ডিজিটাল ফরেনসিক ল্যাব গাইডলাইন, ২০২৩

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ

ডাক, টেলিযোগাযোগ ও তথ্যপ্রযুক্তি মন্ত্রণালয়

পটভূমি

তথ্য ও যোগাযোগ প্রযুক্তির নূতন নূতন উদ্ভাবন এবং উহার বিশ্বব্যাপী ব্যাপক ব্যবহার মানব জীবনে উন্মোচন করিয়াছে ক্রম-সম্প্রসারণশীল এক নূতন দিগন্ত। মাননীয় প্রধানমন্ত্রী ঘোষিত 'ডিজিটাল বাংলাদেশ' উদ্যোগের মাধ্যমে দেশের সামগ্রিক কার্যক্রমকে ডিজিটালাইজেশনের মাধ্যমে অধিকাংশ সেবাসমূহ জনগণের দোরগোড়ায় পৌঁছানো সম্ভব হইয়াছে। ফলশ্রুতিতে বাংলাদেশের জনগণ তাহাদের ব্যক্তিগত, দাপ্তরিক, বাণিজ্যিক ও সামাজিক যোগাযোগের ক্ষেত্রে দেশের অভ্যন্তরে ও বিশ্বের যে কোনো প্রান্তে সহজে ও নিমিষে কাঙ্ক্ষিত কার্যক্রম সম্পন্ন করিতে সক্ষম।

তথ্য ও যোগাযোগ প্রযুক্তি নির্ভর সেবাসমূহের দ্রুত বিস্তারের পাশাপাশি ইহার মাধ্যমে অপরাধ সংগঠনের মাত্রাও বৃদ্ধি পাইয়াছে। ডিজিটাল মাধ্যমে ক্রমবর্ধমানহারে সংযুক্ত ডিভাইস যেমন- কম্পিউটার, স্মার্টফোন, স্মার্ট ঘড়ি, জিপিএস ইত্যাদিতে তথ্য সংরক্ষণ করিতে পারে; যাহা ডিজিটাল মাধ্যমে অপরাধের প্রমাণক হিসাবে ব্যবহার হইতে পারে। ডিজিটাল মাধ্যমে সংগঠিত অপরাধের তদন্তের জন্য বিশেষায়িত এবং প্রযুক্তিগত দক্ষতার প্রয়োজন হয়। ডিজিটাল ফরেনসিক পদ্ধতি অনুসরণ করিয়া ডিজিটাল মাধ্যমে এই বিষয়ে কারিগরী দক্ষতাসম্পন্ন পেশাজীবীগণ যথাযথ পদ্ধতি অনুসরণপূর্বক ফরেনসিক প্রতিবেদন প্রস্তুত করেন, যাহা অপরাধের বিশ্বাসযোগ্য প্রমাণ হিসেবে আদালত বা প্রযোজ্য ক্ষেত্রে উপস্থাপন করা হইয়া থাকে।

ডিজিটাল মাধ্যমে সংঘটিত অপরাধে অতিরাষ্ট্রিক (Borderless) মাত্রা যুক্ত হওয়ায় এবং দেশ-বিদেশের আদালতে অপরাধের সাক্ষ্য প্রমাণ গ্রহণযোগ্যভাবে উপস্থাপন করিবার নিমিত্ত আন্তর্জাতিক মান ও পদ্ধতি অনুসরণ আবশ্যক। 'ডিজিটাল নিরাপত্তা আইন, ২০১৮'-ধারা ১০ অনুসারে ডিজিটাল ফরেনসিক ল্যাবরেটরি স্থাপন ও ধারা ১১ অনুসারে উহার মাননিয়ন্ত্রণ বাঞ্ছনীয়। এই লক্ষ্যে 'ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০' এর বিধি ১৩ হইতে বিধি ১৬ পর্যন্ত ডিজিটাল ফরেনসিক ল্যাব স্থাপন, উহার মাননিয়ন্ত্রণ, ডিজিটাল সাক্ষ্যের ফরেনসিক বিশ্লেষণ ও ফরেনসিক ল্যাবের জনবল কাঠামো বর্ণিত হইয়াছে। ডিজিটাল ফরেনসিক ল্যাবের বাস্তবায়ন ও পরিচালনা সহজীকরণ করিবার লক্ষ্যে এই গাইডলাইন প্রণয়ন করা হইয়াছে।

তথ্য ও যোগাযোগ প্রযুক্তির নূতন নূতন উদ্ভাবনসমূহের সাথে সামঞ্জস্যপূর্ণভাবে ডিজিটাল ফরেনসিক সংক্রান্ত কার্যক্রম পরিচালনার লক্ষ্যে গাইডলাইনটি ভবিষ্যতে পরিবর্ধন বা পরিমার্জনের সুযোগ থাকিবে। ইহার উৎকর্ষ সাধনের নিমিত্ত যে কোন পরামর্শ সাদরে গৃহীত হইবে।

সূচীপত্র

অংশ-০১: প্রারম্ভিক 4

১। শিরোনাম ও প্রবর্তন 4

২। সংজ্ঞা 4

অংশ-০২: গাইডলাইন প্রণয়নের উদ্দেশ্য ও পরিধি 6

৩। গাইডলাইন প্রণয়নের লক্ষ্য ও উদ্দেশ্য 6

৪। গাইডলাইন এর প্রয়োগ ও পরিধি 6

অংশ-০৩: ডিজিটাল ফরেনসিক 6

৫। ইলেকট্রনিক বা ডিজিটাল সাক্ষ্যের স্বীকৃতি 6

৬। ইলেকট্রনিক বা ডিজিটাল সাক্ষ্য প্রক্রিয়াকরণ, ইত্যাদির চ্যালেঞ্জসমূহ 6

৭। ইলেকট্রনিক বা ডিজিটাল সাক্ষ্যের গ্রহণযোগ্যতার বৈশিষ্ট্য 7

৮। ইলেকট্রনিক বা ডিজিটাল সাক্ষ্য বিশ্লেষণের নীতি 7

অংশ-০৪: ডিজিটাল ফরেনসিক ল্যাব ব্যবস্থাপনা 8

৯। ডিজিটাল ফরেনসিক ল্যাবের অবস্থান 8

(ক) স্থান নির্বাচন: ডিজিটাল ফরনেসিক ল্যাবের স্থান নির্বাচনকালে বিবেচ্য বিষয়সমূহ: 8

