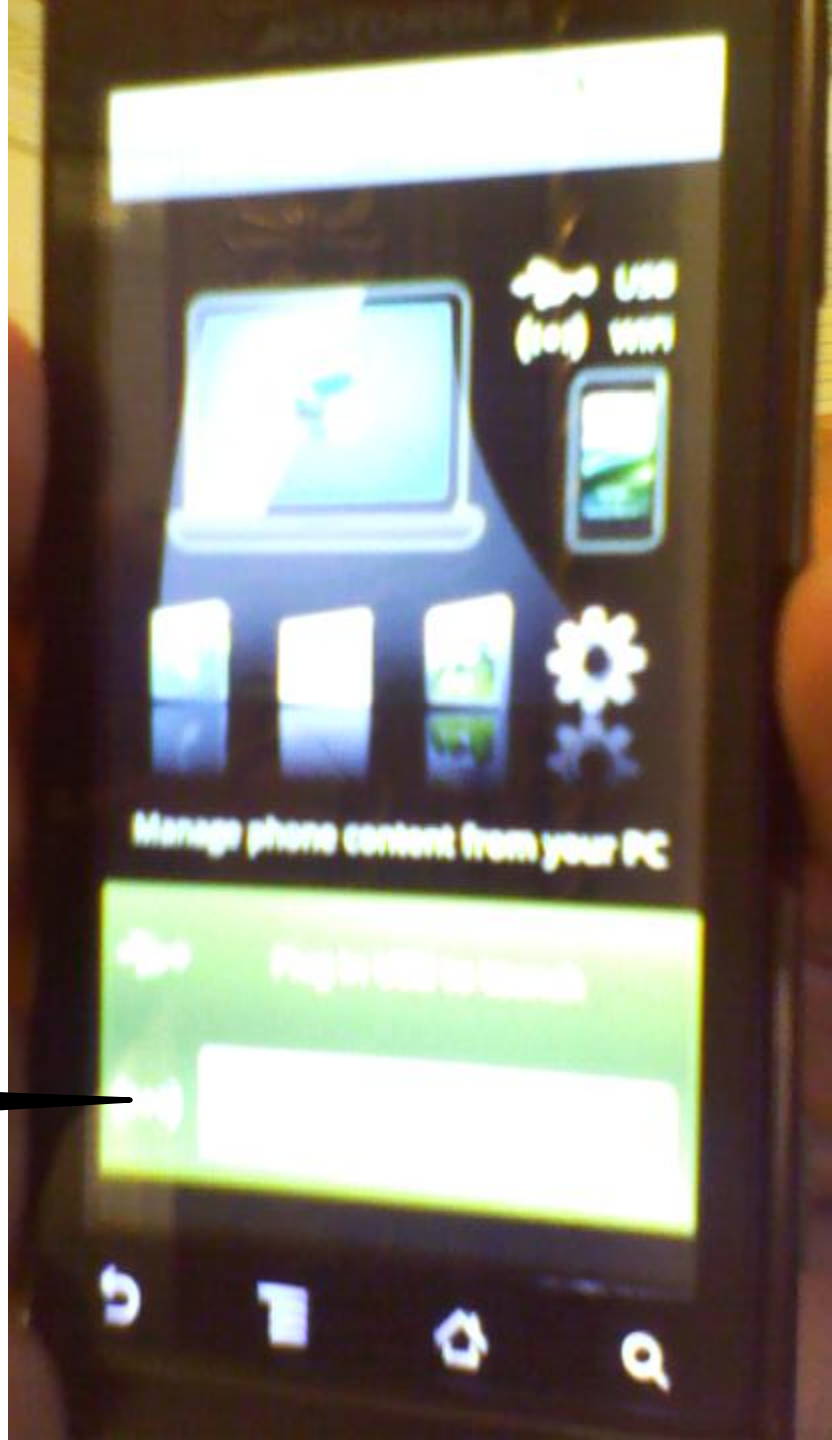
Phone Security Case Study

- Milestone
  - Motorolla / Android phone
- Can be controlled from your computer
- from any web browser
- The phone does run a web server

