**Questions About WiFi-Sniffer**

## What is a WiFi Access Point?

WiFi Access Point or AP for short is a mode over the WiFi chip that gives It router capabilities. i.e. stations\clients can connect to it and receive access through it.

This is a SW mode not a device.

Not all WiFi chips\drivers support this mode the Raspberry-Pi chip\driver does – that is one of the reasons it was selected.

There are 3 modes that should be of interest to you:

1. AP mode – the device acts as a router - according to configuration a network will be available on the Air and devices can connect to it
2. Station mode (managed) – the device acts as a client it can scan for APs and connect to them as well as receive an IP and get network access services
3. monitor mode – the device can monitor the traffic in the air but not participate (i.e. does not connect to an AP nor does it provide a network for devices to connect to)

suggested reading:

<https://en.wikipedia.org/wiki/Monitor_mode>

<https://askubuntu.com/questions/512926/how-to-configure-wifi-adaptor-to-monitor-mode>

<https://null-byte.wonderhowto.com/how-to/enable-monitor-mode-packet-injection-raspberry-pi-0189378/>

## Do we get any tools from your company for the project? For example the Raspberry Pi

TandemG will provide you with the HW, But you need to know exactly what you want – and it should be a part of your design document (see last section [Guidelines](#_toc54)) – after you understand what and how you want to do write a section detailing what you need, and we will provide

## Why is the Host PC needed? From our experience the Raspberry Pi can perform all of the actions needed.

The main idea of the project is to provide a device that works out of the box for any developer. Due to the way that the developer works there is a need for the data to be accessible by the developers workstation (developer workstation == host PC) According to item 1.4.1 in the requirements document – one can see the reason for the choice, i.e. shared responsibility between the host PC and the raspberry PI

* the RPI responsibility is to capture network traffic
* host PC responsibility is to analyze the traffic using a standard tool – in this case Wireshark

the concept behind this is that the device can be connected to both Linux based systems with Wireshark (which has the plugin installed) or a windows based system with Wireshark (again with plugin)

as for the statement that the RPI can also handle the analysis – it is true, But consider the device output where is the data displayed?

* Screen – let’s assume that you are running a GUI on the RPI and connecting keyboard and mouse to it – all the development will be done on the RPI however the usage is compromised, a developer usually uses a lot of other tools and since a standalone RPI is not connected to the developers PC there will be a need to develop a communication mechanism between the devices in order to transfer the data   
  NOTE; as far as development goes you will still need to write a plugin for Wireshark so not much is gained
* on host-PC, the RPI analyzes the packets and then transfers the analyzed data to the host – in this case you will need to write an application for the host to receive and display the data according to the requirements ( coloring, filtering etc.) which will probably require a great amount of work

As far as we are concerned the analyzed data must be displayed and available on a host-PC (that is a requirement) what type of work is done on each device is in your hands (of course after we decided it together)

## Does the Raspberry Pi need to be connected to the AP? Should the AP be aware that the Raspberry Pi is connected to it?

Well, there isn’t a simple answer to the question and this is something that we need to discover during the research stage of the project.

* In order to monitor traffic there usually no need to connect to the remote AP (farAP) – the device can just listen to traffic over the air and analyze the message headers to receive some data about the message
* data is usually encrypted between AP and station so there are limitations on what can be received without connecting to the network(AP)

one issue that should be resolved – and we would like your comments on this – is exactly that

* what data can be received without connecting to the network(AP)?
* What added data can be received while connected to the AP?
* If message data can be viewed\analyzed in either case (data encryption)?

NOTE: the question is: “Should the RPI be connected to the far-AP or not?” - to clarify a device cannot connect to a far-AP without the far-AP ‘knowing’

## How do we copy network traffic without being connected to it?

A combination of monitor mode and Wireshark – that is one of the main targets of the project

## Do we need to use the Man In the Middle method?

In order to fulfill all the requirements perhaps – but then of course the issue of ethics comes in to play.  
I will state that we do NOT intend to create a hacking device but we do want to get the most data possible within the ethical realm

you are expected to – outline what data is available And what isn’t – if you think that a man-in-the-middle will provide extra data, we are open to discuss what that means in the ethical perspective – and should it be implemnted

## We never worked with an AP, how do we use it?

See my e-mail from yesterday and the answer to the first question

## We never implemented a network through USB, we would like some guidance regarding it.

There are many ways to move data over USB – for each type of data we can match a solution – however as of now to data scheme was not defined so it is hard to match a specific solution  
I would suggest that you will define what data should be transferred between the devices and I will then help you find what SW elements should be used to implement that data transfer scheme

## Guidelines

I am aware that the task seems a bit daunting at the moment and there are a lot of unknowns that might make the task look too big to handle,

remember we are not asking you to be a keyboard-jockey (a term used to describe a programmer that just writs code that somebody else wrote) we want you to think as developers – which means that most of the work that needs to be done on the task is answering the big questions – so a lot of reading and research is coming your way

to help with breaking it down I wish to share with you how a developer should go about these types of tasks

1. first and always document – from the very first thing you do – write it down, that helps keeping the thinking process focused
2. break down – you can learn everything you need online, but if you don’t know what you're looking for you can’t find anything
3. schematics – draw a block-diagram of what you wish to accomplish
   1. for each block write what tasks it should perform
   2. try and understand what are you missing in order to make that block do what you wish
   3. research that issue, try different codes from the internet until you understand what should work – it can be done on either a PC at home school\work computer or an RPI the idea is not to solve the issue but to understand what can solve it? And which solution is better\worse
4. write down a design document
   1. this is how developers do it, and so should you
   2. the document must include a block diagram
   3. a detail of what should each element perform
   4. a section detailing what is still unknown and suggestion for solving it.   
      For example:   
       we are not sure if the device should or shouldn't be connected to the far-AP  
       if it is unconnected we can get A B C  
       if it is connected we can also get D E but F will not work as well  
      now, this can be discussed and together we shall decide what to do from there
   5. wait with RPI – when going about these kind of developmental task, wait with working on HW\SW start with understanding what you wish to do – when that is covered you will find it is much easier to write the code \ activate the HW