

# ডিজিটাল ফরেনসিক অ্যান্ড ইনভেস্টিগেশন

আরিফ মঈনুদ্দীন



আদিত্য প্রকাশ



### লেখক পরিচিতি

আইটি বিশেষজ্ঞ জনাব আরিফ মঈনুদ্দীন পড়াশোনা করেছেন ঢাকা বিশ্ববিদ্যালয়ের ইসলামিক স্টাডিজ বিভাগে। ইসলামিক স্টাডিজ বিভাগে পড়াশোনা করলেও তার আগ্রহ ছিল আইটি সিকিউরিটি নিয়ে। কম্পিউটার সায়েন্সে না পড়ার কারণে তাকে অনেক বাধার সম্মুখীন হতে হয়েছে। সব প্রতিকূলতা অতিক্রম করে তিনি নিজেকে গড়ে তোলেন আইটি বিশেষজ্ঞ হিসেবে, অর্জন করেন বেশ কিছু ভেঙের সার্টিফিকেশন CEH, CHFI, CSA, CSCU, ECSA, CEI, OSINT and Red Hat এর RHSCA. এ ছাড়া তিনি EC-Council-এর অধীনে একজন সার্টিফাইট ইন্ট্রাকটর। ক্যারিয়ারের প্রথম দিকে তিনি চাকরি করেছেন ওয়েব ডেভেলপার হিসেবে একটি আইটি ফার্মে, পরবর্তী সময়ে তথ্য নিরাপত্তা নিয়ে পুরোদমে কাজ শুরু করেন, কাজ করেছেন বিভিন্ন গোয়েন্দা সংস্থার সঙ্গে এবং প্রশিক্ষণ দিয়েছেন আইন প্রয়োগকারী সংস্থা ও সরকারি কর্মকর্তাদের। তিনি কাজ করেছেন এবং প্রশিক্ষণ দিয়েছেন RAB, PBI, DMP, CMP, BMP, ATU, CID, DB, District Police, Bangladesh Army, Bank, Telecommunication Sector এবং ICT Division-কে। বর্তমানে তিনি সাইবার সিকিউরিটির কথা মাথায় রেখে এবং দক্ষ এক্সপার্ট তৈরি করতে প্রতিষ্ঠা করেন Decodes Lab Limited ([www.decodeslab.com](http://www.decodeslab.com)). তিনি বর্তমানে এই প্রতিষ্ঠানের

ব্যবস্থাপনা পরিচালক ও প্রশিক্ষক হিসেবে কর্মরত, এই প্রতিষ্ঠান থেকে প্রায় ৫০০-এর অধিক ব্যক্তি ট্রেনিং নিয়ে দেশে-বিদেশে বিভিন্ন মাল্টিন্যাশনাল প্রতিষ্ঠান, আর্থিক প্রতিষ্ঠান, ব্যাংক, আইটি ফার্ম ও গোয়েন্দা সংস্থাতে দক্ষতার সঙ্গে কর্মরত আছেন। পাশাপাশি সবার কথা চিন্তা করে আইটি সিকিউরিটির ওপর দক্ষতা বৃদ্ধি করতে একটি অনলাইনভিত্তিক ই-লার্নিং প্ল্যাটফর্ম তৈরি করেছেন ([www.cyberskillbd.com](http://www.cyberskillbd.com)), যেখান থেকে সহজে যে কেউ কোর্স করে নিজেকে দক্ষ করে গড়ে তুলতে পারবে। এর পাশাপাশি তিনি বিভিন্ন সময়ে তথ্য নিরাপত্তার বুঁকি নিয়ে সচেতনতা বৃদ্ধিতে বিভিন্ন স্কুল, কলেজ ও ইউনিভার্সিটিতে ওয়ার্কশপ ও সেমিনার পরিচালনা করেছেন এবং দেশের লিড টিভি মিডিয়াগুলোতে সাক্ষাৎকার প্রদান করে চলছেন। তার কর্মতৎপরতার মধ্যে আরও রয়েছে বিভিন্ন প্রতিষ্ঠান ও কোম্পানির দুর্বলতা মূল্যায়ন ও পেনিট্রেশন টেস্টিং, ডেটা প্রাইভেসি মূল্যায়ন, কনসালটেন্সি ও কর্পোরেট ট্রেনিং। তিনি সাইবার অপরাধের ভুক্তভোগীদের পরামর্শও দিয়ে থাকেন। তিনি বাংলাদেশ কারিগরি শিক্ষা বোর্ড ও জাতীয় দক্ষতা উন্নয়ন কর্তৃপক্ষ-প্রধানমন্ত্রীর কার্যালয়ের অধীনে সাইবার সিকিউরিটি ও ডিজিটাল ফরেনসিকের ওপর সিলেবাস প্রণয়ন ও মানদণ্ড নির্ধারণ কমিটির সদস্য ছিলেন।

