এ ইলেকট্রনিক আলামত ও যন্ত্রপাতি স্পর্শকরণ, ছবিতোলা, খাদ্য ও পানীয় বহন সংক্রান্ত নিষেধাজ্ঞা স্পষ্টভাবে উল্লেখিত থাকিতে হইবে।

১০। ডিজিটাল ফরেনসিক ল্যাব এর জনবল:

(ক)ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি ১৬ (পরিশিষ্ট ০২: ডিজিটাল ফরেনসিক ল্যাব এর জনবল) এর বিধান অনুসারে-

(অ) ডিজিটাল ফরেনসিক ল্যাব এর জনবল নির্ধারণ করিতে হইবে; এবং

(আ) জনবল তাহাদের অর্পিত দায়িত্ব পালন করিবেন;

(খ) ডিজিটাল ফরেনসিক ল্যাব এর চাহিদা অনুযায়ী উহাতে নিয়োগকৃত জনবল পরিশিষ্ট ০৩ এ বর্ণিত কারিগরি দক্ষতা থাকিতে হইবে।

অংশ-০৫: ডিজিটাল ফরেনসিক ল্যাব এর উপকরণ

১১। যন্ত্রপাতি:

(ক) ফরেনসিক নমুনা বা আলামত হইতে সঠিক ফলাফল আহরণ করিতে হইলে ল্যাবে প্রয়োজনীয় ফরেনসিক পরীক্ষার যন্ত্রপাতি থাকিতে হইবে;

(খ) ল্যাবে নিম্নবর্ণিত ধরনের যন্ত্রপাতি থাকিবে-

(অ) হার্ডওয়্যার;

(আ) সফটওয়্যার (ওপেন সোর্স বা বাণিজ্যিক);

(গ) যন্ত্রপাতি ব্যবহারের পূর্বে উহা অবশ্যই পরীক্ষা এবং যাচাই করিতে হইবে, যেন উহা সঠিক ফলাফল প্রদানে

সক্ষম হয়।

১২। সফটওয়্যার সংক্রান্ত বিষয়াদি:

(ক) নিম্নবর্ণিত বিষয়াদি বিবেচনাক্রমে সফটওয়্যার ক্রয় বা সংগ্রহ করা যাইতে পারে, যথা: -

(অ) সফটওয়্যার এর ক্রয়মূল্য বা বাৎসরিক লাইসেন্স ফি;

(আ) সফটওয়্যার এর ব্যবস্থাপনা ও রক্ষণাবেক্ষণ ব্যয়;

(ই) সফটওয়্যারের ব্যবহারিক প্রশিক্ষণ প্রদান সুবিধা।[২]

(খ) ফরেনসিক ল্যাবে ডিজিটাল কেস ব্যবস্থাপনার জন্য স্বীকৃত মানসম্পন্ন সফটওয়্যার থাকিতে হইবে;

(গ) উক্ত সফটওয়্যার এর রেকর্ড লগে ল্যাবে প্রাপ্ত সকল ফরেনসিক কেস এর নিম্নবর্ণিত তথ্য এ সংরক্ষণ করিতে হইবে, যথা: -

(অ) নমুনা বা আলামত গ্রহণকারী ও সরবরাহকারী ল্যাব কর্মকর্তার নামসহ উহা সরবরাহ বা গ্রহণের দিন ও তারিখ,
(আ) নমুনা বা আলামত ও সংশ্লিষ্ট কেস নাম্বার;
(আ) কেস অধিযাচনকারীর নাম ও যোগাযোগের ঠিকানা;
(ই) ফরেনসিক পরীক্ষার চাহিদাপত্র ও কেসের বিস্তারিত বর্ণনা;
(ঈ) ফরেনসিক বিশ্লেষণের ফলাফল প্রদানের সম্ভাব্য তারিখ ও তৎসংশ্লিষ্ট তথ্যাদি;
(উ) ফরেনসিক কেসের বিশ্লেষণ প্রক্রিয়ার বিবরণ (যেমন- ইমেজিং, আহরণ, হ্যাশ ভ্যালু, ইত্যাদি);
(ঊ) বিশ্লেষণের ফলাফল ও সংশ্লিষ্ট ফরেনসিক বিশেষজ্ঞের নাম;
(এ) অধিযাচনকারীর সহিত কেস সংক্রান্ত বিষয়ে আলোচনার বিস্তারিত বিবরণ;
(ঐ) চেইন অব কাস্টডি সংক্রান্ত তথ্যাদি।

১৩। হার্ডওয়্যার সংক্রান্ত বিষয়াদি:

(ক) উপাত্ত সংরক্ষণ এবং উহার ব্যাকআপ রাখিবার জন্য উপাত্তের ভলিউম অনুসারে বৃহৎ পরিসরের এবং দ্রুতগতির স্টোরেজ ক্ষমতা সম্বলিত সার্ভার বা হার্ডওয়্যার থাকিতে হইবে।

(খ) ডিজিটাল ফরেনসিক ল্যাব পরিচালনার জন্য, ফরেনসিক বিশ্লেষণের চাহিদার আলোকে, প্রয়োজনীয় সংখ্যক হার্ডওয়্যার থাকিতে হইবে।

১৪। হার্ডওয়্যার ও সফটওয়্যার এর তালিকা:

সাধারণ প্রয়োজনীয়তার ভিত্তিতে ফরেনসিক ল্যাবে হার্ডওয়্যার ও সফটওয়্যার সম্বলিত নিম্নবর্ণিত যন্ত্রপাতি থাকিতে হইবে: -

- ল্যাপটপ ও ডেস্কটপ
- ফরেনসিক বিশ্লেষণ সফটওয়্যার
- উপাত্ত পুনরুদ্ধারকরণ সফটওয়্যার
- মোবাইল ডিভাইস বিশ্লেষণ সফটওয়্যার
- ড্রোন সিস্টেম বিশ্লেষণ হার্ডওয়্যার বা সফটওয়্যার

[২] INTERPOL Global guidelines for digital forensic laboratories, 3.4.1 Digital Forensics

- ইন্টারনেট ও তৎসংশ্লিষ্ট প্রমাণাদি বিশ্লেষণ সফটওয়্যার
- ভার্চুয়াল মেশিন সফটওয়্যার
- ইমেজিং হার্ডওয়্যার
- ডকিং সিস্টেম
- রাইট ব্লকার
- আলামত হইতে আহরিত উপাত্ত, স্বল্প ও দীর্ঘ মেয়াদে, সংরক্ষণের জন্য স্টোরেজ মিডিয়া (যেমন- পেন ড্রাইভ, পোর্টেবল হার্ড ডিস্ক, সার্ভার, ইত্যাদি)
- পিসি টুলকিট

১৫। টুলস এবং এক্সেসরিস:

ডিজিটাল ফরেনসিক ল্যাবে ফরেনসিক বিশ্লেষণ কার্যক্রমকে সুষ্ঠুভাবে সম্পাদনের নিমিত্তে যথাযথ মানদন্ডের নিম্নবর্ণিত টুলস ও এক্সেসরিস ল্যাবে থাকিতে হইবে:-

- প্রিন্টার
- নথি বিনষ্টকরণ যন্ত্র (Document Shredder)
- পাওয়ার এক্সটেনশন কেবল
- লিডস এবং আডাপ্টরস
- স্ক্রু ড্রাইভারস
- ক্যামেরা ও ডিডিও রেকর্ডার
- ম্যাগনেটিক টেপ
- যোগাযোগ যন্ত্র (Communication Device)
- স্টোরেজ বক্স
- টর্চ
- আতশি কাঁচ (Magnifying Glass)
- আলামত সিলগালা করিবার ব্যাগ (Evidence Sealing Bag)
- ট্যাম্পার প্রুফ স্টিকার
- স্থায়ী মার্কার (Permanent Marker)
- ফ্যারাডে ব্যাগ।

অংশ-০৬ ডিজিটাল ফরেনসিক কেস ব্যবস্থাপনা

১৬। কেস ব্যবস্থাপনা পদ্ধতি: [৩]

(১) নিম্নবর্ণিত পর্যায়সমূহ অনুসরণক্রমে প্রতিটি ফরেনসিক কেস ব্যবস্থাপনা সম্পন্ন করিতে হইবে, যথা: -

(ক) ফরেনসিক পরীক্ষার অধিযাচন;
(খ) ফরনেসিক পরীক্ষার নিবন্ধন;
(গ) ফরেনসিক পরীক্ষার চাহিদা পর্যালোচনা

[3] INTERPOL Global guidelines for digital forensic laboratories, Section 4, page: 27

(ঘ) ফরেনসিক পরীক্ষার তথ্য প্রমান নির্ধারণ;
(ঙ) ফরেনসিক নমুনা বা আলামতের বিশ্লেষণ;
(চ) ফরেনসিক নমুনা বা আলামত প্রত্যর্পণ;
(ছ) সমাপ্তি ও প্রতিবেদন দাখিল।

(২) ফরেনসিক কেস ব্যবস্থাপনা পর্যায়সমূহ সহজে অনুধাবনার্থ উহা নিম্নের চিত্রে বিধৃত করা হইল:

১৭। ফরেনসিক পরীক্ষার অধিযাচন (Requisition):

(১) ডিজিটাল ফরেনসিক ল্যাব কোনো অনুরোধকারীর নিকট হইতে আনুষ্ঠানিক পত্র বা ইমেইল-যোগে অনুরোধ পাইবার পর পরিশিষ্ট ০৪ এ বিধৃত ডিজিটাল ফরেনসিক পরীক্ষার অধিযাচন ফরমে লিপিবদ্ধ করিবেন এবং আনুষ্ঠানিকভাবে উক্ত বিষয়ে উহার কার্যক্রম শুরু করিবে।

(২) উক্ত অনুরোধ পত্রে, অন্যান্য বিষয়ের মধ্যে, অপরাধের বিবরণ ও ধরন, ইলেকট্রনিক সাক্ষ্য-প্রমাণের বিস্তারিত বিবরণ এবং ফরেনসিক পরীক্ষা বা বিশ্লেষণের উদ্দেশ্য অন্তর্ভুক্ত করিতে হইবে।

১৮। ফরেনসিক কেস নিবন্ধন:

ফরেনসিক কেস ব্যবস্থাপনা কার্যক্রম শুরু করিবার পূর্বে ল্যাব এ প্রেরিত ফরেনসিক নমুনা বা আলামতসমূহ গ্রহণের সময় নিম্নবর্ণিত তথ্যাদি ও অন্যান্য বিষয় ল্যাব কর্তৃপক্ষ কর্তৃক নির্ধারিত ফরমে লিপিবদ্ধ করিয়া নিবন্ধন করিতে হইবে, যথা:-

(ক) নমুনা বা আলামত সংগ্রহের আইনগত ভিত্তি;
(খ) নমুনা বা আলামত সিলগালা করা রহিয়াছে কিনা;
(গ) ফরেনসিক নমুনা বা মামলার বর্ণনা;
(ঘ) সংস্লিস্ট হার্ডওয়্যার, সফটওয়্যার ও নথিসহ অন্যান্য প্রমাণাদি;
(ঙ) ফরেনসিক নমুনা বা আলামতের অবস্থা ও ছবি;
(চ) ফরেনসিক নমুনা বা আলামত সংগ্রহের পারিপার্শ্বিক অবস্থা।

১৯। ফরেনসিক পরীক্ষার চাহিদা পর্যালোচনা:-

ফরেনসিক পরীক্ষার কেস অধিযাচন ফরমে কেসের অনুরোধ গ্রহণের পর ল্যাব সুপারভাইজার নিম্নবর্ণিত বিষয়ে ফরেনসিক পরীক্ষার চাহিদা পর্যালোচনা করিবেন-

(ক) ফরেনসিক পরীক্ষার অধিযাচনপত্র প্রদানকারীর আইনগত ক্ষমতা;

(খ) পূর্ণাঙ্গ সহায়তা চাওয়া হইয়াছে কিনা উহা নিশ্চিতকরণ;

(গ) চেইন অব কাস্টডি এর পূর্ণাঙ্গ নথিপত্র যাচাই (পরিশিষ্ট ০৫ দ্রষ্টব্য);

(ঘ) অধিযাচনপত্রে প্রেরিত কেসের আলোকে ডিজিটাল ফরেনসিক পরীক্ষার পরিধি নির্ণয়।

২০। ফরেনসিক পরীক্ষার তথ্য প্রমাণ নির্ধারণ (Evidence Assessment):

নিম্নবর্ণিত বিষয়াদি বিবেচনাক্রমে অধিযাচনপত্র প্রেরণকারী বা মামলার তদন্তকারী কর্মকর্তার সহিত ল্যাব সুপারভাইজার এর আলোচনার মাধ্যমে ফরেনসিক পরীক্ষায় যে ফলাফল পাওয়া যাইতে পারে বা পারে না উহা অবহিত করিতে হইবে, যথা:[৪]

(ক) চিহ্নিত আলামত আর অন্যকোনো ফরেনসিক পদ্ধতিতে পরীক্ষা করিতে হইবে কিনা (যেমন: কি ওয়ার্ড, টুল মার্কস, ট্রেস, সন্দেহজনক নথি [key words, tool marks, trace and question documents] তল্লাশির বিষয়);

(খ) আরও ডিজিটাল তথ্য প্রমাণ সংগ্রহের নিমিত্তে অন্যপ্রকার তদন্ত (যেমন: ইন্টারনেট সার্ভিস প্রোভাইডার (আইএসপি)কে সংরক্ষণ আদেশ (preservation order) প্রদান করা হইবে কিনা, দূরবর্তী স্থানের তথ্য সংরক্ষণাগার চিহ্নিত করা, ই-মেইল সংগ্রহ) প্রক্রিয়া অনুসরণ করা হইবে কিনা উহার সম্ভাব্যতা যাচাই;

(গ) ফরেনসিক পরীক্ষার স্বার্থে পারিপার্শ্বিক বা প্রাসঙ্গিক কোনো উপাদানের সম্পর্ক বিবেচনায় ফরেনসিক নমুনা বা আলামত ব্যতীত অন্যান্য নমুনা বা আলামত সংগ্রহ (যেমন- জালিয়াতি বা প্রতারণা মামলায় কম্পিউটার বহির্ভূত অন্যান্য যন্ত্রপাতি, লেমিনেটর, স্ক্যানার, প্রিন্টার, অলিখিত ক্রেডিট কার্ড, চেকবই এবং অনুরুপ কোনো আলামত, ইত্যাদি);

(ঘ) সম্ভাব্য যেসকল আলামত (যেমন: ছবি, স্প্রেডসিট, দলিল, ডাটাবেইজ, হিসাব সংক্রান্ত কাগজপত্র এবং অনুরুপ আলামত) অনুসন্ধান করা হইবে উহা নির্ণয়;

(ঙ) ফরেনসিক কেসের নিমিত্তে প্রয়োজনীয় অতিরিক্ত তথ্যাবলী (যেমন: ছদ্মনাম বা অন্যনাম (aliases), ই-মেইল ঠিকানা, আইএসপি সেবা প্রদানকারীর নাম, নেটওয়ার্ক কনফিগারেশন ও এর ব্যবহারকারী (user), সিস্টেম লগ, পাসওর্য়াড, ইউজার নেম); এই সকল তথ্যাদির সংশ্লিষ্ট সিস্টেম এডমিনিস্ট্রটর, ব্যবহারকারী (user) এবং সংশ্লিষ্ট প্রতিষ্ঠানের কর্মচারীদের সাক্ষাৎকার গ্রহণ করিয়া সংগ্রহ করিতে হইবে;

(চ) জড়িত ডিজিটাল ডিভাইস/সন্দেহভাজন কম্পিউটার ব্যবহারকারীদের দক্ষতা মান নির্ধারণ, কেননা আলামত গোপন বা ধ্বংস করিতে সক্ষম এইরূপ দক্ষ ব্যবহারকারী অত্যাধুনিক কায়দা-কানুন প্রয়োগ করিয়া থাকিতে পারেন (উদাহরণস্বরূপ: এনক্রিপশন, বুবি ট্রাপস, স্টেগানোগ্রাফি [Encryption, booby traps, steganography);

(ছ) যে ক্রমানুসারে সাক্ষ্যগুলো পরীক্ষা করা হইবে তাহার প্রাধিকার নির্ণয়;

(জ) অতিরিক্ত কোন জনবলের প্রয়োজন হইবে কিনা উহা নির্ধারণ;

(ঝ) যেসকল যন্ত্রপাতি প্রয়োজন হইবে উহা নির্ধারণ।

[উল্লেখ্য: ডিজিটাল ফরেনসিক ল্যাবের বাহিরে যে কোনো কাজ/ প্রমাণের ক্ষেত্রে ডিজিটাল নিরাপত্তা এজেন্সি এর মহাপরিচালকের অনুমোদন নিতে হইবে]

২১। ডিজিটাল নমুনা বা আলামত বিশ্লেষণ

(১) **অংশ ১০** এ বিধৃত পদ্ধতিতে ডিজিটাল নমুনা বা আলামত বিশ্লেষণ করিতে হইবে।

[৪] ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০, প্রথম অধ্যায়, সেকশন ২

(২) ডিজিটাল নমুনা বা আলামত বিশ্লেষণ প্রক্রিয়ার অংশ হিসাবে নমুনা বা আলামত বিশ্লেষণের সহিত সংশ্লিষ্ট বিশেষজ্ঞ বা পরীক্ষককে আবশ্যিকভাবে ডিজিটাল নমুনা বা আলামত বিশ্লেষণের জন্য অনুরোধকারী ব্যক্তির সহিত নিবিড়ভাবে যোগাযোগ রক্ষা করিতে হইবে।

(৩) ডিজিটাল নমুনা বা আলামত বিশ্লেষণের সহিত সংশ্লিষ্ট বিষয়ে কোন কারিগরি বা অন্যান্য সীমাবদ্ধতা দেখা দিলে উক্ত বিষয়াদি সম্পর্কে অনুরোধকারীকে অবহিত করিতে হইবে।

(৪) ডিজিটাল নমুনা বা আলামত বিশ্লেষণের ক্ষেত্রে পরিশিষ্ট ০৬ এ বিধৃত ফ্লো-চার্ট অনুসরণ করা যাইতে পারে।

২২। ডিজিটাল সাক্ষ্য-প্রমান প্রত্যর্পণ:

