2017 2(1) 7-12

Submission: 2017/04/30, Peer review: 2017/05/10, Accepted: 2017/06/25, Published: 2017/06/30

International journal of justice & law

Publication state: Japan
ISSN: 2423-8767

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: shik71@hanmail.net

Peer reviewer
E-mail: editor@j-institute.jp

http://dx.doi.org/10.22471/law.2017.2.1.07



# LEGAL Proposal for Digital Evidence Seizure and Admissibility in KOREA

**Kim Burm-shik**

*Seonam University, Asan, Republic of Korea*

## Abstract

*Today, the digital revolution has completely changed all areas of society, and the evidence of crime has also become digitalized. Therefore, it is no exaggeration to say that the success or failure of investigation to reveal the truth depends on how digital evidence is secured and recognized. In this way, our society is rapidly changing into a digital society, but the law has not been completely restored, and it maintains the analog legal system of the past. In other words, the provision related to digital evidence is only Article 106 (3), (4) and (313) of the Criminal Procedure Act. However, these few words alone can not solve all the problems related to digital evidence. This study is based on the evaluation of the problems of Article 106 (3) and (4) of the Criminal Procedure Act and recently revised Articles 313 and 314 of the Criminal Procedure Act, the purpose is to present a new legislative alternative.*

*Current deficiencies in the acceptability of digital evidence should be addressed through amendments to the law. First of all, the digital evidence corresponding to the specialization is subject to the existing special law, so there are certain limitations on the ability of evidence. However, there are exceptions to the special law, I believe that it is reasonable to allow valuable evidence that is essential to substantiate the fact.*

*And any digital evidence that does not contain a statement should be able to acknowledge evidence capability only if it is proven authentic to establish the truth and credibility of the data. That is, errors in systems and software, and authenticity requirements to ensure the reliability of digital evidence exposed to the risk of unauthorized access, has proven that there has been no such error or danger. The accuracy and reliability of the system and the procedures are mainly presented as such authenticity verification methods. However, more specific requirements for the authenticity of digital evidence should be laid out in a manner that is based on technical standards established by experts, but can be easily applied to legal judgments*

**[Keywords]** ***Digital Evidence, Search and Seizure, Participation Rights, Cooperation Duty, Password Submission Order System***

## 1. Introduction

Today, the digital revolution has completely changed all areas of society, and the evidence of crime has also become digitalized. Therefore, it is no exaggeration to say that the success or failure of investigation to reveal the truth depends on how digital evidence is secured and recognized. In this way, our society is rapidly changing into a digital society, but the law has not been completely restored, and it maintains the analog legal system of the past. In other words, the provision related to digital evidence is only Article 106 (3), (4) and (313) of the Criminal Procedure Act. However, these few words alone can not solve all the problems related to digital evidence.

Already in many advanced countries, severallegislative measures are being taken to secure digital evidence in response to these

digital changes. In other words, in view of the characteristics of digital evidence, in order to establish the seizure and search rule for digital evidence itself and to be able to recognize evidence of digital evidence, objective evidence to admit that the testimony or the author of a forensic investigator, (Ie log records, comparisons with other electronic information, details that only the author can know, or that the author has used only). This study is based on the evaluation of the problems of Article 106 (3) and (4) of the Criminal Procedure Act and recently revised Articles 313 and 314 of the Criminal Procedure Act, The purpose is to present a new legislative alternative.

## 2. Legal Regulations and Assessments on the Seizure and Evidence of Digital Evidence

### 2.1. Regulation and evaluation of seizure search of digital evidence

In order to respond to the changing digital environment, the Korean legislator newly established Article 106 (3) and (4) of the Criminal Procedure Act for the seizure and search of digital evidence through amendment of the Criminal Procedure Act(Law No. 10864) on July 18.

***Article 106 (Seizure) (3) Where the object to be seized is a computer disc or other data storage medium similar thereto (hereafter referred to as "data storage medium or such" in this paragraph), the court shall require it should be submitted after the data therein are printed out or it is copied within the specified scope of the data stored: Provided, That the data storage medium or such may be seized, when it is deemed substantially impossible to print out or copy the specified scope of the data or deemed substantially impracticable to accomplish the purpose of seizure.***

***(4) Where the court receives the data pursuant to paragraph (3), it shall inform, without delay, the subject of information defined in subparagraph 3 of Article 2 of the Personal Information Protection Act, of the relevant fact.***

In other words, Article 106 (3) and (4) of the Criminal Procedure Act can output and confiscate digital evidence stored in an information storage medium such as a computer and confiscate an information storage medium such as a computer in an exceptional case. However, Article 106 (1) of the current Criminal Procedure Act restricts confiscation to "evidence or confiscated articles". In addition, Article 106 (3) does not “confiscate information stored in information storage medium such as computer disk” but “confiscated object is computer disk or other similar information storage medium”, The object of seizure is still centered on “fluid as information storage medium". In conclusion, Article 106 (3) of the Criminal Procedure Act is merely a "confiscation method" for information storage media, and the subject of confiscation is still "digital information itself" The question of whether digital evidence can be seen as an object of seizure[1].

