

Forum:[Hack Forums](#)

Thread: [\[OpenSource\] WiFiSpy - A visual WiFi Network Analyzing Tool](#)

DragonHunter - March 23, 2015, 1:13 pm

Soo... it's been a while tbh that I've shared/uploaded something and thought I'd be a good time to release something again

This is something different that you've seen from me so far, as may know, I'm not only a coder in my free time ?

Ok so I've been looking for tools that would visualize the traffic for WiFi, like the stations connected to a Access Point, beacons etc... the good stuff

Couldn't find many tools out there so I simply gave it a shot myself to code it as I needed it aswell just for fun

So what does this tool do you ask ?

WiFiSpy is a WiFi Network Analyzing Tool that will show you cool information about your surroundings and more!

It's able to analyze from your surroundings how many devices are in your area, figure out if it's a Android, Mac, iPad, iPhone device etc

It will show you to which websites your target went to (hence the spying) aswell

It will steal your WiFi connection history, if you've connected to a "McDonald's Free Wifi" recently, this will show you if the device was

And there's alot more to come, at the moment I am focused at grabbing information from devices and such

This tool will be great if you're traveling a lot and are coming across a lot of Free Wifi networks

I need to dissappoint people, but this tool only works with Open Wifi's, no WPA/WEP etc, this is only for Open free Wifi's

But there are so many open wifi's in cities that this tool will make GREAT advantage

This tool will only analyze Cap Files, you need Airodump, Aircrack-ng to run yourself, google how to do these things as I will not help u with this

WiFi Spy

Stealing the WiFi History list

Watch their traffic & HTTP Locations/Websites

Source Code: <https://github.com/AnguisCaptor/WiFiSpy>

FeaturesGet a hourly overview of the Stations, (Hidden) Access Points

Get a weekly overview of the Unique stations and more

Access Point overview with how many were seen, is WPS enabled, how many are Hidden

Overview of all the stations (Including with filters)

View the traffic of every station

View all the WiFi Repeaters

View all the Access Points with all the stations connected to them

Live Capture from a linux machine using the Aircrack-Ng Suite (Live capture over the Internet is also possible)

Get information from a station: GPS coordinates, Device Type (Android, Apple... etc), Device Version, Last Seen at, Local IP Address(es), Probe List

CSV and GPX Formats for GPS is supported

Detect Rogue Access Points (will be shown in Red)

De-Cloak an Access Point to reveal it's real name if a station connected to it while listening for traffic

Get all the coordinates where a station was seen and convert it to a GPS KML extension file to view it in google maps

If I was not clear enough about some stuff, just post it or compile/run it for it to make sence ?

Convenience comes at a price, don't ever connect to Open Wifi Networks

Have a good 1 ?

Only3 - March 23, 2015, 1:24 pm

? u should call it wifi stealer its hf after all
good to have

Temploit - March 23, 2015, 2:01 pm

I actually really want to try this out now o.o Too bad there are no public networks around me now :!
You don't post a lot, but when you do it's more hq than 99% things posted in the last month. Great work! ?

btw: WiFiSpy/WiFiSpy/src/Packets/BeaconFreame.cs
You spelled Frame wrong :p

tyxik - March 23, 2015, 2:04 pm

(Mar 23, 2015 01:13 PM)DragonHunter Wrote: [\[CITE\]](#) I need to dissapoint people, but this tool only works with Open Wifi's,
what the fuck is this supposed 2 mean

DragonHunter - March 23, 2015, 2:28 pm

(Mar 23, 2015 02:01 PM)Temploit Wrote: [\[CITE\]](#) I actually really want to try this out now o.o Too bad there are no public networks around me now :!

You don't post a lot, but when you do it's more hq than 99% things posted in the last month. Great work! ?

btw: WiFiSpy/WiFiSpy/src/Packets/BeaconFrame.cs

You spelled Frame wrong :pOh lol thanks for noticing, fixed the spelling mistake and uploaded some missing libraries ?

