Advances in Digital Forensics VI

Chapter 7

A Forensic Readiness Model for Wireless Networks

Sipho Ngobeni [1, 2], Hein Venter[1], Ivan Burke[1, 2]

1Council for Scientific and Industrial Research, Pretoria, South Africa

[2] *University of Pretoria, Pretoria, South Africa*

Abstract

Over the past decade, wireless mobile communications technology based on IEEE 802.11 wireless local area networks (WLANs) has been adopted worldwide on a massive scale. However, as the number of wireless users has soared, so has the possibility of cyber crime, where criminals deliberately and actively break into WLANs with the intent to cause harm or access sensitive information. WLAN digital forensics is seen not only as a response to cyber crime in wireless environments, but also as a means to stem the increase of cyber crime in WLANs. The challenge in WLAN digital forensics is to intercept and preserve all the communications generated by the mobile devices and conduct a proper digital forensic investigation. This paper attempts to address this issue by proposing a wireless forensic readiness model designed to help monitor, log and preserve wireless network traffic for digital forensic investigations. A prototype implementation of the wireless forensic readiness model is presented as a proof of concept.