In this regard, in practice, a seizure and search warrant for digital evidence is issued based on Article 106 (3)[2][3]. However, on the other hand, digital evidence has different characteristics from that of liquid evidence, so it is argued that separate procedures for the seizure and search of digital evidence should be established[4].

### 2.2. Provision and evaluation of evidence capability of digital evidence

On May 29, 2016, Korea`s legislator amended the Code of Criminal Procedure Act(Law No. 14179) on the ability of evidence of digital evidence.

***Article 313 (Statement, etc.) (1) Except as provided in the preceding two Articles, a written statement prepared by a criminal defendant or any other person, or a document containing the statement, if there being the handwriting, or the signature or seal of a person who prepared such statement or document or a stater, shall be admissible as evidence, if the authenticity of its formation is proved by a statement made by the person who prepared such statement or document or the stater at a preparatory hearing or***

***during a trial: Provided, That the document containing the statement of the criminal defendant shall be admissible as evidence regardless of the statement made by the criminal defendant at a preparatory hearing or during trial, only when the authenticity of its formation is proved by a statement made by the person who prepared the document at a preparatory hearing or during trial and the statement entered in the document was made in a particularly reliable state.***

***(2) If, despite the text of paragraph 1, the author of the affirmation denies the petition of the Constitution on the date of the trial or the date of the trial, it shall be evidence when the authenticity of the constitution is proved by objective methods such as digital forensic materials, Can be. However, a statement made by a non-accused person shall require that the defendant or his or her lawyer be able to report the writer on the written matter at the hearing or trial date.***

***(3) The documents describing the progress of the emotions and the results are also the same as in paragraphs 1 and 2.***

In other words, through amendment of Article 313 of the Criminal Procedure Act, despite the text of Article 313 (1), a statement (a computer disk for information such as texts, photographs, and images including statements made or written by a defendant or a defendant, Or similar information stored on storage media) denies the allegation of its establishment on the date of the trial or the hearing, evidence should be provided in the event that the authenticity of the establishment is proved by objective methods such as digital forensic materials, , But the defendant's written statement required the defendant or counsel to be able to report the writer on the date of the trial or trial[5].

Yet another problem arises from the fact that these legislations do not solve all the problems to acknowledge the evidence of digital evidence[6]. In other words, any of the techniques of digital forensics and the question of which of the forensic investigators will be accepted remains a matter of interpretation[7].

## 3. Legislative Proposal for Digital Evidence Seizure and Evidence Capability

Digital evidence can not be solved by the existing seizure and search system due to physical evidence and other special characteristics. Accordingly, the Criminal Procedure Act of Korea established the Article 106 (3) and (4) and tried to deal with it through the amendment of Article 313.

Despite these legislative responses, however, there are many problems that arise in the ability to seize, search, and test evidence of digital evidence. In other words, there is a problem of the possibility of confiscation of all digital information when it is impossible to confiscate and confiscate digital evidence, the problem of confiscation and search ability of digital evidence, the problem of confiscation and search of remote servers, 'Problem of search', 'participation in participation', 'problem of application of special rule of digital evidence'. These problems can be said to be inadequate to solve the problems arising from confiscation and search of digital evidence by the provisions of Articles 106 and 313 of the current Criminal Procedure Act.

The most fundamental way to solve this problem is to solve the problem through solving through the seizure and search of digital evidence rather than solving the problem through interpretation. In order to do this, I think it is appropriate to establish the regulations for the seizure and search of the digital evidence itself in Article 106 of the Criminal Procedure Act and to establish various regulations that can solve the problems arising from seizure and search of digital evidence. Therefore, the amendment to the current Criminal Procedure Act or the practical solution will be presented below.

### 3.1. Establishment of seizure and search regulations for digital evidence itself

As we have seen in the Problems of Article 106 (3) of the current Criminal Procedure Act, it is necessary to first legislate (Article 106 (3))

which seeks digital seizure itself as confiscation and search[8].