(খ) ভৌত নিরাপত্তা সংক্রান্ত বিষয়াদি: 8

(গ) ফরেনসিক ল্যাবের অবকাঠামোর অংশসমূহ: 9

(ঘ) ফরেনসিক ল্যাবের দর্শনার্থী প্রবেশ সংক্রান্ত নিয়মাবলী: 9

১০। ডিজিটাল ফরেনসিক ল্যাবের জনবল 10

অংশ-০৫: ডিজিটাল ফরেনসিক ল্যাবের উপকরণ 10

১১। যন্ত্রপাতি 10

১২। সফটওয়্যার সংক্রান্ত বিষয়াদি 10

১৩। হার্ডওয়্যার সংক্রান্ত বিষয়াদি 11

১৪। হার্ডওয়্যার ও সফটওয়্যার এর তালিকা 11

১৫। যন্ত্রপাতি ও আনুষঙ্গিক যন্ত্রাংশ (tools & accessories) 11

অংশ-০৬ ডিজিটাল ফরেনসিক কেস ব্যবস্থাপনা 12

১৬। কেস ব্যবস্থাপনা পদ্ধতি 12

১৭। ফরেনসিক পরীক্ষার অধিযাচন (Requisition) 12

১৯। ফরেনসিক পরীক্ষার চাহিদা পর্যালোচনা 13

২০। ফরেনসিক পরীক্ষার তথ্য প্রমাণ নির্ধারণ (Evidence Assessment) 13

২১। ডিজিটাল নমুনা বা আলামত বিশ্লেষণ 14

২২। ডিজিটাল সাক্ষ্য-প্রমাণ প্রত্যর্পণ 14

২৩। ফরেনসিক কেসের সমাপ্তি ও প্রতিবেদন 14

অংশ-০৭: ফরেনসিক পরীক্ষার পর্যায় 14

২৪। ডিজিটাল ফরেনসিক পরীক্ষার পর্যায়সমূহ 14

অংশ-০৮: ডিজিটাল নমুনা বা আলামত অধিগ্রহণ ও উপাত্ত আহরণ 15

২৫। উপাত্ত অধিগ্রহণ প্রক্রিয়া 15

২৬। কম্পিউটার সিস্টেম হইতে উপাত্ত অধিগ্রহণ 15

২৭। মোবাইল ডিভাইস হইতে উপাত্ত আহরণ (Extraction) 17
অংশ-০৯: ডিজিটাল ফরেনসিক নমুনা বা আলামত পরীক্ষণ 21
২৮। নমুনা বা আলামত পরীক্ষণ 21
২৯। কম্পিউটার পরীক্ষণ পদ্ধতি 21
অংশ-১০: ডিজিটাল ফরেনসিক নমুনা বা আলামত বিশ্লেষণ 24
৩১। ফরেনসিক নমুনা বা আলামত বিশ্লেষণ 24
৩২। কম্পিউটার সিস্টেম বিশ্লেষণ 24
৩৩। মোবাইল ডিভাইস এর উপাত্ত বিশ্লেষণ 25
অংশ-১১: ফরেনসিক প্রতিবেদন প্রস্তুতকরণ ও উপস্থাপন 26
৩৫। ফরেনসিক ফলাফল উপস্থাপন 26
৩৬। ইলেকট্রনিক বা ডিজিটাল সাক্ষ্য প্রমাণাদির গ্রহণযোগ্যতা 26
অংশ ১২: ডিজিটাল ফরেনসিক ল্যাবরেটরির অনুসরণীয় মানদন্ড 27
অংশ-১৩: ফরেনসিক ল্যাবের গুণগতমান নিশ্চিতকরণ (Quality Assurance) 27
৩৮। গুণগতমান নিশ্চিতকরণ 27
৩৯। গুণগতমান নিশ্চিতকরণের উপাদান (Component) 27
অংশ-১৪: বিবিধ বিষয়াবলী 27
৪০। নমুনা বা আলামতের তথ্য-উপাত্ত সংরক্ষণ 27
৪১। ফরেনসিক পরীক্ষা সম্পাদনের সময়সীমা 28
৪২। তথ্য-উপাত্তের গোপনীয়তা 28
৪৩। ডিজিটাল ফরেনসিক ল্যাব পরিচালনা 28
৪৪। নির্দেশ প্রদানের ক্ষমতা 28
৪৫। অব্যাহতি 28
৪৬। গাইডলাইনের সীমাবদ্ধতা 28
পরিশিষ্টসমূহের তালিকা 29
পরিশিষ্ট-০১: ডিজিটাল ফরেনসিক ল্যাবের জনবলের দক্ষতা 30
পরিশিষ্ট-০২: ডিজিটাল ফরেনসিক পরীক্ষার কেস অধিযাচন ফরম 32
পরিশিষ্ট-০৩: চেইন অফ কাস্টডি (Chain of Custody) 34
পরিশিষ্ট-০৪: ডিজিটাল নমুনা বা আলামত বিশ্লেষণ প্রক্রিয়া 36
পরিশিষ্ট-০৫: ডিজিটাল নমুনা বা আলামত অধিগ্রহণ প্রক্রিয়ার ফ্লো-চার্ট 37
পরিশিষ্ট-০৬: কম্পিউটার পরীক্ষণ প্রক্রিয়ার ফ্লো-চার্ট 38
পরিশিষ্ট-০৭: গুণগতমান নিশ্চিতকরণ চেকলিস্ট 39
পরিশিষ্ট-০৮: ফরেনসিক ল্যাবে প্রবেশের নিবন্ধন বহি 41

অংশ-০১: প্রারম্ভিক

১। শিরোনাম ও প্রবর্তন

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

(২) ইহা অবিলম্বে কার্যকর হইবে।

২। সংজ্ঞা

(১) বিষয় বা প্রসঙ্গের পরিপন্থী কোন কিছু না থাকিলে, এই গাইডলাইনে-

(ক) "অধিযাচন (Requisition)" অর্থ কোন ফৌজদারী মামলার তদন্তকারী কর্মকর্তা বা কোন প্রতিষ্ঠান প্রধান, ডিজিটাল ফরেনসিক ল্যাবরেটরিকে প্রেরিত ফরেনসিক তদন্ত কার্যক্রম পরিচালনার অনুরোধপত্র (পরিশিষ্ট-০২);

(খ) "ইলেকট্রনিক ডিসকভারি (Electronic Discovery)" অর্থ ইলেকট্রনিক পদ্ধতিতে সংরক্ষিত তথ্যাবলি উদঘাটন যাহাতে তথ্য চিহ্নিতকরণ, সংরক্ষণ, বিশ্লেষণ, পর্যালোচনা ও সৃজন অন্তর্ভুক্ত;

(গ) "ইলেকট্রনিক পদ্ধতিতে সংরক্ষিত তথ্যাবলি (Electronically stored information)" অর্থ কোন ইলেকট্রনিক মিডিয়া যথা ই-মেইল, ই-ডকুমেন্ট, স্প্রেডশিট, ডাটাবেইজ, প্রেজেন্টশন বা অন্যান্য ইলেকট্রনিক ফরমেটে সংরক্ষিত ডাটা বা তথ্য;

(ঘ) "ইলেকট্রনিক সাক্ষ্য (Electronic Evidence)" অর্থ কম্পিউটার বা ডিজিটাল ডিভাইস বা অন্যান্য ডিজিটাল স্টোরেজ মিডিয়ায় সংরক্ষিত ডাটা;

(ঙ) "ঘটনা (Incident)" অর্থ কোন অনাকাঙ্খিত বা অবৈধ একক বা সিরিজ ঘটনা যার দ্বারা কোন তথ্যের বা কার্যক্রমের শুদ্ধতা বা নিরাপত্তা লঙ্ঘিত হইতে পারে এবং যাহা অপরাধমূলক হইতেও পারে বা নাও হইতে পারে;

(চ) "চেইন অফ কাস্টডি (Chain of Custody)" অর্থ ডিজিটাল বা অন্য নির্ধারিত ছকে এক বা একাধিক দলিল/রেকর্ড যাহা ডিজিটাল স্বাক্ষ্যের গতিবিধি ও হেফাজতকারীর বিবরণ নথীভুক্ত করে[1] (পরিশিষ্ট-০৩)।

(ছ) "ডিজিটাল তদন্ত (Digital Investigation)" অর্থ এমন কার্যক্রম যাহা বৈজ্ঞানিক পদ্ধতিতে ডিজিটাল সাক্ষ্য চিহ্নিতকরণ, সংগ্রহ, স্থানান্তকরণ, সংরক্ষণ, বিশ্লেষণ, ব্যাখ্যা ও উপস্থাপন করা হইয়াছে এবং যে সাক্ষ্য অপরাধমূলক হইতে পারে বা নাও হইতে পারে;

(জ) "ডিজিটাল ফরেনসিক (Digital Forensic)" অর্থ কম্পিউটার, ডিজিটাল ডিভাইস বা অন্য ডিজিটাল স্টোরেজ মিডিয়ায় সংরক্ষিত বা অবস্থিত ডাটা চিহ্নিত, অধিগ্রহণ ও বিশ্লেষণ করিয়া প্রকৃত ঘটনা উদঘাটন ও উপস্থাপন করে এবং ইহার প্রধান লক্ষ্য হইতেছে ডিজিটাল ডিভাইস

1 বিস্তারিত অনুচ্ছেদ ৬.১, ISO/IEC/BDS 27037 ডিজিটাল সাক্ষ্য সনাক্তকরণ, সংগ্রহ, অধিগ্রহণ এবং সংরক্ষণ নির্দেশিকা [Guidelines for identification, collection, acquisition, and preservation of digital evidence] I

হইতে উদঘাটিত ডাটা বিশ্লেষণ করিয়া দায়দায়িত্ব নিরুপণ বা সংঘটিত অপরাধ চিহ্নিত করিয়া অভিযুক্তকে বিচারের মুখোমুখি করা;

(ঝ) "ডিজিটাল ফরেনসিক ল্যাবরেটরি সুপারভাইজার (Digital Forensic Laboratory Supervisor)" অর্থ একজন কর্মকর্তা যিনি ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি ১৬(৩) এর যাবতীয় দায়িত্ব পালন করেন;

(ঞ) "ডিজিটাল ফরেনসিক ল্যাবরেটরি বিশেষজ্ঞ (Digital Forensic Laboratory Expert)" অর্থ একজন কর্মকর্তা যিনি ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি ১৬(৪) এবং অত্র গাইডলাইনে বর্ণিত দায়িত্ব পালন করেন;

(ট) "ডিজিটাল সাক্ষ্য (Digital Evidence)" অর্থ বাইনারি ফর্মে সংরক্ষিত বা স্থানান্তরিত তথ্য যাহা সাক্ষ্য হিসাবে ব্যবহৃত হইতে পারে;

(ঠ) "ডিজিটাল সাক্ষ্যের প্রথম তদন্তকারী (Digital Evidence First Responder)" অর্থ যিনি কোন ঘটনাস্থলে ডিজিটাল সাক্ষ্য সংগ্রহ ও অধিগ্রহণে দায়িত্বপ্রাপ্ত, যিনি ডিজিটাল ফরেনসিক তদন্তকারী (হার্ডওয়্যার) বা সহকারি ডিজিটাল ফরেনসিক তদন্তকারী হিসাবেও বিবেচিত;

(ড) "ডিজিটাল সাক্ষ্য বিশেষজ্ঞ (Digital Evidence Expert)" অর্থ যিনি ডিজিটাল সাক্ষ্যের তদন্তকারীর যাবতীয় দায়িত্ব পালনে সক্ষম এবং ডিজিটাল ফরেনসিকের টেকনিক্যাল বিষয়ে নির্ধারিত বিশেষজ্ঞ জ্ঞান ও দক্ষতার অধিকারী;

