


*C1 - Series*

## **C1 – Series : The ultimate covert device**

### **The new technology for Wireless Forensics**

**C1** is the latest technology for Wireless Forensics developed by our Wireless and IT experts. The C1 is a covert tool that is ideal for discrete use. Other Condor products are designed for long term monitoring and passive interception however the C1 blends active attacks with passive interception in the palm of your hand or in your pocket. When targets are in Internet cafés or other hotspots they might be out of reach for the C4 or C15 device, the highly portable C1 is the ideal solution for tactical surveillance.

#### *Technology for Tactical operations*

**The C1** is the ideal product for covert operations. Were a target is out of the range or scope of either the C4 or C15, for instance in a pedestrian only area or in a tower block, the C1 allows an operative to simply carry the device in hand or pocket. For rapid response personnel the C1 can be mounted or carried on a motor cycle. The C1 includes the ability to capture data on one channel whilst monitoring activity on all other channels. Target location can be tracked using signal strength and with the ability to generate active attacks such as ARP or denial of service it is possible to cause a target device to initialise new hand shake routines that are essential when recovering encryption keys for WPA/WPA2 with the C4 or C15.

#### *Operation Mode*

- Palm size unit and professional case
- Passive and Active mode
- Ability to capture the data from the selected channel and save into storage drive.
- Store data from targets on 1 radio channel ( pcap format )



- Export and import pcap data from/to C1
- Filtering and classifying targets
- Finding targets, visualizing networks
- Decryption of WEP, fast and easy
- Denial of services attack against target MAC



### Technology in the palm of your hand

Experience The C1 in the palm of your hand. The mobility is excellent and with a HDD of 120 Gig gives you the power to store huge amounts of data. With 3G/GPRS you can easily connect to the device for remote control applications.

### Specification

- 1.86 GHz Intel Atom processor Z540
- Linux base system for stability use
- Vivid OLED display
- Built in Wi-Fi and Bluetooth
- Intuitive Interface and keyboard, sliding up the 5" WVGA LCD of the model 2+ reveals a 58-key thumb keyboard and track stick.
- 2GB DDR2 SDRAM
- 120 GB HDD or SSD Technology 60GB
- Weight 1Lb (0.453kg) with standard battery and hard drive
- Dimension 5.6" x 3.3" x 1.0" (14.224cm x 8.382cm x 2.45cm)
- Battery Li – ion polymer with 4500mAh for 3.5 hours using

## Challenges with Wi-Fi interception

Understanding the problems and challenges with Wi-Fi interception is fundamental to design a tool that can do the job well. The expertise of the Condor team allows Condor to offer product and technology training so you can benefit more from investing in our products. Following are some examples of problem's that would be covered in a Condor training class to enable users to become highly skilled Wi-Fi Interception experts:

### Encryption, WEP and WPA/2:

In the early days of Wi-Fi WEP encryption or nothing at all was used to safe guard user data from hackers, now strong encryption such as WPA and WPA2 are gaining popularity making it difficult and time consuming to decrypt. It takes dictionaries and clever software designed for this specific purpose and high performance hardware to crack WPA/2.

### Roaming between AP's , 14 different radio channels in 802.11b, g:

Client can change radio channel's in the middle of communication (roam) and half of data might be lost if you only data from one channel/radio is stored. This means laptops that can only capture data on one channel are not suitable for long term monitoring. Also the target AP can change channel at anytime. In the case of long term monitoring large amounts of data can be lost due to this.

### Wi-Fi popularity means a lot of data in the air:

As Wi-Fi is growing extremely fast there is an increasing amount of data in the air. You need to be able to filter out the targets of interest and decrypt and analyze the traffic fast. There might also be local laws only permitting you to look at a specific MAC client or AP. In this case you must be able to filter only on that specific traffic but at the same time be able to use filter on as many radio channels as possible in case the client chooses to roam on to another, unknown channel.



北京财富佳美科技有限  
[www.caifujiamei.com](http://www.caifujiamei.com)