In this regard, the United States has a stipulation for this. In other words, for digital evidence stored in information storage media, US federal criminal lawsuits are limited to tangible objects in the properties subject to confiscation and search in section 41 (a) (2) (A) And it is legally resolved that digital information is subject to confiscation and search by including information itself. However, even before reflecting information as an object of confiscation in the rules, the US courts had recognized the possibility of confiscation of the information, saying that the rules of federal criminal lawsuits on the subject of confiscation were exemplary through interpretation[9].

In addition, the US Federal Criminal Procedure Rules states that Article 41 (e) (2) (B) provides for a Warrant Seeking Electronically Stored Information, It is possible to seize the electronic storage medium itself or to confiscate or duplicate electronic information only in parallel, so that the subject of confiscation can be selected according to the specific situation. Unless otherwise specified, it permits unlimited later review of the storage media or information on the warrant.

It is proposed to revise Article 106 (3) and (4) of the Criminal Procedure Law of the Republic of Korea as follows by referring to the US legislation.

***Article 106 (Seizure) (3) The evidence or article under Paragraph (1) includes information stored in a computer disk or other similar information storage medium (hereinafter referred to as "information storage medium").***

***(4) If the information is provided pursuant to Article 115 (2), the court shall notify the information subject to Article 2 (3) of the 「Personal Information Protection Act」 without delay. Provided, however, that this shall not apply when there is a fear of disturbing the trial in progress.***

### 3.2. Establishment of digital evidence confiscation, search method and participation rights, establishment of confiscation and search ground rules for remote servers

The Criminal Procedure Act of Korea defines the methods of seizure and search as 'principle and exception'. However, with regard to the search for digital evidence, it will be necessary to enact legislation (Article 115, Paragraph 2, Paragraph 1 of Article 115), which provides only a method of seizure search without priority[6].

In order to guarantee the fundamental rights of the person to be imprisoned, Regarding the method of seizure and search of digital evidence[10], it will be necessary to legislate the basis of seizure and search for remote servers which are not stipulated in our law (Article 115-2, Paragraph 3). To this end, it proposes to establish Article 115 (2) as follows.

***Article 115-2(Execution of confiscation of information) (1) Confiscation of information may be done by any of the following methods. In cases 2 and 3, only information that is deemed relevant to the case may be confiscated.***

***1. How to set up a range of information that is memorized and output or duplicate it***

***2. A method of seizing an information storage medium in which electronic information is stored***

***3. How to transfer and confiscate electronic information only.***

***(2) A suspect, an attorney, or a person provided for in Article 129 may participate in the categorization of information related to an incident during the course of paragraph (1).***

***(3) If there is a reasonable reason to believe that the information to be enforced is stored in the information processing device such as the confiscated or searched computer and the information storage medium connected to the information communication network, the information may be transferred to the information***

***processing device or other storage medium You can confiscate or search by cloning or printing. In this case, it can not be executed beyond the authority of the information processing apparatus administrator concerned.***

### 3.3. Other rules of procedure

In the case of confiscation and search for digital evidence, it will be necessary to prescribe in law the contents used in the practice of issuing warrants. To this end, it proposes to establish Article 115 (3) as follows.

***Article 115-3 (Confiscation of information Special conditions after execution) (1) When the information is confiscated pursuant to Article 115-2 (1), it may be reproduced or viewed on another storage medium, in whole or in part, to determine the relevance of the information to the incident. In this case, information copied to other storage media that is deemed irrelevant to the incident should be returned to the owner, holder or custodian of the information or discarded.***

***(2) In the case of Paragraph 1, when copying all the information stored in the information storage medium or the like to another storage medium, the relevant information storage medium, etc. shall be returned to the owner, etc. in accordance with Article 133 or Article 134 without delay.***

***(3) In the case of paragraph 1, a list of confiscated information shall be issued to the person prescribed in Article 129.***

***(4) The court shall notify the accused, the lawyer, or the person prescribed in Article 129 of the date and time in advance in order to carry out the procedure of paragraph 1. Provided, however, that this shall not apply to cases where the person who will be notified stipulates not to participate, when notice is impossible or difficult, or when there is a fear of disturbing the trial in progress.***

### 3.4. Establishment of cooperation duty and password submission order system

If digital evidence is cryptographic, there is a need to create new rules that force it. In the case of the United Kingdom with such provisions, Part Ⅲ of RIPA(Regulation of Investigatory Powers Act 2000) and the "Investigation of Protected Electronic Information Code of Practice" apply to encrypted information(para. 37). RIPA requires certain law enforcement agencies to order individuals or companies to provide a password or cryptographic key to read encrypted information or files. If anyone do not comply with this, criminal punishment can be made(para. 38). It is proposed that, with reference to the British legislation, Article 120-2 shall be newly established as follows.