### লেখকের সঙ্গে যোগাযোগ:

Website: [www.arifmainuddin.com](http://www.arifmainuddin.com)

Email: [devarif22@gmail.com](mailto:devarif22@gmail.com)

Mobile: 8801795204246

Facebook: <https://www.facebook.com/arifvai99>

# সূচিপত্র

<b>অধ্যায়- ১: ডিজিটাল ফরেনসিক</b>	<b>১৩</b>
১.১ ডিজিটাল বলতে কী বোঝায়?	১৩
১.২ ফরেনসিক কী?	১৩
১.৩ ডিজিটাল ফরেনসিক কী?	১৩
১.৪ কম্পিউটার ফরেনসিক কী?	১৩
১.৫ সাইবার ক্রাইম কী?	১৪
১.৬ সাইবার ক্রাইমের উপাদান	১৪
১.৭ সাইবার ক্রাইমের উদাহরণ	১৫
১.৮ সাইবার ক্রাইম ইনভেস্টিগেশন	১৫
১.৯ ডিজিটাল এভিডেন্স কী?	১৬
১.১০ ডিজিটাল আলামত কত প্রকার হতে পারে?	১৬
১.১১ ডিজিটাল সাক্ষ্য বলতে আমরা কী বুঝি?	১৬
১.১২ ডিজিটাল এভিডেন্স কেন সংগ্রহ করা প্রয়োজন?	১৬
১.১৩ ডিজিটাল এভিডেন্স হিসেবে আমরা কী পেতে পারি?	১৭
১.১৪ ডিজিটাল ডকুমেন্টের Hash value কীভাবে সংরক্ষণ করব?	১৮
১.১৫ ডিজিটাল ডিভাইস হতে কী কী তথ্য উদঘাটন সম্ভব?	১৮
১.১৬ আলামতের Chain of Custody কী?	১৮
১.১৭ ডিজিটাল সাক্ষ্যের স্পর্শকাতরতা	১৯
১.১৮ ডিজিটাল ডিভাইস সংক্রান্ত বিশেষজ্ঞ মতামত কেন প্রয়োজন?	১৯
১.১৯ ডিজিটাল এভিডেন্স সংগ্রহ করার সময় কোন কাজটি করা যাবে না?	১৯
১.২০ ডিজিটাল এভিডেন্স কোন কোন অবস্থায় পাওয়া যেতে পারে?	১৯
<b>অধ্যায়-২: কম্পিউটার ফরেনসিক তদন্ত প্রক্রিয়া</b>	<b>২০</b>
২.১ ফরেনসিক প্রস্তুতি পরিকল্পনা	২০
২.২ ডিজিটাল ফরেনসিক তদন্ত প্রক্রিয়া	২০
২.২.১ প্রাক তদন্ত পর্যায়	২১
২.২.২ তদন্ত পর্যায়	২২
২.২.৩ তদন্ত পরবর্তী পর্যায়	২২
২.৩ ডিজিটাল প্রমাণ সংগ্রহের জন্য প্রয়োজনীয় সরঞ্জাম	২৩
২.৪ কম্পিউটার আলামত জব্দ পরবর্তী কার্যক্রম	২৪
২.৫ আলামত পরিবহন ও সংরক্ষণ	২৫
২.৬ মালখানায় কম্পিউটার/আলামত যথাযথভাবে হেফাজতকরণ	২৫
২.৭ আলামত জব্দ করার ক্ষেত্রে করণীয়	২৫