(১) ডিজিটাল নমুনা বা আলামতসমূহ প্রত্যর্পণের সময় উহার শুদ্ধতা অক্ষুণ্ন রাখিবার স্বার্থে উহাকে সুরক্ষিত (Tamper-proof) ব্যাগে এমনভাবে সিলগালা করিতে হইবে যাহাতে নমুনা বা আলামতসমূহ নষ্ট বা বিকৃত না হইয়া যায়।

(২) উপ-অনুচ্ছেদ (১) এ বর্ণিত সিলগালা করা ব্যাগের উপর সংশ্লিষ্ট নমুনা বা আলামত পরীক্ষকের স্বাক্ষর, কেস নং, আলামতের নং, স্বাক্ষর প্রদানের তারিখ ও সময় উল্লেখ করিতে হইবে।

(৩) ডিজিটাল নমুনা বা আলামত প্রত্যর্পণের ক্ষেত্রে পরিশিষ্ট ০৪ এ বিধৃত ডিজিটাল ফরেনসিক পরীক্ষার অধিযাচন ফরমের অনুচ্ছেদ নং ৭ এ উল্লেখিত তথ্যাদি পূরণপূর্বক উহা প্রত্যর্পণের রেকর্ড রাখিতে হইবে।

২৩। ফরেনসিক কেসের সমাপ্তি ও প্রতিবেদন:

(১) ডিজিটাল ফরেনসিক ল্যাব কর্তৃক ডিজিটাল ফরনেসিক পরীক্ষা বা বিশ্লেষণের পর ডিজিটাল নিরাপত্তা এজেন্সি কর্তৃক নির্ধারিত সময়ের মধ্যে দায়িত্বপ্রাপ্ত কর্মকর্তা কর্তৃক উহার প্রতিবেদন প্রস্তুতকরত উহা ডিএসএ মহাপরিচালকের অনুমোদনক্রমে অধিযাচনকারীকে প্রদান করিতে হইবে।

(২) উক্তরুপে অধিযাচনকারীকে প্রতিবেদন প্রদানের পর, ল্যাব এ ফরেনসিক পরীক্ষা বা অধিযাচনকৃত কার্যটি সম্পন্ন হইবে।

অংশ-০৭: ফরেনসিক পরীক্ষার পর্যায়

২৪। ডিজিটাল ফরেনসিক পরীক্ষার পর্যায়সমূহ:

(১) ইলেকট্রনিক সাক্ষ্য-প্রমাণ পরীক্ষা/বিশ্লেষণের ক্ষেত্রে নিম্নবর্ণিত পর্যায়সমূহ অনুসরণ করিতে হইবে: [৫]

(ক) ফরেনসিক নমুনা বা আলামত অধিগ্রহণ (Acquisition);

(খ) ফরেনসিক নমুনা বা আলামত পরীক্ষা (Examination);

(গ) ফরেনসিক নমুনা বা আলামত বিশ্লেষণ (Analysis);

(ঘ) নথিভূক্তকরণ ও প্রতিবেদন প্রস্তুতকরণ (Documentation and Reporting)।

(২) ইলেকট্রনিক সাক্ষ্য-প্রমাণের শুদ্ধতা নিরাপদ রাখিয়া উহার চেইন অব কাস্টডি সর্বদাই হালনাগাদ করিতে হইবে।

[5] INTERPOL Global guidelines for digital forensic laboratories, Section 5, page: 30

(৩) কেস অধিযাচনকারীর সন্তুষ্টি সাপেক্ষে উপ-অনুচ্ছেদ (১) এ উল্লেখিত ফরেনসিক নমুনা বা আলামত পরীক্ষা বা বিশ্লেষণ পর্যায় প্রয়োজনে পুনরাবৃত্তি করা যাইতে পারে।

(৪) ইলেকট্রনিক সাক্ষ্য-প্রমাণের চেইন অব কাস্টডি ও শুদ্ধতা অক্ষুণ্ন রাখিয়া উহা পরীক্ষা/বিশ্লেষণ পর্যায় নিম্নের চিত্রে উপস্থাপন করা হইল: -

অংশ-০৮: ডিজিটাল নমুনা বা আলামত অধিগ্রহণ ও উপাত্ত আহরণ

২৫। উপাত্ত অধিগ্রহণ প্রক্রিয়া:

(১) ডিজিটাল ডিভাইস (যেমন- হার্ডডিস্ক, থাম্ব ড্রাইভ, পেন ড্রাইভ, সার্ভার, ইত্যাদি) হইতে নমুনা বা আলামতের ফরেনসিক অনুলিপি, উহার বিষয়বস্তু পরিবর্তন না করিয়া, ইমেজ ফাইল আকারে তৈরির মাধ্যমে উপাত্ত অধিগ্রহণ করিতে হইবে।

(২) ডিজিটাল নমুনা বা আলামতের শুদ্ধতা অক্ষুণ্ন রাখিয়া ডিজিটাল ডিভাইস হইতে উপাত্ত অধিগ্রহণ করিতে হইবে।

(৩) ডিজিটাল নমুনা বা আলামত অধিগ্রহণের ক্ষেত্রে ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর তফসিলে বর্ণিত দ্বিতীয় অধ্যায়ের ফরেনসিক নমুনা বা আলামত অধিগ্রহণ পদ্ধতি অনুসরণ করিতে হইবে (পরিশিষ্ট ০৭ দ্রষ্টব্য);

(৪) ডিজিটাল নমুনা বা আলামত অধিগ্রহণে সহায়ক হিসেবে পরিশিষ্ট ০৮ তে বর্ণিত ফ্লো-চার্ট অনুসরণ করা যাইবে।

২৬। কম্পিউটার সিস্টেম হইতে উপাত্ত অধিগ্রহণ:

নিম্নবর্ণিত দুই পর্যায়ে উপাত্ত অধিগ্রহণ করিতে হইবে-

(ক) ভৌত উপাত্ত অধিগ্রহণ: উহাতে সকল অরুপান্তরিত উপাত্ত (Raw data) অন্তর্ভুক্ত থাকে (যেমন- একটি ডিস্ক লেভেলের পার্টিশন স্কিম, সমস্ত পার্টিশন বা পার্টিশনবিহীন অংশসহ সম্পূর্ণ ডিস্ক অন্তর্ভুক্ত থাকে);

(খ) লজিক্যাল উপাত্ত অধিগ্রহণ: উহাতে ডিস্ক লেভেলে অরুপান্তরিত উপাত্তের কেবল বরাদ্দকৃত অংশ (Allocated Space) অন্তর্ভুক্ত থাকে।

(১) একটি ডিস্কের সম্পূর্ণ ভৌত কপি সংগ্রহ করিতে হইবে যাহাতে মুছিয়া ফেলা বা মুছিয়া যাওয়া উপাত্ত এবং অবারাদ্ধকৃত পরিসর (Unallocated Space) উক্ত কপিতে অন্তর্ভুক্ত থাকে।

(২) যেক্ষেত্রে সম্পূর্ণ ডিস্ক বা ডিস্কের উপাত্ত এনক্রিপশন করা অবস্থায় থাকিলে সেইক্ষেত্রে এনক্রিপ্ট করা ডিস্কের ভৌত কপি বা উপাত্ত অধিগ্রহণ না করিয়া উহা আনলক করা অবস্থায় উপাত্তের লজিক্যাল অনুলিপি অধিগ্রহণ করিতে হইবে।

(৩) ফরেনসিক অনুলিপি/ইমেজের বিশুদ্ধতা রক্ষার লক্ষ্যে উহা এমন মিডিয়ামে সংরক্ষণ করিতে হইবে যাহাতে পরীক্ষাধীন কেসের সহিত সম্পর্কিত উপাত্ত ব্যাতীত অন্য কোন তথ্য বা উপাত্ত না থাকে; উক্ত ক্ষেত্রে মিডিয়াম বিশুদ্ধ (Sterilize) করিতে বা ওভাররাইট করিয়া সকল উপাত্ত মুছিয়া ফেলিতে হইবে।

(৪) হার্ডওয়্যার রাইট-ব্লকার বা সফটওয়্যার রাইট-ব্লকার ডিস্কের ইমেজ গ্রহণের সময় ডিস্কে লিখতে বাধা দেয় এবং শুধুমাত্র পড়িতে অনুমোদন দেয় বিধায় উহা দ্বারা, ডিস্কের উপাত্তে কোন পরিবর্তন ব্যতীত, ইমেজ গ্রহণ করা যাইবে।

(৫) ইমেজিং টুলস (Imaging tools): ইমেজিং সফটওয়্যার বা টুলস ব্যবহার করিয়া স্টোরেজ মিডিয়া ইমেজিং সম্পন্নকরণ, ফরেনসিক ইমেজ বিন্যাস রীতি (Format) অনুযায়ী বিট-বাই-বিট কপিকরণ, এবং উক্ত কপি যাচাই করিতে সক্ষম এমন নির্ভরযোগ্য এবং দ্রুতগতির সফটওয়্যার দ্বারা ইমেজ সম্পাদন করিতে হইবে।

(৬) উপ-অনুচ্ছেদ (৫) এ উল্লেখিত ইমেজিং সফটওয়্যার ও যন্ত্রপাতির বৈশিষ্ট্যসমূহ নিম্নরূপ -

(ক) লুকানো বা অপ্রদর্শিত (Hidden) স্টোরেজ শনাক্তকরণ;
(খ) যুগপৎভাবে একাধিক ডিভাইস ইমেজিং সম্পন্নকরণ;
(গ) একই সময়ে একাধিক টার্গেট ডিভাইসে ইমেজিং সম্পন্নকরণ;
(ঘ) সারিবদ্ধভাবে (Queue) ইমেজিং সম্পন্নকরণ;
(ঙ) প্রচলিত হ্যাশ (#) অ্যালগরিদম দ্বারা হ্যাশ যাচাইকরণ;
(চ) ইমেজিং প্রক্রিয়ার বিভিন্ন পর্যায়ে হ্যাশ যাচাইকরণ;
(ছ) উপ-অনুচ্ছেদ (৭) এ উল্লেখিত ফরেনসিক ইমেজ ফরম্যাটসমূহ সমর্থন;
(জ) এনক্রিপ্টেড এবং কমপ্রেসড ইমেজিং সম্পন্নকরণ;
(ঝ) ইমেজ অধিগ্রহণ প্রক্রিয়া বিঘ্নিত হইলে উহা পুনরায় সম্পন্নকরণ;
(ঞ) ত্রুটি সম্পন্ন হার্ডওয়্যার হইতে ইমেজ অধিগ্রহণ সম্পন্নকরণ।

(৭) ফরেনসিক ইমেজ ফরম্যাট:

ইমেজ ফরম্যাট-এর মধ্যে বিল্ট-ইন চেকসাম এবং কেস মেটাডাটা থাকিবার কারণে সহজে হেরফের (Manipulation) করা যায় না বিধায় প্রচলিত ফরম্যাট যেমন এক্সপার্ট উইটনেস ফরম্যাট (EWF (x)/E (x) 01) বা অ্যাডভান্সড ফরেনসিক ফরম্যাট (AFF) এ স্টোরেজের সকল উপাত্তের অরূপান্তরিত ইমেজ (raw/dd) সংরক্ষণ করিতে হইবে; এবং ইমেজ ফরম্যাট-এর বৈশিষ্ট্যসমূহ নিম্নরূপ -

(ক) উপাত্তের সংকোচনকরণ (Compression);
(খ) উপাত্তের এনক্রিপশনকরণ(Encryption);
(খ) ত্রুটি পরীক্ষাকরণ;
(খ) কেস মেটাডাটা (Metadata) চিহ্নিতকরণ;
(খ) ফাইল হ্যাশ-এর যোগফল;
(খ) ইমেজ খন্ডাংশে বিভক্তকরণ।

(৮) ভিন্ন ভিন্ন ফরেনসিক সফটওয়্যারে ইমেজ ফরম্যাট ভিন্ন ভিন্ন হওয়ায় ডিজিটাল ফরেনসিক বিশ্লেষণ কাজ যাহাতে বিঘ্নিত না হয় তজ্জন্য উপ-অনুচ্ছেদ (৭) এ বর্ণিত ফরম্যাট-এ ইমেজ সংরক্ষণ করিতে হইবে।

(৯) ডিজিটাল নমুনা বা আলামতের ইমেজ ফাইল যাচাইকরণ:

(ক) ফরেনসিক কপিতে পরবর্তী সকল প্রক্রিয়াকরণ ও বিশ্লেষণের নিমিত্তে মূল স্টোরেজ মাধ্যম এবং ইমেজ ফাইলে একই উপাত্ত রহিয়াছে কিনা উহা যাচাই করিবার জন্য উভয় উপাত্তের সেটে SHA-1, SHA-256 বা অন্য কোনো গাণিতিক অ্যালগরিদম প্রয়োগ করিতে হইবে এবং উহা দ্বারা 'হ্যাশ ভ্যালু' নামে একটি জটিল সংখ্যা উৎপন্ন হইবে;

(খ) যদি উভয় উপাত্তের সেটে হ্যাশ ভ্যালুর মান একই হয়, তাহা হইলে উক্ত উপাত্তের ফাইল/ডিভাইসগুলি অভিন্ন বলিয়া গণ্য হইবে এবং উপাত্তে সামান্য পরিবর্তনের ফলে হ্যাশ ভ্যালুতে বড় ধরনের পরিবর্তন পরিলক্ষিত হইবে।

(গ) যেহেতু একক হ্যাশ অ্যালগরিদম ব্যবহার দ্বারা উৎপন্ন হ্যাশ সাংঘর্ষিক অবস্থার সৃষ্টি করিতে পারে বিধায় ইমেজ ফাইলে উপাত্ত যাচাই করিতে কমপক্ষে দুইটি হ্যাশ অ্যালগরিদম ব্যবহার করিতে হইবে।

(ঘ) ইমেজিং প্রক্রিয়ার দুইটি পয়েন্টে হ্যাশ যাচাই করিতে হইবে। মূল ফাইল হ্যাশ মান তৈরির নিমিত্তে ইমেজিং প্রক্রিয়ার শুরুতে প্রথম হ্যাশ এবং ইমেজিং প্রক্রিয়ার শেষে দ্বিতীয় হ্যাশ গণনা করিতে হইবে। এই দ্বিতীয় গণনাটি মূল ফাইলের পাশাপাশি ইমেজ ফাইলের উপাত্তেও প্রয়োগ করিতে হইবে যাহাতে প্রমাণ করা যায় যে, মূল ফাইলের উপাত্ত ইমেজিং প্রক্রিয়ার সময় পরিবর্তিত হয় নাই এবং ইমেজ ফাইলের উপাত্ত ঠিক মূল ফাইলের অনুরূপ।

(১০) ফরেনসিক কপির ব্যাকআপ:

ফরেনসিক ল্যাবে ফরেনসিক কপি ব্যাকআপ রাখিবার নিমিত্তে স্টোরেজ সুবিধা থাকিতে হইবে এবং উক্ত কপির ব্যাকআপ রাখার পাশাপাশি অন্য সিস্টেমে (যেমন- ইমেজিং সার্ভার, ইত্যাদি) অফ-সাইট ব্যাকআপও রাখিতে হইবে।

২৭। মোবাইল ডিভাইস হইতে উপাত্ত আহরণ (Extraction):

(১) বিশ্লেষণ বা পরীক্ষা কার্যক্রম শুরু করিবার পূর্বে, ফরেনসিক বিশ্লেষক বা পরীক্ষককে ডিজিটাল নমুনা বা আলামত হইতে কোন ধরনের উপাত্ত আহরণের প্রয়োজন হইবে উহা নির্ণয়ের উদ্দেশ্যে কেস অধিযাচনকারী কর্তৃক প্রদত্ত কাগজপত্র পর্যালোচনা করিতে হইবে, এবং বিশ্লেষণ বা পরীক্ষা কার্যক্রম পরিচালনাকালীন মোবাইল ডিভাইস আনলক করিবার জন্য বিশ্লেষক বা পরীক্ষককে উক্ত ডিভাইস এর সকল পাসকোড, পাসওয়ার্ড এবং নমুনা বা আলামতের ধরন সংগ্রহ করিতে হইবে।

(২) দফা (১) এর অধীন কার্য-সম্পাদনের ক্ষেত্রে ফরেনসিক বিশেষজ্ঞ বা পরীক্ষককে সর্বোত্তম তথ্য উপাত্ত আহরণ নিশ্চিত করিতে হইবে এবং উক্ত উদ্দেশ্যে নিম্নবর্ণিত পর্যায়ক্রমিক স্তরসমূহ ব্যবহারক্রমে মোবাইল ডিভাইস হইতে উপাত্ত আহরণ করা যাইবে, যথা: -

(ক) **ভৌত আহরণ (Physical Extraction):** ডিভাইসের স্টোরেজ হইতে সমস্ত অরুপান্তরিত (Raw data) বাইনারি উপাত্ত অধিগ্রহণ প্রক্রিয়াই হইল ভৌত আহরণ। এই ধরনের আহরণের ক্ষেত্রে অরুপান্তরিত উপাত্তসমূহকে পরবর্তীতে বিভিন্ন ফরেনসিক সফটওয়্যারের মাধ্যমে বিশ্লেষণ ও প্রক্রিয়াজাত করা প্রয়োজন হইবে। এই পদ্ধতিতে বিশ্লেষককে বা পরীক্ষককে লাইভ এবং মুছে ফেলা উপাত্ত, অপারেটিং সিস্টেম ফাইল এবং ডিভাইসে অভিগম্যতা প্রদান করে যেখানে সাধারণভাবে কোনো ব্যবহারকারীর অভিগম্যতা থাকে না।

(খ) **ফাইল সিস্টেম ডাম্প (FSD) পদ্ধতিতে আহরণ**: ফাইল সিস্টেম ডাম্প আহরণ পদ্ধতি হইতেছে ভৌত আহরণ ও লজিক্যাল আহরণের হাইব্রিড প্রক্রিয়া। এই পদ্ধতিতে উপাত্ত প্রক্রিয়াকরণ পর্যায়ে ডিভাইস ফাইল সিস্টেম পুনরুদ্ধার ও উহা বিশ্লেষণ করা যায়। যেক্ষেত্রে লজিক্যাল আহরণ বা ভৌত আহরণের মাধ্যমে উপাত্তভান্ডার হইতে মুছিয়া যাওয়া তথ্য বা উপাত্ত পুনরুদ্ধার করা সম্ভব হয় না সেইক্ষেত্রে ফাইল সিস্টেম ডাম্প আহরণ পদ্ধতিতে উপাত্ত আহরণ করা যায়। ভৌত আহরণের মাধ্যমে যেই সকল মুছিয়া যাওয়া উপাত্ত

