No. D7-49369/2020/PHQ
Police Headquarters, Kerala
Thiruvananthapuram – 695010
Phone: 0471-2721547
Email: phq.pol@kerala.gov.in
Dated: 05/04/2020

Circular No. 13/2020

Sub: **Production of electronic evidence in the Courts - Forensic guidelines for the Police Officers – Reg.**

Ref: (1) PHQ Circular No. 43/2015 dtd 21/11/2015.
(2) PHQ Circular No. 17/2016 dtd 21/09/2016.
(3) PHQ Circular No. 09/2010 dtd 18/02/2010.

All Investigating Officers are hereby advised to keep in mind the following points, as "electronic evidence" can be presented only by strictly following the Section 65B of the Indian Evidence Act,.

1. The Indian Evidence Act is very clear that any electronic document can be produced only under the category of primary evidence except under certain exceptional circumstances mentioned in the Sec. 65B of the Act.

2. Primary (electronic) evidence is often collected or seized by following the Standard Procedure and also by electronically locking the storage devices of the seized device using a standard Hashing software tool by following Sec. 62 and 64 of the Indian Evidence Act.

3. By definition, any original electronic document submitted to the court is primary evidence and is often marked as "Exhibits" by the courts.

4. The laptops, mobile phones, hard disks, pen drives, CDs, DVDs etc (which are not evidence per se but are suspected / claimed to contain electronic documents with evidential value) are also considered as primary evidence but are often marked as "Material Objects". Although no party has right to ask for a "copy" of a thing which is marked as a "Material object", the SC recently allowed the defense to take copy of an electronic file in a electronic device which is marked as "Material Object"

5. Copies of the original electronic documents (for example, a file in a CD) are considered only as secondary evidence and its evidential value can be proved only in accordance with the procedure prescribed under Sec. 65B of the Act. In other words, the procedure prescribed under Sec. 65B is applicable only in the case of electronic records which are produced as secondary (electronic) evidence.

6. The admissibility of a computer output as an electronic evidence depends on its satisfaction of the four conditions u/s. 65B (2) of the Indian Evidence Act and the person who produces the computer output is expected to give a certificate or a statement that the computer output satisfies the four conditions u/s. 65B (2) to the best of his / her knowledge and belief.

7. In order to achieve maximum accuracy, integrity and the reliability, the Sec. 65B (4) of the Indian Evidence Act prescribes that the cyber forensic expert, while submitting a piece of electronic record as evidence, is expected to also give a certificate or a statement which

a) properly identifies the electronic record;

b) generally describes the manner in which these electronic records are produced by the computer or a combination of computers;

c) generally mentions the configuration of all the devices involved in the production of the electronic record by the computer;

d) clearly describes the manner in which these electronic records are extracted by the expert;

e) precisely mentions the configuration of all the devices involved in the process of extraction of the electronic record by the expert;

f) clearly states that *the information contained in the electronic record was derived or was reproduced from the information fed into the computer in the ordinary course of its activities;*

g) properly establishes the degree of accuracy, reliability and the integrity of the evidence produced; and

h) appropriately establishes the qualification and the official position of the expert who carries out the cyber forensic task and who presents the evidence in the court of law.

8. In many cases, practically it is not easy for the Investigating Officer to obtain a certificate with 7(b) and 7(c) above. For example, a certificate is difficult to obtain from an email operator (GMAIL, YAHOO etc.) in case of an email being produced as evidence. This difficulty is because the computer in question may not be physically accessible to the expert. Noticing this inability, the Hon. Supreme court has observed that such a certificate is "not mandatory" in certain special cases (Shafi Mohammad Vs. The State of Himachal Pradesh, SLP (Crl.), No.2302 of

2017). This "not mandatory" clause is to be read only as "certain pieces of information are not mandatory in the certificate" and not as "the certificate itself is not mandatory". For example, the expert is expected to certify that *the information contained in the electronic record was derived or was reproduced from the information fed into the computer in the ordinary course of its activities* and such a certificate is expected to contain 7(a), 7(d), 7(e), 7(f), 7(g) and 7(h) above.