২.৮ ইন্টারনেটের মাধ্যমে অপরাধ সংঘটনের প্রক্রিয়া	২৫
২.৯ কম্পিউটার যন্ত্রাংশ জব্দ করার ক্ষেত্রে করণীয়	২৬
২.১০ ইন্টারনেট ক্রাইম অনুসন্ধান আইএসপি-এর ভূমিকা	২৬
<b>অধ্যায়- ৩: হার্ডডিস্ক এবং ফাইল সিস্টেম বোঝা</b>	<b>২৭</b>
৩.১ Disk Drive কী?	২৭
৩.২ Hard Disk Drive (HDD)	২৮
৩.৩ Solid State Drive (SSD)	২৮
৩.৪ HDD-এর প্রধান উপাদান	২৯
৩.৫ Booting Process কী?	৩১
৩.৬ ফাইল সিস্টেম (File Systems)	৩২
৩.৭ রেইড স্টোরেজ সিস্টেম	৩৪
<b>অধ্যায়- ৪: অ্যান্টি ফরেনসিক টেকনিক</b>	<b>৩৫</b>
৪.১ Anti-Forensics কী?	৩৫
৪.২ Anti-Forensics-এর উদ্দেশ্য	৩৫
৪.৩ অ্যান্টি ফরেনসিক কৌশল	৩৬
<b>অধ্যায়- ৫: উইভোজ ফরেনসিক</b>	<b>৪৩</b>
৫.১ Order of volatility	৪৩
৫.২ ডেটা একুইজিশনের সর্বোত্তম অনুশীলন	৪৪
৫.৩ Live/ Volatile Data Acquisition	৪৫
৫.৪ উইভোজ মেমোরি ক্যাপচার করা	৫৭
৫.৫ উইভোজ মেমোরি অ্যানালাইসিস করা	৫৯
৫.৬ Static/ Non-Volatile Data Acquisition	৬০
৫.৭ Non-Volatile Data অ্যানালাইসিস করা	৬৮
৫.৮ উইভোজ রেজিস্ট্রি অ্যানালাইসিস	৭২
৫.৯ ইভেন্ট লগ অ্যানালাইসিস	৭৭
৫.১০ মেটাডেটা ইনভেস্টিগেশন	৭৯
৫.১১ উইভোজ ফাইল অ্যানালাইসিস	৮০
৫.১২ ক্যাশ, কুকি, এবং হিস্টোরি অ্যানালাইসিস	৮০
<b>অধ্যায়- ৬: লিনাক্স ফরেনসিক</b>	<b>৮৪</b>
৬.১ লিনাক্স ফরেনসিক	৮৪
৬.২ Volatile ডেটা সংগ্রহ	৮৫
৬.৩ Non-Volatile ডেটা সংগ্রহ	৮৬
৬.৪ লিনাক্স লগ লোকেশন	৮৭