পুনরুদ্ধার করা সম্ভবপর হয়, ফাইল সিস্টেম ডাম্প আহরণ পদ্ধতিতে সেই সকল উপাত্ত পুনরুদ্ধার করা সম্ভব নাও হইতে পারে।

(গ) **লজিক্যাল আহরণ (Logical Extraction)**: লজিক্যাল আহরণ হইতেছে মোবাইল ডিভাইস হইতে বিশ্লেষণের উদ্দেশ্যে তথ্য উপাত্ত সংগ্রহ। ফরেনসিক সফটওয়্যার ব্যবহারের মাধ্যমে এই পদ্ধতিতে লাইভ তথ্য বা উপাত্ত আহরণ করা যায়।

(ঘ) **ম্যানুয়াল আহরণ পদ্ধতি**: যদি উপরে বর্ণিত পদ্ধতিতে কোনো উপাত্ত আহরণ করা না যায়, তাহা হইলে ম্যানুয়াল পদ্ধতিতে উপাত্ত আহরণ করা যাইবে। এই পদ্ধতিতে ডিভাইসে অভিগমণের মাধ্যমে উহার স্ক্রিনে প্রদর্শিত উপাত্তের ফটোগ্রাফ গ্রহণ, ভিডিও রেকর্ডিং বা ট্রান্সক্রাইব করা হয়। এই পদ্ধতিতে মোবাইল ডিভাইস এর ডেভেলপার মোড চালু করিয়া উহাকে এডিবি কমান্ড এর সহিত সংযুক্ত করিবার প্রয়োজন হইতে পারে।

(ঙ) **জেট্যাগ (JTAG) আহরণ পদ্ধতি**: ক্ষতিগ্রস্ত বা পাসওয়ার্ড দ্বারা লক করা মোবাইল ডিভাইসের ক্ষেত্রে JTAG এবং চিপ-অফ আহরণ পদ্ধতি প্রয়োগ করা যাইবে; এবং এই আহরণ পদ্ধতিতে মোবাইল ডিভাইসকে লজিক্যাল বোর্ডে আনায়নক্রমে উক্ত বোর্ডের নির্দিষ্টকৃত সংযোগের সহিত ডিভাইসের নির্দিষ্টকৃত কেবলের সোল্ডারিং এর প্রয়োজন হইবে ও মোবাইল ডিভাইসের স্টোরেজ হইতে অরুপান্তরিত (raw data) বাইনারি উপাত্ত আহরণ করা যাইবে।

(চ) চিপ-অফ (Chif-Off) আহরণ পদ্ধতি:
চিপ-অফ আহরণ পদ্ধতিতে অরুপান্তরিত বাইনারি উপাত্ত আহরণ করা যাইবে এইক্ষেত্রে মোবাইল ডিভাইস হইতে ইহার স্টোরেজকে সম্পূর্ণ বিচ্ছিন্ন করিতে হইবে; এবং উক্তরুপে বিচ্ছিন্ন করা হইলে মোবাইল ডিভাইসটি নস্ট হইয়া যাইতে পারে। যেক্ষেত্রে আইওটি ডিভাইসের স্টোরেজ এ উপাত্ত ক্লিয়ার টেক্সট রুপে সংরক্ষিত থাকে, সেইক্ষেত্রে এই আহরণ পদ্ধতি কার্যকর হইবে।

(ছ) রুটিং বা জেইল ব্রেকিং (Rooting or Jail Breaking) আহরণ পদ্ধতি:

লিনাক্স অপারেটিং সিস্টেম এর Root অ্যাক্সেস করিবার সময় ইহার ব্যবহারকারী যেমন অপারেটিং সিস্টেম এর ফাইলে পরিবর্তন করিতে পারেন, ঠিক তেমনই রুটিং বা জেইল ব্রেকিং আহরণ পদ্ধতিতে মোবাইল ডিভাইসের ব্যবহারকারী ইহার অ্যানড্রয়েড অপারেটিং সিস্টেম এর ফাইলে পরিবর্তন করিয়া ফেলিতে পারেন, যাহার ফলে ডিভাইসটির সমূহ ক্ষতি হইতে পারে এবং সেইজন্য এই কৌশলের প্রয়োগ কম হওয়া বাঞ্চনীয়।

(৩) তথ্য উপাত্ত আহরণের টুল:

মোবাইল ডিভাইস বিশ্লেষণের নিমিত্ত সাধারণত ডেডিকেটেড সফটওয়্যার, যথাযথ পাওয়ার কেবল, ডাটা কেবল, সোল্ডারিং সরঞ্জাম ও অন্যান্য প্রয়োজনীয় যন্ত্রপাতি বা সরঞ্জাম ব্যবহার করিতে হইবে ।

(৪) উপাত্ত আহরণের ফাইল ফরম্যাট:

ডেডিকেটেড টুলস ব্যবহার করিয়া উপাত্ত আহরণ করিবার প্রয়োজনে মোবাইল ডিভাইস এর তথ্য উপাত্ত স্বত্তাধিকারি (proprietary) ফরম্যাটে আহরণ করিতে হইবে। প্রয়োজনীয়তার নিরিখে বিভিন্ন যন্ত্রপাতির ডিকোডিং ক্ষমতাকে কাজে লাগানোর উদ্দেশ্যে এই ফরম্যাটের উপাত্তগুলি বিভিন্ন যন্ত্রপাতির মধ্যে স্থানান্তর করা যাইবে। অন্যান্য non-proprietary ফাইল ফরম্যাট এর মধ্যে বিন ফাইল (.bin) এবং অরুপান্তরিত ফাইল (.raw) অন্তর্ভুক্ত হইবে।

(৫) মোবাইল ডিভাইসের আলামত আহরণ প্রক্রিয়া:

নিম্নবর্ণিত পদক্ষেপ গ্রহণক্রমে মোবাইল ডিভাইস হইতে উপাত্ত আহরণ করিতে হইবে:

(ক) ডিজিটাল নমুনা বা আলামত চিহ্নিতকরণ:

মোবাইল ডিভাইস হইতে ফরেনসিক নমুনা বা আলামত অধিগ্রহণের পূর্বে ইহা চিহ্নিত করিতে হইবে। সাধারণত ডিভাইসের অভ্যন্তরে সংযুক্ত লেবেলে উক্ত ডিভাইসের ইন্টারন্যাশনাল মোবাইল ইকুইপমেন্ট আইডেন্টিফাই নম্বর (IMEI), মোবাইল ইকুইপমেন্ট আইডেন্টিটি নম্বর (MEID) বা সিরিয়াল নম্বর থাকে যাহার মাধ্যমে পৃথকভাবে ডিভাইসটি সনাক্ত করা যায়। IMEI, MEID ও সিরিয়াল নম্বর ব্যবহার করিয়া ফরেনসিক সফটওয়্যার এর কোন স্তরের সহায়তা পাওয়া যাইবে তাহা নির্ধারণ করিতে হইবে;

(খ) স্টোরেজ মিডিয়া প্রস্তুতকরণ:

আহরিত উপাত্ত সংরক্ষণ করিবার উদ্দেশ্যে একটি স্টোরেজ মিডিয়া বা, ক্ষেত্রমত, পরিচ্ছন্ন ক্লোন সিমকার্ড প্রস্তুত করিতে হইবে;

(গ) ডিজিটাল নমুনা বা আলামত নেটওয়ার্ক হইতে পৃথকীকরণ (Isolation):

(অ) মোবাইল ডিভাইস এর উপাত্ত নষ্ট, ক্ষতি বা পরিবর্তন রোধকল্পে উহার সকল ধরনের নেটওয়ার্ক সংযোগ হইতে বিচ্ছিন্ন রাখিতে হইবে, কেননা অধিকাংশ আধুনিক ডিভাইসের দূর নিয়ন্ত্রণ ব্যবস্থার মাধ্যমে উক্ত ডিভাইসের উপাত্ত মুছিয়া ফেলিবার সক্ষমতা রহিয়াছে;

(আ) অনেক মোবাইল ডিভাইস 'লাইভ' অবস্থায় উপাত্ত আহরণের প্রয়োজন হয় সেইক্ষেত্রে ডিভাইসটি পাওয়ার অন করা অবস্থায় চালু থাকিতে হইবে;

(ই) নিম্নবর্ণিত পদ্ধতি প্রয়োগক্রমে মোবাইল ডিভাইসকে নেটওয়ার্ক হইতে পৃথকীকরণ করা যায়:

(১) **সিম/আইডিইএন কার্ড ক্লোন করা:** ক্লোন করা সিম/আইডিইএন কার্ড মোবাইল ডিভাইসের মূল সিম/আইডিইএন কার্ড হিসাবে চিহ্নিত হইবে কিন্তু উহা কোন মোবাইল নেটওয়ার্কের সহিত সংযোগ স্থাপনে সক্ষম হইবে না;

(২) **নেটওয়ার্ক শিল্ডেড রুমে উপাত্ত আহরণ**: নেটওয়ার্ক শিল্ডেড রুমে মোবাইল ডিভাইস হইতে উপাত্ত আহরণের জন্য নেটওয়ার্ক বিচ্ছিন্নতার নিমিত্তে ফ্যারাডে শিল্ডিং (Faraday shielding) -সহ একটি ডেডিকেটেড ল্যাবরেটরি সংস্থাপন করিতে হইবে;

(৩) **ওয়্যারলেস জ্যামিং সরঞ্জাম ব্যবহার**: আইনগত বৈধতা সাপেক্ষে, ওয়্যারলেস সংকেত যাহাতে নমুনা বা আলামতে পৌঁছাইতে না পারে এবং সংকেত প্রতিরোধ করিতে পারে এইরূপ জ্যামিং সরঞ্জাম সংস্থাপন করিয়া ওয়াই-ফাই (Wi-Fi) এবং ব্লুটুথ (Bluetooth) সিগন্যালের সংযোগ রোধ করিতে হইবে;

(৪) **ম্যানুয়াল পদ্ধতির ব্যবহার:** জ্যামিং সরঞ্জাম ব্যবহারের পরিবর্তে ম্যানুয়াল পদ্ধতি ব্যবহার করিয়া ওয়্যারলেস সংকেত যাহাতে নমুনা বা আলামতে পৌঁছাইতে না পারে এবং সংকেত প্রতিরোধ করিতে পারে উহার ব্যবস্থা করা যাইবে। এই প্রক্রিয়ায় আলামত পরিবর্তনের ঝুঁকি

থাকে বিধায় এই পদ্ধতি ব্যবহারের পূর্বে মোবাইল ডিভাইসকে "ফ্লাইট মুডে" বা, ক্ষেত্রমত, অন্যকোনো ব্যবস্থাপনায় ডিভাইসের ওয়াই-ফাই এবং ব্লুটুথ সিগন্যাল ও অন্যান্য নেটওয়ার্ক সিগন্যাল বন্ধ করিতে হইবে।

(ঘ) সংশ্লিষ্ট উপাত্ত আহরণ:

প্রত্যেক মোবাইল ডিভাইসের তিনটি স্বতন্ত্র মিডিয়া থাকে যাহা হইতে উপাত্ত আহরণের জন্য পৃথক পৃথক কৌশল অবলম্বন করা প্রয়োজন-

(১) **সিম/আইডিইএন কার্ড**: এইক্ষেত্রে অগ্রসর প্রযুক্তির মোবাইল ফোন ফরেনসিক সরঞ্জাম ব্যবহার করিতে হইবে;

(২) **মেমরি কার্ড**: মোবাইল ডিভাইসের মেমরি কার্ডকে কম্পিউটারের হার্ডডিস্ক বা ফ্ল্যাশ ড্রাইভের মতই পরীক্ষা করা যাইবে, তবে এইক্ষেত্রে ভৌত ও লজিক্যাল উভয় ধরনের আহরণ পদ্ধতি প্রয়োগ করা যাইবে;

(৩) **ডিভাইসের অভ্যন্তরীণ মেমরি:** এইক্ষেত্রে অগ্রসর প্রযুক্তির মোবাইল ফোন ফরেনসিক সরঞ্জাম ব্যবহার করিতে হইবে।

ব্যাখ্যা।— উপ-অনুচ্ছেদ (ঘ) উদ্দেশ্য পূরণকল্পে, -

(অ) সিম/আইডিইএন কার্ডের জন্য লজিক্যাল অধিগ্রহণ এবং মেমোরি কার্ডের জন্য ফিজিক্যাল অধিগ্রহণ করিতে হইবে। ফরেনসিক নমুনা বা আলামত সংরক্ষণ ও সুরক্ষার জন্য মেমরি কার্ডের বিট-টু-বিট ক্লোন প্রস্তুত করিতে হইবে। মোবাইল নেটওয়ার্ক হইতে ডিভাইসটি যাহাতে আলাদা থাকে সেইজন্য উক্ত ডিভাইসে পাওয়া সিম/আইডিইএন কার্ড পরীক্ষার চলাকালীন সময় পর্যন্ত নমুনা বা আলামত হইতে পৃথক রাখিতে হইবে;

(আ) মোবাইল ডিভাইস এর ফরেনসিক পরীক্ষার নিমিত্ত উক্ত ডিভাইসে একটি বুট লোডার (Boot Loader) আপলোড করিয়া মোবাইল বুট করিতে হইবে এবং ডিভাইসের ব্যবহারকারীর উপাত্তে কোনও পরিবর্তন না করিয়াই ডিভাইসের অভ্যন্তরীণ মেমোরিতে প্রবেশ করিতে হইবে। এই ধরনের একটি ভৌত পরীক্ষা মোবাইলের পিন বা প্যাটার্নের মতো যেকোনো ডিভাইসের লক কোড পুনরুদ্ধার করিয়া ফরেনসিক বিশেষজ্ঞ বা পরীক্ষককে উক্ত ডিভাইসে পরিপূর্ণভাবে প্রবেশাধিকার প্রদান করে;

(ই) যদি-

(১) ডিভাইসটি উপরোক্ত (আ) তে বর্ণিত কাজের উপযুক্ত না হয়, তাহা হইলে উক্ত ডিভাইস মোবাইল নেটওয়ার্কসহ যেকোনো নেটওয়ার্ক হইতে বিচ্ছিন্ন অবস্থায় রাখিতে হইবে; এবং

(২) ডিভাইসে ইহার ব্যবহারকারী কর্তৃক আরোপিত সুরক্ষা (যেমন- পিন, পাসওয়ার্ড বা প্যাটার্ন) দেওয়া থাকে, তাহা হইলে উক্ত ডিভাইসের ফরেনসিক পরীক্ষককে উক্ত আরোপিত সুরক্ষা ব্যবস্থা ভাঙ্গার সময় যাহাতে উহার সিস্টেমে কোন অনাকাঙ্ক্ষিত পরিবর্তন না হয় সেইজন্য সর্বোচ্চ সতর্কতা অবলম্বন করিতে হইবে;

(ঈ) যদি-

(১) মোবাইল ডিভাইসের পিন, পাসওয়ার্ড বা প্যাটার্ন পূর্ব হইতেই জানা থাকে, তাহা হইলে উক্ত পিন, পাসওয়ার্ড বা প্যাটার্ন উহাতে এমনভাবে প্রয়োগ করিতে হইবে যাহাতে ডিভাইসে পরিপূর্ণ প্রবেশাধিকার পাওয়া যায়; এবং

(২) মোবাইল ডিভাইস সুরক্ষিত অবস্থায় রাখিয়া প্রবেশ করিতে যথাযথ সমাধান পাওয়া সম্ভবপর না হয়, তাহা হইলে উক্ত ডিভাইসের উপাত্তে প্রবেশ করিবার জন্য সাধারণ পিন বা প্যাটার্ন প্রয়োগ করা যাইবে; ইহা একটি ঝুঁকিপূর্ণ প্রক্রিয়া, কারণ অনেক কোড বা ভুল কোড অনেকবার প্রয়োগ করিলে মোবাইল ডিভাইস হইতে নিরাপদ উপাত্ত নষ্ট হইয়া যাইবে।

(ঊ) এইক্ষেত্রে সফটওয়্যার এর মাধ্যমে "ব্রুট-ফোর্স" (Brute force) পদ্ধতি প্রয়োগ করা যাইবে।

অংশ-০৯: ডিজিটাল ফরেনসিক নমুনা বা আলামত পরীক্ষণ

২৮। নমুনা বা আলামত পরীক্ষণ:

(১) যথাযথ ফরেনসিক পদ্ধতি ব্যবহারের মাধ্যমে ডিজিটাল সাক্ষ্য প্রমাণ পরীক্ষা করিতে হইবে এবং প্রযোজ্য ক্ষেত্রে মূল ফরেনসিক নমুনা বা আলামতের উপর পরীক্ষা করা হইতে বিরত থাকিতে হইবে।

(২) ফরেনসিক বিশ্লেষক বা পরীক্ষককে আবশ্যিকভাবে নমুনা বা আলামতের ইমেজ ফাইলের উপর কার্য-সম্পাদন করিতে হইবে। মূল ফরেনসিক নমুনা বা আলামতের উপর সরাসরি পরীক্ষা করিতে হইলে সংলিস্ট ফরেনসিক কপিকে অবশ্যই রাইট ব্লকার দ্বারা সুরক্ষিত রাখিতে হইবে।

(৩) কতিপয় ক্ষেত্রে, ফরেনসিক বিশ্লেষক বা পরীক্ষককে ল্যাবরেটরিতে পূর্ব নির্ধারিত বা পৃথক কোন স্থানে পরীক্ষণ কার্যসম্পাদন করিতে হইবে।

(৪) কম্পিউটার ও মোবাইল ডিভাইস পরীক্ষণে সাধারণভাবে পরিশিষ্ট ০৯ তে বর্ণিত কম্পিউটার পরীক্ষণ ফ্লো-চার্ট অনুসরণ করা যাইবে।

২৯। কম্পিউটার পরীক্ষণ পদ্ধতি:

(১) ডেড সিস্টেম (Dead System) এর উপর পরীক্ষণ:

“ডেড সিস্টেম” পাওয়ার সংযোগ বিচ্ছিন্ন অবস্থায় বন্ধ করা থাকে, ফলে ইহার ভোলাটাইল (Volatile) মেমরি (যেমন- র‍্যাম (RAM) মেমরি, রানিং প্রসেস, ক্যাশ ডাটা, চলমান অ্যাপ্লিকেশান, ইত্যাদি) এর উপাত্তসমূহ পাওয়া যায় না বিধায় ডেড সিস্টেম পরিচালনার ক্ষেত্রে নিম্নবর্ণিত উপাত্তসমূহ বিবেচনা করিতে হইবে-