9. A list of such important details to be included in the certificate that is produced by the cyber forensic expert in the court of law is given below.

9.1 Details about the nature of the electronic evidence presented by the forensic expert. These details include

9.1.1 Nature of the original electronic document in which the evidence is submitted: As electronic document / As Paper document / As electronic as well as paper document

9.1.2 File format of the original electronic document (For example, if the electronic evidence presented is a digital image in JPEG format, then enter here "Digital Image in JPEG format")

9.1.3 Other superficial meta-details of the electronic document (as found in the "Properties" icon of the electronic document)

9.1.4 A brief account (preferably with date-stamp and time-stamp) of the content of the document presented and also the medium (for example, CD, DVD) in which the electronic evidence is presented in electronic format, if any.

9.1.5 A statement by the forensic expert who accessed this file for the forensic purpose that the details 9.1.1. to 9.1.4. above are correct to the best of his / her knowledge and belief

9.2 Details of the device (including a mobile phone or a computer or the combination of computers) that preserved and processed the basic data and that produced the basic information that in turn led on to or produced the evidence. These details include

9.2.1 The details of the geographical location of the device and of the organization where the device was found installed

9.2.2 The hardware configuration of the device

9.2.3 The operating system specification of the device

9.2.4 The network configuration, if any, of the device

9.2.5 A brief account of how the basic data was fed into, preserved, and processed and how the evidential information was produced by the device, all of which preferably supported by the IP addresses, date-stamps and time-stamps

9.2.6 A statement by the cyber forensic expert who has accessed the device (and another statement by the person responsible to administer the device) that the details 9.2.1. to 9.2.5. above are correct to the best of his / her knowledge and belief. Details as part of 9.2.1., 9.2.2., 9.2.3., and 9.2.4.are not mandatory if the device is physically inaccessible to the cyber forensic expert and also to the investigation team (See 8 above). In such cases, the cyber forensic expert is expected to mention in the certificate that the device was physically inaccessible to him/her but was accessible online and the details given under 9.2.5. is correct to the best of his / her knowledge and belief.

9.3 Details of the forensic device(s) (for example, a mobile phone or a computer or a combination of computers) used to extract the evidence (from the device mentioned in 9.2 above). These details include

9.3.1 The details of the geographical location and the organization where the device was installed for the purpose of extracting evidence

9.3.2 The hardware configuration of the device

9.3.3 The operating system specification of the device

9.3.4 The network configuration, if any, of the device

9.3.5 A brief note on the Computer Engineering protocols, processes and procedures followed by the expert to set up the device for the purpose of extracting the evidence. Also, a brief note that gives proper reasons for setting up of and using such advice (of that particular configuration) for extracting evidence

9.3.6 A statement by the expert who performed 9.3.1. to 9.3.5., mentioned above, that the details given vide 9.3.1. to 9.3.5. above are correct to the best of his / her knowledge and belief

9.4 Details of the forensic protocols, processes and procedures used to extract the evidence. These details include

9.4.1 A brief account of how the pieces of basic information were extracted for the purpose of collecting the evidence (including the basic forensic steps carried out by the expert using the device mentioned in item 3 above)

9.4.2 The configuration of the forensic hardware tools used in addition to (and may be in combination with) the device mentioned in item 9.3 above

9.4.3 The configuration of each of the software tools used to extract the evidence by using the device mentioned in item 9.3 above and also vide 9.4.2. above

9.4.4 A proof of forensic authenticity of each of the forensic software tool (mentioned in 9.4.3. above) and the hardware tool (mentioned in 9.4.2. above) both of which were used to extract the evidence. [This proof can be in the form of a government order or an article appearing in a world-renowned peer-reviewed journal or any technical document that is convincing to the judiciary. In this regard, the Daubert Conditions which are followed by the US judiciary can be of help.]

9.4.5 A statement by the expert who performed the forensic task that the details given vide 9.4.1. to 9.4.4., mentioned above, are correct to the best of his / her knowledge and belief.