(ঢ) "পরীক্ষা (Examination)" অর্থ এক বা একাধিক সূত্র হইতে কোন সম্ভাব্য ডিজিটাল তথ্য প্রমাণ চিহ্নিত ও উদ্ধারে ব্যবহৃত পদ্ধতি;

(ণ) "পরীক্ষক (Examiner)" অর্থ সরকারী গেজেটে প্রজ্ঞাপন মারফত ঘোষিত ফরেনসিক বিশেষজ্ঞ যিনি ডিজিটাল ফরেনসিক পরীক্ষা কার্যক্রম পরিচালনা করিয়া ডিজিটাল তথ্য-প্রমানের বিষয়ে কোন আদালত বা কর্তৃপক্ষের নিকট বিশেষজ্ঞ মতামত প্রদান করেন;

(ত) "পরীক্ষাগার" বলিতে এজেন্সি স্বীকৃত পরীক্ষাগার যা ডিজিটাল ফরনসিক কার্যক্রম পরিচালনায় একই সাথে টেস্টিং ও ক্যালিব্রেশন পরীক্ষাগার।

(২) এই গাইডলাইনে ব্যবহৃত যে সকল শব্দ বা অভিব্যক্তির সংজ্ঞা প্রদান করা হয় নাই, সেই সকল শব্দ বা অভিব্যক্তি তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ এবং ডিজিটাল নিরাপত্তা আইন, ২০১৮ বা ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি ১৪ -তে বর্ণিত ISO/IEC/BDS ১৭০২৫, ISO/IEC/BDS ১৫৪৮৯, ISO/IEC/BDS ২৭০৩৭, ISO/IEC/BDS ২৭০৪১, ISO/IEC/BDS ২৭০৪২, ISO/IEC/BDS ২৭০৪৩, ISO/IEC/BDS ২৭০৫০ -এ যে অর্থে ব্যবহৃত হইয়াছে সেই অর্থে ব্যবহৃত হইবে।

অংশ-০২: 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 তথ্য-উপাত্ত শনাক্তকরণ, অধিগ্রহণ, প্রক্রিয়াকরণ, বিশ্লেষণ, ইত্যাদির উপর আলোকপাত করে।

এই গাইডলাইন প্রণয়নের মুখ্য উদ্দেশ্য হইতেছে ডিজিটাল ফরেনসিক ল্যাবরেটরি প্রতিষ্ঠা, ব্যবস্থাপনা এবং ইলেকট্রনিক যন্ত্রপাতি ও ডিজিটাল ডিভাইস হইতে ডিজিটাল সাক্ষ্য উদ্ধার ও ফরেনসিক বিশ্লেষণ করিয়া ঘটনার সত্যতা যাচাই ও অপরাধ বা দুর্ঘটনার দায়দায়িত্ব নিরূপণের নিমিত্ত জাতীয় ও আন্তর্জাতিকভাবে স্বীকৃত মান ও উত্তম চর্চাসমূহ অনুসরণপূর্বক কার্যক্রম গ্রহণ করা। তাছাড়া ডিজিটাল ফরেনসিক ল্যাব হইতে প্রস্তুতকৃত ফরেনসিক প্রতিবেদন দেশের ও আন্তর্জাতিক আদালতসমূহে এই সংক্রান্ত অপরাধ বিচার কার্যক্রমে উপস্থাপনের যোগ্য করিয়া তোলা।

এই গাইডলাইন ডিজিটাল ফরেনসিক ল্যাবের পরিচালনা ও ক্ষেত্রমত, ব্যবস্থাপনার মৌলিক নির্দেশনা হিসাবে ভূমিকা পালন করিবে।

৪। গাইডলাইন এর প্রয়োগ ও পরিধি

এই গাইডলাইন ডিজিটাল নিরাপত্তা আইন, ২০১৮ এর ধারা ১০ অনুসারে স্থাপিত বা প্রত্যায়িত বা স্বীকৃত এবং ধারা ১১ -এ বিধৃত মানদণ্ডের উদ্দেশ্য পূরণকল্পে, সকল ডিজিটাল ফরেনসিক ল্যাবের ক্ষেত্রে প্রযোজ্য হইবে।

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 হিসাবে গ্রহণযোগ্য ও স্বীকৃত হয়।

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

(ক) কোনো তথ্য-উপাত্ত আহরণ করা;

(খ) উক্ত তথ্য-উপাত্তকে কার্যকর তথ্যে পরিণত করা; এবং

(গ) কোনো আইনগত কার্যধারায় উহার ফলাফল উপস্থাপন করা।

৬। ইলেকট্রনিক বা ডিজিটাল সাক্ষ্য প্রক্রিয়াকরণ, ইত্যাদির চ্যালেঞ্জসমূহ

ডিজিটাল সাক্ষ্য প্রক্রিয়াকরণ ও বিশ্লেষণের ক্ষেত্রে, এতদসংক্রান্ত অন্যান্য বিষয়াবলীর মধ্যে, নিম্নবর্ণিত বিষয়াদি বিবেচনা করিতে হইবে:

(ক) ইলেকট্রনিক বা ডিজিটাল তথ্য-উপাত্ত দেশের গণ্ডি ছাড়িয়া বিভিন্ন ভৌত অবস্থানে বিক্ষিপ্ত বা, ক্ষেত্রমত, বিস্তৃত অবস্থায় থাকিতে পারে;

(খ) ইলেকট্রনিক বা ডিজিটাল তথ্য-উপাত্ত অনায়াসে এবং মুহূর্তের মধ্যে এক দেশ হইতে অন্য দেশে

স্থানান্তর করা যায়;

(গ) ইলেকট্রনিক বা ডিজিটাল তথ্য-উপাত্ত সহজেই পরিবর্তনযোগ্য, কেননা কীবোর্ড বাটন চাপ দিয়া সহজে ইহাকে পরিবর্তন, পরিমার্জন, ক্ষতিগ্রস্ত বা ধ্বংস করা যায়;

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

(ঙ) অন্যান্য ভৌত 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। ইলেকট্রনিক বা ডিজিটাল সাক্ষ্যের গ্রহণযোগ্যতার বৈশিষ্ট্য

ডিজিটাল সাক্ষ্য-প্রমাণ গ্রহণযোগ্যতার বৈশিষ্ট্যসমূহ নিম্নরূপ:

(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 (Reproducibility): 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। ইলেকট্রনিক বা ডিজিটাল সাক্ষ্য বিশ্লেষণের নীতি

ইলেকট্রনিক বা ডিজিটাল সাক্ষ্য বিশ্লেষণের ক্ষেত্রে নিম্নেবর্ণিত বিষয়সমূহ পরিপালন করিতে হইবে:

(ক) ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০' এর বিধি ১৩, ও বিধি ১৪ তে পদ্ধতি অনুসরণ ব্যতীত কোনো ইলেকট্রনিক বা ডিজিটাল সাক্ষ্য-প্রমাণ সংগ্রহ করা যাইবে না;

(খ) ইলেকট্রনিক বা ডিজিটাল সাক্ষ্য-প্রমাণ বিশ্লেষণকারী বা পরীক্ষাকারী সুপারভাইজার ও বিশেষজ্ঞকে ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি-১৫ অনুসারে উপযুক্ত দক্ষতা ও প্রশিক্ষণ থাকিতে হইবে;

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

(ঘ) ইলেকট্রনিক বা 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

ডিজিটাল ফরেনসিক ল্যাব প্রতিষ্ঠার জন্য প্রয়োজনীয় প্রক্রিয়াসমূহ ল্যাব স্থাপনা পরিকল্পনা গ্রহণ, প্রয়োজনীয় সম্পদ সংগ্রহ এবং ল্যাবের দৈনন্দিন কার্যক্রম ও রক্ষণাবেক্ষণ ব্যাখ্যা করে।

৯। ডিজিটাল ফরেনসিক ল্যাবের অবস্থান

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

(ক) স্থান নির্বাচন: ডিজিটাল ফরনেসিক ল্যাবের স্থান নির্বাচনকালে বিবেচ্য বিষয়সমূহ:

i. ফরনেসিক ল্যাবের যন্ত্রপাতি পরিচালনের ক্ষেত্রে পর্যাপ্ত ও নিরাপদ বিদ্যুৎ সরবরাহের ব্যবস্থা থাকিতে হইবে এবং প্রয়োজনে বিদ্যুৎ সরবরাহের ব্যাকআপ (যেমন, জেনারেটর, ইউপিএস ইত্যাদি) এর ব্যবস্থা থাকিতে হইবে;

ii. ফরেনসিক ল্যাবের স্থান ভবনের উপরের দিকে অবস্থিত হইলে ইলেকট্রনিক সাক্ষ্য-প্রমাণাদি স্থানান্তরের জন্য পর্যাপ্ত লিফট বা উপযুক্ত ব্যবস্থা থাকিতে হইবে;

iii. ফরেনসিক ল্যাবের ভৌত কাঠামোগত পরিবেশ যাহাতে বিঘ্নিত না হয়, সেইজন্য এর

iv. পরিবেশগত ক্ষতি, প্রাকৃতিক দুর্যোগ ও মানবসৃষ্ট ক্ষতি হইতে সুরক্ষিত হইতে হইবে;

v. হার্ডওয়্যার ও অন্যান্য যন্ত্রপাতি রক্ষার জন্য পর্যাপ্ত শীতাতপ নিয়ন্ত্রণের ব্যবস্থা থাকিতে হইবে;

vi. ফরনেসিক ল্যাব বাইরের যে কোনো আক্রমণ বা অননুমোদিত অনুপ্রবেশ হইতে রক্ষার জন্য যথাযথ নিরাপত্তা ব্যবস্থা থাকিতে হইবে।