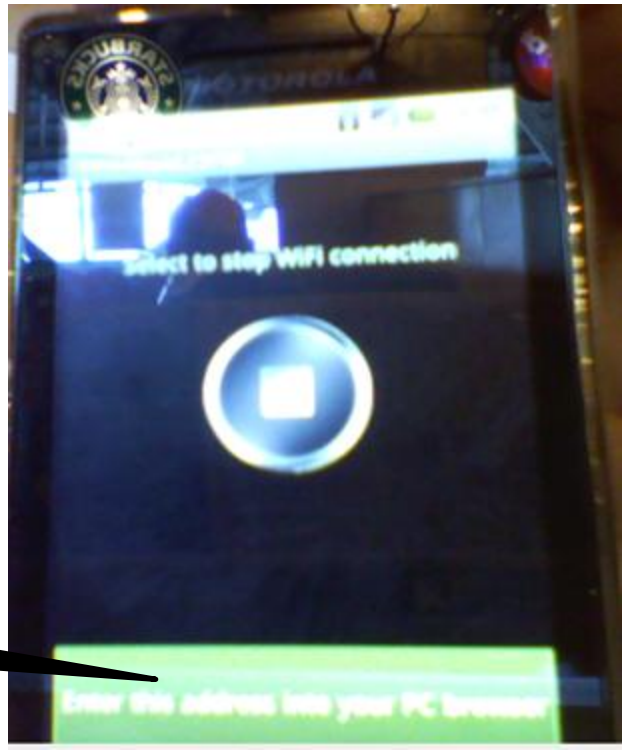
From the Phone

- Enable service over wifi!



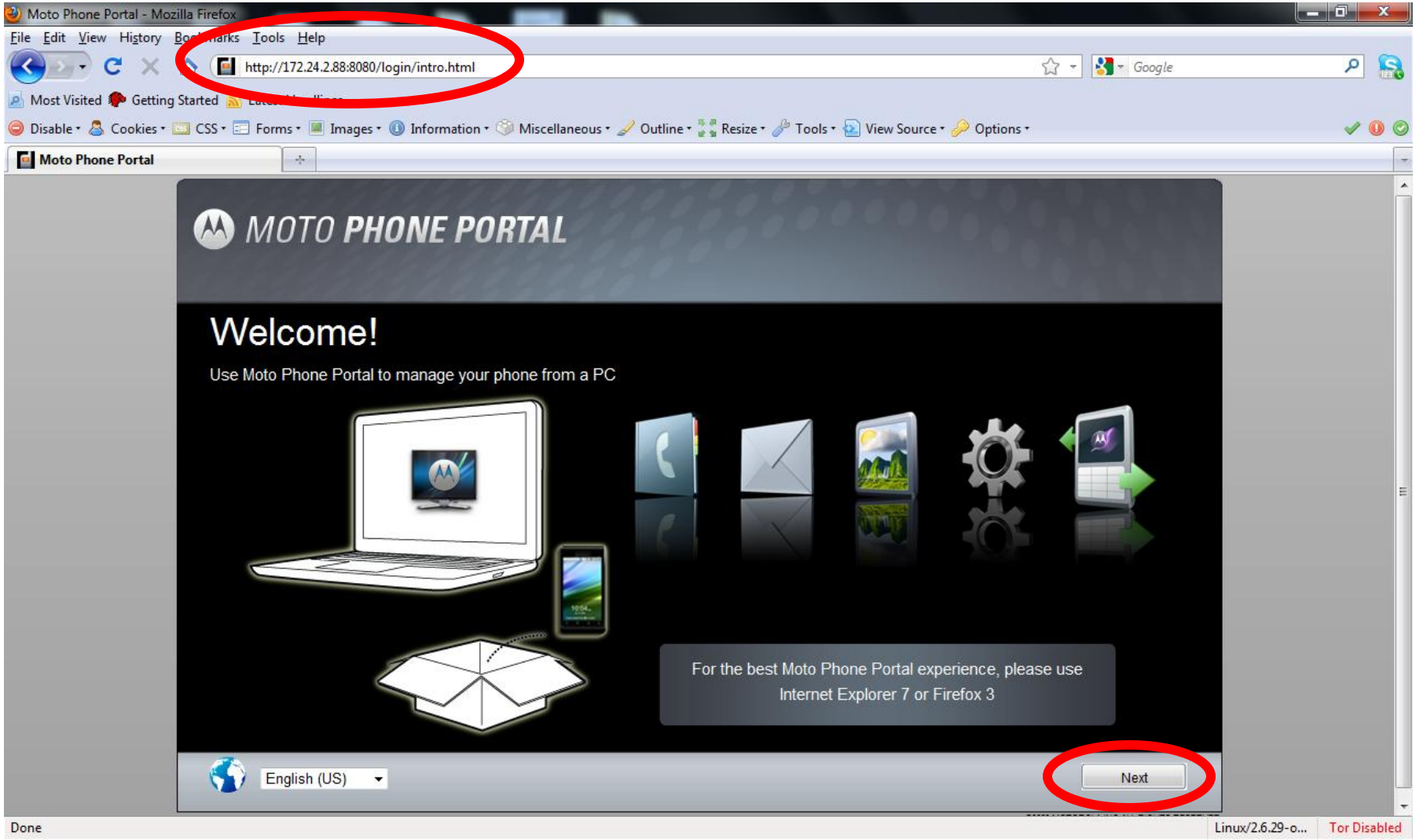
Connect with WIFI

- Message telling you how to access your phone from anywhere in the connected word!