Note: While the steps 9.1 to 9.4, given above, are expected to be followed in order to give a clear picture of the nature of the evidence, its source and also the way in which it was extracted, the following steps (that means, Steps 9.5 to 9.7) are expected to be followed only when the cyber forensic expert needs to additionally prove the originality (or authenticity or accuracy or legitimacy or genuineness) of the electronic record which is submitted as evidence in the court of law. Originality of a submitted electronic record can be generally proved by proving that the record (submitted in the court) is a copy of the originally created file and is not tampered or manipulated or interfered with.

9.5 **Hex-details of the digital products which are produced by the expert in the court as proof of the degree of originality of the evidence.** These digital products include screenshots, images, audio clippings, and video clippings and their hex-details are primarily intended to prove or disprove their originality in the court of law. These details are in addition to the items 9.1 to 9.4 above and should include

9.5.1 The source details, specification and the configuration of the hex-editing software tool used by the expert to extract the hex-details of the digital product

9.5.2 Output (which, in Computer Science, is called a hex-dump) of the hex-editing tool after loading each of such digital products. [Each of these outputs can be produced as a text file in digital form. Such text files can be extremely large. For example, the text file of the hex-dump of a digital image can have 50-55 A4 size pages and that of a 1-minute video clipping can have 70,000 to 80,000 A4 size pages but only 1 or 2 of these pages can be relevant to the court case. See 9.5.3. below.]

9.5.3 Screenshot of the relevant portions of each output (mentioned in 9.5.2. above). [These relevant portions include the portions that mentions the configuration of the device (for example, the camera) used to capture the particular digital product including the date-stamp and time-stamp of capturing (and also the location of capturing, if provided there). If the digital product was found edited or manipulated, then the above relevant portions should include the details of the software tool used to edit the particular digital product including the date-stamp and time-stamp of editing (and also the location of capturing, if provided there)]

9.5.4 A statement by the expert who performed the forensic task that the details given vide 9.5.1. to 9.5.3. above are correct to the best of his / her knowledge and belief

9.6 Digital transaction logs presented by the expert in the court as proof of the degree of originality of the evidence. Any automatically-created transaction log (if found automatically preserved in a way that is inaccessible to ordinary users) can be presented as evidence with the objective of proving or disproving the originality of a particular digital transaction (or a set of digital transactions) in question. While producing any transaction log, the expert is expected to include (in addition to the items 9.1 to 9.4 above)

9.6.1 The source details of these transaction log (for example, the configuration of the hardware including the storage devices, the path and other details of the digital location where the particular transaction log was found, the format of the log file etc.)

9.6.2 The specification and the configuration of the software tool used to extract the transaction logs. [For example, Apex software tool used to extract the transaction log of an SQL Server Database]

9.6.3 The output of the software tool after loading the transaction log. [This can be produced either as a text file or in any digital but human-readable form that is convincing to the judiciary]

9.6.4 Screenshot of the relevant portions of the transaction log (mentioned in 6.b. above) to prove or disprove the originality of the transaction (or a set of transactions) in question. [These relevant portions include the portions that explain and detail the transaction including the portions where date-stamp and time-stamp of the transaction do appear.]

9.6.5 A statement by the expert who performed the forensic task that the details given vide 9.6.1. to 9.6.4. above are correct to the best of his / her knowledge and belief

9.7 Source code presented by the expert in the court as proof of the degree of originality of the evidence. If found necessary, any source code (including the source of an email or of a webpage) can be presented by the cyber forensic expert in the court of law with the objective of proving or disproving the originality of the particular electronic evidence in question. While producing a source code, the expert is expected to include

9.7.1 The details of the hardware source of the source code (for example, the configuration of the hardware, including the location details, where the source code was found and then extracted from)

9.7.2 The specification and the configuration of the software tool used to extract the source code

9.7.3 The output of the software tool after loading the source code. [This can be produced either as a text file or in any digital but human-readable form that is convincing to the judiciary.]

9.7.4 Screenshots of the relevant portions of the output (mentioned in 9.7.3. above) to prove or disprove the originality of the electronic evidence in question. [These relevant portions include the portions that explain and substantiate the electronic evidence including the date-stamp and time-stamp of the creation / manipulation of the electronic evidence.]