<b>অধ্যায়- ৭: ডেটা রিকভারি</b>	<b>৮৮</b>
৭.১ ডেটা রিকভারি উইথ iCare Data Recovery	৮৮
৭.২ ডেটা রিকভারি উইথ EaseUS Data Recovery Wizard	৯৩
৭.৩ ডেটা রিকভারি বিভিন্ন টুলস	৯৬
<b>অধ্যায়- ৮: মোবাইল ও সিমকার্ড ফরেনসিক</b>	<b>৯৭</b>
৮.১ সেলুলার নেটওয়ার্ক কী?	৯৭
৮.২ Subscriber Identity Module (SIM) কী?	৯৮
৮.৩ সিম গঠন এবং ফাইল সিস্টেম	৯৮
৮.৪ সিম কার্ড সংবেদনশীল তথ্য	৯৯
৮.৫ মোবাইল ডিভাইসে কী কী থাকে?	১০০
৮.৬ মোবাইল ডিভাইস ফরেনসিক প্রসেস	১০০
৮.৭ সিডিআর (CDR) কী?	১০১
৮.৮ আইপিডিআর (IPDR) কী?	১০২
৮.৯ মোবাইলের IMEI জানার উপায়	১০৩
৮.১০ IMEI দিয়ে ডিভাইসের তথ্য খুঁজে বের করা	১০৩
৮.১১ ফোন লকিং সিস্টেম	১০৪
৮.১২ মোবাইল ফরেনসিক টুলস	১০৪
৮.১৩ মোবাইল ডিভাইস হারালে বা চুরি হলে করণীয়	১০৫
৮.১৪ IPTSP নাম্বার অ্যানালাইসিস	১০৬
<b>অধ্যায়- ৯: সোশ্যাল মিডিয়া ফরেনসিক</b>	<b>১০৭</b>
৯.১ ফেসবুক (Facebook)	১০৭
৯.২ টুইটার (Twitter)	১০৮
৯.৩ ইন্সটাগ্রাম (Instagram)	১০৯
৯.৪ ইউটিউব (Youtube)	১১০
৯.৫ টিকটক (tiktok)	১১০
৯.৬ অনলাইন নিউজ পোর্টাল	১১১
<b>অধ্যায়- ১০: ই-মেইল ফরেনসিক</b>	<b>১১২</b>
১০.১ ই-মেইল ফরেনসিক কী?	১১২
১০.২ ই-মেইল-সম্পর্কিত অপরাধ	১১২
১০.৩ ই-মেইল অপরাধ তদন্ত প্রক্রিয়া	১১৩
১০. ৪ ই-মেইল হেডার কনটেন্ট	১১৩
১০.৫ Gmail হেডার অ্যানালাইসিস	১১৪
১০.৬ Yahoo হেডার অ্যানালাইসিস	১১৬
১০. ৭ Microsoft Outlook হেডার অ্যানালাইসিস	১১৭
১০.৮ Webmail হেডার অ্যানালাইসিস	১১৮
১০.৯ রিকভারি ডিলেটেড ই-মেইল	১১৯
১০.১০ ই-মেইল অ্যাড্রেস সার্চ	১২০
১০.১১ ই-মেইল অ্যাড্রেস আপস হয়েছে কি না?	১২১