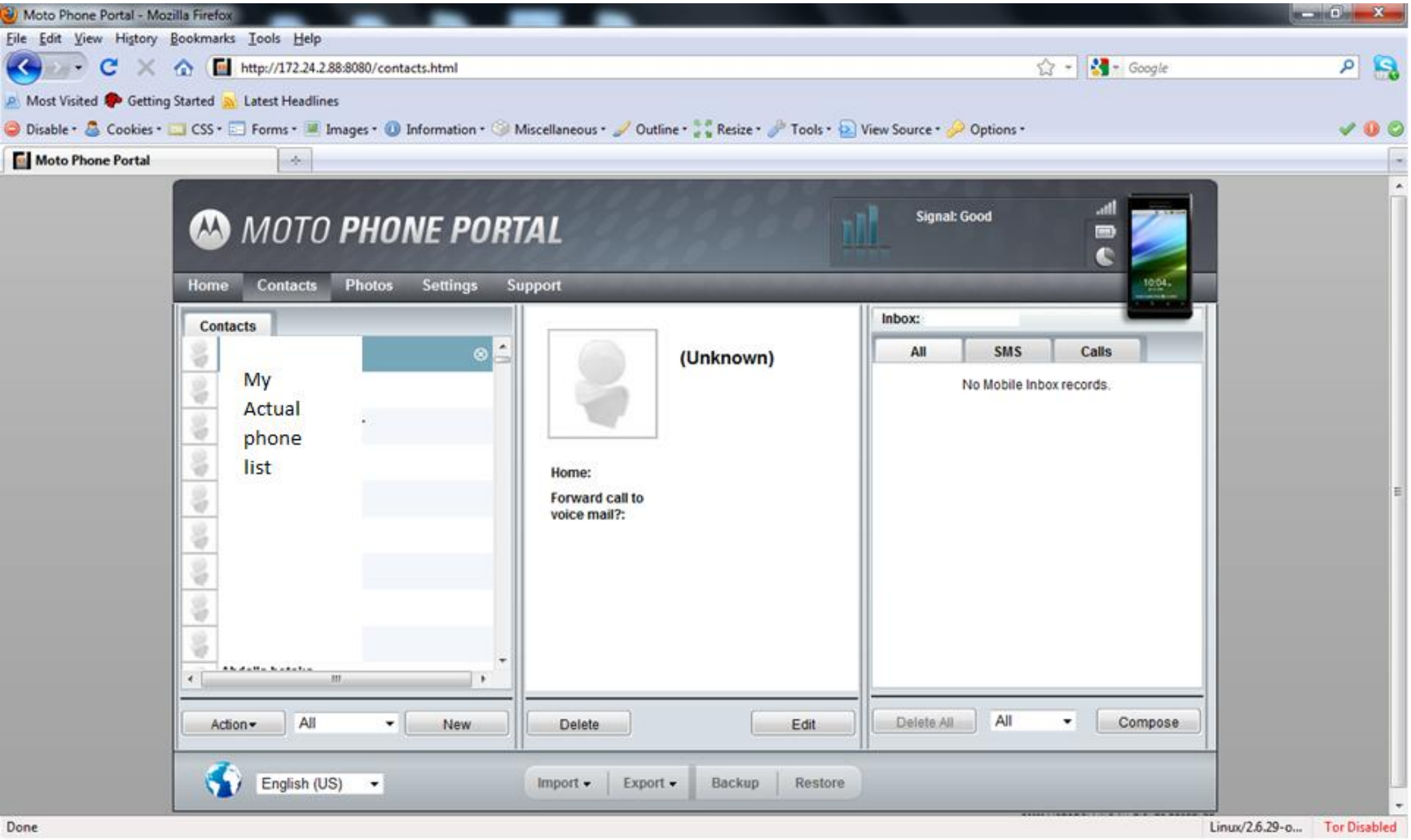


Type
http://172.24.2.88:8080/
In your PC browser

- Type in the URL and you'll get the page below
- Then hit next

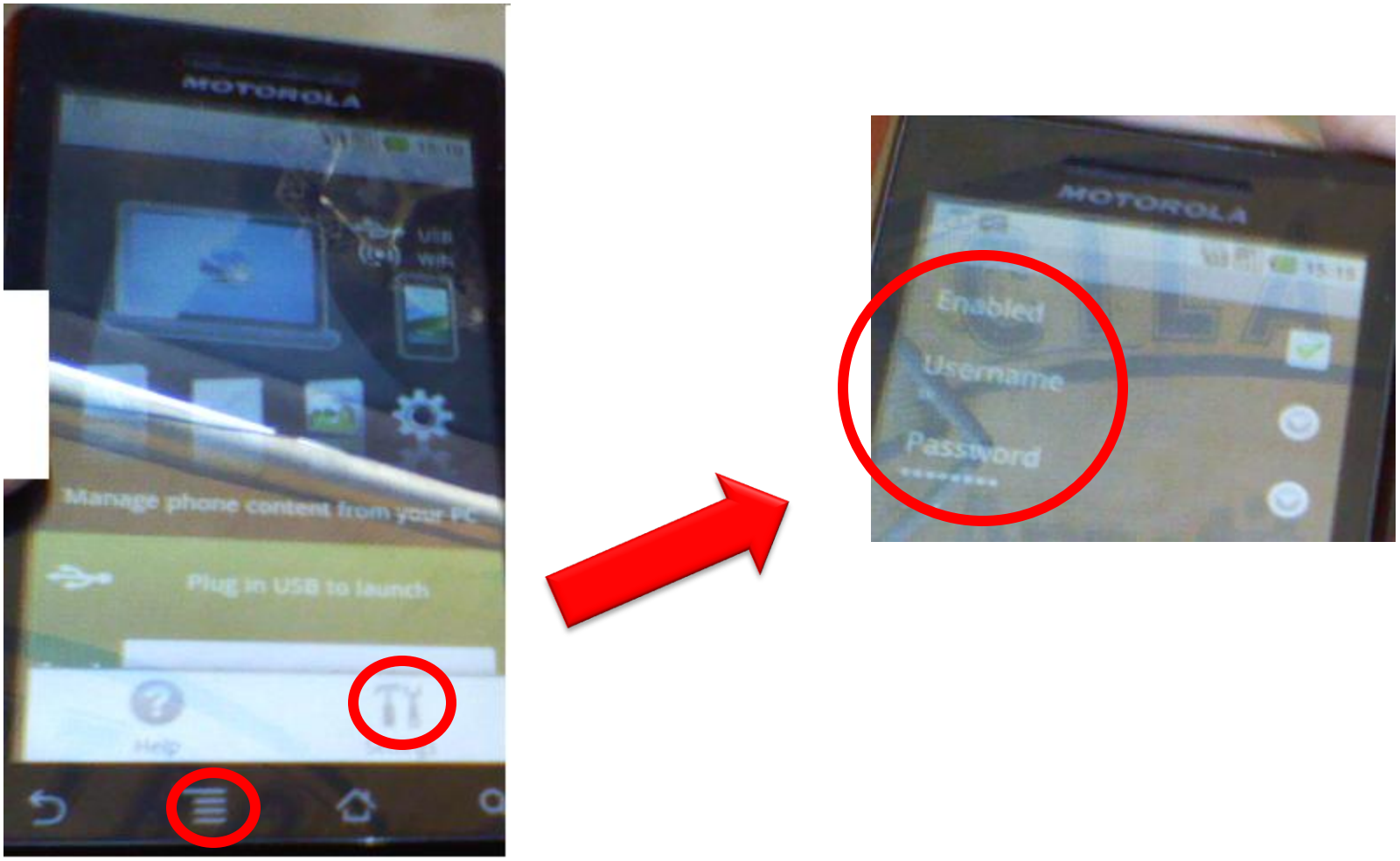


