

Aircapture – Wireless Network Survey & Analysis

AIRCAPTURE

WLAN



AirCapture Technical Specifications

AIRCAPTURE is the first commercial tool available for WLAN forensics, and captures all data in all channels available in 802.11 simultaneously and stores the data for later analysis. All scanning and capturing of data is passive and not visible to others. GPS logging is standard to provide evidence as to the location where data is collected.

Data captured by AIRCAPTURE WLAN 14 is analysed offline by experts using in-house tools. To facilitate and speed up forensics analysis, offline, we supply functionality such as filters that help identify the relevant data to be extracted with AIRCAPTURE.

AIRCAPTURE can be used as a stationary detector or in a mobile site e.g. in a car. Easy and secure access is controlled through a browser from and operating system with a LAN interface. AIRCAPTURE detectors provide feedback through a central processing unit to a user friendly display via a network connection.

AIRCAPTURE detectors come with an external 2.4 GHz omni-directional antenna with a 6 dBi gain, which can be mounted on a car or building or other stable platform. The high-performance RF components in the receiver chain of AIRCAPTURE produce superior sensitivity and range, and depending on the antenna (plus location and environmental conditions) can capture even very weak WLAN signals on all 802.11 channels up to 1 mile.

Aircapture – Wireless Network Survey & Analysis

AIRCAPTURE benefits :

- Unit is stealthy (not visible from the air when operating), and totally passive, i.e. not detectable
- Upgradeable to support next generation wireless forensics platforms
- Superior RF equipment, range > 4 km tested with high gain antenna
- Easy to use by the officer in the field, no training needed
- Forensic related feature such as GPS logs and encrypted files included
- Mobility and roaming issues solved by simultaneous monitoring all 14 channels
- Can be used as a portable unit or as a distributed system
- In-built filter functionality supports surveillance of a certain MAC address on all possible channels
- Produces pcap files that can be easy imported to a required analyser
- No need for internal tools, WLAN 14 is supported by most experts in Wireless forensics
- XML is supported to automate configuration & simplify handling of PCAP files from remote units.
- Automated decryption of WEP and WPA integrated into the WLAN 14 capture engine.

AIRCAPTURE Targeted Users :

- Military and Law Enforcement agencies in need of Automated Wireless Forensic tools for use in battle field or in other surveillance operations. WLAN is easy to use and cheap as a method of communication by terrorists and criminals – WLAN is growing in use and becoming available in mobile phones, used for voice, video and data.
- Equity/bond traders such as banks need to store business data not only from the wired network but also the wireless network, and to be able to provide evidence if hacked through the wireless network. Data should be stored for months and when needed detailed logs would be required in investigation.
- Engineering and quality assurance (QA) teams developing and testing WLAN can use Aircapture WAN 14 as a method of testing time related issues between radio channels. WLAN 14 simultaneously captures data on all 14 channels and provides an accurate time stamp on each pcap file produced. Roaming time can be analyzed between channels and the pcap files can be merged and exported to any analyzer.

AIRCAPTURE Specifications :

- PC computer with P4 CPU & 1GB RAM memory
- SATA1 7200RPM HDD, 80GB(system)+300GB(data)
- External mounting 3 SATA1 HDD with 19" 4U rack case
- 15 channel WLAN b/g module with one (1) antenna
- Power splitter and low noise LNA (low noise amplifier)
- 2.4 GHz omni-directional antenna with 6 dBi gain (user can connect to a higher gain antenna)
- Integrated GPS with SIRF III chipset

Contact Details

sales@icardforensics.com

**iCard Forensics
5 River Road., Ste. 21
Wilton, CT 06897
Tel: (203) 563-9900
Fax: (203) 563-9832**

www.icardforensics.com