<b>অধ্যায়- ১১: ডার্ক ওয়েব ফরেনসিক</b>	<b>১২২</b>
১১.১ ডার্ক ওয়েব কী?	১২২
১১.২ TOR কী?	১২২
১১.৩ TOR নেটওয়ার্ক কী?	১২২
১১.৪ TOR ব্রাউজার কী?	১২৩
১১.৫ ডার্ক ওয়েব ফরেনসিক	১২৩
<b>অধ্যায়- ১২: ম্যালওয়্যার ফরেনসিক</b>	<b>১২৯</b>
১২.১ ম্যালওয়্যার ফরেনসিক পদ্ধতি	১২৯
১২.২ স্ট্যাটিক ম্যালওয়্যার ফরেনসিক	১৩০
১২.৩ অনলাইন ম্যালওয়্যার ফরেনসিক	১৩৩
১২.৪ ডাইনামিক ম্যালওয়্যার ফরেনসিক	১৩৫
১২.৫ র্যানসমওয়্যার ফরেনসিক	১৩৭
<b>অধ্যায়- ১৩: ওয়েব অ্যান্ড ডেটাবেস ফরেনসিক</b>	<b>১৩৯</b>
১৩.১ ডোমেইন ইনভেস্টিগেশন	১৩৯
১৩.১ DNS ইনভেস্টিগেশন	১৪০
১৩.৩ IP ইনভেস্টিগেশন	১৪১
১৩.৪ ওয়েবসাইট অনুসন্ধান	১৪২
১৩.৫ ওয়েবসাইট ক্লোন করা	১৪২
১৩.৬ ওয়েবসাইট লগ ইনভেস্টিগেশন	১৪৩
১৩.৭ ডেটাবেস ইনভেস্টিগেশন	১৪৩
১৩.৮ ইমেইজ ইনভেস্টিগেশন	১৪৫
<b>অধ্যায়- ১৪: নেটওয়ার্ক ফরেনসিক</b>	<b>১৪৬</b>
১৪.১ নেটওয়ার্ক ফরেনসিক	১৪৬
১৪.২ ইউএসবি ফরেনসিক	১৫০
১৪.৩ ওয়াইফাই ফরেনসিক	১৫২
<b>অধ্যায়- ১৫: ফরেনসিক টুলস অ্যান্ড OS ডিস্ট্রিবিউশন</b>	<b>১৫৩</b>
১৫.১ Tsurugi Linux	১৫৩
১৫.২ Santaku OS	১৫৪
১৫.৩ Caine OS	১৫৫
১৫.৪ DEFT Linux	১৫৬
১৫.৫ Kali linux	১৫৭
১৫.৬ OS Forensic	১৫৮
<b>অধ্যায়- ১৬: তথ্য ও যোগাযোগপ্রযুক্তি অপরাধসংশ্লিষ্ট আইন</b>	<b>১৫৯</b>
রেফারেন্স	১৫৯
Decodes Lab Limited	১৬০

# অধ্যায়- ১

## ডিজিটাল ফরেনসিক

### ১.১ ডিজিটাল বলতে আমরা কী বুঝি?

ডিজিটাল বলতে আমরা বুঝি ধারাবাহিক কতগুলো বাইনারি সংখ্যার মাধ্যমে কোনো তথ্য কম্পিউটারের মাধ্যমে উপস্থাপন করা।

### ১.২ ফরেনসিক কী?

ফরেনসিক বলতে আমরা যা বুঝি তা হলো, অপরাধ বা দুর্ঘটনাস্থল থেকে নানারকম আলামত, সূত্র বা ক্লু সংগ্রহ করা। এক কথায় ফরেনসিককে ময়নাতদন্ত বলা হয়ে থাকে। বিভিন্ন তথ্য উদ্ঘাটনের জন্য ময়নাতদন্ত করা হয়ে থাকে। ফরেনসিক সায়েন্স দুই প্রকার।

- ▶ মেডিকেল ফরেনসিক।
- ▶ ডিজিটাল ফরেনসিক।

### ১.৩ ডিজিটাল ফরেনসিক কী?

কম্পিউটার বা স্মার্ট ডিজিটাল কোনো ডিভাইস ব্যবহার করে কোনো অপরাধ সংঘটিত হলে স্মার্ট ডিভাইস বা কম্পিউটার ফরেনসিক করা হয়। কোনো ঘটনার শুরু থেকে থেকে শেষ পর্যন্ত যা করেছে তা ভিক্টিম/আসামির কম্পিউটার-স্মার্ট ফোন ব্যবহার করে সব তথ্য রিকভারি করে এমনকি ডিলেট করা অডিও, ভিডিও, কল লিস্ট, ই-মেইল ইউজার নেম পাসওয়ার্ড ইত্যাদিও রিকভার করা যায়।

### ১.৪ কম্পিউটার ফরেনসিক কী?

কম্পিউটার ফরেনসিক, ডিজিটাল ফরেনসিকের একটি শাখা। কম্পিউটারভিত্তিক যদি কোনো অপরাধ সংঘটিত হয় সেই অপরাধ সম্পর্কিত তথ্য ও মতামত চিহ্নিতকরণ, সংরক্ষণ, পুনরুদ্ধার, বিশ্লেষণ ও উপস্থাপনের লক্ষ্যে সেই কম্পিউটারের ফরেনসিক পরীক্ষা করা।