- Now you'll get access to phone functions

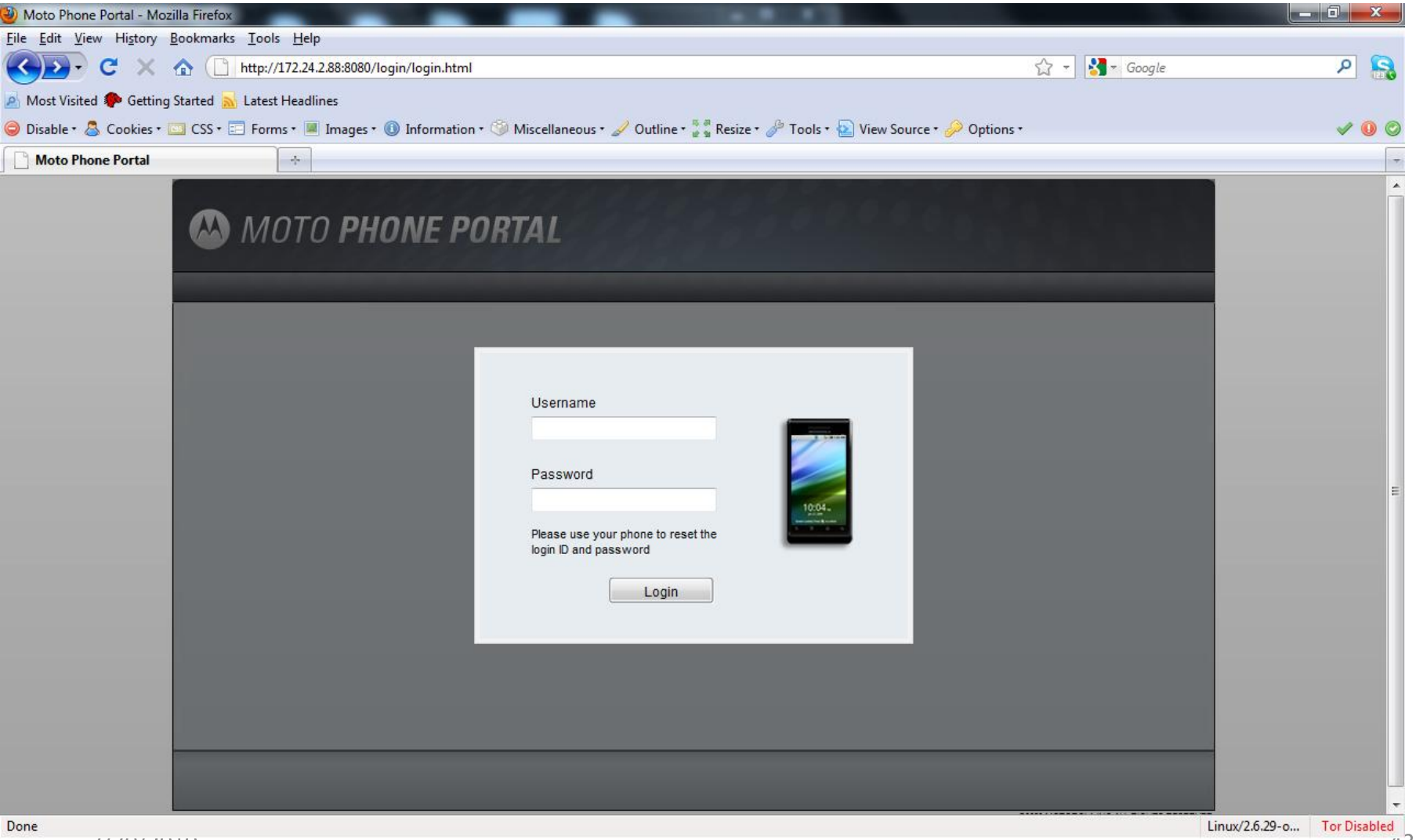


- Notice:
  - It didn’t ask for a password!
  - There is no authentication
