Digital Investigation 11 (2014) S104–S111

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Out of sight, but not out of mind: Traces of nearby devices' wireless transmissions in volatile memory

Wicher Minnaard

Netherlands Forensic Institute, Department of Digital Technology & Biometry, PO Box 24044, 2490 AA The Hague, The Netherlands

Keywords:
Network forensics
Wifi probe requests
Wifi beacons
IEEE 802.11
Network carving
Memory analysis

ABSTRACT

An IEEE 802.11 wireless device can leave traces of its presence in the volatile memories of nearby wireless devices. While the devices need to be in radio range of each other for this to happen, they do not need to be connected to the same network—or to any network at all. Traces appear in the form of full wire-type frames; a residue of the signals in the ether. We examine types of information that can be extracted from such residual frames and explore the conditions under which traces develop and persist. Their availability is determined by factors in both in the external environment (the types of signals in the ether) and the internal environment (the configuration and particulars of a device's wifi stack). To isolate some of these factors, we have created memory dumps of devices in various environments and configurations. Analysis of the dumps has offered insights into the conditions determining creation and decay of the traces. The results indicate that they will be available in a limited number of real-world scenarios. We conclude with practical advice on triaging and preservation.

Introduction

Since it was such a simple experiment that sparked our interest on the topic of residual wifi traces, we can best introduce the subject of this investigation by describing that initial experiment here.

A wifi-equipped[1] smartphone was brought in range of a wifi access point of which the RAM could be easily dumped. The smartphone had previously been connected to some networks, but it had never been connected to this particular access point. The phone was merely a passerby, as it were. On dumping the access point's memory, we were fascinated to find that, despite having no other relation to each other than simply having been in vicinity, names of networks to which the phone had connected previously could be found in the memory dump. Closer inspection of the dump showed that these names were embedded in the wire format of probe request frames; a format defined in the IEEE 802.11 standard. Thus it appeared that the frames had ended up *verbatim*, in network order, in the physical memory of the access point.

The implications of this find are quite unexpected for the smartphone user, who would certainly wonder why the name of his home network can be found in the memory of an access point which he simply happened to pass on his way to work. From an engineering perspective the phenomenon is less surprising—a data link frame may have to be buffered somewhere before can be decided that it should be discarded or unlinked. For some researchers in digital forensics, the phenomenon might not come as a complete surprise either. In 2011, Beverly, Garfinkel and Cardwell have addressed a related phenomenon (Beverly et al., 2011). Their work involves recovering "long-terminated network data in memory" of

E-mail addresses: wicher@holmes.nl, wicher@nontrivialpursuit.org.

[1] When using the terms '802.11' and the informal 'wifi', we are referring to radio technology based on the IEEE 802.11 standard (IEEE, 2007).

http://dx.doi.org/10.1016/j.diin.2014.03.013

which they find copious amounts—counter to their (and our) intuitions, which were *"[…] that portions of the Ethernet and/or IP protocol would be handled in hardware for performance reasons and not exposed to the operating system"*. As their goal is to extract IP and MAC addresses, they go on to develop a carver-generating technique that exploits statistical properties of the patterns in the context that the addresses appear in. This yields excellent results when compared to orthodox memory analysis; their efforts, as ours, show that there is information to be found beyond what is reachable by traversing the OS structures that reflect some 'current' state of the memory snapshot.

From a more general forensic perspective, the phenomenon of the retained probe request frames is interesting for the high potential value of this type of trace—precisely because the radio transmissions that lead to its creation are unintentional, ubiquitous, and unrelated to the nature of a crime. Any crime scene where wifi equipment can be found may thus contain these digital leads as to who was there, regardless of whether the crime itself had any digital component to it. In that respect the trace is rather like a digital version of a personal scent that lingers.[2]

The goals of our research into this novel type of trace are twofold: to identify types of information that can be discovered using recovered wifi frames, and to determine whether there could be real-world circumstances in which these wifi frames could be available for recovery. The latter is hardly a given—from a high level functional perspective there is no reason to keep them around for long (or at all, depending on frame contents).

Forensic artefacts in 802.11 management frames

In investigative law enforcement work, the goal is often to identify a person ('who'), to place him or her at a specific location ('where'), and preferably at a specific time ('when'). We show how these three goals relate to information present in two particular 802.11 management frame types: the beacon frames transmitted by the access point (AP), and the broadcast probe request frames transmitted by the wifi device (STA).

Preliminaries

To be able to discuss 802.11, we need to establish some common ground. In this paper we will refer to, but not reiterate frame formats defined in the 2007 1184-page IEEE 802.11 specification.[3] To aid in quickly understanding the gist of the parts of the standard relevant to our research, we offer some comments on sections in the standard that we deem particularly informative.

§**5.2.3 Distribution system (DS) concepts**

Central to 802.11 is the notion of a 'base service set' (BSS), which, in an infrastructure network, is a set of stations (STAs) served by an access point (AP). Multiple BSSes can be connected to form an extended service set (ESS), but in the common domestic case the ESS consists of just one BSS, one AP, and some STAs. Ultimately the SSID identifies an ESS and is what the end user sees as "the network name". The SSID is not used for addressing purposes (the ESS is not logically addressable; an SSID is an identifier rather than an address) and is present in only a limited number of packets.

§**7.1.3.3 Address fields**

Frames can contain up to four addresses. This section explains their meaning. The base service set is addressable through the BSSID. In the common 'infrastructure' network, this address is equal to the MAC address of the wireless interface of the AP. In an 'ad-hoc' network without APs—an IBSS, not to be confused with the 'infrastructure' BSS—this is not the case.

§**11.1.2 Maintaining synchronization**

This section introduces the 'Timing Synchronization Function', which is at the basis of the timestamp field that we will encounter in beacon frames. The TSF is a timer with μs resolution, and its value is stored in a 64-bit wide field. Interestingly, this results in a surprisingly large rollover time of almost 585,000 years. In an IBSS it is used in a mechanism to orchestrate the generation of beacon frames across the IBSS. The timer previously also played a role in the coordination of a frequency hopping mechanism that was enabled in the original 1997 802.11 standard.

§**11.1.3 Acquiring synchronization, scanning**

This section explains how a station can find what users call 'networks'—ESSes and their BSSes. It describes the passive approach in which a station quietly listens for beacon frames as well as the active approach of sending out probe request frames. It does not describe why a station would prefer one or the other, but it raises a question: Why do we have probe request frames when we already have beacon frames for which we could simply listen?

Obviously, a probe request is needed to find a certain 'hidden' network that does not broadcast its SSID in its beacons. Less obvious is the fact that an active scan may be preferred since it can save power—it finishes much sooner since probe responses typically come in within tens of milliseconds, whereas beacon intervals and thus the required channel dwell times can be in the order of seconds. Since the antenna circuit can be powered down when further traffic is not expected, energy savings can be significant. A second benefit of scanning actively is that by receiving a probe response it is not only established that the device can hear the AP—it is also established that the AP can hear the device.

§**11.2 Power management**

This section deals with power management. A STA can signal the AP to buffer packets destined for it while it sleeps for a moment. This implies that even when a STA is associated, it is not necessarily continuously listening.

[2] Testament to the forensic utility of such smartphone scent trails is the fact that they are being exploited commercially, most infamously with the recent deployment of 'smart' litter bins on the streets of the City of London (BBC News, 2013).

[3] The 2007 specification is available through IEEE Get, http://standards.ieee.org/getieee802/download/802.11-2007.pdf. The 2012 specification is over twice its size and its additions are not relevant to our research.