(খ) ভৌত নিরাপত্তা সংক্রান্ত বিষয়াদি:

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

i. ফরেনসিক ল্যাবে অবৈধ, অননুমোদিত প্রবেশ প্রতিরোধের জন্য নিবিড় নজরদারির ব্যবস্থা থাকিতে হইবে এবং এতদুদ্দেশ্যে সিসি ক্যামেরাসহ অন্যান্য নিরাপত্তামূলক ব্যবস্থা স্থাপন করিতে হইবে;

ii. সিস্টেমে অনুপ্রবেশ প্রতিরোধের জন্য ইলেকট্রনিক কি-প্যাড, সোয়াইপ কার্ড, বায়োমেট্রিক অ্যাক্সেস, ইত্যাদির ব্যবস্থা রাখিতে হইবে;

iii. অগ্নিদুর্ঘটনা জনিত নিরাপত্তা নিশ্চিতের জন্য প্রয়োজনীয় শনাক্তকরণ ও অগ্নি-নির্বাপণ যন্ত্রপাতির মজুদ থাকিতে হইবে;

iv. নিরবচ্ছিন্ন বিদ্যুৎ সরবরাহ নিশ্চিতের জন্য পর্যাপ্ত পাওয়ার সকেট, ফিউজ, সার্কিট ব্রেকার, ইত্যাদি যন্ত্রপাতি স্থাপন করিতে হইবে;

v. ক্ষতিকর ইলেক্ট্রো-স্ট্যাটিক ডিসচার্জ প্রতিরোধের জন্য ল্যাবের মেঝেতে এন্টি স্ট্যাটিক (Anti

Static) ব্যবস্থা থাকিতে হইবে;

vi. ল্যাবের নিজস্ব ইন্টারনেট ব্যবস্থায় বাইরের অনুপ্রবেশ প্রতিরোধের জন্য প্রযোজ্য ক্ষেত্রে সিগনাল জ্যামিং (Signal Jamming) বা অন্যান্য স্বীকৃত ব্যবস্থা রাখিতে হইবে;

vii. ডিজিটাল নমুনা বা আলামত সংরক্ষণ ও সার্ভার কক্ষ পর্যাপ্ত শীতাতপ নিয়ন্ত্রণের আওতায় থাকিতে হইবে;

viii. ডিজিটাল নমুনা বা আলামতের অফসাইট সংরক্ষণের পর্যাপ্ত ব্যবস্থা থাকিতে হইবে;

ix. ডিজিটাল নমুনা বা আলামত আইনগত বিধি-বিধান অনুসারে সংরক্ষণের ব্যবস্থা থাকিতে হইবে।

(গ) ফরেনসিক ল্যাবের অবকাঠামোর অংশসমূহ:

i. 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;

ii. ইলেক্ট্রনিক নমুনা বা আলামত সংরক্ষণাগার: এই স্থানটি কেবল ইলেক্ট্রনিক নমুনা বা আলামত সংরক্ষণের স্থান হিসেবে নিবেদিত হইতে হইবে, তবে উক্ত কক্ষে সার্ভারও রাখা যাইবে;

iii. 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;

iv. ল্যাবরেটরির কার্যক্রমসমূহ ইলেকট্রনিক নমুনা বা আলামতের ধরন অনুযায়ী ফরেনসিক ল্যাবের এক বা একাধিক কক্ষ থাকিতে পারে (যেমন, কম্পিউটার ফরেনসিক ল্যাব, মোবাইল ফোন ফরেনসিক ল্যাব, ড্রোন ফরেনসিক ল্যাব, ইত্যাদি);

v. কর্মকর্তাদের দাপ্তরিক ডেস্ক: কর্মকর্তাদের অফিসের দাপ্তরিক কাজের ডেস্ক ফরনেসিক বিশ্লেষণের কর্মসম্পাদন স্থান হইতে পৃথক হইতে হইবে;

vi. নিজস্ব ইন্টারনেট সুবিধা: ফরনেসিক ল্যাবে ম্যালওয়্যার ও ভাইরাসের আক্রমণ হইতে সুরক্ষিত ইন্টারনেট সুবিধা রাখিতে হইবে।

(ঘ) ফরেনসিক ল্যাবের দর্শনার্থী প্রবেশ সংক্রান্ত নিয়মাবলী:

i. ডিজিটাল ফরনেসিক ল্যাবে সুপারভাইজার, ফরেনসিক বিশেষজ্ঞ ও দায়িত্বপ্রাপ্ত কর্মচারীর অনুমোদিত প্রবেশাধিকার সংরক্ষিত থাকিবে; অন্য কোনও ব্যক্তির উক্ত ল্যাবে প্রবেশ করিতে হইলে ল্যাব কর্তৃপক্ষের অনুমোদন থাকিতে হইবে;

ii. ল্যাবে প্রবেশাধিকার সীমিত ও নির্দিষ্ট সময়ের জন্য হইবে এবং ল্যাব কর্তৃপক্ষের অনুমোদিত নয় এমন কোনো কর্মকান্ড পরিচালনা করা যাইবে না;

iii. (i) তে বর্ণিত ব্যক্তিগণ ফরেনসিক ল্যাবে প্রবেশের পূর্বে আবশ্যিকভাবে নির্ধারিত ফরমে (পরিশিষ্ট-০৮) নিবন্ধন করিতে হইবে;

iv. ল্যাবে প্রবেশের ক্ষেত্রে দর্শনার্থীকে একটি সাময়িক আইডি কার্ড/পরিচয়পত্র ইস্যু করা যাইতে পারে;

v. ডিজিটাল ফরেনসিক ল্যাবের একজন কর্মকর্তা সার্বক্ষণিকভাবে দর্শনার্থীর সহিত গাইড

(Escort) হিসাবে থাকিবেন;

vi. ফরেনসিক ল্যাবে অবশ্যই ল্যাব পরিদর্শনের নিয়মাবলী লিখিত ও দৃশ্যমান থাকিতে হইবে, যথা: ল্যাবে ইলেকট্রনিক আলামত ও যন্ত্রপাতি স্পর্শকরণ, ছবিতোলা, খাদ্য ও পানীয় বহন সংক্রান্ত নিষেধাজ্ঞা নিয়মাবলীতে স্পষ্টভাবে উল্লেখ থাকিতে হইবে।

১০। ডিজিটাল ফরেনসিক ল্যাবের জনবল

(ক) ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি ১৬ এর বিধান অনুসারে-

i. ডিজিটাল ফরেনসিক ল্যাবের জনবল নিয়োগ করিতে হইবে; এবং

ii. জনবল তাহাদের উপর অর্পিত দায়িত্ব পালন করিবেন;

(খ) ডিজিটাল ফরেনসিক ল্যাবের চাহিদা অনুযায়ী উহাতে নিয়োগকৃত জনবল **পরিশিষ্ট-০১** এ বর্ণিত কারিগরি দক্ষতা থাকিতে হইবে।

অংশ-০৫: ডিজিটাল ফরেনসিক ল্যাবের 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 ও সফট্ওয়্যার থাকিবে-

i. হার্ডওয়্যার;

ii. সফটওয়্যার (ওপেন সোর্স বা বাণিজ্যিক);

(গ) যন্ত্রপাতি ব্যবহারের পূর্বে উহার গুণগত মান ও ব্যবহারযোগ্যতা অবশ্যই পরীক্ষা এবং যাচাই করিতে হইবে।

১২। সফটওয়্যার সংক্রান্ত বিষয়াদি

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

i. সফটওয়্যার এর ক্রয়মূল্য বা বাৎসরিক লাইসেন্স ফি;

ii. সফটওয়্যার এর ব্যবস্থাপনা ও রক্ষণাবেক্ষণ ব্যয়;

iii. সফটওয়্যারের ব্যবহারিক প্রশিক্ষণ প্রদান সুবিধা।

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

(গ) উক্ত সফটওয়্যার এর রেকর্ড লগে ল্যাবে প্রাপ্ত সকল ফরেনসিক আলামত এর নিম্নবর্ণিত তথ্য সংরক্ষণ করিতে হইবে:

i. নমুনা বা আলামত গ্রহণকারী ও সরবরাহকারী ল্যাব কর্মকর্তার নামসহ উহা গ্রহণ ও সরবরাহের দিন ও তারিখ;

ii. নমুনা বা আলামত ও সংশ্লিষ্ট কেস নাম্বার;

iii. কেস অধিযাচনকারীর নাম ও যোগাযোগের ঠিকানা;

iv. ফরেনসিক পরীক্ষার চাহিদাপত্র ও কেসের বিস্তারিত বর্ণনা;

v. ফরেনসিক বিশ্লেষণের ফলাফল প্রদানের সম্ভাব্য তারিখ ও তৎসংশ্লিষ্ট তথ্যাদি;

vi. ফরেনসিক কেসের বিশ্লেষণ প্রক্রিয়ার বিবরণ (যেমন- ইমেজিং, আহরণ, হ্যাশ ভ্যালু, ইত্যাদি);
vii. বিশ্লেষণের ফলাফল ও সংশ্লিষ্ট ফরেনসিক বিশেষজ্ঞের নাম;
viii. অধিযাচনকারীর সহিত কেস সংক্রান্ত বিষয়ে আলোচনার বিস্তারিত বিবরণ;
ix. 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 সংবলিত নিম্নবর্ণিত যন্ত্রপাতি থাকিতে হইবে:

