15 –ാം കേരള നിയമസഭ

9 –ാം സമ്മേളനം

നക്ഷത്രചിഹ്നമിട്ട ചോദ്യം നം. 172 **13-09-2023 - ൽ മറുപടിയ്ക്ക്**

സൈബർ കുറ്റകൃത്യങ്ങളും ഫോറൻസിക് ലാബുകളുടെ സേവനവും

ചോദ്യം		ഉത്തരം	
ശ്രീ കടകംപള്ളി സുരേന്ദ്രൻ, ശ്രീ. കെ.പി.കുഞ്ഞമ്മദ് കുട്ടി മാസ്റ്റർ, ശ്രീ. കെ. എം. സച്ചിൻദേവ്, ശ്രീമതി യു പ്രതിഭ		**ശ്രീ. പിണറായി വിജയൻ (മുഖ്യമന്ത്രി)**	
(എ)	സൈബർ കുറ്റകൃത്യങ്ങളിലെ ഇരകളുടെ പരാതികൾക്ക് പരിഹാരം കണ്ടെത്തുന്നതിനും സൈബർ തട്ടിപ്പുകാരെ കണ്ടെത്തുന്നതിനും ഡാറ്റ വീണ്ടെടുക്കുന്നതിനും ശാസ്ത്രീയമായ തെളിവുകൾ ശേഖരിച്ച് പ്രോസിക്യൂഷന് മുന്നിൽ സമർപ്പിച്ച് നീതി ഉറപ്പാക്കുന്നതിനും സർക്കാർ ഫോറൻസിക് ലാബുകൾ വഹിക്കുന്ന പങ്ക് വിലയിരുത്തിയിട്ടുണ്ടോ; എങ്കിൽ വിശദമാക്കുമോ;	(എ)	ഉണ്ട്. സംസ്ഥാനത്ത് സൈബർ കുറ്റകൃത്യങ്ങൾ ഉൾപ്പെടെ ഗുരുതരമായ കുറ്റകൃത്യങ്ങളിൽ ഏർപ്പെടുന്ന കുറ്റവാളികൾക്ക് ഉചിതശിക്ഷ ലഭിക്കുംവിധം മികച്ച Justice Delivery System ഉറപ്പാക്കുന്നതിനുള്ള നടപടികളാണ് സർക്കാർ സ്വീകരിച്ചുവരുന്നത്. കേസന്വേഷണം മികവുറ്റതാക്കുന്നതിനാവശ്യമായ ശാസ്ത്രീയ തെളിവുകൾ പ്രധാനമായും ലഭ്യമാക്കുന്നത് സംസ്ഥാനത്തെ ഫോറൻസിക് സയൻസ് ലബോറട്ടറികളാണ്. ഇത്തരം കുറ്റകൃത്യങ്ങളിൽ ഉൾപ്പെട്ടിട്ടുള്ള വസ്തുക്കളുടെ പരിശോധനയ്ക്ക് ഉതകുന്ന നൂതന സാങ്കേതിക വിദ്യയിലധിഷ്ഠിതമായ സംവിധാനങ്ങൾ സംസ്ഥാനത്തെ എല്ലാ സൈബർ ഡിവിഷനുകളിലും സജ്ജമാക്കിയിട്ടുണ്ട്. ഇതിലേക്കായി നടപ്പു സാമ്പത്തിക വർഷം സർക്കാർ 80 ലക്ഷം രൂപ അനുവദിച്ചിട്ടുണ്ട്. സൈബർ കുറ്റകൃത്യങ്ങളും അതിക്രമങ്ങളും തടയുന്നതിനായി രൂപീകരിച്ചിട്ടുള്ള കേരള സൈബർ ക്രൈം കോ-ഓർഡിനേഷൻ സെന്റർ (K4C), ഇന്ത്യൻ സൈബർ ക്രൈം കോ-ഓർഡിനേഷൻ സെന്റർ (I4C)-മായി സഹകരിച്ചാണ് പ്രവർത്തിക്കുന്നത്. സാമ്പത്തിക തട്ടിപ്പുകളുമായി ബന്ധപ്പെട്ട് ദ്രുതഗതിയിലുള്ള നടപടികൾ സ്വീകരിക്കുന്നതിനായി രാജ്യത്തെ വിവിധ ഏജൻസികളുടെ സംയോജിത പ്ലാറ്റ്ഫോമായ നാഷണൽ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ് പോർട്ടലിന്റെ സേവനവും ഉപയോഗപ്പെടുത്തിവരുന്നു. പ്രസ്തുത പോർട്ടൽ മുഖേനയും 1930 എന്ന നമ്പരിലേക്ക് ഫോൺ മുഖാന്തിരവും	