FRANKIE - March 23, 2015, 2:32 pm

Could you not use this on your own network?

backshifted - March 23, 2015, 2:34 pm

(Mar 23, 2015 02:32 PM)FRANKIE Wrote: [\[CITE\]](#) Could you not use this on your own network? This works as long as you are connected (have access) to the network At least, it should.

DragonHunter - March 23, 2015, 2:41 pm

(Mar 23, 2015 02:34 PM)backshifted Wrote: [\[CITE\]](#) This works as long as you are connected (have access) to the network At least, it should.If you knew the tools I talked about in the thread, you would know that this does not require you to be on the same network
Hence again the name "Spy" in the tool heh :)

Snoweyes - March 23, 2015, 3:05 pm

Looks really cool! Gonna check this out tomorrow, thank you for sharing :)

GhostCode - March 23, 2015, 3:13 pm

Actually this is a very interesting and nice release.
I think you just motivated me to work on a small WEP key cracker tool :D
Mind if I ask how long you've been coding on that project?

DragonHunter - March 23, 2015, 3:18 pm

(Mar 23, 2015 03:13 PM)GhostCode Wrote: [\[CITE\]](#) Actually this is a very interesting and nice release.

I think you just motivated me to work on a small WEP key cracker tool :D
Mind if I ask how long you've been coding on that project?I think I've been working on it for like 2 week orso, just when I had time I worked on it really ?

backshifted - March 23, 2015, 3:38 pm

(Mar 23, 2015 02:41 PM)DragonHunter Wrote: [\[CITE\]](#) If you knew the tools I talked about in the thread, you would know that this does not require you to be on the same network
Hence again the name "Spy" in the tool heh :)
Hence the 'Access to' because without access to a network you're gonna have to bruteforce it baby and i don't think you are gonna do that just for a wifi spy :P

But if you do, great job man that is pretty neat

DragonHunter - March 24, 2015, 12:49 pm

(Mar 23, 2015 03:38 PM)backshifted Wrote: [\[CITE\]](#) Hence the 'Access to' because without access to a network you're gonna have to bruteforce it baby and i don't think you are gonna do that just for a wifi spy :P

But if you do, great job man that is pretty neatAirodump just does that stuff without needing to be on the network, just google it or whatever

Just committed a few updates, this will improve performance by ALOT if you're having +200MB cap

files ?

<https://github.com/AnguisCaptor/WiFiSpy/commit/79e7c2b71de39dfbfe6d479e97038a1cd03d6b6a>
<https://github.com/AnguisCaptor/WiFiSpy/commit/962522aaa40e20ad37568d36e679cbf4d3ca9454>

Ghostenigma - March 24, 2015, 2:59 pm

Good post op.Nice program.I will check this out

traczthefox - March 24, 2015, 4:08 pm

This looks awesome. does it only work on the network you are on network?

SIM-1456245 - March 28, 2015, 10:34 am

Looks great man, as always. I will give it a shot later.

Transporter007 - March 29, 2015, 12:12 pm

nice tool will be using for personal use.

DragonHunter - March 30, 2015, 11:31 am

Some updates since first initial release...

Increased the performance of loading overall
Fixed the OUI Parser for Mac Addresses to Names
DataFrame no longer copies Payload
Show the device version + Model, only Android is currently being supported
GPS csv Format Location Parser
You're now able to look at all the possible WiFi Repeaters
Small bugfix in PcapDevice
Check if WPS is enabled
Grab all the Station IP Addresses and show them in the station list

A preview of the WiFi Repeater update, it's aswell in the github

Sorry for such big images :P

0xDEAD10CC - March 31, 2015, 10:01 pm

So this doesn't capture anything it scans a cap file? Not bad, but it would've been better if it could do a realtime scan.

sk0rg3 - April 2, 2015, 11:58 am

i like alot :) cant wait to give this a try.
what language is this in??

woahxx - April 2, 2015, 1:03 pm

This is unbelievable cool. It's like Wireshark, thanks.

Ki?d?'s - April 3, 2015, 3:52 pm

You may want to blackout your wifi history if it is yours, as I was able to figure out a lot of personal stuff by it

DragonHunter - April 4, 2015, 3:20 am

(Apr 3, 2015 03:52 PM)Pr?stige Wrote: [\[CITE\]](#) You may want to blackout your wifi history if it is yours, as I was able to figure out a lot of personal stuff by itNo need to worry, this info was captured miles away from home ?

what do you mean by "personal stuff" ?