- ল্যাপটপ ও ডেস্কটপ
- ফরেনসিক বিশ্লেষণ সফটওয়্যার
- উপাত্ত পুনরুদ্ধারকরণ সফটওয়্যার
- মোবাইল ডিভাইস বিশ্লেষণ সফটওয়্যার
- ড্রোন সিস্টেম বিশ্লেষণ হার্ডওয়্যার বা সফটওয়্যার
- 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। যন্ত্রপাতি ও আনুষঙ্গিক যন্ত্রাংশ (tools & accessories)

ডিজিটাল ফরেনসিক ল্যাবে ফরেনসিক বিশ্লেষণ কার্যক্রমকে সুষ্ঠুভাবে সম্পাদনের নিমিত্ত যথাযথ মানদণ্ডের নিম্নবর্ণিত যন্ত্রপাতি ও আনুষঙ্গিক যন্ত্রাংশ ল্যাবে থাকিতে হইবে:

- প্রিন্টার
- নথি বিনষ্টকরণ যন্ত্র (Document Shredder)
- পাওয়ার এক্সটেনশন কেবল
- লিডস এবং অ্যাডাপ্টরস
- স্ক্রু ড্রাইভারস
- ক্যামেরা ও ভিডিও 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

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

(ক) ফরেনসিক পরীক্ষার অধিযাচন;

(খ) ফরনেসিক পরীক্ষার নিবন্ধন;

(গ) ফরেনসিক পরীক্ষার চাহিদা পর্যালোচনা;

(ঘ) ফরেনসিক পরীক্ষার তথ্য প্রমাণ নির্ধারণ;

(ঙ) ফরেনসিক নমুনা বা আলামতের বিশ্লেষণ;

(চ) ফরেনসিক নমুনা বা আলামত প্রত্যর্পণ;

(ছ) সমাপ্তি ও প্রতিবেদন দাখিল।

১৭। ফরেনসিক পরীক্ষার অধিযাচন (Requisition)

(১) ডিজিটাল ফরেনসিক ল্যাব কোনো অনুরোধকারীর নিকট হইতে আনুষ্ঠানিক পত্র বা ইমেইল-যোগে অনুরোধ পাইবার পর **পরিশিষ্ট-০২** 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 ল্যাবে প্রেরিত ফরেনসিক নমুনা বা আলামতসমূহ গ্রহণের সময় নিম্নবর্ণিত তথ্যাদি ও অন্যান্য বিষয় ল্যাব কর্তৃপক্ষ কর্তৃক নির্ধারিত ফরমে (পরিশিষ্ট-০২) লিপিবদ্ধ করিয়া নিবন্ধন করিতে হইবে:

(ক) নমুনা বা আলামত সংগ্রহের আইনগত ভিত্তি;

(খ) নমুনা বা আলামত সিলগালা করা রহিয়াছে কিনা;

(গ) ফরেনসিক নমুনা বা মামলার বর্ণনা;

(ঘ) সংশ্লিষ্ট 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 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-০৩ 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:

(ক) চিহ্নিত আলামত আর অন্যকোনো ফরেনসিক পদ্ধতিতে পরীক্ষা করিতে হইবে কিনা (যেমন: কী-ওয়ার্ড, টুল-মার্কস, ট্রেস, সন্দেহজনক নথি [keywords, toolmarks, trace and question documents] তল্লাশির বিষয়);

(খ) আরও ডিজিটাল তথ্য-প্রমাণ সংগ্রহের নিমিত্ত অন্য প্রকার 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 অনুরূপ কোনো আলামত, ইত্যাদি);

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

(ঙ) ফরেনসিক কেসের নিমিত্ত প্রয়োজনীয় অতিরিক্ত তথ্যাবলী (যেমন: ছদ্মনাম বা অন্যনাম (alias), ই-মেইল ঠিকানা, আইএসপি সেবা প্রদানকারীর নাম, নেটওয়ার্ক কনফিগারেশন ও এর ব্যবহারকারী (user), সিস্টেম লগ, পাসওর্য়াড, ইউজার নেম সংগ্রহ করা); এই সকল তথ্যাদির সংশ্লিষ্ট সিস্টেম এডমিনিস্ট্রেটর, ব্যবহারকারী (user) এবং সংশ্লিষ্ট প্রতিষ্ঠানের কর্মচারীদের সাক্ষাৎকার গ্রহণ করা যাইতে পারে;

(চ) ব্যবহৃত 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 কার্যক্রম গ্রহণ ও সাক্ষ্য-প্রমাণ সংগ্রহের ক্ষেত্রে ডিজিটাল নিরাপত্তা এজেন্সি'র মহাপরিচালকের অনুমোদন নিতে হইবে]

২১। ডিজিটাল নমুনা বা আলামত বিশ্লেষণ

(১) অংশ ১০ -এ বিধৃত পদ্ধতিতে ডিজিটাল নমুনা বা আলামত বিশ্লেষণ করিতে হইবে;

(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 ফরেনসিক বিশ্লেষণের স্বার্থে প্রয়োজন হইলে যোগাযোগ করিতে পারিবেন;

(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-০৪** -এ বিধৃত ফ্লো-চার্ট অনুসরণ করা যাইতে পারে।

২২। ডিজিটাল সাক্ষ্য-প্রমাণ প্রত্যর্পণ

(১) ডিজিটাল নমুনা বা আলামতসমূহ প্রত্যর্পণের সময় উহার শুদ্ধতা অক্ষুণ্ণ 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-০২** -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 মহাপরিচালকের অনুমোদনক্রমে অধিযাচনকারীকে প্রদান করিতে হইবে।

(২) উক্তরূপে অধিযাচনকারীকে প্রতিবেদন প্রদানের পর, ল্যাবে 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:

(ক) ফরেনসিক নমুনা বা আলামত গ্রহণ (Receipt);

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

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

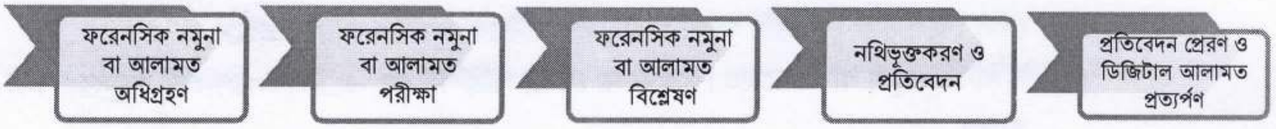
(ঘ) নথিভুক্তকরণ ও প্রতিবেদন প্রস্তুতকরণ (Documentation and Reporting)

ঙ) প্রতিবেদন প্রেরণ ও ডিজিটাল আলামত প্রত্যর্পণ।

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

(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 অক্ষুণ্ণ রাখিয়া উহা পরীক্ষা/বিশ্লেষণসমূহ 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 অক্ষুণ্ণ 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;

(৪) ডিজিটাল নমুনা বা আলামত অধিগ্রহণে সহায়ক হিসেবে **পরিশিষ্ট-০৫** এ 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 অবিকল 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 অরূপান্তরিত 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 অবরাদ্দকৃত 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 লিখিতে 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) ০১) বা অ্যাডভান্সড ফরেনসিক ফরম্যাট (AFF) -এ স্টোরেজের সকল উপাত্তের অবিকল ইমেজ (raw/dd) সংরক্ষণ করিতে হইবে; এবং ইমেজ ফরম্যাট-এর বৈশিষ্ট্যসমূহ নিম্নরূপ-

(ক) উপাত্তের সংকোচনকরণ (Compression);
(খ) উপাত্তের এনক্রিপশনকরণ (Encryption);
(গ) ত্রুটি পরীক্ষাকরণ;
(ঘ) কেস মেটাডাটা (Metadata) চিহ্নিতকরণ;
(ঙ) ফাইল হ্যাশ-এর যোগফল;
(চ) 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 ফরম্যাটে ইমেজ সংরক্ষণ করিতে হইবে।

(৯) ডিজিটাল নমুনা বা আলামতের ইমেজ ফাইল যাচাইকরণ:

(ক) ফরেনসিক কপিতে পরবর্তী সকল প্রক্রিয়াকরণ ও বিশ্লেষণের নিমিত্ত মূল স্টোরেজ মাধ্যম এবং ইমেজ ফাইলে একই উপাত্ত রহিয়াছে কিনা উহা যাচাই করিবার জন্য উভয় উপাত্তের সেটে SHA-১, SHA-২৫৬ 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 নিমিত্ত 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 নিমিত্ত 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 ডিভাইসের সকল পাসকোড, পাসওয়ার্ড এবং নমুনা বা আলামতের ধরণ সংগ্রহ করিতে হইবে।

(২) উপ-অনুচ্ছেদ (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 অবিকল (Raw data) বাইনারি উপাত্ত অধিগ্রহণ প্রক্রিয়াই হইল ভৌত আহরণ। এই ধরনের আহরণের ক্ষেত্রে অরূপান্তরিত 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

প্রবেশযোগ্যতা প্রদান করে যেখানে সাধারণভাবে কোনো ব্যবহারকারীর প্রবেশযোগ্যতা 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 ডিভাইসের 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 অবিকল (raw data) বাইনারি উপাত্ত আহরণ করা যাইবে।

(চ) চিপ-অফ (Chip-Off) আহরণ পদ্ধতি: চিপ-অফ আহরণ পদ্ধতিতে অবিকল বাইনারি উপাত্ত আহরণ করা যাইবে এইক্ষেত্রে মোবাইল ডিভাইস হইতে ইহার স্টোরেজকে সম্পূর্ণ বিচ্ছিন্ন করিতে হইবে; এবং উক্তরূপে বিচ্ছিন্ন করা হইলে মোবাইল ডিভাইসটি নস্ট হইয়া যাইতে পারে। যেক্ষেত্রে আইওটি ডিভাইসের স্টোরেজ এ উপাত্ত ক্লিয়ার টেক্সট রূপে 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 সিস্টেমের 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 বাঞ্ছনীয়।

(৩) তথ্য উপাত্ত আহরণের যন্ত্রপাতি (Tools): 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 যন্ত্রপাতি (Tools) ব্যবহার করিয়া উপাত্ত আহরণ করিবার প্রয়োজনে মোবাইল ডিভাইস এর তথ্য-উপাত্ত স্বত্বাধিকারী (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 অবিকল 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 শনাক্ত 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:

(i) 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;

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

(iii) 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;

(iv) 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 মোডে" 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-

i. ডিভাইসটি উপরোক্ত (আ) তে বর্ণিত কাজের উপযুক্ত না হয়, তাহা হইলে উক্ত

ডিভাইস মোবাইল নেটওয়ার্কসহ যেকোনো নেটওয়ার্ক হইতে বিচ্ছিন্ন অবস্থায় রাখিতে হইবে; এবং

ii. 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-

i. 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

ii. 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।

(উ) 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 সংশ্লিষ্ট 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-০৬** 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;

(গ) 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 ফাইলসমূহ 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:

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

ii. যে সকল তথ্য বা উপাত্ত অপারেটিং সিস্টেম বা ফাইল সিস্টেমের অন্তর্গত নয় সেইগুলি মূলশব্দ (Keyword) দ্বারা খুঁজিয়া বাহির করা;

iii. যে সকল তথ্য বা উপাত্ত অপারেটিং সিস্টেম বা ফাইল সিস্টেমের অন্তর্গত নয় সেইগুলি পুনরুদ্ধার ফাইল শনাক্তকরণ দ্বারা খুঁজিয়া বাহির করা;

iv. 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:-

i. নির্ণীত হ্যাশ মানের সহিত বিশুদ্ধ ফাইলের হ্যাশ মানের তুলনা করিয়া পরিচিত ফাইল নিরূপণ ও নির্ধারণ;

ii. ড্রাইভে ফাইলের নাম ও ধরন, ফাইলের হেডার এবং অবস্থানের ভিত্তিতে পরীক্ষার জন্য প্রাসঙ্গিক ফাইলসমূহ আহরণ;

iii. মুছিয়া ফেলা ফাইলসমূহ পুনরুদ্ধার;

iv. পাসওয়ার্ড দ্বারা সুরক্ষিত, এনক্রিপ্টেড ও জিপ করা ফাইলসমূহ পুনরুদ্ধার;

v. ফাইলসমূহের মধ্যবর্তী ফাঁকা স্থান শনাক্তকরণ;

vi. অবণ্টনকৃত স্থান শনাক্তকরণ।

(৫) ফিল্টারিং: ফরেনসিক বিশ্লেষণের পরিমাণ 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 ব্ল্যাকলিস্টিং পদ্ধতিতে জানা অবৈধ ফাইলসমূহের উপাত্ত-ভান্ডারে হ্যাশ প্রযুক্তির মাধ্যমে ম্যাচিং করানো হইয়া থাকে।

৩০। মোবাইল ডিভাইস পরীক্ষণ পদ্ধতি

মোবাইল ডিভাইসের অসংখ্য ব্র্যান্ড ও মডেল, মোবাইলে সংরক্ষিত উপাত্ত ও মোবাইলের ধরনের প্রাচুর্যতার কারণে 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 পরিমাণ 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' শিরোনামের আওতাধীন পদ্ধতি অনুসরণ করিতে হইবে;

(২) সহায়ক হিসেবে **পরিশিষ্ট-০৪** 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 শনাক্তযোগ্য আবার কিছু চিহ্ন সহজে উদ্ঘাটযোগ্য নহে।

(খ) সহজেই শনাক্তযোগ্য চিহ্নসমূহ নিম্নে উল্লেখ করা হইলো:

(i) স্লাক স্পেস (Slack space);

(ii) অবরাদ্দকৃত স্পেস (Unallocated space);

(iii) MFT এন্ট্রিস;

(iv) RAM;

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

(i) থাম্ব ক্যাশ;

(ii) সদ্য ব্যবহৃত ফাইলের লিস্ট;

(iii) লগ ফাইল;

(iv) ব্রাউজার হিস্টোরি;

(v) ব্রাউজার ক্যাশ;

(vi) সর্বাধিক ব্যবহৃত প্রোগ্রামসমূহ;

(vii) ফরম উপাত্ত;

(viii) Pagefiles.sys

(ix) Hiberfil.sys

(x) ভলিউম শ্যাডো কপি;

(xi) 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 প্রমাণ পাওয়া যায়, যথা:

(i) ওয়েবসাইট ব্রাউজ হিস্টোরি;

(ii) লোকাল ক্যাশ বা টেম্পরারি ইন্টারনেট ফাইল;

(iii) বুকমার্ক বা ফেভারিটস;

(iv) সেশান তথ্যাবলী;

(v) কুকিজ সমূহ;

(vi) সংরক্ষিত ইউজার নেম ও পাসওয়ার্ড;

(vii) ফরম ফিল্ড এর এন্ট্রি সমূহ;

(viii) ইন্টারনেট কি ওয়ার্ড সার্স;

(ঙ) সফটওয়্যার;

(চ) নিম্নবর্ণিত বিষয়সমূহে কম্পিউটার ইউজার অ্যাক্টিভিটি লগ সংরক্ষিত থাকে;

(i) ডিভাইস পাওয়ার অন এবং শাটডাউন টাইম;

(ii) সফটওয়্যার সেটিংস;

(iii) সাম্প্রতিক ব্যবহৃত হওয়া ফাইলসমূহ;

(iv) ডিভাইসের ব্যবহার বিস্তারিত;

(v) ইউজার লগইন;

(vi) ওয়াই-ফাই সংযোগ;

(vii) পছন্দনীয় প্রোগ্রামের তালিকা;

(viii) ইউজার এনভাইরনমেন্ট এর সেটআপ;

(ix) বেশি ব্যবহৃত প্রোগ্রামসমূহ, ইত্যাদি।

(ছ) লগ ফাইলসমূহ;

(জ) এনক্রিপশন;

(ঝ) অবরাদ্দকৃত 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 নির্দিষ্ট 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) কন্ট্যাক্ট 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 অ্যাকাউন্ট;

(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 'নথিভুক্তকরণ ও প্রতিবেদন প্রস্তুতকরণ' শিরোনামার আওতাধীন পদ্ধতি অনুসরণ করিতে হইবে।

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 কার্যসম্পাদনের পর প্রাপ্ত পর্যবেক্ষণ ও ফলাফল ফরেনসিক প্রতিবেদনে অন্তর্ভুক্ত করিতে হইবে;

(৩) এইক্ষেত্রে অন্যান্য ডিজিটাল সাক্ষ্য প্রমাণের সহিত সামঞ্জস্য রাখিবার প্রয়োজনে বিশেষায়িত সফটওয়্যার বা যন্ত্রপাতি (Tools) এর সহযোগিতা গ্রহণ করা যাইতে পারে।

৩৬। ইলেকট্রনিক বা ডিজিটাল সাক্ষ্য প্রমাণাদির গ্রহণযোগ্যতা

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

(ক) সঠিকতা (Authenticity): ফরেনসিক প্রতিবেদনে যে কোনো 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 (Trustworthyness): 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 ১৭০২৫: টেস্টিং ও ক্যালিব্রেশন পরীক্ষাগারের যোগ্যতার সাধারণ মাপকাঠি;

(খ) ISO/IEC/BDS ১৫৪৮৯: রেকর্ডস ব্যবস্থাপনা;

