



Wireless Connections

Getting Started with Detective

The Wireless Connections section presents the history of Wireless connections in one list and shows the place where the Internet was used. Information about every Wi-Fi hotspot is found in this section and includes the SSID, MAC address, time of the first and last connections. The program also displays the history of Bluetooth connections and the list of frequent locations extracted from iOS devices.

All sections and analytics are laid out in a 3 column fashion across the board making it easier to find the information you are seeking. This document will walk you through which information will be found in each column.

The screenshot displays the Detective software interface. The main window is divided into three columns:

- Column 1:** A sidebar on the left containing navigation options like 'Categories' (160 items) and 'Locations' (155 items).
- Column 2:** A central table with columns for 'Type', 'Time stamp (Fakaofu)', and 'Description'. The table lists numerous 'Cell point' entries with their respective coordinates and timestamps. A large red 'COLUMN 2' is overlaid on this section.
- Column 3:** A 'Details' panel on the right showing information for a selected entry, including 'Source', 'Type', 'Time stamp', 'Coordinates', 'MAC address', and 'Cell info' (Horizontal and Vertical accuracy).

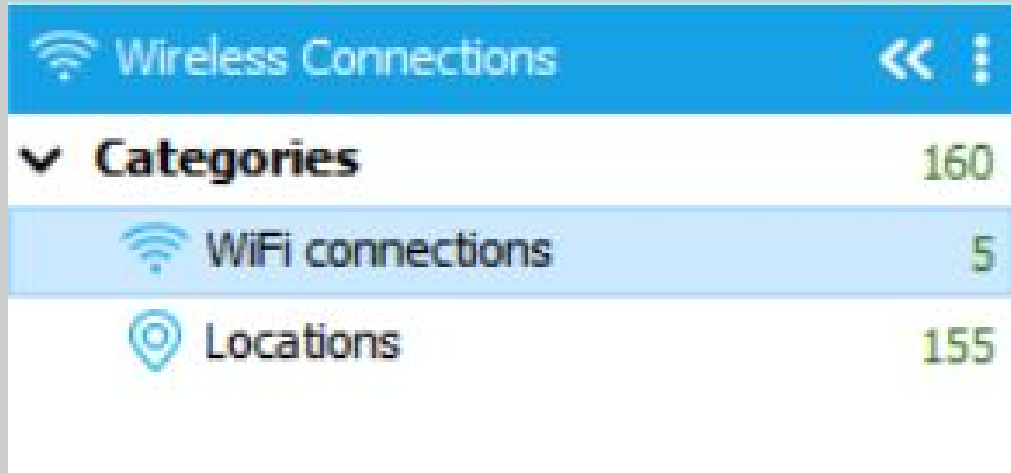
At the bottom of the interface, there is a map showing the geographic distribution of the connections. A red '1' is placed near the sidebar, and a red '3' is placed near the details panel. The interface also includes a search bar, 'Export' and 'Reset filters' buttons, and a 'View' dropdown menu.



Column 1

Where: On the left-hand side of the section

Uses: This is your dropdown menu that displays all that you will see in Column 2. If you click on any particular link, such as the gmail account in the photo below, that information will show in Column 2.



Here you will find 2 categories under wireless connections. You can click Categories to view all data in the WiFi Connections and Locations sections in Column 2 or choose which you want to view by clicking on the links individually.

In the lower section of Column 1 you will find a “Find text...” box. This is a quick filter box. Once you start typing in the word or name you are searching for it will automatically highlight the matching characters in the column.





Column 2

Where: In the center of the section.

Uses: This is your main grid column. Here is where you will see all the content that you have filtered down to on display.