***Article 120-2 (cooperation duty and password submission order system) (1) A person who executes a confiscation / search warrant for information may request cooperation such as the operation of an information storage medium or the like to an owner, holder or manager of an information or information storage medium, or access to other information storage media connected to the information communication network , Those who are requested to cooperate should cooperate unless there is unavoidable reason.***

***(2) Confiscation of information The person who executes the search warrant may order the owner, holder, or manager of the information or information storage medium to specify the scope of information stored, output, duplicate or submit.***

***(3) The court may impose a fine of up to KRW 100 million or a compulsory transitional compulsory deposit of up to KRW 10 million per day if the recipient of the request under paragraph 1 fails to do so without justifiable reasons. Provided, however, that the owner, holder or manager of information or information storage media shall be the defendant.***

## 4. Outro – Suggestions for Evidence of Digital Evidence

Current deficiencies in the acceptability of digital evidence should be addressed through amendments to the law. First of all, the digital evidence corresponding to the specialization is subject to the existing special law, so there are certain limitations on the ability of evidence. However, there are exceptions to the special law, I believe that it is reasonable to allow valuable evidence that is essential to substantiate the fact[11]. In this respect, the amendment of Article 313 of the Criminal Procedure Act is considered to be valid. However, it seems that the issue of how our courts take their operations is a matter of concern. And any digital evidence that does not contain a statement should be able to acknowledge evidence capability only if it is proven authentic to establish the truth and credibility of the data. That is, errors in systems and software, and authenticity requirements to ensure the reliability of digital evidence exposed to the risk of unauthorized access, has proven that there has been no such error or danger. The accuracy and reliability of the system and the procedures are mainly presented as such authenticity verification methods. However, more specific requirements for the authenticity of digital evidence should be laid out in a manner that is based on technical standards established by experts, but can be easily applied to legal judgments.

## 5. References

### 5.1. Journal articles


[2] Son DK. A Study on the Search and Seizure of Digital Evidence in Amendment Criminal Procedure Acts. *Korean Journal of Criminology*, 23(2), 325-349 (2011).

[3] Rhee JW. Study on the Improvement of Seizure and Search of Digital Evidence. *Anam Law Review*, 37, 151-199 (2012).

[4] Lee EM. The Problems on Investigation for Electronic Records. *Journal of Criminal Law*, 23, 156-175 (2005).

[5] Cho GH. The Direction for Rational Interpretation of the Article 313 of Revised Criminal Procedure Code Especially Focusing on the Objective Method in the Clause 2 of Article 313. *Lawyers Association journal*, 66(1), 220-271 (2017).

[6] Roh MS. Amendment of Criminal Procedure Law Article 313 Its Drawbacks and Ways to Improve. *Korean Lawyers Association Journal*, 65(9), 5-38 (2016).

[7] Kim, JH. The Principle of Digital Forensics and the Method of Evidence Valuation under the Real Case Proceeding. *Kyung Hee Law Journal*, 52(1), 103-156 (2017).

[9] Roh MS. Precedent Trends and Comparative Consideration Regarding Search and Seizure of Digital Evidence. *Prosecute Service*, 43, 139-194 (2014).

[10] Park WS. The Study of Right to Participate and Confiscation for Another Digital Evidence Focus on National Security Crime. *Police Science Institute*, 30(3), 261-294 (2016).


### 5.2. Thesis degree


[1] Jeong BG. A Study on the Collection and Admissibility of Digital Evidence. Chosun University, Doctoral Thesis (2012).

[8] Lee SY. Handling and Admissibility of Digital Evidence in Criminal Procedure. Korea University, Doctoral Thesis (2011).

[11] Park MW. A Study on the Due Process of Law in Search and Seizure of Digital Evidence. Korea University, Doctoral Thesis (2016).



**Author**

**Kim Burm-shik** / Seonam University Senior Profrssor
B.A. Dongguk University
M.A. Dongguk University
Ph.D. Sungkyunkwan University

Research field
- Problem of Criminal Mediation in Korea- Does Criminal Mediation in Korea Based on Restorative Community, Korean Journal of Victimology, 23(3) (2015).
- A Study on the Necessity of the Immunity and Sentence Reduction System for Judicial Cooperators, Korean Journal of Comparative Criminal Law, 18(4) (2016).

Major career
- 2010~present. Seonam University, Profrssor.
- 2017~present. International Society for Justice & Law, Member.