(গ) ISO/IEC/BDS ২৭০৩৭: ডিজিটাল সাক্ষ্য শনাক্তকরণ, সংগ্রহ, অধিগ্রহণ এবং সংরক্ষণ নির্দেশিকা;

(ঘ) ISO/IEC/BDS ২৭০৪১: ঘটনা তদন্ত পদ্ধতির গ্রহণযোগ্যতা ও উপযুক্ততা নিরূপণের মাপকাঠি/নির্দেশিকা;

(ঙ) ISO/IEC/BDS ২৭০৪২: ডিজিটাল সাক্ষ্য বিশ্লেষণ ও স্পষ্টিকরণ নির্দেশিকা;

(চ) ISO/IEC/BDS ২৭০৪৩: ঘটনা তদন্তের পদ্ধতি ও নীতিমালা;

(ছ) ISO/IEC/BDS ২৭০৫০: ইলেকট্রনিক ডিসকভারি।

(ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি ১৪ এর উপ-বিধি (১) -এ নির্ধারিত)

অংশ-১৩: ফরেনসিক ল্যাবের গুণগতমান নিশ্চিতকরণ (Quality Assurance)

৩৮। গুণগতমান 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।

(ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি ১৪ এর উপ-বিধি (২) অনুসারে মান নিশ্চিত করিতে হইবে)

৩৯। গুণগতমান নিশ্চিতকরণের উপাদান (Component)

গুণগতমান নিশ্চিতকরণ ও বাস্তবায়নার্থে ডিজিটাল ফরেনসিক ল্যাবরেটরি এতদুদ্দেশ্যে **পরিশিষ্ট-০৭** এ বর্ণিত গুণগতমান নিশ্চিতকরণের উপাদান সম্পর্কিত চেকলিস্ট অনুসরণ করিবে।

অংশ-১৪: বিবিধ বিষয়াবলী

৪০। 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।

৪১। 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।

৪২। তথ্য-উপাত্তের গোপনীয়তা

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

৪৩। 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।

৪৪। নির্দেশ প্রদানের ক্ষমতা

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

৪৫। অব্যাহতি

মহাপরিচালক, কোনো বিশেষ পরিস্থিতি পরিহারের উদ্দেশ্যে, কোনো ডিজিটাল ফরেনসিক ল্যাব কর্তৃপক্ষের আবেদনের প্রেক্ষিতে, কোনো নির্দিষ্ট সময়ের জন্য এই গাইডলাইনের সুনির্দিষ্ট কোনো বিধানের প্রয়োগ হইতে, মহাপরিচালক কর্তৃক আরোপিত শর্ত সাপেক্ষে অব্যাহতি প্রদান করিতে পারিবে।

৪৬। গাইডলাইনের সীমাবদ্ধতা

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

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

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

পরিশিষ্টসমূহের তালিকা

পরিশিষ্ট-০১	:	ডিজিটাল ফরেনসিক ল্যাবের জনবলের দক্ষতা
পরিশিষ্ট-০২	:	ডিজিটাল ফরেনসিক পরীক্ষার কেস অধিযাচন ফরম
পরিশিষ্ট-০৩	:	চেইন অফ কাস্টডি
পরিশিষ্ট-০৪	:	ডিজিটাল নমুনা বা আলামত বিশ্লেষণ প্রক্রিয়া
পরিশিষ্ট-০৫	:	ডিজিটাল নমুনা বা আলামত অধিগ্রহণ প্রক্রিয়ার ফ্লো-চার্ট
পরিশিষ্ট-০৬	:	কম্পিউটার পরীক্ষণ প্রক্রিয়ার ফ্লো-চার্ট
পরিশিষ্ট-০৭	:	গুণগতমান নিশ্চিতকরণ চেকলিস্ট
পরিশিষ্ট-০৮	:	ফরেনসিক ল্যাবে প্রবেশের নিবন্ধন বহি

পরিশিষ্ট-০১: ডিজিটাল ফরেনসিক ল্যাবের 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 HDD and 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-০২: ডিজিটাল ফরেনসিক পরীক্ষার কেস অধিযাচন ফরম

তারিখ: 00-00-0000

১। অধিযাচনপত্র প্রেরণকারী প্রতিষ্ঠানের নাম:

ঠিকানা :

টেলিফোন :

ইমেইল :

২। অধিযাচনপত্র প্রেরণকারী কর্মকর্তার নাম:

পদবী :

যোগাযোগের ঠিকানা :

৩। মামলার বিবরণ

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

৪। ডিজিটাল ফরেনসিক পরীক্ষার প্রেরিত আলামতের (exhibit) বিবরণ

আলামতের (exhibit) আইডি ও সংক্ষিপ্ত বিবরণ	
কোথায়, কে, কখন ও কিভাবে আলামতটি পাওয়া গিয়াছে?	
আলামতের উৎস	
আলামতের সহিত সংশ্লিষ্ট আসামী/ভিকটিম/অন্য কেহ	
মন্তব্য	

৫। আলামত প্রেরণের বিবরণ এবং নমুনা সীল

(স্বাক্ষর/-)
নাম, পদবী
মোবাইল

ডিজিটাল ফরেনসিক ল্যাব কর্তৃক পূরণীয়

৬.১। পরীক্ষার নিমিত্ত 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):

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

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।

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।

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-০৩: চেইন অফ কাস্টডি (Chain of Custody)

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	

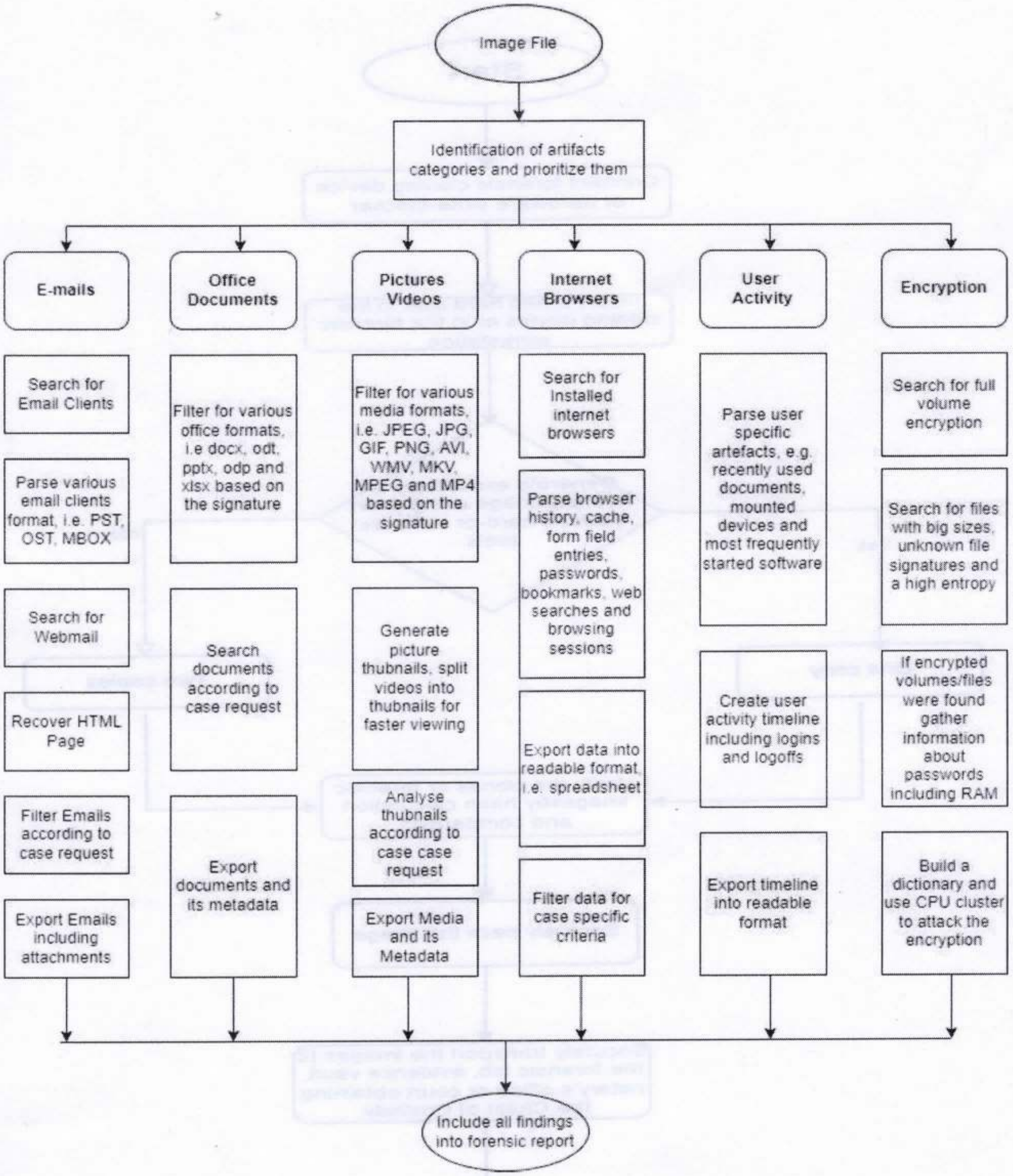
আইটেম নম্বর	পরিমাণ	বিবরণ (মডেল, ক্রমিক নম্বর, অবস্থা, বিশেষ চিহ্ন নোট করুন)