## ১.৫ সাইবার ক্রাইম কী?

সাইবার ক্রাইম কথাটা ইন্টারনেট, কম্পিউটার এবং কম্পিউটার নেটওয়ার্কের সঙ্গে সম্পর্কিত, ইন্টারনেট ব্যবহার করে যেসব অপরাধ সংঘটিত হয় তাই সাইবার ক্রাইম বা সাইবার অপরাধ নামে পরিচিত। সাইবার ক্রাইমের ক্ষেত্রে ডিজিটাল ডিভাইস হলো অপরাধ সংঘটনের মাধ্যম অথবা অপরাধ সংঘটনের টার্গেট।

## ১.৬ সাইবার ক্রাইমের উপাদান

একটি ডিজিটাল অপরাধ প্রমাণ করার জন্য, একজন তদন্তকারী হিসেবে আপনার নিম্নলিখিত উপাদানগুলো বের করতে হবে। সমস্ত উপাদান একে অপরের সঙ্গে কমবেশি সম্পর্কযুক্ত হবে।

### ELEMENTS OF A CRIME



ছবি: সাইবার ক্রাইম সংযুক্ত উপাদান।



## ১.৭ সাইবার ক্রাইমের উদাহরণ

বর্তমানে সাইবার ক্রাইম বেড়ে চলছে, সাইবার ক্রাইমের বিভিন্ন ধরন আছে। এর মধ্যে বেশ কিছু নিচে তুলে ধরা হল।

- ▶ গুপ্তচরবৃত্তি
- ▶ ডেটা ম্যানুপুলেশন
- ▶ তথ্য চুরি
- ▶ ফিশিং, স্পুফিং
- ▶ জালিয়াতি
- ▶ ম্যালওয়্যার অ্যাটাক
- ▶ তথ্য গোপন করা
- ▶ অনলাইন চাঁদাবাজি
- ▶ ইন্টারনেট স্ক্যাম
- ▶ ওয়েব সার্ভার অ্যাটাক
- ▶ ওয়েব অ্যাপ্লিকেশন অ্যাটাক
- ▶ নেটওয়ার্কভিত্তিক অ্যাটাক
- ▶ ই-মেইলভিত্তিক থ্রেট ইত্যাদি।

## ১.৮ সাইবার ক্রাইম ইনভেস্টিগেশন

সাইবার ক্রাইম অভ্যন্তরীণ অ্যাটাক ও বাহ্যিক অ্যাটাক যেকোনো একটা মাধ্যমে ঘটতে পারে।

- ▶ **সিভিল ইনভেস্টিগেশন:** civil বা দেওয়ানি মামলাগুলো চুক্তি এবং মামলা লঙ্ঘনের জন্য হয়, যেখানে দোষীকে ফলাফলের জন্য সাধারণত বাদীকে আর্থিক ক্ষতির সম্মুখীন হতে হয়।
- ▶ **ক্রিমিনাল ইনভেস্টিগেশন:** Criminal বা ফৌজদারি মামলাগুলো সাধারণত আইন প্রয়োগকারী সংস্থাগুলোর দ্বারা আইনের সন্দেহভাজন লঙ্ঘনের প্রতিক্রিয়া হিসাবে গণ্য হয়, যেখানে দোষী ফলাফলের জন্য আর্থিক ক্ষতি বা কারাদণ্ড বা উভয়ই হতে পারে।
- ▶ **এডমিনিস্ট্রেটিভ ইনভেস্টিগেশন:** Administrative বা প্রশাসনিক তদন্তে সাধারণত একটি এজেন্সি বা সরকার জড়িত থাকে যা তার নিজস্ব ব্যবস্থাপনা এবং কার্যকারিতার রেফারেন্সে তথ্য শনাক্ত করতে অনুসন্ধান চালায়।