  - Not such a great default
    - What might work for the USB cable doesn’t seem right for wifi!

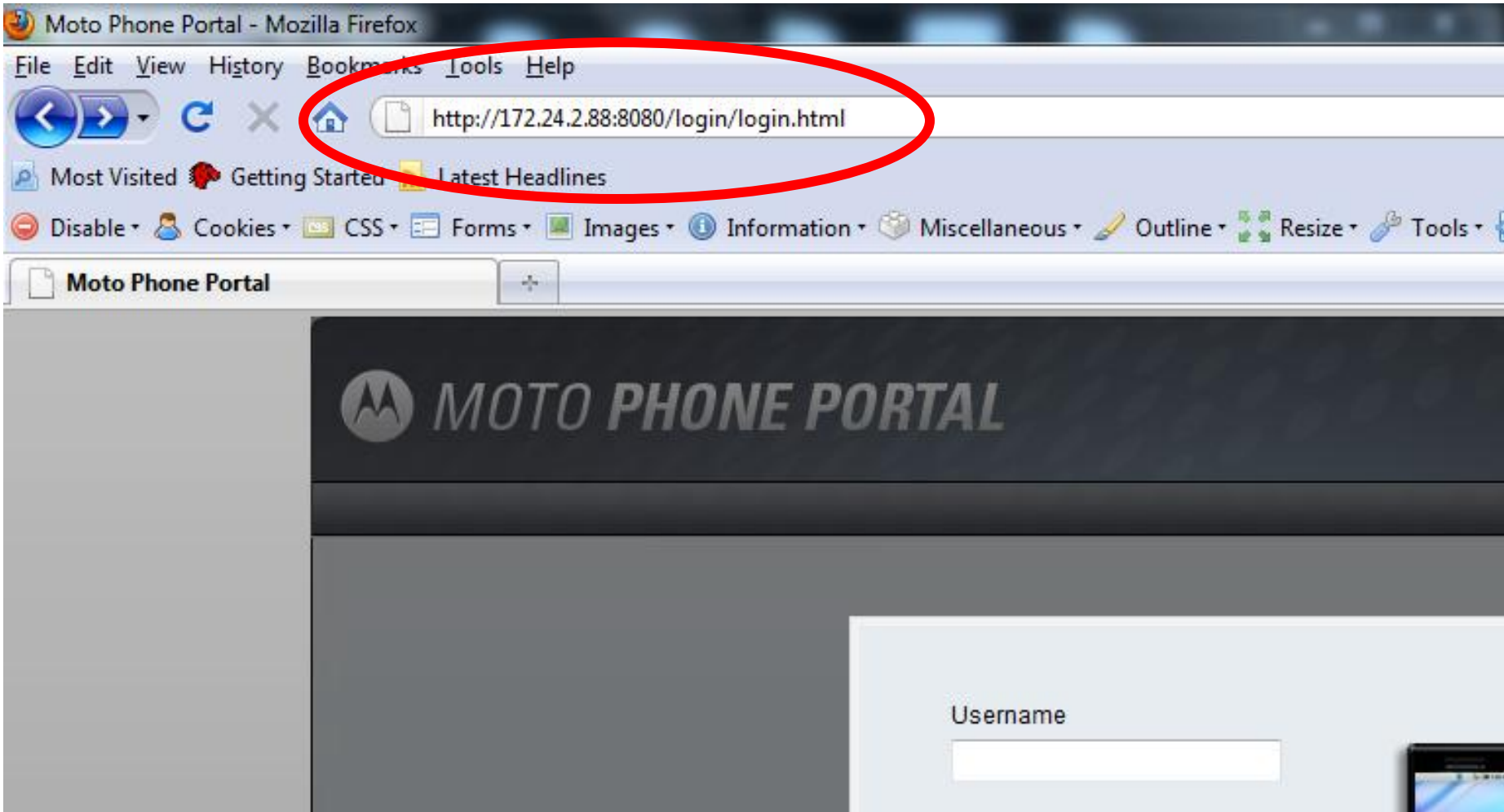
- Configure it properly
- Add Secure username and password