(ক) সক্রিয় ফাইল, মুছিয়া ফেলা ফাইল, স্টাক ফাইল, স্লাক পার্টিশন (slack partitions), স্লাক ডিস্ক (slack disk), শ্যাডো ফাইল (shadow file), ইত্যাদি;

(খ) ডিভাইস আর্টিফ্যাক্টস (যেমন- অপারেটিং সিস্টেম এর ফাইল, রেজিস্ট্রি এর ফাইল, মেটাডাটা ফাইল, এনক্রিপ্টেড ফাইল, লগ ফাইল ও ডাটাবেজ ফাইল, ইত্যাদি;

(ঘ) ব্রাউজিং হিস্টোরি, ইমেইল, সোশ্যাল মিডিয়া, পিয়ার টু পিয়ার ফাইল শেয়ারিং, ইত্যাদি।

(২) লাইভ সিস্টেম এর উপর পরীক্ষণ:

লাইভ সিস্টেম হইলো সেই সিস্টেম যেখানে অ্যাপ্লিকেশান চলমান ও হালনাগাদ অবস্থায় রহিয়াছে এবং উপাত্তসমূহ ক্রমাগতভাবে প্রক্রিয়াকৃত ও হালনাগাদকৃত হইতেছে বিধায় লাইভ সিস্টেম হইতে মূল্যবান ডিজিটাল নমুনা বা আলামত উদ্ঘাটন করা সম্ভব। ডিভাইসের সুইচ অফ করিলে ভোলাটাইল মেমরি হইতে মূল্যবান উপাত্ত (যেমন- ক্লাউডে সংরক্ষিত উপাত্ত, এনক্রিপ্টেড উপাত্ত, রানিং প্রসেস, নেটওয়ার্ক সংযোগ সম্পর্কিত উপাত্ত, মাউন্টেড ফাইল সিস্টেম, ইত্যাদি) হারাইয়া যাইতে পারে বিধায় লাইভ সিস্টেম পরীক্ষণের সময় র‍্যাম (RAM), রানিং প্রসেস, নেটওয়ার্ক সংযোগ, সিস্টেম সেটিংস, স্টোরেজ মিডিয়া এবং ক্লাউড সার্ভিস সংক্রান্ত উপাত্তসমূহ বিবেচনা লইতে হইবে।

(৩) স্বয়ংক্রিয় প্রক্রিয়াকরণ:

ফরেনসিক সফটওয়্যারে প্রাপ্তিসাধ্য বৈশিষ্ট্যসমূহ ব্যবহার করিয়া স্বয়ংক্রিয় প্রক্রিয়াকরণের কার্য সম্পন্ন করিতে হইবে। পরীক্ষণ কার্যক্রম শুরু করিবার পূর্বে ফরেনসিক বিশ্লেষক বা পরীক্ষক উহার পরীক্ষার পরিধি নির্ণয় করিবেন। স্বয়ংক্রিয় প্রক্রিয়াকরণ পদ্ধতিতে যেসকল কার্যক্রম ধারাবাহিকভাবে সম্পন্ন করিতে হইবে, উহা নিম্নরূপ:

(ক) অপারেটিং সিস্টেম ও ইউজার উপাত্ত আহরণ;

(খ) ZIP, RAR এবং এনক্রিপ্টেড ফাইলসমূহ;

(গ) মেইল বক্স, ইন্টারনেট হিস্টোরি, ইত্যাদি আহরণ;

(ঘ) ডিজিটাল স্বাক্ষর বিশ্লেষণ;

(ঙ) মুছিয়া ফেলা ফাইলসমুহ পুনরুদ্ধার;

(চ) মুছিয়া ফেলা পার্টিশন পুনরুদ্ধার;

(ছ) বিশেষ ধরনের ফাইল চিহ্নিতকরণ;

(জ) অপারেটিং সিস্টেম এর লগ প্রসেসিং।

(৪) উপাত্ত পুনরুদ্ধার:

সাধারণত ভৌত ও লজিক্যাল পদ্ধতিতে উপাত্ত পুনরুদ্ধার সম্পন্ন হইয়া থাকে। ফাইল সিস্টেম যাহাই হউক না কেন ভৌত পুনরুদ্ধার পদ্ধতিতে উপাত্ত চিহ্নিত করিয়া উহা উদ্ধার করিতে হইবে এবং লজিক্যাল উদ্ধার পদ্ধতিতে স্থাপিত (Installed) অপারেটিং সিস্টেম, ফাইল সিস্টেম, অথবা এপ্লিকেশন এর ভিত্তিতে উপাত্ত চিহ্নিত ও পুনরুদ্ধার করা হয় ।

(ক) **ভৌত পুনরুদ্ধার:** এই পদ্ধতিতে ড্রাইভে যে প্রকারেই ফাইল সিস্টেম বিন্যস্ত থাকুক না কেন, নিম্নবর্ণিতভাবে শুধুমাত্র ভৌত স্তর হইতে উপাত্ত পুনরুদ্ধার করিতে হইবে:

(অ) মূলশব্দ (Keyword) খুঁজিয়া বাহির করা, ফাইল সনাক্তকরণ (File Carving), এবং ভৌত ড্রাইভ হইতে অব্যবহৃত স্থান (Un-Allocated Space), বিভাজন টেবিল (Partition table) বাহির করা;

(আ) যে সকল তথ্য বা উপাত্ত অপারেটিং সিস্টেম বা ফাইল সিস্টেমের অন্তর্গত নয় সেইগুলি

মূলশব্দ (Keyword) দ্বারা খুঁজিয়া বাহির করা;

(ই) যে সকল তথ্য বা উপাত্ত অপারেটিং সিস্টেম বা ফাইল সিস্টেমের অন্তর্গত নয় সেইগুলি পুনরুদ্ধার ফাইল সনাক্তকরণ দ্বারা খুঁজিয়া বাহির করা;

(ঈ) সমগ্র হার্ড ড্রাইভের ভৌত আকার বিভাজন টেবিল পরীক্ষা করিয়া ফাইল সিস্টেমের বিন্যাস বাহির করা।

(খ) **লজিক্যাল পুনরুদ্ধার:** ড্রাইভে ফাইল সিস্টেমের ভিত্তিতে এই পদ্ধতিতে ডাটা, (যথা: সক্রিয় ফাইলসমূহ, মুছিয়া ফেলা ফাইল, ফাইলের মধ্যবর্তী স্থান, অবণ্টনকৃত স্থান ইত্যাদি) পুনরুদ্ধার করা হইয়া থাকে। ফাইল সিস্টেমের তথ্য পুনরুদ্ধার করিতে ফাইলের বিভিন্ন বৈশিষ্ট্য, যথা: ফাইলের অবকাঠামো, ফাইলের ধরন, ফাইলের নাম, সাইজ, অবস্থান, তারিখ, সময় ও অন্যান্য বিষয়ের উপর নির্ভর করিয়া নিম্নবর্ণিত ধাপসমূহ অনুসরণ করিতে হইবে, যথা:-

(অ) নির্ণীত হ্যাশ মানের সহিত বিশুদ্ধ ফাইলের হ্যাশ মানের তুলনা করিয়া পরিচিত ফাইল নিরূপন ও নির্ধারণ;

(আ) ড্রাইভে ফাইলের নাম ও ধরন, ফাইলের হেডার এবং অবস্থানের ভিত্তিতে পরীক্ষার জন্য প্রাসঙ্গিক ফাইলসমূহ আহরণ;

(ই) মুছিয়া ফেলা ফাইলসমূহ পুনরুদ্ধার;

(ঈ) পাসওয়ার্ড দ্বারা সুরক্ষিত, এনক্রিপ্টেড ও জিপ করা ফাইলসমূহ পুনরুদ্ধার;

(উ) ফাইলসমূহের মধ্যবর্তী ফাঁকা স্থান সনাক্তকরণ;

(ঊ) অবণ্টনকৃত স্থান সনাক্তকরণ।

(৫) ফিল্টারিং:

ফরেনসিক বিশ্লেষণের পরিমান কমাইয়া আনিবার জন্য ডিজিটাল নমুনা বা আলামতকে বিশ্লেষণের পূর্বেই ফিল্টারিং করা যাইবে। এই ক্ষেত্রে হোয়্যাইট লিস্টিং পদ্ধতিতে হ্যাশ প্রযুক্তির মাধ্যমে জানা অপারেটিং সিস্টেম অথবা প্রোগ্রাম ফাইলসমূহকে ফিল্টার আউট করা ও ব্লাকলিস্টিং পদ্ধতিতে জানা অবৈধ ফাইলসমূহের উপাত্ত-ভান্ডারে হ্যাশ প্রযুক্তির মাধ্যমে ম্যাচিং করানো হইয়া থাকে।

৩০। মোবাইল ডিভাইস পরীক্ষণ পদ্ধতি:

মোবাইল ডিভাইসের অসংখ্য ব্রান্ড ও মডেল, মোবাইলে সংরক্ষিত উপাত্ত ও মোবাইলের ধরনের প্রাচুর্যতার কারনে ইহার ডিজিটাল ফরেনসিক এর ক্ষেত্রে বিশেষ জটিল সমস্যা বিরাজমান। মোবাইল ডিভাইস এর ফরেনসিক এর সাধারণ পদ্ধতিসমূহ নিম্নরূপ:

(ক) স্বয়ংক্রিয় প্রক্রিয়াকরণ:

মোবাইল ডিভাইস এর বিভিন্ন ধরনের হার্ডওয়্যার, সফটওয়্যার ব্যবহৃত হওয়ায় ইহার ফরেনসিক বিশ্লেষণে ভিন্ন মাত্রা প্রয়োজন। ইহার জন্য বিশেষায়িত ফরেনসিক টুল যাহা স্বয়ংক্রিয়ভাবে বিপুল পরিমান তথ্য উপাত্ত প্রক্রিয়াকরণ করিলেও মাঝে মাঝে ম্যানুয়াল পদ্ধতিতে যাচাই করিবার প্রয়োজন হয়।

(খ) ফিল্টারিং:

সাধারণত মোবাইল ডিভাইস এর তথ্য উপাত্তের টাইপ অনুযায়ী ইহার ফিল্টারিং করা হয়। যেমন যোগাযোগ উপাত্ত, এসএমএস ও অন্যান্য মিডিয়া ফাইল এর মতো ফাইলগুলো সংশ্লিষ্ট সফটওয়্যার বা টুলস দ্বারা প্রক্রিয়াকরণ এর সময় দ্রুত ফিল্টার করা যাইবে।

অংশ-১০: ডিজিটাল ফরেনসিক নমুনা বা আলামত বিশ্লেষণ

৩১। ফরেনসিক নমুনা বা আলামত বিশ্লেষণ:

(১) ডিজিটাল নমুনা বা আলামত বিশ্লেষণ ক্ষেত্রে ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর তফসিলের তৃতীয় অধ্যায়ের দফা (৩) এ বর্ণিত 'আহরিত ফাইলের বিশ্লেষণ' শিরোনামার আওতাধীন পদ্ধতি অনুসরণ করিতে হইবে (পরিশিষ্ট ১০ দ্রষ্টব্য);

(২) সহায়ক হিসেবে পরিশিষ্ট ০৬ তে বর্ণিত 'আলামত বিশ্লেষণ প্রক্রিয়া' অনুসরণ করা যাইবে।

৩২। কম্পিউটার সিস্টেম বিশ্লেষণ:

(১) ডিজিটাল চিহ্ন (Trace) এর প্রকারভেদ:

(ক) অন্যান্য অপরাধ সংগঠনের মতই কম্পিউটার বা ডিজিটাল ডিভাইস দ্বারা অপরাধ সংগঠনের ক্ষেত্রেও সাধারণভাবে অপরাধীরা ডিজিটাল চিহ্ন রাখিয়া আসে। ইহার মধ্যে কিছু চিহ্ন সহজেই আবিষ্কারযোগ্য আবার কিছু চিহ্ন সহজে আবিষ্কারযোগ্য নহে।

(খ) সহজেই আবিষ্কারযোগ্য চিহ্নসমূহ নিম্নে উল্লেখ করা হইলো:

(অ) স্লাক স্পেস (Slack space);

(আ) অবরাদ্দকৃত স্পেস (Unallocated space);

(ই) MFT এন্ট্রিস;

(ঈ) RAM;

(গ) সহজে আবিষ্কারযোগ্য নহে এমন চিহ্নসমূহ নিম্নে উল্লেখ করা হইলো:

(অ) থাম্ব ক্যাশ;

(আ) সদ্য ব্যবহৃত ফাইলের লিস্ট;

(ই) লগ ফাইল;

(ঈ) ব্রাউজার হিস্টোরি;

(উ) ব্রাউজার ক্যাশ;

(ঊ) সর্বাধিক ব্যবহৃত প্রগ্রামসমূহ;

(ঋ) ফরম উপাত্ত;

(এ) Pagefiles.sys

(ঐ) Hiberfil.sys

(ও) ভলিউম শ্যাডো কপি;

(ঔ) ডাউনলোড হিস্টোরি।

(২) বিভিন্ন প্রকার চিহ্ন আহরণ পদ্ধতি:

(ক) ইমেইল;

(খ) অফিস নথি (ওয়ার্ড, স্প্রেড শিট, প্রেজেন্টেশন);

(গ) ছবি ও ভিডিও;

(ঘ) ইন্টারনেট ব্রাউজার: গুরুত্বপূর্ণ নমুনা বা আলামত হিসেবে ইন্টারনেট ব্রাউজার থেকে নিম্নোক্ত প্রমান পাওয়া যায়, যথা:

(অ) ওয়েবসাইট ব্রাউজ হিস্টোরি;
(আ) লোকাল ক্যাশ বা টেম্পরারি ইন্টারনেট ফাইল;
(ই) বুকমার্ক বা ফেভারিটস;
(ঈ) সেশান তথ্যাবলী;
(উ) কুকিজ সমূহ;
(ঊ) সংরক্ষিত ইউজার নেম ও পাসওয়ার্ড;
(ঋ) ফরম ফিল্ড এর এন্ট্রি সমূহ;
(এ) ইন্টারনেট কি ওয়ার্ড সার্স;

(ঙ) সফটওয়্যার;

(চ) নিম্নবর্ণিত বিষয়সমুহে কম্পিউটার ইউজার আক্টিভিটি লগ সংরক্ষিত থাকে;

(অ) ডিভাইস পাওয়ার অন এবং শাটডাউন টাইম;
(আ) সফটওয়্যার সেটিংস;
(ই) সাম্প্রতিক ব্যবহার হওয়া ফাইলসমূহ;
(ঈ) ডিভাইসের ব্যবহার বিস্তারিত;
(উ) ইউজার লগইন;
(ঊ) ওয়াই-ফাই সংযোগ;
(ঋ) পছন্দনীয় প্রোগ্রামের তালিকা;
(এ) ইউজার এনভাইরনমেন্ট এর সেটআপ;
(ঐ) বেশি ব্যবহৃত প্রোগ্রামসমূহ, ইত্যাদি।

(ছ) লগ ফাইলসমুহ;

(জ) এনক্রিপশন;

(ঝ) অবরাদ্ধকৃত স্পেস (Unallocated Space);

(ঞ) ক্লাউড এবং রিমোট স্টোরেজ;

(ট) কম্পিউটার মেমরি।

৩৩। মোবাইল ডিভাইস এর উপাত্ত বিশ্লেষণ:

(১) মোবাইল ডিভাইসে পারস্পারিক যোগাযোগের রেকর্ড, লগ ফাইল এবং ইহার সহিত যোগাযোগের নির্দিস্ট সময় ও তারিখ সংরক্ষিত থাকে। তাহাছাড়া মোবাইল ডিভাইসে মিডিয়া ফাইল, ছবি, জিপিএস লোকেশন, ইত্যাদি সংরক্ষিত থাকে।

(২) মোবাইল ডিভাইসের ডিজিটাল চিহ্নের (Trace) শ্রেণিবিন্যাস:

(ক) যোগাযোগের উপাত্ত;

(খ) মিডিয়া ফাইলসমূহ;

(গ) অন্যান্য উপাত্ত।

(৩) মোবাইল ডিভাইসের বিভিন্ন প্রকার চিহ্ন আহরণ পদ্ধতি:

(ক) কল হিস্টোরি;

(খ) কন্ট্রাক্ট লিস্ট;

(গ) টেক্সট মেসেজ এবং ইমেইল;

(ঘ) ছবি, ভিডিও এবং অডিও;

(ঙ) ইন্টারনেট ব্রাউজিং হিস্টোরি এবং কি ওয়ার্ড সার্স;

(চ) চ্যাট লগ এবং মেসেজিং অ্যাপ্লিকেশান;

(ছ) সোশ্যাল মিডিয়া আকাউন্ট;

(জ) ক্যালেন্ডার এবং নোটসমূহ;

(ঝ) মোবাইল নেটওয়ার্ক, ওয়াই-ফাই, ব্লু-টুথ সংযোগ;

(ঞ) লোকেশন, ডাইরেকশন ও ফেভারিটসমূহ;

(ট) ডকুমেন্ট, পিডিএফ ও অন্যান্য ফাইল প্রক্রিয়াকরণ সফটওয়্যার, ইত্যাদি।

অংশ-১১: ফরেনসিক প্রতিবেদন প্রস্তুতকরণ ও উপস্থাপন

৩৪। ফরেনসিক প্রতিবেদন প্রস্তুতকরণ ও উপস্থাপন:

ফরেনসিক প্রতিবেদন প্রস্তুতকরণ ও উপস্থাপনের ক্ষেত্রে ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর তফসিলের চতুর্থ অধ্যায়ে বর্ণিত 'নথিভূক্তকরণ ও প্রতিবেদন প্রস্তুতকরণ' শিরোনামার আওতাধীন পদ্ধতি অনুসরণ করিতে হইবে (পরিশিষ্ট ১১ দ্রষ্টব্য)।

৩৫। ফরেনসিক ফলাফল উপস্থাপন:

(১) ডিজিটাল ফরেনসিক বিশ্লেষক বা পরীক্ষককে ফলাফল উপস্থাপনের সময় জটিল প্রযুক্তিগত বিষয়সমুহকে এমনভাবে ব্যাখ্যা এবং অনুবাদ করিতে হইবে যাহাতে সংশ্লিষ্ট সকলেই সহজেই উহা বুঝিতে সক্ষম হয়।