			പൊതുജനങ്ങൾക്ക് പരാതികൾ അറിയിക്കാവുന്നതാണ്. **<u>സൈബർ ഓപ്പറേഷൻ വിഭാഗം</u>** സൈബർ കുറ്റകൃത്യങ്ങൾ തടയുന്നതിന് ആവശ്യമായ സാങ്കേതിക നിർദ്ദേശങ്ങൾക്കും പ്രവർത്തനങ്ങളുടെ കേന്ദ്ര-സംസ്ഥാന ഏകോപനത്തിനുമായി സൈബർ ഓപ്പറേഷൻ വിഭാഗം രൂപീകരിച്ച് ഐ.ജി (സൈബർ ഓപ്പറേഷൻസ്) SP ICT ആന്റ് സൈബർ ഓപ്പറേഷൻസ് എന്നീ തസ്തികകൾ സൃഷ്ടിച്ച് ചുമതല നൽകിയിട്ടുണ്ട്. സൈബർ മേഖലയിലുള്ള ചലനങ്ങൾ നിരീക്ഷിക്കുന്നതിനും ആവശ്യമായ നയരൂപീകരണത്തിനുമായി ടെക്നിക്കൽ ഇന്റലിജൻസ് വിഭാഗത്തിൽ പുതിയതായി ഒരു എസ്.പിയെ കൂടി ചുമതലപ്പെടുത്തിയിട്ടുണ്ട്. **<u>സൈബർ ഡോം</u>** സൈബർ മേഖലയിൽ സ്വകാര്യ പങ്കാളിത്തത്തോടെ ഗവേഷണം നടത്തുന്നതിനും സൈബർ കുറ്റകൃത്യങ്ങളുമായി ബന്ധപ്പെട്ട വെല്ലുവിളികൾ നേരിടുന്നതിനും സമയബന്ധിതമായി പരിഹാരം കാണുന്നതിനും തിരുവനന്തപുരം, കൊച്ചി, കോഴിക്കോട് എന്നിവിടങ്ങൾ കേന്ദ്രീകരിച്ച് സൈബർ ഡോമുകളും സ്ഥാപിച്ചിട്ടുണ്ട്. സൈബർ ഇടങ്ങൾ ഉപയോഗപ്പെടുത്തിയുള്ള സാമ്പത്തിക തട്ടിപ്പുകൾ, മയക്കുമരുന്ന്, ആയുധ വ്യാപാരം, ലൈംഗിക വ്യാപാരം, ഡാറ്റാ മോഷണം, ഹാക്കിംഗ് ടൂളുകൾ എന്നിവയുൾപ്പെടെ നിയമവിരുദ്ധമായ ക്രയവിക്രയങ്ങൾ നടത്തുന്ന കുറ്റകൃത്യങ്ങൾ സൈബർ ഡോം വികസിപ്പിച്ച Grapnel സോഫ്റ്റ് വെയർ ഉപയോഗിച്ച് കണ്ടെത്തുവാൻ സാധിക്കുന്നുണ്ട്. സൈബർ കുറ്റകൃത്യങ്ങളുമായി ബന്ധപ്പെട്ട് കഴിഞ്ഞ മൂന്ന് വർഷത്തിനിടയിൽ 2978 കേസുകളിൽ ഫോറൻസിക് പരിശോധന പൂർത്തിയാക്കി റിപ്പോർട്ട് സമർപ്പിച്ചിട്ടുണ്ട്. സംസ്ഥാന ഫോറൻസിക് സയൻസ് ലാബ് നൽകിയ ഇത്തരം തെളിവുകളുടെ പ്രാധാന്യം ആറ്റിങ്ങൽ ഇരട്ടക്കൊലപാതക കേസിലെ വിധിന്യായത്തിലടക്കം ബഹു. കോടതിയുടെ പ്രത്യേക പരാമർശത്തിന് വിധേയമായിട്ടുണ്ട്.
(ബി)	സർക്കാർ ഫോറൻസിക് ലാബുകളിൽ വേണ്ടത്ര സൗകര്യമില്ലാത്തതും സ്വകാര്യ ഫോറൻസിക്	(ബി)	സംസ്ഥാനത്തെ സർക്കാർ ഫോറൻസിക് ലാബുകൾ IT ആക്ട് സെക്ഷൻ 79 A പ്രകാരം Examiner of Electronic Evidence (EEE)