## ১.৯ ডিজিটাল এভিডেন্স কী?

ডিজিটাল এভিডেন্স বলতে আমরা ঐসব বস্তু বা ডিভাইসকে বোঝাই যারা ইলেকট্রনিক্যালি তথ্য সংরক্ষণ করতে পারে। ডিজিটালি তথ্য সঞ্চয় করে এমন যে কোনো বস্তুকে ডিজিটাল এভিডেন্স হিসেবে সংজ্ঞায়িত করা যেতে পারে।

## ১.১০ ডিজিটাল আলামত কত প্রকার হতে পারে?

ডিজিটাল আলামত দুই প্রকার,

### ▶ পরিবর্তনশীল ডেটা- Volatile Data

পরিবর্তনশীল ডেটা ডিভাইস বন্ধ করার সঙ্গে সঙ্গে মুছে যায়।

যেমন, RAM, Command History, Open Files, System Time etc.

### ▶ অপরিবর্তনশীল ডেটা- Non Volatile Data

অপরিবর্তনশীল ডেটা ডিভাইস বন্ধ করলেও থেকে যায়।

যেমন, Hard Disk, Event Logs, Pendrive etc.

## ১.১১ ডিজিটাল সাক্ষ্য বলতে আমরা কী বুঝি?



অপরাধ বা ঘটনার সঙ্গে যেসব ডিজিটাল ডিভাইস বা মিডিয়াম জড়িত কিংবা ঘটনা সংঘটনের উপাদান হিসেবে যেসব ডিজিটাল বস্তু ব্যবহৃত হয়ে থাকে, তাদের আমরা ডিজিটাল সাক্ষ্য বলতে পারি।




## ১.১২ ডিজিটাল এভিডেন্স কেন সংগ্রহ করা প্রয়োজন?

▶ মামলা বা অভিযোগ তদন্তের প্রয়োজনে।

▶ বিচারকালে ঘটনা প্রমাণের জন্য সাক্ষ্য হিসেবে।

## ১.১৩ ডিজিটাল এভিডেন্স হিসেবে আমরা কী পেতে পারি?

<p>Hard Disk (Internal &amp; External)</p> 	<p>Floppy Disks,</p> 
<p>CDs/DVDs</p> 	<p>Pen Drives (Dongles)</p> 
<p>Mobile Phones</p> 	<p>Cameras</p> 
<p>MP3 Players</p> 	<p>Networks Devices</p>  <p>Types of Network Devices</p>

<p>SD/ Micro SD Memory Card</p> 	<p>Laptop or Computer</p> 
<p>SIM Card etc.</p> 	

### ১.১৪ ডিজিটাল ডকুমেন্টের Hash value কীভাবে সংরক্ষণ করব?

ডিজিটাল ডকুমেন্টের হ্যাস নম্বর বের করার জন্য বাজারে বিনামূল্যের অর্থাৎ free software সহ (যেমন- Hashcalc) সফটওয়্যার পাওয়া যায়। সেই টুলস পিসিতে ইন্সটল করে সেখানে সেই ডিজিটাল ডকুমেন্ট বা ফাইলটি দেখিয়ে দেওয়া এবং ক্যালকুলেট অপশনে ক্লিক করলে আপনি md5 ও sha-এর হ্যাস নম্বর পাবেন, তা জন্ম তালিকায় উল্লেখ করতে হবে।