(২) ফরেনসিক বিশ্লেষক বা পরীক্ষককে তাহার বিশ্লেষণ কার্যসম্পন্নের পর প্রাপ্ত পর্যবেক্ষণ ও ফলাফল ফরেনসিক প্রতিবেদনে অন্তর্ভুক্ত করিতে হইবে।

(৩) এইক্ষেত্রে অন্যান্য ডিজিটাল সাক্ষ্য প্রমানের সহিত সামঞ্জস্য রাখিবার প্রয়োজনে বিশেষায়িত সফটওয়্যার বা টুলস এর সহযোগিতা গ্রহণ যাইতে পারে।

৩৬। ডিজিটাল সাক্ষ্য প্রমাণাদির গ্রহণযোগ্যতা:[৬]

ফরেনসিক বিশ্লেষক বা পরীক্ষককে নিম্নবর্ণিত ইলেকট্রনিক সাক্ষ্য প্রমাণ গ্রহণযোগ্যতার মানদণ্ড বিবেচনায় লইয়া ডিজিটাল সাক্ষ্য প্রমাণ মূল্যায়ন করিতে হইবে-

(ক) সঠিকতা (Authenticity): ফরেনসিক প্রতিবেদনে যেকোনো সাইবার ইন্সিডেন্ট বা ঘটনা এমনভাবে উপস্থাপিত হইতে হইবে যেন ঘটনাকে বিতর্কিত না করে এবং ডিজিটাল নমুনা বা আলামতের বিশ্লেষণ মূল ঘটনার সহিত সামঞ্জস্যপূর্ণতাকে নির্দেশ করে;

(খ) সম্পূর্ণতা (Completeness): ডিজিটাল নমুনা বা আলামতের বিশ্লেষণ সম্পর্কে যেকোন মতামত এবং প্রমাণসমূহ সাইবার ঘটনা সম্পর্কে সম্পূর্ণভাবে বর্ণনা করিবে এবং সমগ্র ঘটনাকে কোনভাবে খাটো করিয়া চাহিদা মাফিক বা নিজস্ব অনুকূলে বর্ণনা করিবে না;

(গ) নির্ভরযোগ্যতা (Reliability): ডিজিটাল নমুনা বা আলামত সংগ্রহ ও ব্যবহারের যথার্থতা ও বিশ্বাসযোগ্যতা সম্পর্কে যাহাতে কোন প্রকার সন্দেহের সৃষ্টি না হয় সেই বিষয়ে প্রয়োজনীয় ব্যবস্থা গ্রহণ করিতে হইবে;

(ঘ) বিশ্বাসযোগ্যতা (Convincing): ডিজিটাল সাক্ষ্য-প্রমাণ বিশ্বাসযোগ্যভাবে উপস্থাপন করিতে হইবে যাহাতে উহা মূল ঘটনার সহিত পরিপূরক হয়;

(ঙ) সমানুপাতিকতা (Proportionality): ডিজিটাল সাক্ষ্য প্রমাণ সংগ্রহের উদ্দেশ্যে ব্যবহৃত পদ্ধতি সমানুপাতিক ও ন্যায্য হইতে হইবে।

অংশ ১২: ডিজিটাল ফরেনসিক ল্যাবরেটরির অনুসরণীয় মানদণ্ড

৩৭। ল্যাব কর্তৃক অনুসরণীয় মানদণ্ড:

ডিজিটাল ফরেনসিক ল্যাব ডিজিটাল ফরেনসিক কার্যক্রমের সকল ধরনের মানদণ্ডের অনুসরণ নিশ্চিত করিবে এবং ব্যবহারিক দিক হইতে ডিজিটাল ফরেনসিক ল্যাব সাধারণভাবে নিম্নবর্ণিত মানদণ্ড অনুসরণ করিবে, যথা: -

(ক) ISO/IEC/BDS 17025: টেষ্টিং ও ক্যালিব্রেশন পরীক্ষাগারের যোগ্যতার সাধারণ মাপকাঠি (পরিশিষ্ট

[6] INTERPOL Global guidelines for digital forensic laboratories, Section 5.4.1, page: 52

১২ক দ্রষ্টব্য);

(খ) ISO/IEC/BDS 15489: রেকর্ডস ব্যবস্থাপনা (পরিশিষ্ট- ১২খ দ্রষ্টব্য);

(গ) ISO/IEC/BDS 27037: ডিজিটাল সাক্ষ্য সনাক্তকরণ, সংগ্রহ, অধিগ্রহণ এবং সংরক্ষণ নির্দেশিকা (পরিশিষ্ট- ১২গ দ্রষ্টব্য);

(ঘ) ISO/IEC/BDS 27041: ঘটনা তদন্ত পদ্ধতির গ্রহণযোগ্যতা ও উপযুক্ততা নিরুপণের মাপকাঠি/নির্দেশিকা (পরিশিষ্ট- ১২ঘ দ্রষ্টব্য);

(ঙ) ISO/IEC/BDS 27042: ডিজিটাল সাক্ষ্য বিশ্লেষণ ও স্পষ্টিকরণ নির্দেশিকা (পরিশিষ্ট- ১২ঙ দ্রষ্টব্য);

(চ) ISO/IEC/BDS 27043: ঘটনা তদন্তের পদ্ধতি ও নীতিমালা (পরিশিষ্ট- ১২চ দ্রষ্টব্য);

(ছ) ISO/IEC/BDS 27050: ইলেকট্রনিক ডিসকভারি (পরিশিষ্ট- ১২ছ দ্রষ্টব্য) ।

অংশ-১৩: ফরেনসিক ল্যাব এর গুনগতমান নিশ্চিতকরণ (Quality Assurance)

৩৮। গুনগতমান নিশ্চিতকরণ:

ফরেনসিক বিশেষজ্ঞ বা পরীক্ষক কর্তৃক ফরেনসিক প্রতিবেদন উপস্থাপনে বিবেচ্য বিষয়সমূহ:

(ক) ফরেনসিক নমুনা বা আলামত বিশ্লেষণ প্রক্রিয়ার ব্যাখ্যা;
(খ) ফরেনসিক বিশ্লেষক বা পরীক্ষকের দক্ষতা;
(গ) ফরেনসিক নমুনা বা আলামত বিশ্লেষণে ব্যবহৃত যন্ত্রপাতির বিবরণ;
(ঘ) ফরেনসিক নমুনা বা আলামত বিশ্লেষণ পদ্ধতির বিবরণ;
(ঙ) সাক্ষ্য প্রমাণ ব্যবহার পদ্ধতি;
(চ) ফরেনসিক নমুনা বা আলামত বিশ্লেষণ সম্পর্কিত অন্যান্য বিষয়াদি।

৩৯। গুনগতমান নিশ্চিতকরণের উপাদান (Component)

গুনগতমান নিশ্চিতকরণ ও বাস্তবায়নআর্থ ডিজিটাল ফরেনসিক ল্যাবরেটরি এতদুদ্দেশ্যে পরিশিষ্ট ১৩ এ বর্ণিত গুনগতমান নিশ্চিতকরণের উপাদান সম্পর্কিত চেকলিস্ট অনুসরণ করিবে।

অংশ-১৪: বিবিধ বিষয়াবলী

৪০। জরুরি পরিস্থিতিতে মহাপরিচালকের ক্ষমতা:

ডিজিটাল নিরাপত্তা এজেন্সি মহাপরিচালক, কোনো ডিজিটাল ফরেনসিক ল্যাব কর্তৃপক্ষের অনুরোধক্রমে, জরুরী পরিস্থিতিতে বিশেষায়িত সেবার প্রয়োজন হইলে তিনি চাহিদাকৃত বিষয়ে ডিজিটাল ফরেনসিক ল্যাবকে প্রয়োজনীয় সহযোগিতা ও পরামর্শ প্রদান করিতে পারিবেন।

৪১। নমুনা বা আলামতের তথ্য-উপাত্ত সংরক্ষণ:

কম্পিউটার বা ডিজিটাল ডিভাইসে সংরক্ষিত ডিজিটাল নমুনা বা আলামত বা তৎসংশ্লিষ্ট কোনো তথ্য-উপাত্ত সংরক্ষণ করিবার প্রয়োজনে ডিজিটাল ফরেনসিক ল্যাব, মহাপরিচালকের পূর্বানুমোদনক্রমে, উহা তৎকর্তৃক

নির্ধারিত সময় পর্যন্ত সংরক্ষণ করিতে পারিবে এবং উক্তরূপ ডিজিটাল নমুনা বা আলামত বা তথ্য-উপাত্ত সংরক্ষণের ক্ষেত্রে ডিজিটাল স্টোরেজে ইন্টারনেট সংযোগবিহীন অবস্থায় রাখিতে হইবে।

৪২। ফরেনসিক পরীক্ষা সম্পাদনের সময়সীমা:

এই গাইডলাইনের অধীন ফরেনসিক বিশ্লেষণ বা পরীক্ষা মহাপরিচালক কর্তৃক, সময় সময়, সাধারণ বা বিশেষ আদেশ দ্বারা, নির্ধারিত সময়ের মধ্যে সম্পন্ন করিতে হইবে।

৪৩। তথ্যে-উপাত্তের গোপনীয়তা:

ডিজিটাল ফরেনসিক ল্যাবের ফরেনসিক বিশ্লেষক বা পরীক্ষকসহ সকল কর্মকর্তা ও কর্মচারী ফরেনসিক বিশ্লেষণ বা পরীক্ষা সংক্রান্ত সকল তথ্য-উপাত্তের গোপনীয়তা বজায় রাখিবেন।

৪৪। ডিজিটাল ফরেনসিক ল্যাব পরিচালনা:

ডিজিটাল নিরাপত্তা আইন, ২০১৮, ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০, এবং এই গাইডলাইনে বিধৃত বিধি-বিধান অনুসরণক্রমে ডিজিটাল ফরেনসিক ল্যাবের যাবতীয় কার্যক্রম পরিচালিত হইবে।

৪৫। নির্দেশ প্রদানের ক্ষমতা:

কোনো ডিজিটাল ফরেনসিক ল্যাব এই গাইডলাইন প্রতিপালনে অসমর্থ হইলে, মহাপরিচালক, লিখিতভাবে, উক্তরূপ কারণ সম্বলিত ব্যাখ্যা চাহিয়া এই গাইডলাইন অনুসরণের জন্য নির্দেশ প্রদান করিতে পারিবে; এবং উক্তরূপে কোনো নির্দেশ প্রদান করা হইলে সংশ্লিষ্ট ফরেনসিক ল্যাব উহা প্রতিপালনে বাধ্য থাকিবে।

৪৬। অব্যাহতি:

মহাপরিচালক, কোনো বিশেষ পরিস্থিতি পরিহারের উদ্দেশ্যে, কোনো ডিজিটাল ফরেনসিক ল্যাবের আবেদনের পরিপ্রেক্ষিতে, কোনো নির্দ্দিষ্ট সময়ের জন্য, এই গাইডলাইনের সুনির্দ্দিষ্ট কোনো বিধানের প্রয়োগ হইতে, মহাপরিচালক কর্তৃক আরোপিত শর্ত সাপেক্ষে, অব্যাহতি প্রদান করিতে পারিবে।

৪৭। গাইডলাইনের সীমাবদ্ধতা:

(১) ডিজিটাল ফরেনসিক ল্যাব স্ব স্ব ক্ষেত্রে (Domain) সাইবার সিকিউরিটি, আইসিটি নীতিমালা, পরিকল্পনা ও বাস্তব ভিত্তিক অতিরিক্ত সুরক্ষা পদ্ধতি এবং বাস্তবায়ন করিতে হইবে। উক্ত ক্ষেত্রে এই গাইডলাইন ডিজিটাল ফরেনসিক ল্যাব এর জন্য একটি সহায়ক নির্দেশিকা হিসেবে বিবেচিত হইবে।

(২) এই গাইডলাইন এর অন্যতম লক্ষ্য হইবে ডিজিটাল ফরেনসিক ল্যাব এর পরিচালনা ও কার্য-সম্পাদনের নির্দেশনা বাস্তবায়ন করিবার জন্য সাংগঠনিকভাবে প্রাথমিক সরঞ্জাম (Tools) এবং পন্থা (Approaches) সম্পর্কে নির্দেশনা প্রদান করা।

(৩) প্রযুক্তিগত পরিবর্তন, বিভিন্ন মাধ্যম হতে প্রাপ্ত জ্ঞান, বাস্তব অভিজ্ঞতার ভিত্তিতে এই গাইডলাইন নিয়মিতভাবে হালনাগাদ করা যাইবে।

পরিশিষ্ট-০১: ডিজিটাল ফরেনসিক ল্যাব স্থাপন ও মাননিয়ন্ত্রণ

(ডিজিটাল নিরাপত্তা আইন, ২০১৮ এর ধারা ১০ ও ১১)

১০। ডিজিটাল ফরেনসিক ল্যাব ।- (১) এই আইনের উদ্দেশ্য পূরণকল্পে, এজেন্সির নিয়ন্ত্রণ ও তত্ত্বাবধানে, এক বা একাধিক ডিজিটাল ফরেনসিক ল্যাব থাকিবে।

(২) উপ-ধারা (১) এ যাহা কিছুই থাকুক না কেন, এই আইন প্রবর্তনের পূর্বে কোন সরকারি কর্তৃপক্ষ বা সংস্থার অধীন কোন ডিজিটাল ফরেনসিক ল্যাব স্থাপিত হইয়া থাকিলে, ধারা ১১ এর অধীন নির্ধারিত মান অর্জন সাপেক্ষে, এজেন্সি উহাকে স্বীকৃতি প্রদান করিবে এবং সেইক্ষেত্রে উক্ত ল্যাব এই আইনের অধীন স্থাপিত হইয়াছে বলিয়া গন্য হইবে।

(২) উপ-ধারা (১) এর অধীন নির্ধারিত গুনগত মান নিশ্চিত করিবার ক্ষেত্রে অন্যান্য বিষয়ের মধ্যে প্রত্যেক ডিজিটাল ফরেনসিক ল্যাব –

(ক) উপযুক্ত যোগ্যতাসম্পন্ন ও প্রশিক্ষনপ্রাপ্ত জনবল দ্বারা উহার কার্যক্রম পরিচালনা করিবে;
(খ) উহার ভৌত অবকাঠামোগত সুযোগ সুবিধা নিশ্চিত করিবে;
(গ) উহার অধীন সংরক্ষিত তথ্যাদির নিরাপত্তা ও গোপনীয়তা বজায় রাখিবার জন্য প্রয়োজনীয় উদ্যোগ গ্রহণ করিবে;
(ঘ) ডিজিটাল প্রোক্ষার কারিগরি মান বজায় রাখিবার লক্ষ্যে মানসম্পন্ন যন্ত্রপাতি ব্যবহার করিবে; এবং
(ঙ) বৈজ্ঞানিক প্রক্রিয়া অনুসরণক্রমে, বিধি দ্বারা নির্ধারিত পদ্ধতিতে, কার্য সম্পাদন করিবে।

১১। ডিজিটাল ফরেনসিক ল্যাব এর মান নিয়ন্ত্রণ।– (১) এজেন্সি, বিধি দ্বারা নির্ধারিত মানদণ্ড অনুযায়ী প্রত্যেক ডিজিটাল ফরেনসিক ল্যাব এর গুনগত মান নিশ্চিত করিবে।

পরিশিষ্ট-০২: ডিজিটাল ফরেনসিক ল্যাব এর জনবল

(ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর ধারা ১৬)

১৬। **ডিজিটাল ফরেনসিক ল্যাবের জনবল।-** (১) এজেন্সির অনুমোদিত সাংগঠনিক কাঠামো অনুযায়ী ডিজিটাল ফরেনসিক ল্যাবের প্রয়োজনীয় জনবল থাকিবে এবং উক্ত ল্যাবের কার্যাবলী সুষ্ঠুভাবে সম্পাদনের লক্ষ্যে এজেন্সি, প্রযোজ্য বিধি-বিধান অনুসরণক্রমে প্রয়োজনীয় সংখ্যক কর্মচারী নিয়োগ করিতে পারিবে।

(২) ডিজিটাল ফরেনসিক ল্যাবে অন্যূন ১ (এক) জন করিয়া ডিজিটাল ফরেনসিক ল্যাব সুপারভাইজার ও ডিজিটাল ফরেনসিক ল্যাব বিশেষজ্ঞ থাকিবে।

(৩) ডিজিটাল ফরেনসিক ল্যাব সুপারভাইজার এর দায়িত্ব হইবে নিম্নরূপ, যথা: -

(ক) সিনিয়র ফরেনসিক বিশেষজ্ঞ হিসেবে দায়িত্ব পালন;
(খ) আইন ও এই বিধিমালায় বর্ণিত মানদন্ড নিয়ন্ত্রণের উদ্দেশ্যে নিয়োজিত ল্যাব কর্মকর্তাদের প্রশিক্ষণ নিশ্চিতকরণ;

(গ) ল্যাবে কর্মরত কর্মকর্তাগণের বাৎসরিক কর্মদক্ষতা মূল্যায়ন;
(ঘ) ল্যাব কর্মকর্তাগণের প্রস্তুতকৃত প্রামাণিক দলিল বা প্রতিবেদনের প্রশাসনিক ও কারিগরি পর্যালোচনাকরণ;
(ঙ) ল্যাব কর্মকর্তাগণের পারদর্শিতা ও দক্ষতা যাচাইকরণ;
(চ) ল্যাবের হার্ডওয়্যার, সফটওয়্যার ও অন্যান্য যন্ত্রপাতির সঠিক কার্যকারিতা নিশ্চিতকরণ;
(ছ) ফরেনসিক কার্যে ব্যবহৃত হার্ডওয়্যার ও সফটওয়্যারের গুনগতমান ও বৈধতা নিশ্চিতকরণ;
(জ) ফরেনসিক ল্যাবের উপযোগী হার্ডওয়্যার ও সফটওয়্যার ব্যবহারের সুপারিশকরণ।