	ലാബുകൾ വിരളമാണെന്നതും ശ്രദ്ധയിൽപ്പെട്ടിട്ടുണ്ടോ; വ്യക്തമാക്കാമോ;		അംഗീകാരമുള്ളവയാണ്. സംസ്ഥാനത്തെ എല്ലാ ഫോറൻസിക് ലാബുകളിലും മികച്ച പരിശീലനം ലഭിച്ച ഉദ്യോഗസ്ഥരാണ് പരിശോധന നടത്തിവരുന്നത്. ഇവിടെ അന്തർദേശീയ നിലവാരത്തിലുള്ള ആധുനിക സാങ്കേതിക വിദ്യയിലധിഷ്ഠിതമായ മികച്ച പരിശോധനാ ഉപകരണങ്ങൾ സർക്കാർ ലഭ്യമാക്കിയിട്ടുണ്ട്. വിവിധ പദ്ധതികളിൽ ഉൾപ്പെടുത്തി ഫോറൻസിക് സയൻസ് ലബോറട്ടറിക്ക് ലഭ്യമാക്കിയ ഉപകരണങ്ങളുടെ പട്ടിക അനുബന്ധമായി ചേർത്തിട്ടുണ്ട്. കേസന്വേഷണത്തിലെ ശാസ്ത്രീയമായ തെളിവുകളുടെ പ്രാധാന്യം കണക്കിലെടുത്ത് സംസ്ഥാനത്തെ എല്ലാ ജില്ലകളിലും സയൻസ് ലാബുകൾ ആരംഭിക്കുവാൻ സർക്കാർ നയപരമായ തീരുമാനമെടുക്കുകയുണ്ടായി. അതിന്റെ ഭാഗമായി സംസ്ഥാനത്തെ 13 ജില്ലകളിൽ ജില്ലാ ഫോറൻസിക് ലാബുകളുടെ പ്രവർത്തനം ആരംഭിച്ചിട്ടുണ്ട്. വയനാട് ജില്ലയിൽ ഫോറൻസിക് ലബോറട്ടറി ആരംഭിക്കുന്നതിനുള്ള നടപടികൾ സ്വീകരിച്ചിട്ടുണ്ട്. ഇപ്രകാരം എല്ലാ ജില്ലകളിലും ഫോറൻസിക് ലാബ് സ്ഥാപിക്കുന്ന രാജ്യത്തെ ആദ്യത്തെ സംസ്ഥാനമാണ് കേരളം. നിലവിൽ സംസ്ഥാന ഫോറൻസിക് സയൻസ് ലബോറട്ടറി, കണ്ണൂർ, കൊച്ചി, തൃശ്ശൂർ ജില്ലകളിൽ സ്ഥിതിചെയ്യുന്ന റീജിയണൽ ഫോറൻസിക് സയൻസ് ലബോറട്ടറി എന്നിവിടങ്ങളിൽ സൈബർ ഫോറൻസിക് പരിശോധനാ സൗകര്യം ലഭ്യമാക്കിയിട്ടുണ്ട്. അതോടൊപ്പം ഏല്ലാ ജില്ലാ ഫോറൻസിക് സയൻസ് ലാബുകളിലും മൊബൈൽ ഫോൺ പരിശോധനാ സൗകര്യവും ലഭ്യമാക്കിയിട്ടുണ്ട്.
(സി)	ഫോറൻസിക് സയൻസ് ലാബുകളുടെ സേവനം എല്ലാവരിലും എത്തിക്കുന്നതിനും ലാബുകളുടെ എണ്ണം വർദ്ധിപ്പിക്കുന്നതിനും നടപടികൾ സ്വീകരിക്കുമോ?	(സി)	സംസ്ഥാനത്തെ സർക്കാർ ഫോറൻസിക് ലാബുകൾ IT ആക്ട് സെക്ഷൻ 79 A പ്രകാരം Examiner of Electronic Evidence (EEE) അംഗീകാരമുള്ളവയാണ്. സംസ്ഥാനത്തെ എല്ലാ ഫോറൻസിക് ലാബുകളിലും മികച്ച പരിശീലനം ലഭിച്ച ഉദ്യോഗസ്ഥരാണ് പരിശോധന നടത്തിവരുന്നത്. ഇവിടെ അന്തർദേശീയ നിലവാരത്തിലുള്ള ആധുനിക സാങ്കേതിക വിദ്യയിലധിഷ്ഠിതമായ മികച്ച പരിശോധനാ ഉപകരണങ്ങൾ സർക്കാർ ലഭ്യമാക്കിയിട്ടുണ്ട്. വിവിധ പദ്ധതികളിൽ ഉൾപ്പെടുത്തി ഫോറൻസിക് സയൻസ് ലബോറട്ടറിക്ക് ലഭ്യമാക്കിയ ഉപകരണങ്ങളുടെ പട്ടിക അനുബന്ധമായി ചേർത്തിട്ടുണ്ട്. കേസന്വേഷണത്തിലെ ശാസ്ത്രീയമായ തെളിവുകളുടെ പ്രാധാന്യം കണക്കിലെടുത്ത് സംസ്ഥാനത്തെ എല്ലാ