Ki?d?s - April 6, 2015, 4:42 am

(Apr 4, 2015 03:20 AM)DragonHunter Wrote: [\[CITE\]](#) No need to worry, this info was captured miles away from home ?

what do you mean by "personal stuff" ?

Well as I play the same sport as the person in the picture does I could make out that he spend time in a certain city and played a game at a certain club and some more stuff.

DragonHunter - April 14, 2015, 12:59 pm

Fixed a issue now where loading could take too long
And added a simple loading screen ;)

This feature only works if you're having GPS location logs:

Get the Station's GPS Location

Save the Station's GPS Location to a KML File

View the Longitude/Latitude of all station's

Dangerous Beef - April 16, 2015, 8:21 am

This is actually petty cool, great work. But sadly there aren't many open wifi networks where i live except for public places and airports. Which doesn't interest me.

But i have one question can the library you used be used to get the signal strength(dBA) from all networks like WPA ?

I'm on the lookout for a fast dBA "grabber" correct me if I'm wrong but i don't think this is hardware limited. And if it isn't possible can i edit my driver to allowed faster refresh rates.

I'm sorry if I'm way of base but this could be very useful for me.

DragonHunter - June 3, 2015, 1:30 pm

DHCP Reader & Device Name

<https://github.com/AnguisCaptor/WiFiSpy/commit/15d38a0d60fe7884d7a9c15512c3ccfed9469c4>

Reading some of the DHCP Traffic

Device Name will be shown, information is taken from the DHCP ?

Jopper - June 3, 2015, 9:23 pm

Nice to see you still working on this. I'm going to start contributing to this as well.

PureLifeCoding - June 3, 2015, 9:29 pm

Is there I way I could use this live?

I have been looking for something like this and it would be amazing if I could.

DragonHunter - June 4, 2015, 10:00 am

(Jun 3, 2015 09:23 PM)Jopper Wrote: [\[CITE\]](#) Nice to see you still working on this. I'm going to start contributing to this as well.Will be looking forward at your contributions, always appreciated ?

(Jun 3, 2015 09:29 PM)PureLifeCoding Wrote: [\[CITE\]](#) Is there I way I could use this live?

I have been looking for something like this and it would be amazing if I could.The only way I know where you could use it live is at linux, but you'd require wine etc...

And so far I know windows does not support Monitor Mode so well like linux does

I am running debian/ubuntu machines nearly daily, so I could take a look if I could make this compatible with linux (no promises tho) ?

PureLifeCoding - June 4, 2015, 1:27 pm

(Jun 4, 2015 10:00 AM)DragonHunter Wrote: [\[CITE\]](#) Will be looking forward at your contributions, always appreciated ?

The only way I know where you could use it live is at linux, but you'd require wine etc...
And so far I know windows does not support Monitor Mode so well like linux does

I am running debian/ubuntu machines nearly daily, so I could take a look if I could make this compatible with linux (no promises tho) ?
If you could make this work live I would love you!

DragonHunter - June 7, 2015, 5:31 am

(Jun 4, 2015 01:27 PM)PureLifeCoding Wrote: [\[CITE\]](#) If you could make this work live I would love you!! figured I wanted more love, so this is for you ?

Live Capture & DHCP Info

<https://github.com/AnguisCaptor/WiFiSpy/commit/c7b30dbc783cebd77288b63a03863fee0c56d62c>

Few changes to the DHCP Reader

Live capture is now possible, still underconstruction but the beginning is there

At the moment live capture is actually working, but not too much info about AP's/Traffic is being shown yet ?

To be able to start the live capture, we need to use a tool
At the linux machine called "AirServ-ng"

To install the aircrack-ng tool "apt-get install aircrack-ng"

To start the Wi-Fi dongle in monitor mode to capture live traffic
Where "wlan0" is, is your Wi-Fi dongle
sudo airmon-ng start wlan0

To start the AirServ-ng server
sudo aircrack-ng -d mon0 -v 1 -c 1

PureLifeCoding - June 7, 2015, 7:54 am

(Jun 7, 2015 05:31 AM)DragonHunter Wrote: [\[CITE\]](#) I figured I wanted more love, so this is for you ?