(৪) ডিজিটাল ফরেনসিক ল্যাব বিশেষজ্ঞের দায়িত্ব হইবে নিম্নরূপ, যথা:-

(ক) ইলেক্ট্রনিক যন্ত্র হইতে তথ্য উপাত্ত সংগ্রহ ও পুনরুদ্ধার;
(খ) ডিজিটাল তথ্য সংগ্রহ ও পুনরুদ্ধারের ভিত্তিতে নিরপেক্ষ প্রতিবেদন প্রস্তুতকরণ;
(গ) মামলার কারিগরি ও প্রশাসনিক প্রতিবেদন পর্যালোচনা;
(ঘ) ফরেনসিক নমুনা বা ডিজিটাল আলামত চিহ্নিতকরণের নিমিত্ত অপরাধ সংগঠিত হইবার স্থানে আইন প্রয়োগকারী সংস্থাকে সহযোগিতা করা;
(ঙ) আদালতে তথ্য উপাত্তের সত্যতা যাচাইয়ে প্রামাণিক সাক্ষ্য প্রদান;
(চ) কর্মকর্তাগণকে হাতে-কলমে প্রশিক্ষণ, পরামর্শ ও দিক নির্দেশনা প্রদান;
(ছ) ফরেনসিক কার্যে ব্যবহৃত হার্ডওয়্যার ও সফটওয়্যারের গুণগতমান ও কার্যকারিতা নিশ্চিতকরণ;
(জ) ফরেনসিক মামলায় ব্যবহৃত হার্ডওয়্যার ও সফটওয়্যার এর কর্মক্ষমতা নিশ্চিতকরণ।

পরিশিষ্ট-০৩: ডিজিটাল ফরেনসিক ল্যাব এর জনবলের দক্ষতা

দক্ষতার পর্যায়	দক্ষতার বিষয় (Topic)	দক্ষতাসমূহ (Skill Set)
Foundation	Computer Foundation	Organization of Computer; How computer stores data; Bits & Bytes; Evolution of digital media and storage system.
	File System	Decimal, Hexadecimal, binary; Little Endian, big Endian, Sectors, cluster, slack space, Metadata, data, filename, FAT, NTFS, EXT, HFS.
	Introduction to Investigation and Digital Forensics	Law Enforcement and Regulators; Infroduction to Forensic Science, Electronic Evidence and its nature, Categories of Electronic Evidence, Methodology; Forensic Technologies.
Identification	Information Gathering	Gather facts of the Case online; Preserve the gathered facts.
Collection & Examination	Collection and Examination	First responder roles and SOP; Dead Acquisition and Live acquisition; Choosing the best data acquisition method; Triage method; Triage tools.
Analysis	Data Recovery	Storage Technology; Damaged HDDand Flash drive symptoms; Logical and physical recovery; Data recovery tools; Recovery of data using tools.
	Computer Forensics	OS Technology; Metadata Registry; Artefacts; Data Extraction; Data Analysis; Data Hiding Technique; Analytics of large sets of data; Memory Analysis.
	Mobile Phone Forensics	Mobile phone technology and evolution, User, Telecommunication provider technology, types of data, acquire and analysis tools, preservation of data.
	Network Forensics	Network types; Internet history files and Cookies; User credentials; Network forensic tools, preservation of data.
	Audio, Video and Image Forensics	Understanding the technology; Enhancement; File authentication; comparison.
Emerging Technology	• Social Media Forensics • Database Forensics • Drone Forensics • Vehicle Forensics • Shipbourne Forensic • Cryptocurrency Forensics • Biometric Forensic	Understanding the technology; Accessing data from the device; Data extraction; Data analysis; Data interpretation; Reporting the findings.
Presentation	Report Writing	Format of the report; Effective result presentation to stakeholders.
	Law and Mock Court	Laws related to case; International laws; International collaboration; Presenting expert testimony in court; Introduction to court structure; Submitting electronic evidence to court;

Etiquette	Etiquette	Professional code of ethics; ethical and non-ethical code of conduct.
Lab Management	Quality Management	Understanding standards; Conducting audits; Quality management systems.
	Health and Safety	Identify Hazards; Health and Safety measures; Self protection.

পরিশিষ্ট-০৪: ডিজিটাল ফরেনসিক পরীক্ষার কেস অধিযাচন ফরম

তারিখ: *০০-০০-০০০০*

১। অধিযাচনপত্র প্রেরণকারী প্রতিষ্ঠানের নাম:

ঠিকানা :
টেলিফোন :
ইমেইল :

২। অধিযাচনপত্র প্রেরণকারী কর্মকর্তার নাম:

পদবী :
যোগাযোগের ঠিকানা :

৩। মামলার বিবরণ

৩.১। মামলা নং ও ধারা, থানা/ উপজেলা ও জেলা	
৩.২।অভিযোগকারীর নাম, এনআইডি নম্বর (যদি থাকে) ও ঠিকানা	
৩.৩। আসামীদের নাম, এনআইডি নম্বর (যদি থাকে) ও ঠিকানা	
৩.৪। মামলার সংক্ষিপ্ত বিবরণ	

৪। ডিজিটাল ফরেনসিক পরীক্ষার প্রেরিত আলামতের (exhibit) বিবরণ[৭]

৪.১। আলামতের **(exhibit)** আইডি ও সংক্ষিপ্ত বিবরণ	
৪.২। কে, কখন ও কিভাবে আলামতটি পাওয়া গিয়াছে?	
৪.৩। আলামতের উৎস	
৪.৪। আলামতের সহিত সংশ্লিষ্ট আসামী/ভিকটিম/অন্য কেহ[৮]	
৪.৫। মন্তব্য	

[৭] প্রত্যেক আলামতের নিমিত্তে আলাদা বিবরণ। ৪.১ থেকে ৪.৪ আলাদাভাবে পূরণ করিতে হইবে। একাধিক আলামতের ক্ষেত্রে প্রত্যেক ক্রমিকের সাথে ৪.১ক-৪.৫ক, ৪.১খ-৪.৫খ ..... পূরণ করুন।

[৮] Person of interest

৫। আলামত প্রেরণের বিবরণ এবং নমুনা সীল

(স্বাক্ষর/-)
নাম, পদবী
মোবাইল

ডিজিটাল ফরেনসিক ল্যাব কতৃক পূরণীয়

৬.১। পরীক্ষার নিমিত্তে গ্রহণের তারিখ ও সময়:

৬.২। গৃহিত আলামতের বিবরণ

৬.৩। গ্রহণকারী কর্মকর্তার নাম, পদবী ও স্বাক্ষর

৭। পরীক্ষা শেষে আলামত ফেরত প্রদানের তারিখ ও সময়, প্রতিবেদন, নমুনা সীল ও স্বাক্ষরের বিবরণ

৭.১। স্মারক নং, তারিখ ও সময়:	
৭.২। পরীক্ষিত আলামতের বিবরণ	
৭.৩। আলামত পরীক্ষার প্রতিবেদন	

৮। শর্তাবলি (Terms and Conditions):

১. ফরেনসিক বিশ্লেষণ পদ্ধতি নির্বাচন: ডিজিটাল ফরেনসিক ল্যাব আলামত বা নমুনা বিশ্লেষণের জন্য সর্বোত্তম পদ্ধতিই প্রয়োগ করিবে।

২. গোপনীয়তা রক্ষা করা: ডিজিটাল ফরেনসিক ল্যাব ইহার নিশ্চয়তা প্রদান করিতেছে যে, ফরেনসিক পরীক্ষার অধিযাচনকারী কর্তৃক প্রদত্ত যে কোনো তথ্য উপাত্ত এবং ফরেনসিক বিশ্লেষণের ফলে উদ্ভুত যে কোনো তথ্য উপাত্তসমুহ সর্বোচ্চ গোপনীয়তার সহিত ব্যবহার করা হইবে।

৩. নমুনা বা আলামতের নষ্ট বা ক্ষতি: ডিজিটাল ফরেনসিক ল্যাব ইহার নিশ্চয়তা প্রদান করিতেছে যে, বিশ্লেষণ পরিচালনার সময় নমুনা বা আলামতের অখন্ডতা রক্ষার জন্য সর্বদা প্রয়োজনীয় সতর্কতা অবলম্বন করিবে, ইহা সত্ত্বেও অধিযাচনকারী কর্তৃক বা বিশ্লেষণ চলাকালীন নমুনা বা আলামতের কোন নষ্ট বা ক্ষতি সাধিত হইলে দায়ী থাকিবে না।

৪. অতিরিক্ত বা অকার্যকর নমুনা বা আলামত: ফরেনসিক পরীক্ষার অধিযাচনকারী কর্তৃক প্রদত্ত নমুনা বা আলামতের কোনো অংশ অকার্যকর বা অব্যবহারযোগ্য হইলে উক্ত বিষয়ে ফরেনসিক ল্যাব অধিযাচনকারীর সহিত যোগাযোগ করিবেন। উক্ত যোগাযোগের পর ৩০ দিন অতিবাহিত হইলে ফরেনসিক ল্যাব কর্তৃক নির্ধারিত পদ্ধতিতে আলামত নিস্পত্তি করা হইবে। নিস্পত্তির পূর্বে অধিকারিকে অবহিত করা হইবে।

হস্তান্তরকারী কর্মকর্তার নাম, পদবী ও স্বাক্ষর	গ্রহণকারী কর্মকর্তার নাম, পদবী ও স্বাক্ষর

পরিশিষ্ট-০৫: চেইন অফ কাস্টডি

এক্সজিবিট/জব্দ তালিকা নম্বর	হস্তান্তরের তারিখ/ সময়/স্থান	তথ্য প্রমাণের বিবরণ

হস্তান্তরকারীর বিবরণ

গ্রহণকারীর বিবরণ

চেইন অফ কাস্টডি ট্রেকিং ফরম (Chain of Custody Tracking Form)

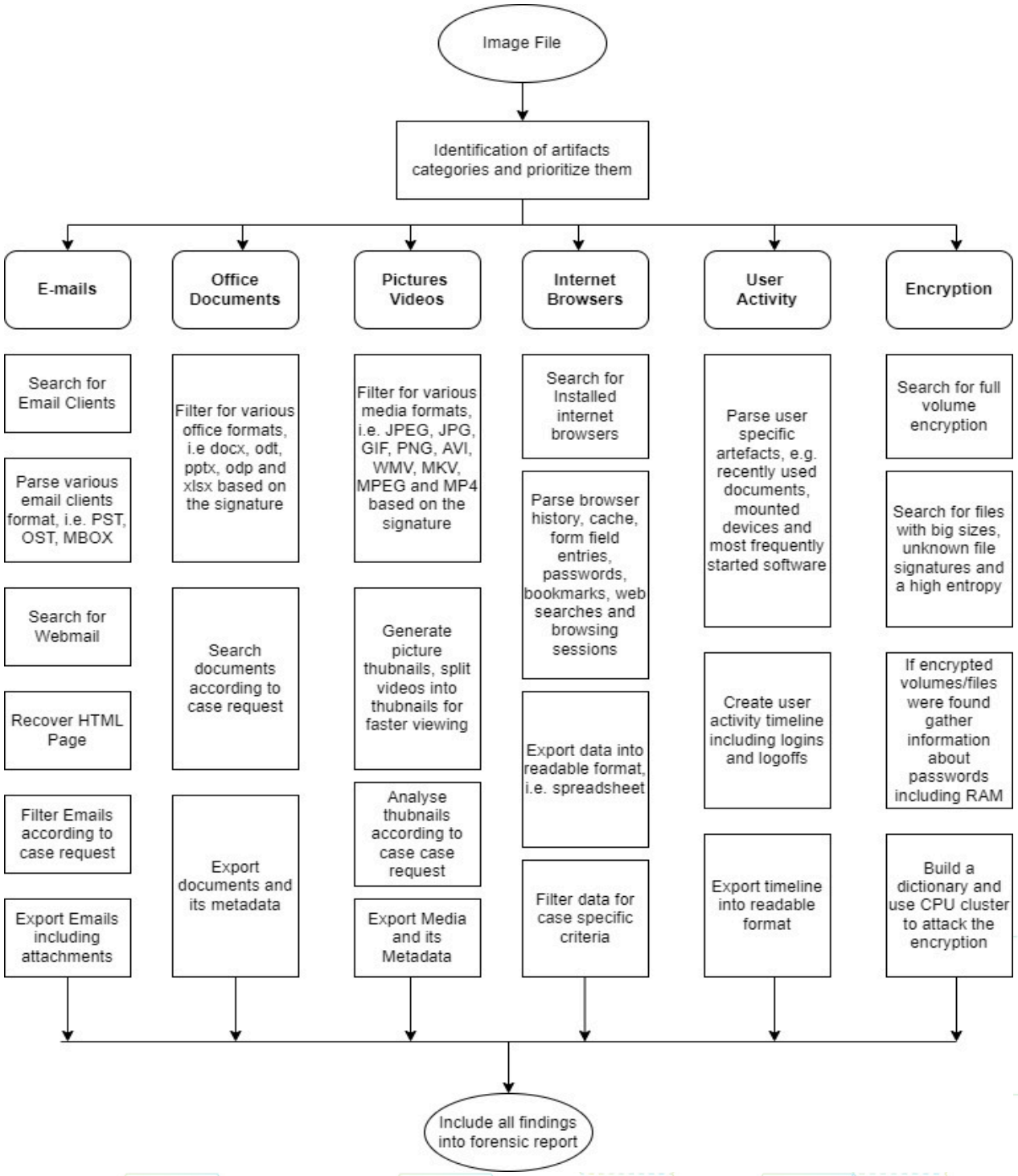
কেস নম্বর		তারিখ
সূত্রঃ নং		
প্রেরক		
পরীক্ষকের নাম ও পদবি		
তথ্য প্রমাণের বিবরণ		
আইটেম নম্বর	পরিমাণ	বিবরণ (মডেল, ক্রমিক নম্বর, অবস্থা, বিশেষ চিহ্ন নোট করুন)

চেইন অফ কাস্টডি				
আইটেম নম্বর	তারিখ ও সময়	প্রেরক (স্বাক্ষর ও আইডি)	প্রাপক (স্বাক্ষর ও আইডি)	মন্তব্য/স্থান

ফেরত প্রদানের স্লিপ	
কেস নম্বর	তারিখ
সূত্রঃ নং	
প্রেরক	
পরীক্ষকের নাম ও পদবি	

তথ্য প্রমাণের বিবরণ		
আইটেম নম্বর	পরিমাণ	বিবরণ (মডেল, ক্রমিক নম্বর, অবস্থা, বিশেষ চিহ্ন নোট করুন)

পরিশিষ্ট-০৬: ডিজিটাল নমুনা বা আলামত বিশ্লেষণ প্রক্রিয়া



পরিশিষ্ট-০৭: নমুনা বা আলামত অধিগ্রহণ প্রক্রিয়া
ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০

তফসিল

দ্বিতীয় অধ্যায়

ফরেনসিক নমুনা বা আলামত অধিগ্রহণ (Acquisition)

ফরেনসিক নমুনা বা আলামত অধিগ্রহণের ক্ষেত্রে নিম্নবর্ণিত ধাপসমূহ অনুসরণ করিতে হইবে, যথা:-

(ক) কার্যপ্রণালী।- নিম্নবর্ণিত বিষয়াদি বিবেচনা করিয়া ফরেনসিক পরীক্ষার জন্য ফরেনসিক নমুনা বা ডিজিটাল আলামত সংগ্রহ করিতে হইবে, যথা:-

(১) মূল ফরেনসিক নমুনা বা ডিজিটাল আলামতের সংরক্ষণ ও সুরক্ষার লক্ষ্যে বিট বাই বিট ইমেজিং এর মাধ্যমে ফরেনসিক পরীক্ষার জন্য কপি প্রস্তুতকরণ;

(২) নির্বাচিত বা ব্যবহৃত হার্ডওয়্যার ও সফটওয়্যারের কনফিগারেশন সিস্টেম নথিভুক্তকরণ;

(৩) নির্বাচিত বা ব্যবহৃত কম্পিউটার সিস্টেমের হার্ডওয়্যার এবং সফটওয়্যারের কার্যক্রম যাচাইকরণ;

(৪) ডিজিটাল ডিভাইসের কেসিং উন্মুক্ত করিয়া স্টোরেজ ডিভাইসে বাহির হইতে প্রবেশাধিকার নিশ্চিতকরণ;

(৫) নির্ধারিত ডিজিটাল ডিভাইসকে স্থির তড়িৎ (Static Electricity) ও চৌম্বক ক্ষেত্র (Magnetic Field) হইতে সুরক্ষা নিশ্চিতকরণ;

(৬) ডিজিটাল ডিভাইসের ভিতর বা বাহিরে রক্ষিত বা উভয় ধরনের স্টোরেজ ডিভাইস চিহ্নিতকরণ;

(৭) ডিজিটাল ডিভাইসের ইন্টারনাল স্টোরেজ ডিভাইস এবং হার্ডওয়্যারের কনফিগারেশন লিপিবদ্ধকরণ;

(৮) ড্রাইভ এর কনফিগারেশন (যথা: মডেল, আকার, জাম্পার সেটিংস, লোকেশন, ড্রাইভ ইন্টারফেস) লিপিবদ্ধকরণ;

(৯) নির্ধারিত ডিজিটাল ডিভাইসের অভ্যন্তরীণ কম্পোনেন্ট বা যন্ত্রাংশ পরীক্ষাকরণ (যথা: সাউন্ড কার্ড, ভিডিও কার্ড, নেটওয়ার্ক কার্ড সহ মিডিয়া অ্যাক্সেস কন্ট্রোল এড্রেস (ম্যাক), পারসনাল কম্পিউটার মেমোরি কার্ড, ইন্টারন্যাশনাল অ্যাসোসিয়েশন (পিসিএমসিআইএ) কার্ড ইত্যাদি);

(১০) নির্ধারিত ডিজিটাল ডিভাইসের ডাটা ধ্বংস, ক্ষতি বা পরিবর্তন রোধকল্পে স্টোরেজ ডিভাইস এর পাওয়ার সাপ্লাই, মাদারবোর্ড ও ডাটা কেবলের সংযোগ বিচ্ছিন্নকরণ;

(১১) সন্দেহজনক ডিজিটাল ডিভাইসের সিস্টেম হইতে কনফিগারেশনের তথ্য নিয়ন্ত্রিত বুটের মাধ্যমে অধিগ্রহণ;

(১২) সন্দেহজনক ডিজিটাল ডিভাইসের CMOS / BIOS তথ্য নিয়ন্ত্রিত বুটের মাধ্যমে অধিগ্রহণ;

(১৩) সন্দেহজনক ডিজিটাল ডিভাইসের বুট সিকোয়েন্স পরীক্ষাকরণ (যথা: ফ্লপি বা সিডি-রম ড্রাইভ হইতে সিস্টেম বুট করিতে বিআইওএস পরিবর্তন করা যাইতে পারে);

(খ) গৃহীত ডিজিটাল ডিভাইসের ফরেনসিক পরীক্ষার নিমিত্ত সিস্টেমের তারিখ ও সময় রেকর্ড ও সংরক্ষণের অনুসরণীয় পদ্ধতি:

(১) ফরেনসিক পরীক্ষার লক্ষ্যে সন্দেহজনক ডিজিটাল ডিভাইসের কার্যকারিতা (functionality) এবং ফরেনসিক বুট ডিস্ক পরীক্ষার লক্ষ্যে ফরেনসিক বুট ডিস্ক হইতে দ্বিতীয়বার নিয়ন্ত্রিত বুট কার্যকর করিতে হইবে।

(২) হার্ডডিস্কের সকল সংযোগ বিচ্ছিন্নক্রমে ফ্লপি বা ইউএসবি পোর্ট বা সিডি-রম বা ডিভিডি-রম ড্রাইভের সংযোগ নিশ্চিত করিতে হইবে।

(৩) ফরেনসিক বুট ডিস্কটি ফ্লপি বা ইউএসবি পোর্ট অথবা সিডি-রম ড্রাইভে রাখিতে হইবে এবং কম্পিউটার বুট করিবার সময় নিশ্চিত করিতে হইবে যে কম্পিউটারটি ফরেনসিক বুট ডিস্ক হইতে বুট করিতে হইবে।

(৪) স্টোরেজ ডিভাইসগুলি পুনরায় সংযুক্ত করিয়া তৃতীয় নিয়ন্ত্রিত বুট ব্যবহারের মাধ্যমে CMOS বা BIOS ড্রাইভের কনফিগারেশন তথ্য সংগ্রহ করিতে হইবে।

(৫) ফরেনসিক পরীক্ষার লক্ষ্যে নির্ধারিত ডিজিটাল ডিভাইসের স্টোরেজ ব্যাবহার করিয়া কম্পিউটারটিকে দুর্ঘটনাক্রমে বুট করা হইতে বিরত রাখিতে, বুট সিকোয়েন্স ফ্লপি বা ইউএসবি পোর্ট বা সিডি-রম ড্রাইভে ফরেনসিক বুট ডিস্ক নিশ্চিত করিয়া ডিজিটাল ডিভাইসটিকে বুট করিতে হইবে।

(৬) ড্রাইভ কনফিগারেশন তথ্যাবলীতে লজিক্যাল ব্লক এড্রেস (এল বি এ), লার্জ ডিস্ক, সিলিন্ডার , হেড, সেক্টর (সিএইচএস) বা অটো ডিটেক্ট অন্তর্ভুক্ত হইবে।

(গ) পাওয়ার সিস্টেম ডাউন।— (১) ফরেনসিক পরীক্ষার লক্ষ্যে নির্ধারিত ডিজিটাল ডিভাইসের স্টোরেজ ডিভাইসটি বাহির করিয়া পরীক্ষকের সিস্টেমে সংযোগের মাধ্যমে তথ্য অধিগ্রহণ করিতে হইবে। পরীক্ষকের সিস্টেমে জব্দকৃত ডিভাইসকে সংযুক্ত করিবার জন্য যথাযথ ব্যবস্থা গ্রহণ করিতে হইবে এবং ব্যতিক্রমী পরিস্থিতিতে জব্দকৃত ডিজিটাল ডিভাইস হইতে স্টোরেজ ডিভাইসগুলি পৃথক না করিবার সিদ্ধান্ত গ্রহণ করা যাইতে পারে তবে এইক্ষেত্রে নিম্নবর্ণিত বিষয়সমূহ বিবেচনা করিতে হইবে, যথা:-

(ক) RAID (Redundant Array of Independent Disk) এর ক্ষেত্রে পৃথকভাবে ডিস্কগুলি অধিগ্রহণ করিলে প্রত্যাশিত ফলাফল অনিশ্চিত হইতে পারে;

(খ) ল্যাপটপের ড্রাইভে প্রবেশ করা কঠিন হইতে পারে কারণ মূল সিস্টেম হইতে ড্রাইভকে বিচ্ছিন্ন করা হইলে ল্যাপটপটি অকেজো হইতে পারে;

(গ) হার্ডওয়্যার নির্ভরতা (লিগাসি সরঞ্জাম) যথা- পুরাতন ড্রাইভ নূতন সিস্টেমের অনুপযোগী হইতে পারে;

(২) যে ডিজিটাল ডিভাইস ব্যবহার করিয়া অপরাধ সংঘটিত হইয়াছে উহাতে ফরেনসিক ল্যাব পরীক্ষকের নিয়ন্ত্রণ বহির্ভূত থাকায় নেটওয়ার্ক ডিভাইস ব্যবহার করিয়া তথ্য অধিগ্রহণ করিতে হইবে;

(৩) স্টোরেজ ডিভাইস হইতে ফরেনসিক পরীক্ষার জন্য নির্ধারিত স্টোরেজ ডিভাইসে তথ্য স্থানান্তরের ক্ষেত্রে

এ স্টোরেজটি সম্পূর্নরূপে নিষ্কণ্টক, ভাইরাস মুক্ত ও পরিচ্ছন্ন হইবে যাহাতে স্থানান্তরিত তথ্যসমূহ অবিকৃতভাবে রক্ষিত থাকে। এইক্ষেত্রে Independent Cyclic Redundancy Check (CRC), Hashing, ইত্যাদি প্রযুক্তি ব্যবহার করিবার ক্ষেত্রে নিম্নবর্ণিত ব্যবস্থা গ্রহণ করা যাইবে,যথা:-

(ক) নির্বাচিত অধিগ্রহণ পদ্ধতির উপর নির্ভর করিয়া যদি হার্ডওয়্যার রাইট প্রটেকশন ব্যবহার করা হইয়া থাকে, তাহা হইলে এই প্রক্রিয়াটি ইতোমধ্যে সম্পন্ন হইয়াছে বলিয়া গণ্য হইবে;

(খ) ডিজিটাল ডিভাইসটির রাইট প্রটেকশন ইনস্টল করিতে হইবে;

(গ) ফরেনসিক ল্যাবের নিজস্ব সিস্টেম হইতে বুট করিতে হইবে (ডিভাইসটি Non-Bootable অবস্থায় সংযুক্ত থাকিবে);

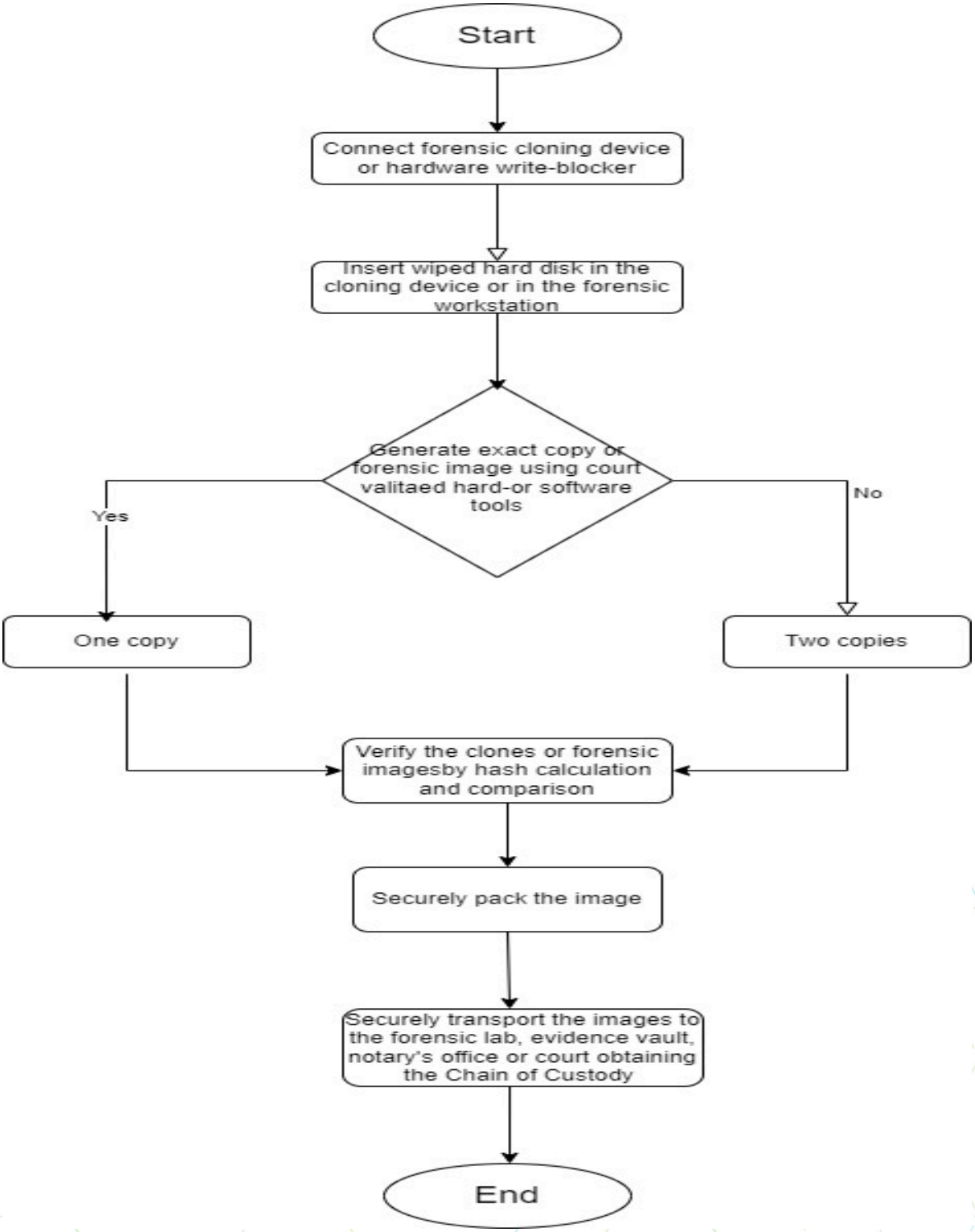
(ঘ) যদি সফ্টওয়্যার রাইট প্রটেকশন ব্যবহার করা হইয়া থাকে, তাহা হইলে ফরেনসিক ল্যাবের নিজস্ব সিস্টেম হইতে বুট করিতে হইবে এবং সফটওয়্যার রাইট প্রটেকশন সক্রিয় করিতে হইবে;

(ঙ) উপযুক্ত সফটওয়্যার ব্যবহারক্রমে জব্দকৃত ডিভাইসের স্টোরেজের পূর্ণাঙ্গ ধারণক্ষমতা ও ব্যবহৃত অব্যবহৃত এলাকা সমুহ চিহ্নিত করিতে হইবে;

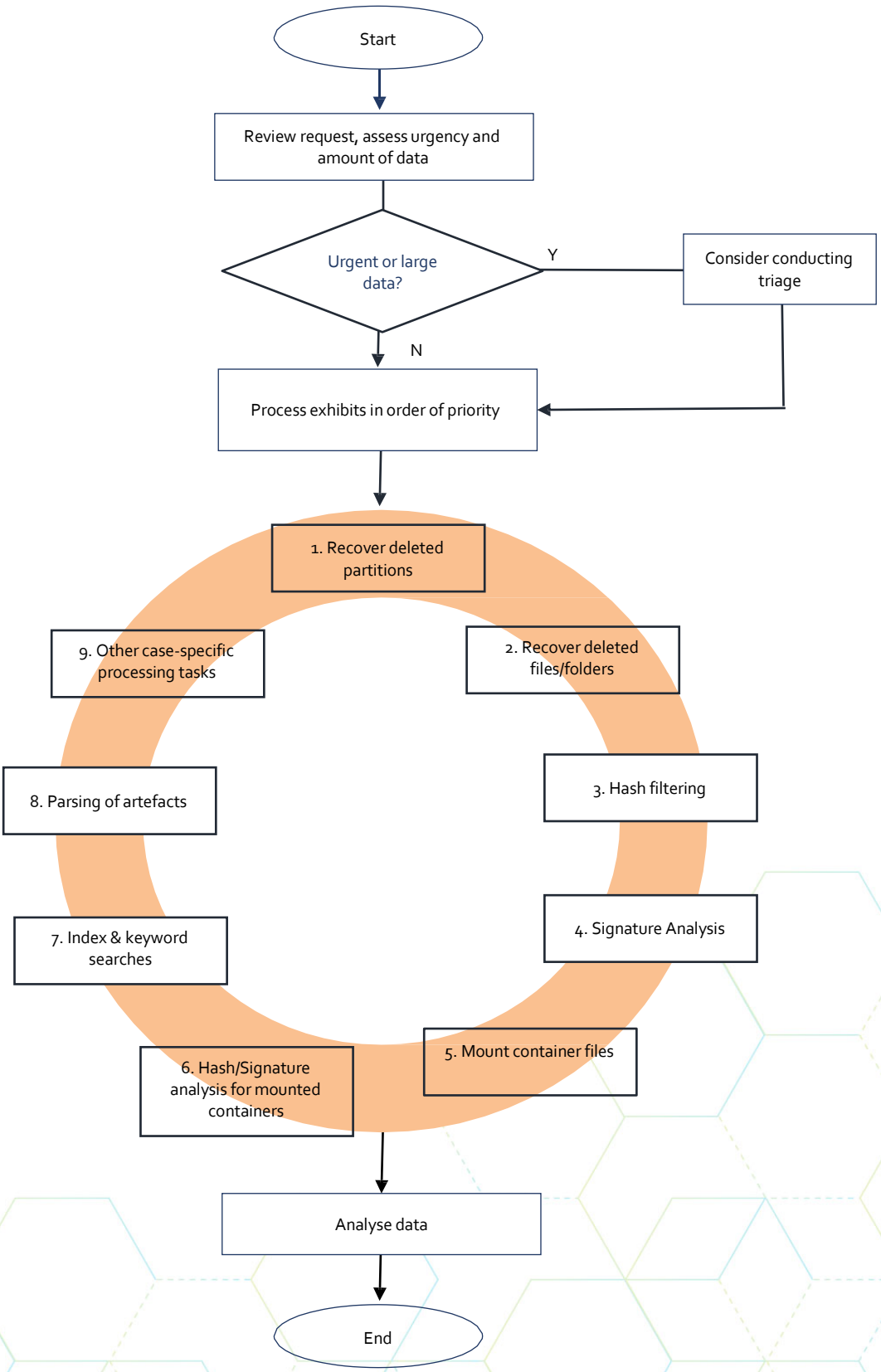
(চ) স্টোরেজ ডিভাইস হইতে ইলেক্ট্রনিক সিরিয়াল নাম্বার, সাক্ষ্যপ্রমাণ, Stand Alone Software, Forensic Software Analysis Suite, Dedicated Hardware Device, ইত্যাদির মাধ্যমে ফরেনসিক ল্যাবের স্টোরেজে অবিকল কপি সংরক্ষণ করিতে হইবে;

(ছ) মূল এবং অনুলিপির কপি Sector-by-Sector তুলনা করিয়া অধিগৃহীত তথ্যের মৌলিকত্ব (Originality) নিশ্চিত করিতে হইবে।

পরিশিষ্ট-০৮: ডিজিটাল নমুনা বা আলামত অধিগ্রহণ প্রক্রিয়ার ফ্লো-চার্ট



পরিশিষ্ট-০৯: কম্পিউটার পরীক্ষণ প্রক্রিয়ার ফ্লো-চার্ট



পরিশিষ্ট-১০: ফরেনসিক নমুনা বা আলামত বিশ্লেষণ
ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০

তফসিল

তৃতীয় অধ্যায়

আহরিত ফাইলের বিশ্লেষণ

ঘটনার সময় আহরিত ডাটা কতটুকু গুরুত্বপূর্ণ উহা বিশ্লেষণপূর্বক ডাটা প্রক্রিয়াকরণের ক্ষেত্রে সময়সীমা, লুক্কায়িত ডাটা, অ্যাপ্লিকেশন ও ফাইল, সত্ত্বাধিকারী ও এখতিয়ার ইত্যাদি বিষয় বিশ্লেষন করিবার সময় এইক্ষেত্রে কম্পিউটারের BIOS এ প্রদর্শিত সময়ের সহিত সিস্টেমে প্রদর্শিত সময়ের পার্থক্য নিম্নবর্ণিতরূপে বিবেচনা করিতে হইবে, যথা:-

(ক) ডিজিটাল ডিভাইসের ব্যবহার সম্পর্কিত সময়ের পর্যালোচনা ও বিশ্লেষণ (Timeframe Analysis): ডিজিটাল ডিভাইসের ব্যবহার সম্পর্কিত সময় পর্যালোচনার মাধ্যমে ঘটনার সময়ের সহিত ব্যবহারকারীদের সংশ্লিষ্টতা সনাক্ত করা যায়। নিম্নবর্ণিত ২ (দুই) পদ্ধতিতে ডিজিটাল ডিভাইসের ব্যবহার সম্পর্কিত সময় পর্যালোচনা ও বিশ্লেষন করা যাইবে, যথা:

(অ) সময়ের সহিত সম্পর্কিত ফাইল সিস্টেমের উপাত্ত (যথা: সর্বশেষ ফাইল সিস্টেমের Read বা Write বা Execute বা Protect অনুমতি পরিবর্তন, সর্বশেষ ব্যবহার, ফাইল সৃষ্টিকরণ এবং ফাইলের সর্বশেষ পরিবর্তন ইত্যাদি) তদন্তের মাধ্যমে নির্ধারিত ফাইলের সাথে ব্যবহারকারীদের সংশ্লিষ্টতা নির্ণয় করা যাইবে;

(আ) Error log, Application Installation Log, Connection Log, Security Log, ইত্যাদি বিষয় বিবেচনাক্রমে অ্যাপ্লিকেশান ও সিস্টেমের লগসমূহ বিশ্লেষণ করিতে হইবে।

(খ) **লুক্কায়িত ডাটার বিশ্লেষণঃ (Hidden Data Analysis):-** লুক্কায়িত ডাটার বিশ্লেষণের মাধ্যমে কম্পিউটারে গোপনীয় ডাটা সনাক্ত ও পুনরুদ্ধার করিবার ক্ষেত্রে নিম্নবর্ণিত পদ্ধতি অনুসরণ করিতে হইবে, যথা:

(অ) ব্যবহারকারী ইচ্ছাকৃতভাবে বা উদ্দেশ্যমূলকভাবে তথ্য পরিবর্তন করিলে ফাইল হেডারকে ঐ ফাইলের এক্সটেনশন এর সহিত তুলনা (Correlate) করিয়া অসামঞ্জস্যতা চিহ্নিত করিতে হইবে;