The top bar above column 2:

- To move back to the device information click on the box “Extraction info”
- At the top of the screen is the “Export” function. Here is where you can form a selective report on this section. You will have the following formats to export your report to: PDF, XLSX, XML, HTML
- To clear out your filters there is a “Reset Filters” button at the top of your screen above Column 2. If the “Reset filters” button is greyed out, this indicates that no filters are active and all available information in this section is being displayed.
- The “View” button allows you to control whether or not you see your tags and thumbnails displayed.
- If the “Maps” button is blue this is an indication that there are geo-locations in this section that can be viewed on OxyMaps.



On the upper right-hand of the grid you will see a box labeled “Find text”. This is to filter through your grid to find specific characters. Once you start typing in your word to be filtered down to, you will see the filtered text start to highlight within the grid. If you press enter, your filtered content will be all that is displayed in the grid.



Once you are in the grid inside the Wireless Connections section:

- The printer icon: Here is where you can select or deselect items to be included in your report.
- The star icon: This is a location to add items as key evidence. If the star is highlighted yellow, your item has been marked.
- The tag icon: Once you start adding tags to your evidence items such as “Important” or “Not relevant” this is where you will start to see your tags show up. If you choose the box “Tags” in the “View” button as mentioned above, you will then not only see a color tag but will see what the tag has been named. This is also a filtering function drop down menu. You can filter to chosen tags only, if you need to do so. You can also arrange the types of tags in an ascending or descending order here.



- Point Kind: Indicates either a cell point or wifi point in which the phone connected to.
- Time Stamp: Time of connection.
- Coordinates: The geo-coordinates attached to the connection. This can be viewed on OxyMaps.
- Mac Address/Cell Info: Local information about the connection and device connected to.
- Accuracy: This is a (horizontal and vertical) variable attached to the geo-coordinates which will be displayed in feet.

The bottom of the grid:

- Here you will find a time filter where you can either use the sidebar or the calendar to filter to the date range you wish to select.
- You can change the view by either looking at the month, day, or hour.

The screenshot displays a data grid with the following columns: Point kind, Time stamp, Coordinates, MAC address / Cell info, Horizontal accuracy, and Vertical accuracy. The data rows show various WiFi and Cell points recorded between June 2012 and February 2013. At the bottom, a timeline view is active, showing a date range from Friday, June 29, 2012 to Monday, February 11, 2013. The timeline view includes a 'Group by' dropdown set to 'Day' and a bar chart representing the data distribution over time.