9.7.5 A statement by the expert who performed the forensic task that the details given vide 9.7.1. to 9.7.4. above are correct to the best of his / her knowledge and belief

10. It is mandatory that *the statement should be signed by a person occupying a responsible official position in relation to the operation or management of the relevant activities* and that *the statement is made to the best of knowledge and belief of the person making it*. As a result, not all investigation officers can certify electronic records as evidence as they may not be the persons who actually extracted the electronic evidence (which is a point often raised by the defense lawyers while challenging the genuineness of the electronic evidence submitted by the prosecution). It also means that, any electronic record extracted by any other person (and certified and presented in the court by the investigation officer) has no legal standing. Only the person who actually extracted the electronic records (from its digital source) can certify certain minutest aspects of the four conditions under Sec. 65B (2). So, the Investigating Officers are advised to ensure that the person who actually extracted evidence is made a signatory and also, a witness.

11. On the authority of the police cyber experts to extract electronic evidence, the Sec. 65B (2) (b) of the Indian Evidence Act says, only either *the person having lawful control over the use of the computer* from which the electronic records were extracted or the person appointed by the court can become the cyber forensic expert. Hence, any electronic record extracted by the cyber forensic expert in the investigation team (and certified and presented in the court by the investigation officer) has no legal standing and can be challenged by the defense lawyers. For instance, in cases where copy of a YAHOO email is presented by the prosecution as evidence of crime, the defense lawyer can raise the point that the copy is not legally valid unless it was extracted by the expert appointed by the court or is certified by the Email Server Administrator of YAHOO. So, the investigation officers are advised to take steps to get the electronic evidence extracted (and then presented to the court) either by *a person having lawful control over the use of the computer* or by a court-appointed expert

12. In order to obtain electronic evidence from outside India, all Investigating Officers are advised to invoke legal provisions of Letter Rogatory or MLAT (Mutual Legal Assistance Treaty) or UNTOC (United Nations Convention against Transnational Organized Crime) or any related international treaty. For example, in order to obtain evidence from the Yahoo Email server (which is physically located outside the jurisdiction of the Indian judiciary), the Investigating Officers are advised to invoke the legal provisions mentioned above and thus, avoid the challenges by the defense lawyer (They may argue that such email evidence, if "certified" only by a "local" cyber forensic expert, is legally invalid).

13. Investigating Officers are advised to get the results of the Cyber Forensic Software Tools and Apps formally substantiated and attested by an expert. This is because the judiciary may not treat an inanimate object (e.g. a forensic software package or other digital products like a digital image or a video clipping) as an expert and so, may not treat results produced by any forensic software package as valid evidence or expert opinion. So, Investigating Officers are advised to get the results of the Cyber Forensic Software Tools and Apps formally substantiated and attested by *a person occupying a responsible official position in relation to the operation or management of the relevant activities*.

14. The Investigating Officers are advised to avoid or minimize oral witness by ensuring submission of complete, conclusive, informative, clear, and self-explanatory cyber forensic report. At the same time, they are advised to ensure all those who extracted the submitted electronic evidence are made expert witness, as according to Sec. 45A of the Indian Evidence Act, *when in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the examiner of electronic evidence referred to in Sec. 79A of the Information Technology Act, 2000 is a relevant fact.*

<u>Summary:</u> The Investigating Officers are expected to follow 65B as much as possible by following the guidelines given above and thus, to convince the originality (or authenticity or accuracy or legitimacy or genuineness) of the electronic record which is submitted as evidence.

Loknath Behera IPS
Director General of Police &
State Police Chief, Kerala

Distribution:- **All List 'D' Officers** (Upto SHO level)

Copy to:- All Unit Heads (including Spl. Units).
All Officers in PHQ.
Dy. Dir, State Police Media Centre, PHQ.
CA to SPC / Circular File / Police Website.

Note: The content of this Circular, a bit technical, featured in The Indian Police Journal, Vol. 66, Number 4, October-December (2019), published by the Bureau & Police Research and Development, (BPR&D), MHA, New Delhi, jointly written by Loknath Behera IPS & Dr. P. Vinod Bhattathiripad, Chief Technology Officer, Kerala Police. DPCs shall make efforts to make all SHOs & others to understand the content.