(আ) সকল পাসওয়ার্ড দ্বারা সুরক্ষিত, এনক্রিপ্টেড ও সংকুচিত ফাইলে প্রবেশাধিকার স্থাপনপূর্বক অযাচিত বা অননুমোদিত হস্তক্ষেপ (Unauthorized Access) নির্ণয় করিতে হইবে;

(ই) Host Protected Area (HPA) এ প্রবেশ করিয়া উক্ত HPA এ ব্যবহারকারী কর্তৃক প্রস্তুতকৃত ডাটার উপস্থিতির ডাটা গোপন করিবার বিষয়টি চিহ্নিত করা যাইবে।

(গ) **অ্যাপ্লিকেশন ও ফাইলের বিশ্লেষণ (Application and File Analysis):** ডিজিটাল ডিভাইসের প্রোগ্রাম ও ফাইলসমূহে তদন্তের সহিত প্রাসঙ্গিক তথ্যসহ সিস্টেম ও ইহার ব্যবহারকারীর সক্ষমতা সম্পর্কে ধারণা লাভের নিমিত্ত নিম্নবর্ণিত পদ্ধতিতে বিবেচনা করিতে হইবে, যথা:

(অ) প্রাসঙ্গিকতা ও প্যাটার্ন বিশ্লেষণের জন্য ফাইলসমূহের নাম পুনর্বিবেচনা;

(আ) ফাইলের বিষয়বস্তু পরীক্ষা;

(ই) ডিজিটাল ডিভাইসের অপারেটিং সিস্টেমসমূহের সংখ্যা ও ধরণ চিহ্নিতকরণ;

(ঈ) ডিজিটাল ডিভাইসে বিদ্যমান অ্যাপ্লিকেশনসমূহের সহিত সম্পর্কিত ফাইলের সামঞ্জস্যতা চিহ্নিতকরণ;

(উ) ডিজিটাল ডিভাইসের ফাইলসমূহের মধ্যে সামঞ্জস্যতা চিহ্নিতকরণ (যথা- ব্যবহারকারীর জব্দকৃত ডিজিটাল ডিভাইসের ইন্টারনেট হিস্টোরি লগের সহিত ব্রাউজারের ক্যাশ (Cache)

ফাইল, ইমেইলের সহিত প্রেরিত সংযুক্তির (Attachment) ও সংশ্লিষ্ট ইমেইলের সামঞ্জস্যতা চিহ্নিতকরণ ইত্যাদি);

(ঊ) ডিজিটাল ডিভাইসের মধ্যকার অপরিচিত ফাইলের ধরণ এবং তদন্তের সহিত উহার সংশ্লিষ্টতা নির্ধারণ;

(ঋ) নির্ধারিত স্থান বা অন্য কোনো স্থানে রক্ষিত ডিজিটাল ডিভাইসের অ্যাপ্লিকেশন ও ইহার সংশ্লিষ্ট ফাইলের সংরক্ষণের স্থান নির্ণয়ের জন্য ব্যবহারকারীর সংরক্ষিত স্থান (Default Storage location) পরীক্ষা;

(এ) ডিজিটাল ডিভাইসের ব্যবহারকারীর কনফিগারেশন পরীক্ষা;

(ঐ) ডিজিটাল ডিভাইসের ফাইলের মেটাডাটা (ফাইল সম্পর্কিত তথ্য) বিশ্লেষণ করিয়া উহার বিষয়বস্তু পর্যালোচনাক্রমে মেটাডাটায় ফাইলের প্রণেতা (Author) কর্তৃক সর্বশেষ সংশোধনের (Edit) সময় কতবার উহা সংশোধন করা হইয়াছে, সেই তথ্য এবং ফাইল সম্পর্কিত অন্যান্য তথ্য অন্তর্ভূক্ত থাকিবে।

(ঘ) **মালিকানা ও ব্যবহার**: যেই ক্ষেত্রে, ডিজিটাল ডিভাইসের ফাইলের প্রণেতা, সংশোধনকারী, প্রবেশকারী, ডাটার মালিক ও জ্ঞাত ব্যবহারকারী নিরূপণ করিবার প্রয়োজনীয়তা উদ্ভুত হইলে সেই ক্ষেত্রে বিশ্লেষণের প্রয়োজনে নিম্নবর্ণিত বৈশিষ্ট্যসমূহ বিবেচনা করা যাইবে, যথা:-

(অ) **ডিজিটাল ডিভাইসের ব্যবহার সম্পর্কিত সময়ের পর্যালোচনা ও বিশ্লেষণ (Timeframe analysis):** ডিজিটাল ডিভাইসের ফাইলকে সুনির্দিষ্ট তারিখ ও সময়ের গন্ডিতে আবদ্ধ করিবার মাধ্যমে ইহার মালিক ও ব্যবহারকারী চিহ্নিতকরণ;

(আ) **অ্যাপ্লিকেশন ও ফাইলের বিশ্লেষণ (Application and File Analysis):** ডিজিটাল ডিভাইসের ফাইল অনির্ধারিত (Non-Default) স্থানে সংরক্ষণ (যথা: "শিশু পর্ণ (Child Porn)" নামে ডিজিটাল ডিভাইসের ব্যবহারকারী কর্তৃক একটি Directory প্রস্তুত করা;

(ই) **অ্যাপ্লিকেশন ও ফাইলের বিশ্লেষণ (Application and File Analysis)**: ডিজিটাল ডিভাইসের ফাইলের নাম হইতে ফাইলের বিষয়বস্তু ও উহার সাক্ষ্যগত মূল্য সম্পর্কে ধারণা প্রাপ্তি;

(ঈ) **লুক্কায়িত ডাটার বিশ্লেষণ (Hidden Data Analysis):** সনাক্তকরণ এড়াইবার লক্ষ্যে ইচ্ছাকৃতভাবে ডাটা লুকাইয়া রাখা;

(উ) **লুক্কায়িত ডাটার বিশ্লেষণ (Hidden (Data Analysis):** যেই ক্ষেত্রে পাসওয়ার্ড দ্বারা সুরক্ষিত ও এনক্রিপ্টেড (Encrypted) ফাইলের পুনরুদ্ধার করিতে হয়, সেই ক্ষেত্রে পাসওয়ার্ডের তত্ত্বাবধায়ককে মালিক বা ব্যবহারকারী হিসাবে চিহ্নিত করা যাইতে পারে;

(ঊ) **অ্যাপ্লিকেশন ও ফাইলের বিশ্লেষণ (Application and File Analysis):** ডিজিটাল ডিভাইসের ফাইলের বিষয়বস্তু হইতে ইহার মালিক বা ব্যবহারকারী চিহ্নিত করা যাইতে পারে।

পরিশিষ্ট-১১: নথিভুক্তকরণ ও প্রতিবেদন প্রস্তুতকরণ

ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০

তফসিল

চতুর্থ অধ্যায়

নথি ও প্রতিবেদন প্রস্তুতকরণের ক্ষেত্রে নিম্নবর্ণিত ধাপসমূহ অনুসরণ করিতে হইবে, যথা:-

(ক) কার্যপ্রণালী।- প্রতিবেদন স্বয়ংসম্পূর্ণ ও নির্ভুল হইতে হইবে এবং সংশ্লিষ্ট কর্তৃপক্ষের বোধগম্য করিয়া প্রণয়ন এবং বিদ্যমান নীতিমালা ও প্রযুক্তি অনুসরণপূর্বক প্রতিবেদন প্রস্তুত এবং সংরক্ষণ করিতে হইবে। পরীক্ষকের প্রতিবেদন প্রস্তুত করিবার সময় নিম্নবর্ণিত বিষয় অন্তর্ভুক্ত থাকিতে হইবে, যথা:

(অ) তদন্তকারী কর্মকর্তা এবং ক্ষেত্রমত সংশ্লিষ্ট আইনজীবীর সহিত পরামর্শ করিবার সময় নোট গ্রহণ;

(আ) ডিজিটাল নমুনা বা আলামত সংগ্রহ পদ্ধতির অনুলিপি সংরক্ষণ;

(ই) ফরেনসিক পরীক্ষার চাহিদাপত্রের অনুলিপি সংরক্ষণ;

(ঈ) চেইন অব কাস্টডি এর অনুলিপি সংরক্ষণ;

(উ) কার্যক্রমের বিস্তারিত বিবরণ নথিতে লিপিবদ্ধকরণ;

(ঊ) নোট গ্রহণের তারিখ, সময়, বিবরণ এবং গৃহীত পদক্ষেপের ফলাফলসমূহ লিপিবদ্ধকরণ;

(ঋ) ফরেনসিক পরীক্ষার সময় পরিলক্ষিত অনিয়ম এবং গৃহীত পদক্ষেপ লিপিবদ্ধকরণ;

(এ) অতিরিক্ত তথ্যাদি (যথা: নেটওয়ার্ক টপোলজি (Topology), অনুমোদিত ব্যবহারকারীদের তালিকা, ব্যবহারকারীর চুক্তি (Agreement) এবং পাসওয়ার্ড (Password) অন্তর্ভুক্তকরণ);

(ঐ) সরকার বা সরকারি সংস্থা বা পরীক্ষকের নির্দেশে সিস্টেম বা নেটওয়ার্ক এ পরিবর্তন করিয়া থাকিলে উহা লিপিবদ্ধকরণ;

(ও) অপারেটিং সিস্টেম এবং সংশ্লিষ্ট সফটওয়্যারের বর্তমান সংস্করণ ও ইনস্টলকৃত পরিবর্তনসমূহ (Installed Patch) লিপিবদ্ধকরণ;

(ঔ) দূরবর্তী স্টোরেজ (Remote storage), প্রান্তিক ব্যবহারকারীর প্রবেশাধিকার (Remote user access) এবং অফসাইট ব্যাকআপ (offsite backups) সম্পর্কিত প্রাপ্ত তথ্য লিপিবদ্ধকরণ।

তবে যেইক্ষেত্রে পরীক্ষা চলাকালীন এইরূপ কিছু ফরেনসিক নমুনা বা ডিজিটাল আলামত পাওয়া যায় যাহার ফরেনসিক বিশ্লেষণ বর্তমানে প্রচলিত আইনী কাঠামোর আওতাধীন নহে, তাহা হইলে উক্ত বিষয়ে অতিরিক্ত অনুসন্ধানের জন্য বিষয়টি ডিজিটাল নিরাপত্তা এজেন্সির মহাপরিচালকের গোচরীভূত করিতে হইবে।

(খ) পরীক্ষকের প্রতিবেদন।- প্রতিবেদন প্রস্তুত করিবার সময় নিম্নলিখিত বিষয়সমূহ অন্তর্ভুক্ত করিতে হইবে, যথা:

(১) প্রতিবেদক এজেন্সির পরিচয়;

(২) তদন্ত সনাক্তকারী বা জমা নম্বর;

(৩) তদন্তকারী কর্মকর্তার পরিচয়;

(৪) জমাদানকারীর পরিচয়;

(৫) প্রাপ্তির তারিখ;

(৬) প্রতিবেদনের তারিখ;

(৭) পরীক্ষার জন্য প্রাপ্ত ফরেনসিক নমুনা বা মামলার আলামতসমূহের সিরিয়াল নম্বর, প্রস্তুতকারক এবং মডেলসহ বিস্তারিত তালিকা;

(৮) পরীক্ষকের পরিচয় এবং স্বাক্ষর;

(৯) পরীক্ষার সময় গৃহীত পদক্ষেপ সমূহের সংক্ষিপ্ত বিবরণ (যথা: স্ট্রিং অনুসন্ধান, গ্রাফিক্স চিত্র অনুসন্ধান এবং মুছিয়া ফেলা ফাইলসমূহ পুনরুদ্ধার ইত্যাদি);

(১০) ফলাফল ও উপসংহার।

(গ) প্রাপ্ত ফলাফলের সারসংক্ষেপ। -প্রাপ্ত ডিজিটাল আলামতের ফরেনসিক পরীক্ষার সংক্ষিপ্ত ফলাফল প্রতিবেদনে লিপিবদ্ধ করিতে হইবে।

(ঘ) প্রাপ্ত ফলাফলের বিস্তারিত বিবরণ।— প্রত্যেক প্রতিবেদনে ফরেনসিক নমুনা বা ডিজিটাল আলামতের ফরেনসিক পরীক্ষার ফলাফলে নিম্নবর্ণিত বিষয়সমূহের বিস্তারিত বিবরণ লিপিবদ্ধ করিতে হইবে, যথা:

(১) চাহিদাপত্রের সহিত সম্পর্কিত জব্দকৃত ডিজিটাল ডিভাইসের ফাইলসমূহ;

(২) ফলাফলকে সমর্থন করিতে পারে এইরূপ মুছিয়া ফেলা ফাইলসহ অন্যান্য ফাইলসমূহ;

(৩) স্ট্রিং অনুসন্ধান, মূলশব্দ (Keyword) অনুসন্ধান এবং টেক্সট স্ট্রিং অনুসন্ধানের ফলাফল;

(৪) ইন্টারনেট সম্পর্কিত প্রমাণাদি বিশ্লেষণ (যথা: Web site traffic analysis, chat logs, cache files, e-mail, and news group activity);

(৫) গ্রাফিক চিত্র বিশ্লেষণ;

(৬) মালিকানা নির্ধারণ ও প্রোগ্রাম রেজিস্ট্রির তথ্যাদি;

(৭) প্রাসঙ্গিক তথ্য বিশ্লেষণ;

(৮) পরীক্ষিত ফরেনসিক নমুনা বা ডিজিটাল আলামতসমূহে বিদ্যমান প্রোগ্রামের বিবরণ;

(৯) তথ্য লুকাইয়া রাখা বা মাস্কিং করিবার জন্য ব্যবহৃত কৌশল, (যথা: এনক্রিপশন, স্টেগানোগ্রাফি) লুক্কায়িত তথ্যের বৈশিষ্ট্য, লুক্কায়িত পার্টিশন এবং অসংগতিপূর্ণ ফাইলসমূহের নাম।

পরিশিষ্ট-১২ক: ISO/IEC/BDS 17025 টেষ্টিং ও ক্যালিব্রেশন পরীক্ষাগারের যোগ্যতার সাধারণ মাপকাঠি

(পৃথকভাবে মুদ্রিত)

পরিশিষ্ট-১২খ: ISO/IEC/BDS 15489 রেকর্ডস ব্যবস্থাপনা

(পৃথকভাবে মুদ্রিত)

পরিশিষ্ট-১২গ: ISO/IEC/BDS 27037 ডিজিটাল সাক্ষ্য সনাক্তকরণ, সংগ্রহ, অধিগ্রহণ এবং সংরক্ষণ নির্দেশিকা

(পৃথকভাবে মুদ্রিত)

পরিশিষ্ট-১২ঘ: ISO/IEC/BDS 27041 ঘটনা তদন্ত পদ্ধতির গ্রহণযোগ্যতা ও উপযুক্ততা নিরুপণের মাপকাঠি/নির্দেশিকা

(পৃথকভাবে মুদ্রিত)

পরিশিষ্ট-১২ঙ: ISO/IEC/BDS 27042 ডিজিটাল সাক্ষ্য বিশ্লেষণ ও স্পষ্টিকরণ নির্দেশিকা

(পৃথকভাবে মুদ্রিত)

পরিশিষ্ট-১২চ: ISO/IEC/BDS 27043 ঘটনা তদন্তের পদ্ধতি ও নীতিমালা

(পৃথকভাবে মুদ্রিত)

পরিশিষ্ট-১২ছ: ISO/IEC/BDS 27050 ইলেকট্রনিক ডিসকভারি

(পৃথকভাবে মুদ্রিত)

পরিশিষ্ট-১৩: গুনগতমান নিশ্চিতকরণ চেকলিস্ট

Quality Assurance Components Checklist	
Laboratory	a. Create an Organization Chart at DFL level and at the organization level. b. Conduct an internal audit annually. c. Establish a procedure to address internal and external complaints. d. Establish a procedure to control documentation.
Facility and Environmental Condition	a. Establish lab premises – access and exits. b. Create an access list and limit access by using keys, individually assigned identification cards, or biometric devices. c. Monitor the lab environment regularly – temperature, humidity, cleanliness. d. Establish a Health and Safety programme. e. Establish visitor policy. f. Conduct regular housekeeping.
Equipment	a. Establish a procedure for handling, transport, storage, use, repair, disposal and planned maintenance for equipment. b. Before putting into use, ensure that the equipment is working according to specifications. c. Implement the maintenance programme. d. Update the firmware according to requirements. e. Maintain equipment documentation, manuals, and warranties.
Staff	a. Employment Qualifications: • Conduct background screening prior to hiring. • Prepare Job Descriptions for staff once hired - See section 3.3 Staff. b. Professional Development and Training: • Establish a training programme for staff - See section 3.3.4 Staff development. • Send staff for training. • Assign mentors for newly-hired staff. • Evaluate staff's competency by conducting Competency Tests for newly-hired staff. • Evaluate existing staff's proficiency by conducting annual Proficiency Tests. • Participate in external or inter-laboratory Proficiency Tests. • Obtain technical certifications.

Forensic Method	a. Establish SOPs for conducting DF examinations. b. Keep a document of forensic methods, such as conducting a live acquisition, updated and available to Examiners. c. Conduct verification on methods introduced to ensure the DFL can use them properly. d. Conduct validation when using any method: non-standard method, lab-developed method or standard method used outside its scope. e. For ease of operation, use an internationally-accepted method in DFL, such as SWGDE.
Service Request	Establish and implement a policy and procedure on the service request. This should contain: a. The process for accepting or rejecting the request. b. The process for resubmission of the request. c. The requirement for having a concise request or case objective. d. Formal acknowledgment from the Requester and the Examiner, indicating that both parties agree with the work before the e. Forms or other methods to be used to document the request.
Evidence Handling	Establish and implement a policy and procedures on evidence handling. This should contain: a. Evidence preservation b. Evidence labelling c. Evidence sealing d. Items to document - including the chain of custody e. Evidence that is left unattended f. Precautions for securing and handling the evidence g. Storage and retention See Appendix K**: Electronic Evidence Handling** for details on evidence handling.
Forensic Result	a. Keep technical records to support the forensic result. The records must indicate the Examiners conducting the process, and the date. Amendments to previous records must be tracked. b. Conduct technical and administrative review of the forensic results. c. Authorize the forensic result before releasing to the Requester. d. Establish a common format for a forensic report. See **Appendix J: Common Requirement for Forensic Report** e. When providing an opinion, it must be clearly marked in the forensic report. f. Establish a process for amending a forensic report.