FORENSIC SCIENCE FORUM / FORUM CRIMINALISTIC
Issue 17/ 1 of 2015 (January-June)/ Volume VIII ISSN 1844-2641
DOI: 10.18283/FORUM.VIII.17.12015.315

Basic aspects concerning the evidence aquisition in digital forensic analysis / Aspecte de bază privind achiziția probelor în cadrul expertizei criminalistice a datelor informatice

Cezara CRĂCIUNESCU[1]

Content description (Eng.):	In acordance with Criminal Procedure Code as law enforcement officers, is necessary to deal with evidence. The evidence is anything that can be used to prove or disprove something related in the penal/civil process. In our days the impact of cybercrime or computer related crime is growing up, and this reflects that digital evidence within "conventional" investigations is widespread. Electronical stored data are quite fragile and only act of accessing it has the potential to alter it. Digital forensic investigations often involve creating and examining disk images. A physical image will contain current files as well as slack space and unallocated space. Relevant forensic artifacts such as, deleted files, deleted file fragments and hidden data may be found in slack and unallocated space. To use the image of a disk in court in an criminal case, it is necessary to demonstrate that the evidence presented in court is exactly the same as was found on the source device and has not been altered in any way during the extraction of the relevant evidence. The most common method used for this verification is a hash comparison, with MD5 or SHA1 value, sometimes called a digital fingerprint.
Keywords:	Digital evidence, forensic image, physical image, logical image, HASH value, storage devices, ESI (electronical stored informations).
Article info:	**Received:** 03/06/2015 **Approved:** 25/06/2015 **Pages/ words:** 6/2796

Rezumatul articolului (Ro)	În conformitate cu Codul de Procedură Penală, ca ofiţer de poliţie, e necesar a interacţiona cu probe. O probă este orice element de fapt ce poate fi folosit pentru a afirma sau a infirma ceva in materia procesului penal sau civil. În zilele noastre, datorită tehnicii actuale, impactul criminalităţii informatice este în creştere, fapt ce dovedeşte că probele digitale sunt tot mai răspândite în investigaţiile curente. Datele stocate electronic sunt foarte fragile şi orice acţiune, de exemplu accesarea lor, le-ar putea modifica sau altera. Investigarea criminalistică a datelor digitale implică adesea crearea şi apoi examinarea imaginilor acestor date. Imaginea fizică va conţine atât fişierele curente cât şi spaţiul asignat şi cel nealocat. Urmele relevante, cum ar fi fişierele şterse sau fragmentele din acestea, cât şi datele ascunse pot fi găsite în spaţiul nealocat sau în cel asignat. Pentru a utiliza imaginea unui disk în justiţie într-un caz penal, e necesar a se demonstra faptul că proba prezentată justiţiei este identică cu cea găsită la faţa locului şi nu a fost alterată în niciun fel în timpul extragerii probelor relevante. Cea mai utilizată metodă este cea a comparării valorii funcţiei HASH prin valorile MD5 sau SHA1, care mai sunt numite şi amprente digitale.
Cuvinte cheie:	Probă digitală, imagine criminalistică, imagine fizică, imagine logică, valoare HASH, suporţi de stocare, ESI (informaţii stocate electronic)
Detalii articol:	**Primit:** 03/06/2015 **Aprobat:** 25/06/2015 **Pagini/ cuvinte:** 6/2796

Article`s content (example):
a.Introduction
b.Principles
c.Forensic image
d.Conclusions
e.Bibliography

Cuprinsul articolului (exemplu):
a.Introducere
b.Principii
c.Imaginea criminalistică
d.Concluzii
e.Bibliografie

♦♦♦♦♦

[1] Forensic specialist, General Inspectorate of Romanian Police - National Forensic Science Institute, cezara.craciunescu@politiaromana.ro.