taken in this research has become part of forensic analysis in digital investigation.

## 7. References

[1] Schuster A, "Searching for processes and threads in microsoft windows memory dumps. ," Digital Forensic Research Workshop (DFRWS), 2006.

[2] Digital Forensic Research Workshop (DFRWS). (2007, July) http://www.dfrws.org/2007/challenge

[3] Carrier BD, Grand J., "A hardware-based memory acquisition procedure for digital investigations.," The International Journal of Digital Forensics & Incident Response, vol. (1), no. 2, pp. 50-61, February 2005.

[4] M. Burdach, "Windows memory forensic toolkit;," Journal of Information and Computing Systems, vol. (5), no. 2, pp. 45-75, March 2007.

[5] Gabriela Limon Garcia, "Forensic Physical Memory Analysis: an overview of tools and techniques," in TKK T-110.5290 Seminar on Network Security, Helsinki, Finland, 2007.

[6] Msuiche. (Accessed 2008, March) Msuiche.net at:, Capture memory under win2k3 or vista with win32dd. http://www.msuiche.net/2008/06/14/capture-memory-under-win2k3-orvista-with-win32dd.

[7] ManTech Memory. (Aceesed 2010, March) at:, ManTech International Corporation. Memory dd. http://www.mantech.com/msma/MDD.asp

[8] Solomon DA. Russinovich ME, Microsoft Windows internal Covering Windows Server 2008 and Windows Vista, 5th ed. Washington, USA: Microsoft Press, 2009.

[9] Agile Risk Management. (Accessed 2009, October) Nigilat32 small footprint, Agile. [Online]. http://www.agilerm.net/nigilant32

[10] Betz C., "Mempaser analysis tool.," in DFRWS 2005 Forensic Challenge Can be accessed at: http://www.dfrws.org/2005/challenge/memparser.shtml, MA, 2005, pp. 100-115.

[11] Volatile Systems. (2009, April) The Volatility framework: volatlile mwmory artifact extraction utility framework.
http://www.volatilesystems.com/default/volatility

[12] Kleiman D. Carvey H, "Windows Forensic Analysis Incident Response and Cybercrime Investigation Secrets," 1st ed. Syngress Publishing; , July 2007.

[13] Olajide F. Savage N, "Forensic Live Response and Events Reconstruction Methods in Linux Systems," in PGNET The Convergence of Telecommunications Networking and Broadcasting, Liverpool, December 2009, pp. 141-147.

[14] Olajide F. Savage N, "Application Level Evidence from volatile memory," Journal of Computing in Systems and Engineering, December 2009.

[15] Olajide F. Savage N, "On the extraction of forensically relevant information from physical memory," in World Congress on Internet Security (WORLDCIS-2011), Technically Co-Sponsored by IEEE UK/RI Computer Chapter, London, 2011.

 