			ജില്ലകളിലും സയൻസ് ലാബുകൾ ആരംഭിക്കുവാൻ സർക്കാർ നയപരമായ തീരുമാനമെടുക്കുകയുണ്ടായി. അതിന്റെ ഭാഗമായി സംസ്ഥാനത്തെ 13 ജില്ലകളിൽ ജില്ലാ ഫോറൻസിക് ലാബുകളുടെ പ്രവർത്തനം ആരംഭിച്ചിട്ടുണ്ട്. വയനാട് ജില്ലയിൽ ഫോറൻസിക് ലബോറട്ടറി ആരംഭിക്കുന്നതിനുള്ള നടപടികൾ സ്വീകരിച്ചിട്ടുണ്ട്. ഇപ്രകാരം എല്ലാ ജില്ലകളിലും ഫോറൻസിക് ലാബ് സ്ഥാപിക്കുന്ന രാജ്യത്തെ ആദ്യത്തെ സംസ്ഥാനമാണ് കേരളം. നിലവിൽ സംസ്ഥാന ഫോറൻസിക് സയൻസ് ലബോറട്ടറി, കണ്ണൂർ, കൊച്ചി, തൃശ്ശൂർ ജില്ലകളിൽ സ്ഥിതിചെയ്യുന്ന റീജിയണൽ ഫോറൻസിക് സയൻസ് ലബോറട്ടറി എന്നിവിടങ്ങളിൽ സൈബർ ഫോറൻസിക് പരിശോധനാ സൗകര്യം ലഭ്യമാക്കിയിട്ടുണ്ട്. അതോടൊപ്പം ഏല്ലാ ജില്ലാ ഫോറൻസിക് സയൻസ് ലാബുകളിലും മൊബൈൽ ഫോൺ പരിശോധനാ സൗകര്യവും ലഭ്യമാക്കിയിട്ടുണ്ട്.

സെക്ഷൻ ഓഫീസർ

- FRED-01 (Forensic Recovery of Evidence Device):- The FREDs are very powerful workstations that serve to secure, save and analyse data from hard drives and other media carriers,
- Logicube(Digital Forensic Solutions):- A forensically sound method of evidence capture that does not alter the metadata or other information stored in the captured files and folders.
- UFEDTouch2 (Universal Forensics Extraction Device):- It provides access to data inaccessible by other methods and speeds up overall data analysis process.
- UFED Physical Analyser:- To recover, decrypt, decode, and review digital data and effectively surface actionable intelligence.
- UFED 4 PC:- Device Extraction via USB and RJ 45. SIM Clone and extraction. Extraction via embedded Bluetooth module.
- EnCase-01:- Traditionally used in Forensics to recover evidence from seized Hard drives It allows the investigator to conduct in-depth analysis of user files to collect evidence such as documents, pictures, internet history and Windows Registry information.
- Magnet Axiom Computer:- A complete digital investigation platform that allows examiners to seamlessly acquire and analyze forensic data, as well as share their findings.
- Magnet Axiom Mobile Phone:- Axiom Software allows you to access critical performance information anytime, anywhere; End users can interact with dashboards, spot trends, conduct ad hoc analysis and make timely, informed decisions regardless of location.
- Magnet Forensic IEF(Internet Evidence Finder):- It is a digital forensics solution that can search a hard drive, live RAM captures or files for Internet-related evidence.
- AccessData FTK (Forensic Toolkit):- digital investigations software that includes many features and capabilities such as full-disk forensic images, decrypt files and crack passwords, parse registry files, collect, process and analyze datasets, and advanced volatile memory analysis.
- Cyber check:- Is a web based forensic data recovery and analysis tool to enable Law Enforcement Officers to quickly and efficiently analyse digital evidence files.
- Adroit Photo Forensic:- To authenticating digital images to determine authenticity or it may refer to the capability of digital forensics software to find and identify photos
- Stego Suite:- Hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.
- DVR Examiner:- To ingest multiple hard drives from the same DVR or multiple DVRs from multiple locations in one case file. Easily follow suspects from

