Importance of Operating Systems Type in Computer Forensics

Hüseyin ÇAKIR, Mehmet Serkan KILIÇ
IT Institute, Gazi University, Ankara, Turkey
hcakir@gazi.edu.tr, mserkanklc@hotmail.com

Abstract

This article works on determining the effect of operating systems on Computer forensic especially in nowadays that the need for Computer forensic is increasing due to the increase in cybercrimes. Suited to the purpose of the study and methods of interview, 15 people with minimum of 4 years of experience in informatics have been interviewed, in addition, the reports of court experts from cases which are continuing in Ankara administration of Justice and domestic and foreign sources have been analyzed technically. With the outcome of the analysis, it has been observed that the studies and investigations are prepared according to an operating system, software or a certain device because of the commercial concerns or habits, for this reason it appears that it would be helpful to make an academic study in; sessions, workshops, seminars about gathering electronic evidences. Article studies the identification of differences and similarities between the operating systems and its effects on forensic studies with 5 headings and subheadings. According to the study, non-existence of a standard Computer forensic process and the need for different specialties are discovered, for this reason it is assessed that the Computer forensic experts need to specialize in sub-specializations especially related to operating systems.

Index terms: computer forensic, cybercrimes, electronic evidence, evidence collection, operating systems

References:

[1]. D.S. Jadhav and S.K. Patil, The Study Of Computer Investigation Methods: Computer Forensics, The International Journal Of Advanced Research In Technology, Vol. 2, Issue.1, pp. 9-17, 2012.

[2]. A. Ho and S. Li, Forensic Authentication of Digital Audio and Video Files" in Handbook of Digital Forensics of Multimedia Data and Devices, Chichester, UK: John Wiley IEEE Press, 2015, pp.133-184.

[3]. D. Comer, "Introduction and Overview" in Operating System Design: The Xinu Approach, 2th ed. NW: CRC Press, 2015, pp. 3-15.

[4]. M.İ. Öztürk, Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri (Models Of Flowchart For Detecting And Evaluating Digital Evidences in IT Equipments), M.S. thesis, Health Sci. Inst., Ankara Univ., Ankara, Turkey, 2007.

[5]. B. Carrier, File System Forensic Analysis, 5th ed. NJ: Pearson Education Inc, 2007.

[6]. Y. Uzunay, "Bilgisayar Ağlarına Yönelik Adli Bilişim" (Computer Forensics Intended for Computer Network) in Computer Forensics Workshop, İzmir Institute of Technology, İzmir, Turkey, 2005.

[7]. AccessData, Windows OS Forensics Training Notes, unpublished.

[8]. W.G. Kruse and J.G. Heiser, Computer Forensics – Incident Response Essentials, 14th ed. IN: Pearson Education Inc, 2010.

[9]. M.K. Rogers, J. Goldman, R. Mislan, T. Wedge and S. Debrota Steve, Computer Forensics Field Triage Process Model, Journal of Digital Forensics, Security and Law, Vol.1 No.2, pp.9-38, 2006.

[10]. T. Henkoğlu, Adli Bilişim, Dijital Delillerin Elde Edilmesi ve Analizi, 1st ed. Ankara: Pusula Yayıncılık, Turkey, 2011.

[11]. M.B. Eryılmaz, Ceza Muhakemesi Hukuku Dersleri, 1st ed. Ankara: Polis Akademisi Yayınları, Turkey, 2012.

[12]. D.S. Thomas and K.A. Forcht, Legal Methods of Using Computer forensics Techniques For Computer Crime Analysis and Investigation, Issues in Information Systems Journal, Vol.5 No:2, pp.692-698, 2004.

[13]. B. Nelson, A. Phillips and C. Steuar, "Expert Testimony in Digital Investigations" in Guide to Computer Forensics and Investigations, 5th ed. USA: Cengage Learning, 2015, pp. 535-567.

[14]. Adalet Bakanlığı, "Çalıştay Raporu", Yargılamada Bilirkişilik Müessesesi Çalıştayı, (Workshop Of Expert Witnesses at Trial), Hakimevi, Ankara, Turkey, 2010.

[15]. Y. Çiçek, "Bilirkişi Raporlarının Hazırlanması", Kamulaştırma Bilirkişiliği Eğitimi Programı (Expert Witnesses at Expropriation Training Program),TMMOB Harita ve Kadastro Mühendisleri Odası, Ankara, Turkey, 2008.

[16]. A. Karagülmez, Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular, 2. Polis Bilişim Sempozyumu (2nd Police IT Symposium), Sheraton Hotel, Ankara, Turkey, 2005.

[17]. H. Çakır and E. Sert, "Bilişim Suçları ve Delillendirme Süreci", Örgütlü Suçlar ve Yeni Trendler. Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumu (International Terrorism and Transnational Crime Symposium), Antalya, Turkey, 2010.

[18]. V. Bıçak, Suç Muhakemesi Hukuku, 1st ed. Ankara: Seçkin Yayınevi, Turkey, 2011.