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

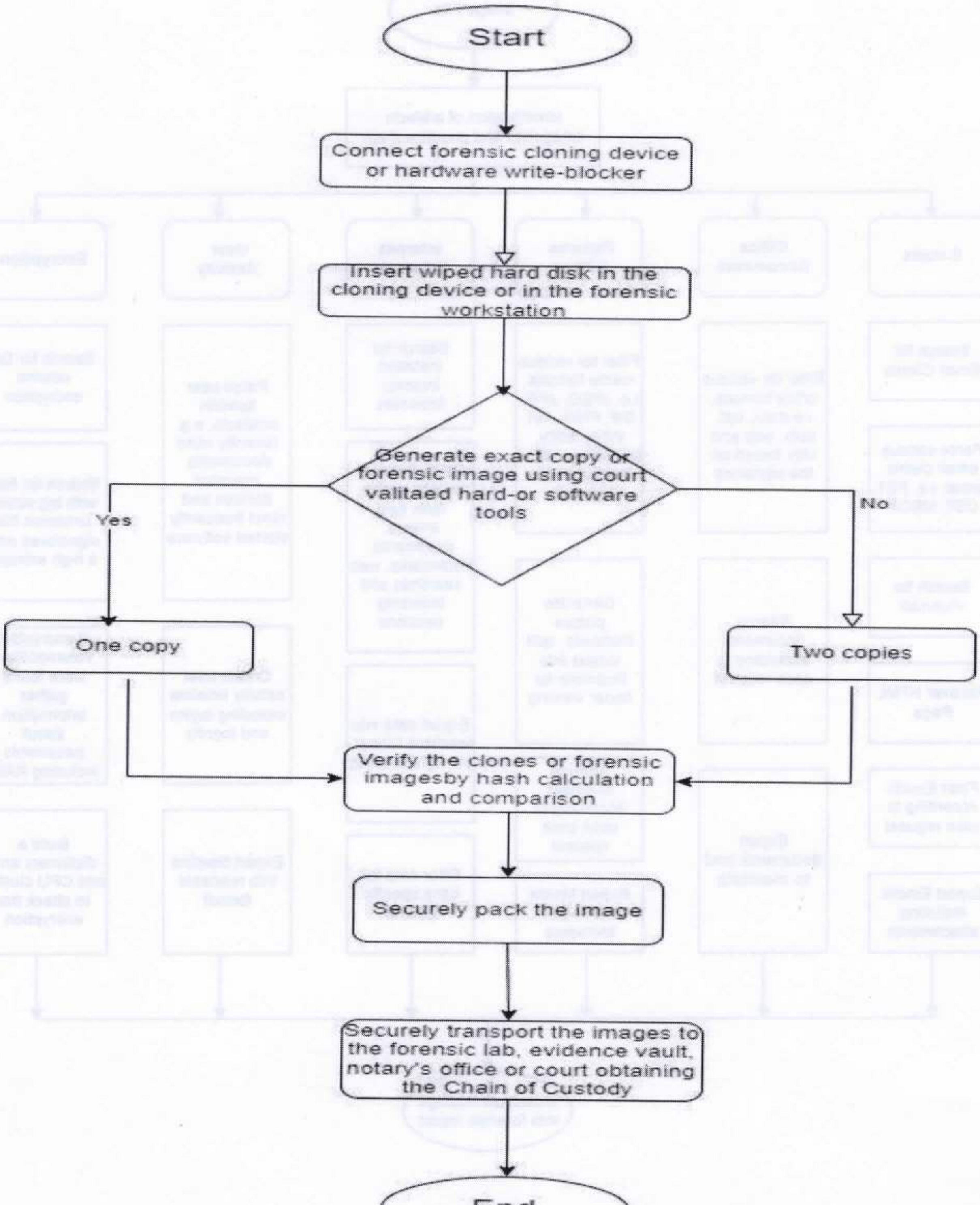
ফেরত প্রদানের স্লিপ	
কেস নম্বর	তারিখ
সূত্রঃ নং	
প্রেরক	
পরীক্ষকের নাম ও পদবি	

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

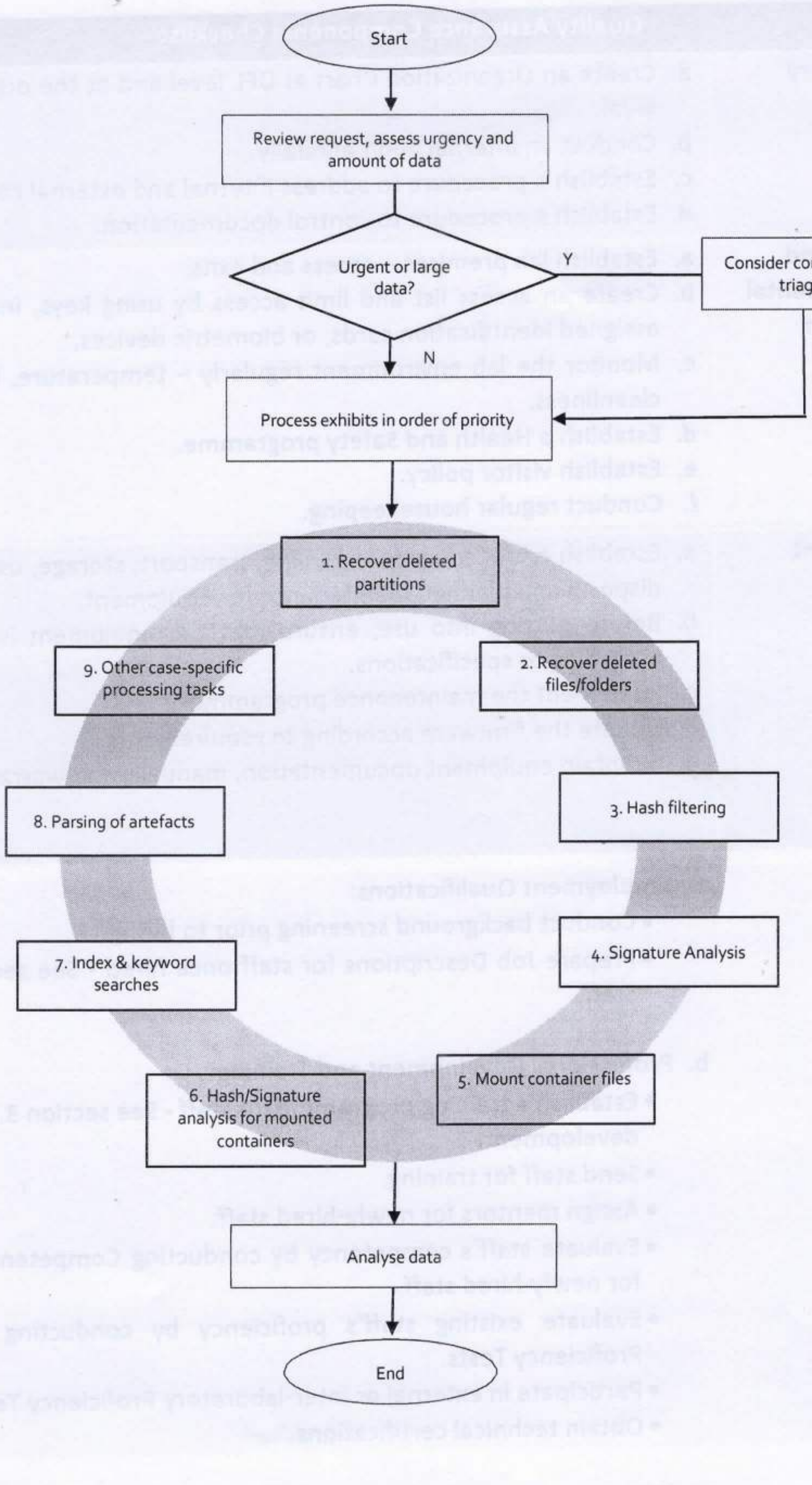
পরিশিষ্ট-০৪: ডিজিটাল নমুনা বা আলামত বিশ্লেষণ প্রক্রিয়া



পরিশিষ্ট-০৫: ডিজিটাল নমুনা বা আলামত অধিগ্রহণ প্রক্রিয়ার ফ্লো-চার্ট



পরিশিষ্ট-০৬: কম্পিউটার পরীক্ষণ প্রক্রিয়ার ফ্লো-চার্ট



পরিশিষ্ট-০৭: গুণগতমান 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.

পরিশিষ্ট-০৮: ফরেনসিক ল্যাবে প্রবেশের নিবন্ধন বহি

ক্রমিক	নাম ও পদবী	কর্মস্থলের ঠিকানা	এনআইডি নাম্বার	ফোন	আগমনের সময়	প্রস্থানের সময়	প্রবেশের উদ্দেশ্য	স্বাক্ষর

17.07.2023

মনির হোসেন চৌধুরী
উপসচিব
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