Point kind	Time stamp	Coordinates	MAC address / Cell info	Horizontal accuracy	Vertical accuracy
WiFi point	02/11/2013 07:31:09 AM		00:23:54:56:89:88		0.0000 ft
WiFi point	02/11/2013 07:31:09 AM	N 55.7362805, E 37.6937881	cc:5d:4e:d9:e9:4a	180.4550 ft	301.8520 ft
WiFi point	02/11/2013 07:31:09 AM	N 55.7363224, E 37.6930328	bc:ae:c5:c4:90:a8	147.6450 ft	301.8520 ft
WiFi point	02/11/2013 07:31:09 AM	N 55.7365427, E 37.6940774	cc:5d:4e:97:d7:f2	180.4550 ft	301.8520 ft
WiFi point	02/11/2013 07:31:09 AM	N 55.7364122, E 37.6957968	cc:5d:4e:98:6a:ac	164.0500 ft	301.8520 ft
Cell point	02/11/2013 07:31:09 AM	N 55.7363880, E 37.6894637	250:99:27651:11007	3192.4130 ft	246.0750 ft
WiFi point	02/11/2013 06:54:59 AM	N 55.7363288, E 37.6964830	f4:ec:38:fb:c9:56	902.2750 ft	285.4470 ft
WiFi point	02/11/2013 06:54:59 AM	N 55.7367413, E 37.6942150	20:10:7a:5f:9b:f4	472.4640 ft	285.4470 ft
WiFi point	02/11/2013 06:54:59 AM	N 55.7365704, E 37.6945420	20:10:7a:40:a1:58	164.0500 ft	301.8520 ft
WiFi point	02/11/2013 06:54:59 AM	N 55.7366939, E 37.6937750	54:04:a6:bc:3c:18	246.0750 ft	301.8520 ft
WiFi point	02/11/2013 06:54:59 AM	N 55.7369814, E 37.6941671	00:1c:f0:e3:66:07	147.6450 ft	301.8520 ft
WiFi point	02/11/2013 06:54:59 AM	N 55.7363615, E 37.6977489	14:da:e9:ba:36:5c	1013.8290 ft	285.4470 ft
WiFi point	02/11/2013 06:54:59 AM	N 55.7369597, E 37.6942302	90:f6:52:76:13:ae	830.0930 ft	285.4470 ft
WiFi point	02/11/2013 06:54:59 AM	N 55.7365810, E 37.6938242	00:25:9c:43:c8:bd	360.9100 ft	301.8520 ft
WiFi point	02/11/2013 06:54:59 AM	N 55.7364893, E 37.6943385	cc:5d:4e:50:16:28	147.6450 ft	301.8520 ft
Cell point	02/11/2013 06:54:59 AM	N 55.7363303, E 37.6916608	250:99:27650:57495288	2175.3030 ft	246.0750 ft
WiFi point	02/11/2013 06:54:44 AM	N 55.7368377, E 37.6941803	68:7f:74:0a:c9:99	147.6450 ft	301.8520 ft
WiFi point	02/11/2013 06:54:44 AM	N 55.7368562, E 37.6955988	0a:cf:30:4c:b3:20	895.7130 ft	285.4470 ft
WiFi point	01/30/2013 01:01:41 PM	N 55.7364740, E 37.6938614	20:10:7a:40:a4:56	147.6450 ft	301.8520 ft
WiFi point	01/30/2013 01:01:41 PM	N 55.7364265, E 37.6941679	20:10:7a:9c:2d:08	180.4550 ft	301.8520 ft
WiFi point	01/30/2013 01:01:41 PM	N 55.7367823, E 37.6938065	68:7f:74:37:0a:71	505.2740 ft	285.4470 ft
WiFi point	01/30/2013 01:01:41 PM	N 55.7367864, E 37.6931123	00:1b:11:30:4c:c0	652.9190 ft	285.4470 ft
WiFi point	01/29/2013 02:24:27 PM		be:b4:1a:5a:a5:ad		0.0000 ft
WiFi point	01/29/2013 02:24:27 PM	N 55.7364365, E 37.6958570	c8:60:00:e8:52:50	823.5310 ft	285.4470 ft
WiFi point	01/29/2013 02:24:27 PM	N 55.7364239, E 37.6949491	10:bf:48:d2:f3:80	147.6450 ft	301.8520 ft
WiFi point	01/29/2013 02:24:27 PM	N 55.7368877, E 37.6941587	00:1b:d4:2b:bc:c0	751.3490 ft	285.4470 ft
WiFi point	01/29/2013 02:24:27 PM	N 55.7365405, E 37.6943182	20:10:7a:40:b3:74	164.0500 ft	301.8520 ft



Column 3

Where: On the right-hand side of the section.

Uses: This is your details pane.

- Here, information will be unique to the event that you have selected on the grid (Column 2).
- On the bottom of this pane you will see the option to add the selected item as key evidence, add a tag, or a note.

>> Details

Source Wireless
Connections

Type Cell point

Time stamp 06/29/2012 10:52:50
(Fakaofu) PM (UTC+13)

Coordinates N 55.7598835, E
37.6446510

MAC address / 250:99:26625:32776

Cell info

Horizontal 1643.7810 ft
accuracy

Vertical 246.0750 ft
accuracy

Key Evidence Add tag Note

Oxygen Forensics
901 N. Pitt St, Suite 100
Alexandria, VA 22314
United States
+1 (877) 9-OXYGEN
+1 (877) 969-9436
+1 (703) 888-2327