camera to camera and location to location. Plus, you can compile and export large amounts of data quickly

- Voom Shadow:- The investigation in real time without prior need to image hard drives and without the need for clumsy virtual viewing software
- Tableau Duplicator-TX1:- A portable alternative to carrying a forensic workstation into the field. It is a network-enabled, fully-forensic imager that offers superior local and network imaging Video.
- Amped Five:- It is designed to answer the need in providing solid, scientific-based forensic image and video enhancement for worldwide legal systems
- UFED Cellebrite Cloud Analyzer:- To extract, preserve and analyze public- and private-domain, social-media data, instant messaging, file storage, web pages and other cloud-based content using a forensically sound process.

- FRED-01 (Forensic Recovery of Evidence Device):- The FREDs are very powerful workstations that serve to secure, save and analyse data from hard drives and other media carriers,
- Logicube(Digital Forensic Solutions):- A forensically sound method of evidence capture that does not alter the metadata or other information stored in the captured files and folders.
- UFEDTouch2 (Universal Forensics Extraction Device):- It provides access to data inaccessible by other methods and speeds up overall data analysis process.
- UFED Physical Analyser:- To recover, decrypt, decode, and review digital data and effectively surface actionable intelligence.
- UFED 4 PC:- Device Extraction via USB and RJ 45. SIM Clone and extraction. Extraction via embedded Bluetooth module.
- EnCase-01:- Traditionally used in Forensics to recover evidence from seized Hard drives It allows the investigator to conduct in-depth analysis of user files to collect evidence such as documents, pictures, internet history and Windows Registry information.
- Magnet Axiom Computer:- A complete digital investigation platform that allows examiners to seamlessly acquire and analyze forensic data, as well as share their findings.
- Magnet Axiom Mobile Phone:- Axiom Software allows you to access critical performance information anytime, anywhere; End users can interact with dashboards, spot trends, conduct ad hoc analysis and make timely, informed decisions regardless of location.
- Magnet Forensic IEF(Internet Evidence Finder):- It is a digital forensics solution that can search a hard drive, live RAM captures or files for Internet-related evidence.
- AccessData FTK (Forensic Toolkit):- digital investigations software that includes many features and capabilities such as full-disk forensic images, decrypt files and crack passwords, parse registry files, collect, process and analyze datasets, and advanced volatile memory analysis.
- Cyber check:- Is a web based forensic data recovery and analysis tool to enable Law Enforcement Officers to quickly and efficiently analyse digital evidence files.
- Adroit Photo Forensic:- To authenticating digital images to determine authenticity or it may refer to the capability of digital forensics software to find and identify photos
- Stego Suite:- Hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.
- DVR Examiner:- To ingest multiple hard drives from the same DVR or multiple DVRs from multiple locations in one case file. Easily follow suspects from

camera to camera and location to location. Plus, you can compile and export large amounts of data quickly

- Voom Shadow:- The investigation in real time without prior need to image hard drives and without the need for clumsy virtual viewing software
- Tableau Duplicator-TX1:- A portable alternative to carrying a forensic workstation into the field. It is a network-enabled, fully-forensic imager that offers superior local and network imaging Video.
- Amped Five:- It is designed to answer the need in providing solid, scientific-based forensic image and video enhancement for worldwide legal systems
- UFED Cellebrite Cloud Analyzer:- To extract, preserve and analyze public- and private-domain, social-media data, instant messaging, file storage, web pages and other cloud-based content using a forensically sound process.