Live Capture & DHCP Info

<https://github.com/AnguisCaptor/WiFiSpy/commit/c7b30dbc783cebd77288b63a03863fee0c56d62c>

Few changes to the DHCP Reader

Live capture is now possible, still underconstruction but the beginning is there

At the moment live capture is actually working, but not too much info about AP's/Traffic is being shown yet ?

To be able to start the live capture, we need to use a tool
At the linux machine called "AirServ-ng"

To install the aircrack-ng tool "apt-get install aircrack-ng"

To start the Wi-Fi dongle in monitor mode to capture live traffic
Where "wlan0" is, is your Wi-Fi dongle
sudo airmon-ng start wlan0

To start the AirServ-ng server
sudo airserv-ng -d mon0 -v 1 -c 1
Holy shit bro. I love you! ???

afrite - June 14, 2015, 1:32 pm

that s cool tn timer i ll check it out

iLogic™ - June 15, 2015, 5:32 am

Great tool bro - thank you for releasing it ?

TheViewer - June 15, 2015, 5:35 am

What are the benefits of this tool, compared to kali linux?

cody8296 - June 15, 2015, 12:33 pm

This is pretty awesome, I love the simple GUI.

DragonHunter - June 18, 2015, 11:01 am

I made some good changes this time, the people who use this tool will like it :)

Commit,

<https://github.com/AnguisCaptor/WiFiSpy/commit/bfb9bf0a3413fb398986ba5838acef329fb62a94>

Improved loading time

Improved linking DataFrames to Stations

Fixed ram usage, does not use +2GB ram anymore

Few changes to the loading screen

Improved the AccessPoint view, it shows the Stations in the APs now aswell

Live capture is kindof broken in this commit, will fix soon

DragonHunter - June 22, 2015, 12:41 pm

De-Cloaking Access Points & GPX Parser & More...

<https://github.com/AnguisCaptor/WiFiSpy/commit/79d31166159aef4bf92fb1906c4f6ba13945c9b4>

De-Cloak hidden access points, needs more work though

Detect if access points could be dangerous by detecting if the AP could be a rogue

Possibly fixed UTC time in traffic (The time was off by hours)

GPX Gps Location Parser

Updated the OP with a feature list ?

Jopper - June 23, 2015, 6:18 pm

(Jun 15, 2015 05:35 AM)TheViewer Wrote: [\[CITE\]](#) What are the benefits of this tool, compared to kali linux?

I don't understand... Kali Linux is an operating system for pen. testing... This is a WiFi Network Analyzing Tool...

0xDEAD10CC - June 24, 2015, 2:18 pm

(Jun 24, 2015 01:32 PM)Odinz Wrote: [\[CITE\]](#) If you can't think of a connection between the two, I don't think pen-testing should be your thing. ?

You can find a connection quite easily at a very abstract and generalized level of understanding. However, his (valid) point was that this is a .NET program, and Kali is a Linux distro... How are they even closely related? Kali provides a bunch of pre-packaged utilities for analysis, and this is just a single program that does what it's meant to do...

?irito - *June 25, 2015, 9:25 pm*

hey i don't have enough posts to pm you. I would appreciate it if you could pm me and help me out with this. When I try to open it on my laptop (kali) then it says something like "Opening WiFi Spy" with wine but it never opens.

CodeAssassin - *July 6, 2015, 9:56 am*

Wow this is really cool, Thanks for all the effort that went into this. ^^

?irito - *July 7, 2015, 3:02 pm*

Hey do you think you could help me set this up? I have no idea what i'm doing >.<

-ExCeL- - *July 8, 2015, 1:27 pm*

Extremely nice. I'll try it out soon.

OP, can you throw another post onto the WiFi section of HF for this tool? I just found this by chance.

samir5000 - *June 20, 2016, 8:09 am*

Thanks for the release. I am curious what i can do with it.