### ১.১৫ ডিজিটাল ডিভাইস হতে কী কী তথ্য উদঘাটন সম্ভব?

কোনো ঘটনা বা মামলায় ডিজিটাল ডিভাইস জন্ম করা হলে জন্মকৃত ডিভাইসে ধারণকৃত কিন্তু পরবর্তী সময়ে মুছে ফেলা স্থিরছবি/অডিও/ভিডিওসহ অন্যান্য গুরুত্বপূর্ণ তথ্য-উপাত্ত উদঘাটন করা সম্ভব যা সর্বোপরি কোনো মামলার প্রকৃত রহস্য উদঘাটন এবং প্রকৃত অপরাধীদের শনাক্ত করতে সহায়তা প্রদান করে। সন্দিহান ব্যক্তি কম্পিউটারের তথ্য মুছে ফেললেও অধিকাংশ সময় তা হার্ডডিস্কে থেকে যায়। অনেক ক্ষেত্রে হার্ডডিস্কে পাওয়া তথ্য দিয়ে আসামির বিরুদ্ধে অপরাধ প্রমাণ করা সম্ভব হয়। আসামি একাধিকবার কোনো ফাইল মুছে থাকলেও বিভিন্ন সফটওয়্যার ব্যবহার করে হার্ডডিস্ক থেকে তা উদ্ধার করা সম্ভব হয়। তথ্য উদঘাটনের পরবর্তী কাজ হচ্ছে জন্মকৃত আলামত বা কম্পিউটারসমূহের যথাযথভাবে সংরক্ষণ করা, যাতে সময়মতো তা আদালতে উপস্থাপন করা যায়।

### ১.১৬ আলামতের Chain of Custody কী?

একটি ডিজিটাল আলামত জন্ম করা হতে আদালতের জিম্মায় অর্থাৎ মালখানায় জমা দেওয়া পর্যন্ত কার কাছ থেকে কার কাছ হস্তান্তরিত হয়েছে তার লিখিত বিবরণকে chain of custody বলা হয়ে থাকে।

## ১.১৭ ডিজিটাল সাক্ষ্যের স্পর্শকাতরতা:

ডিজিটাল সাক্ষ্য অত্যন্ত স্পর্শকাতর সূতরাং সাবধানতার সঙ্গে এটি সংগ্রহ ও সংরক্ষণ করতে হবে। অপরাধী ইন্টারনেট বা ডিজিটাল ক্রাইম করার সময় কিছু ডিজিটাল সাক্ষ্য বা আলামত পেছনে ফেলে রেখে যায়, যার কিছু অংশ কম্পিউটারের হার্ডডিস্কে এবং কখনো কখনো সিডি বা পেনড্রাইভে সংরক্ষিত থেকে যায়। ডিজিটাল সাক্ষ্য সংগ্রহের সময় খুব সাবধানতা অবলম্বন করতে হয়, কেননা তা খুব সহজেই নষ্ট হয়ে যায় বা হারিয়ে যেতে পারে।

## ১.১৮ ডিজিটাল ডিভাইস-সংক্রান্তে বিশেষজ্ঞ মতামত কেন প্রয়োজন?

ডিজিটাল ডিভাইসে সংরক্ষিত তথ্য সুপ্ত প্রকৃতির। কেননা, অপরাধ সংঘটনের পর আসামি সাক্ষ্য-প্রমাণ নষ্ট করার জন্য তার ব্যবহৃত ডিজিটাল ডিভাইস হতে তথ্য মুছে ফেলতে পারে অথবা অন্য কোনোভাবে লুকিয়ে রাখতে পারে। কাজেই কোনো মামলায় জন্মকৃত ডিজিটাল ডিভাইসে সংরক্ষিত তথ্যের সঙ্গে আসামির সম্পৃক্ততা নির্ণয়ে বিশেষজ্ঞ মতামত সহায়ক ভূমিকা রাখতে পারে।

## ১.১৯ ডিজিটাল এভিডেন্স সংগ্রহ করার সময় কোন কাজটি করা যাবে না?

- ▶ তারিখ ও সময় পরিবর্তন করা যাবে না।
- ▶ ফাইল ফোল্ডার পরিবর্তন করা যাবে না।
- ▶ ডিস্ক বা ফাইল ওভাররাইট করা যাবে না।

## ১.২০ ডিজিটাল এভিডেন্স কোন কোন অবস্থায় পাওয়া যেতে পারে?

- ▶ বন্ধ বা খোলা অবস্থায়।
- ▶ পাসওয়ার্ড দেওয়া বা পাসওয়ার্ড ছাড়া অবস্থায়।
- ▶ ইন্টারনেটের সঙ্গে যুক্ত বা বিযুক্ত অবস্থায়।