- Much better!

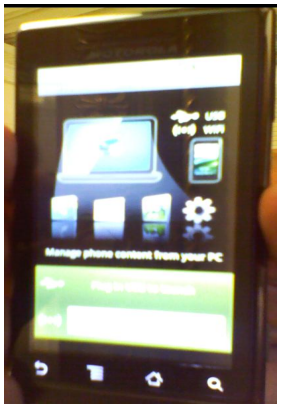

Moto Phone Portal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://172.24.2.88:8080/login/login.html
Google
Most Visited Getting Started Latest Headlines
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
Moto Phone Portal
MOTO PHONE PORTAL
Username
Password
Please use your phone to reset the login ID and password
Login
Done
Linux/2.6.29-o...
Tor Disabled

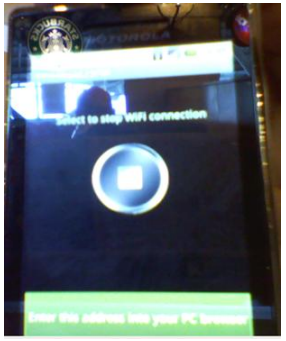
- but wait
- No SSL/TLS
- How can this be a secure password!



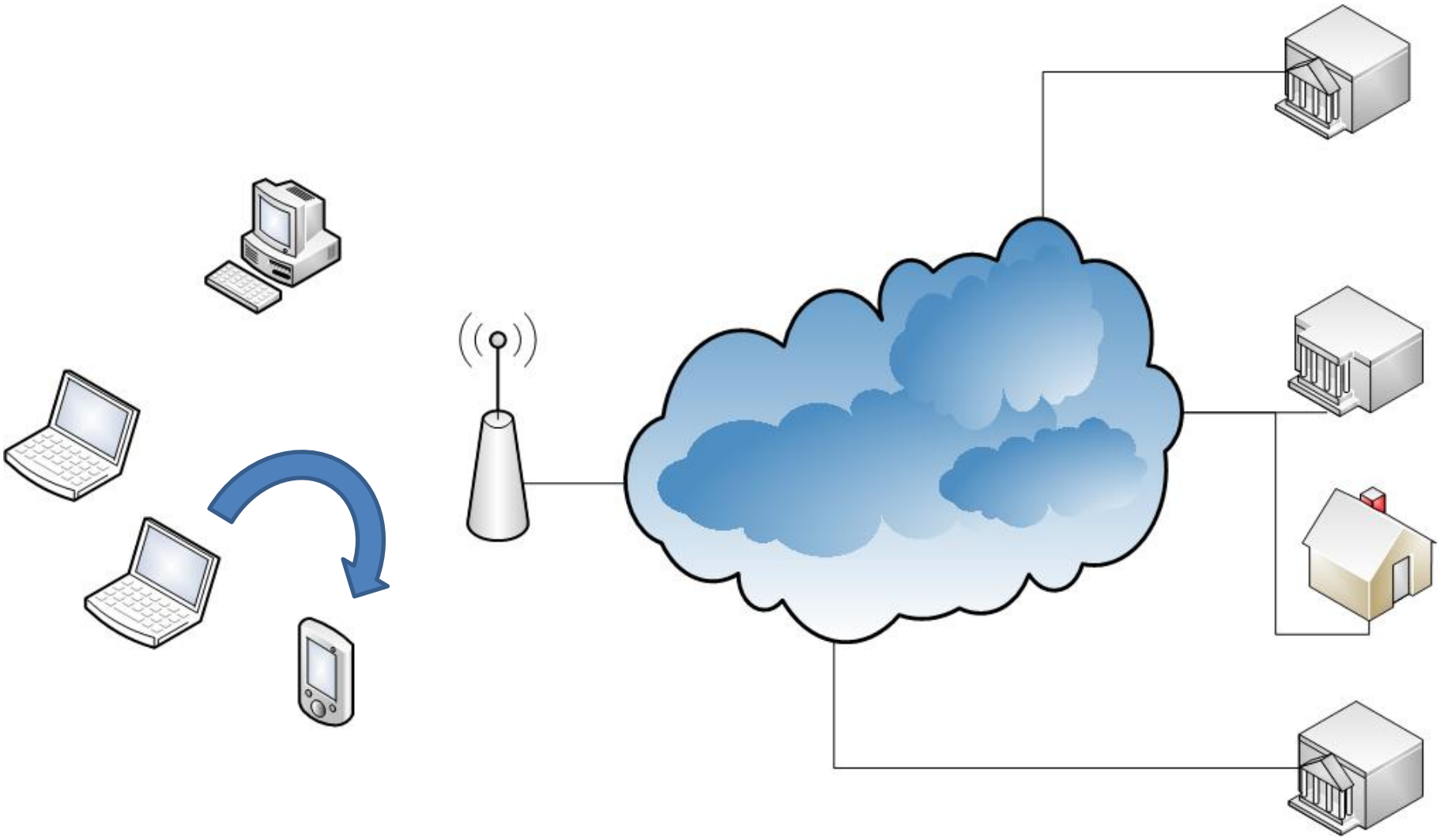
the attack

- In the coffee shop and decide to use phone's portal feature

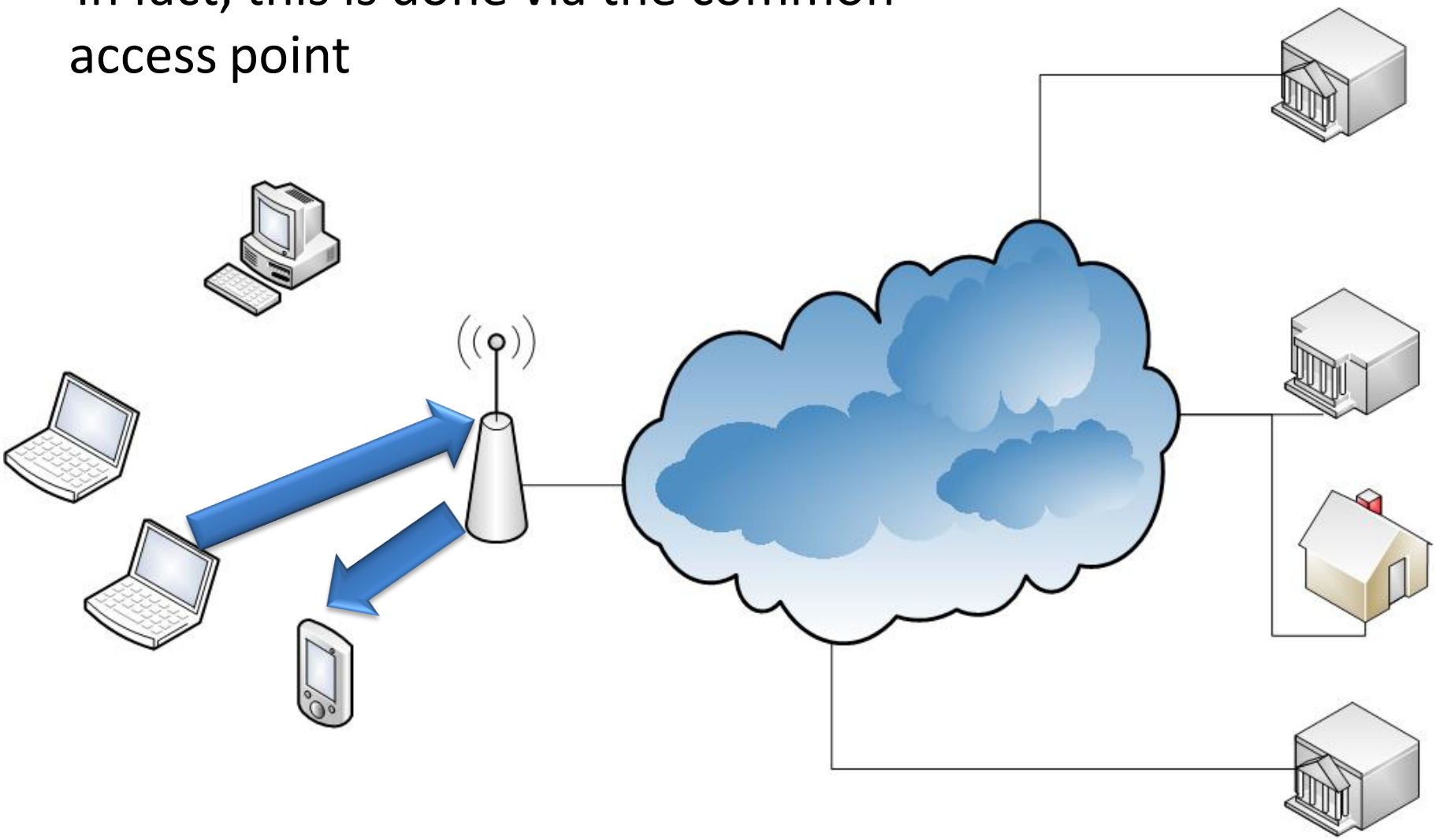




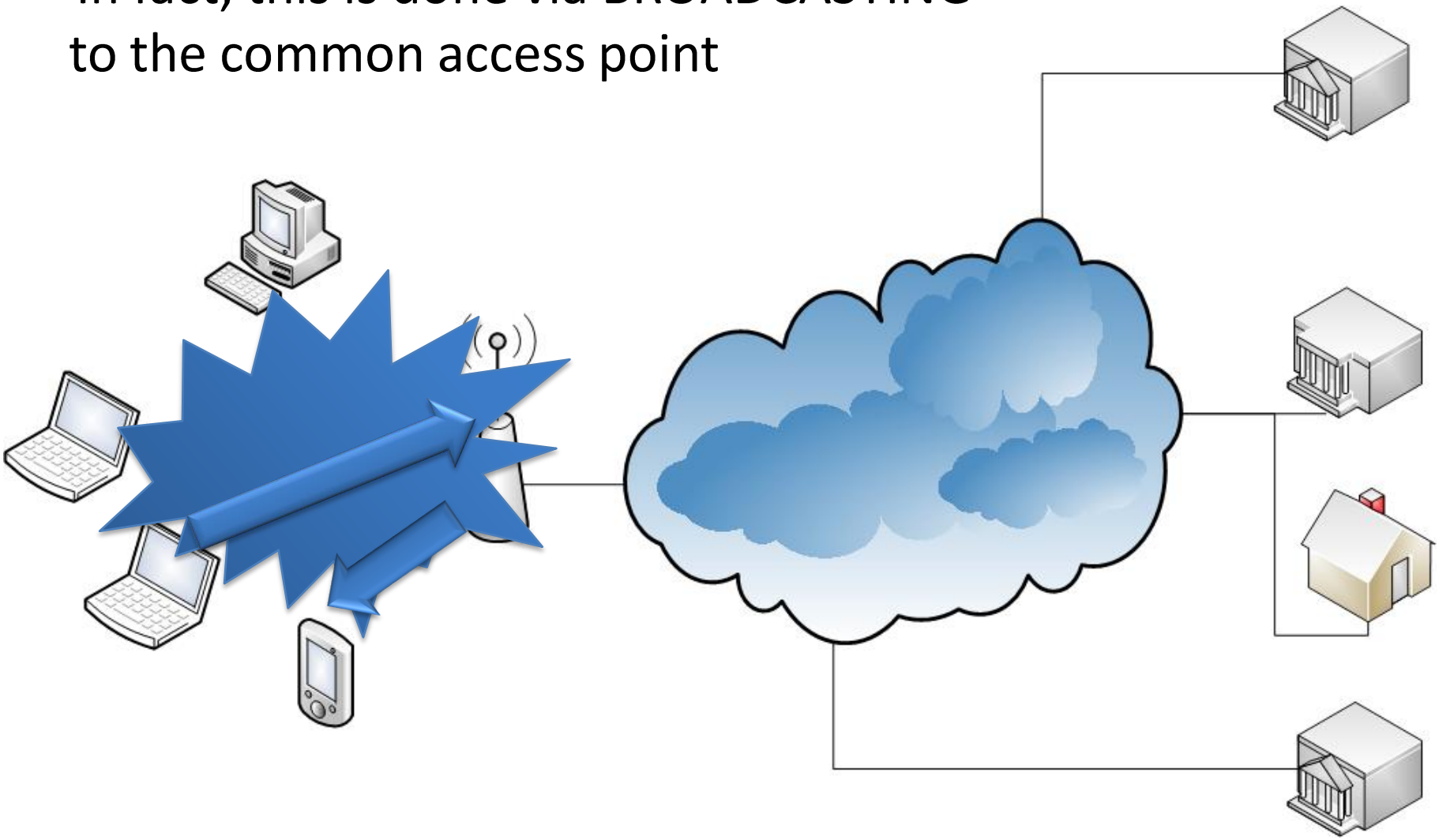
- It might seem that the computer is connecting to the phone directly



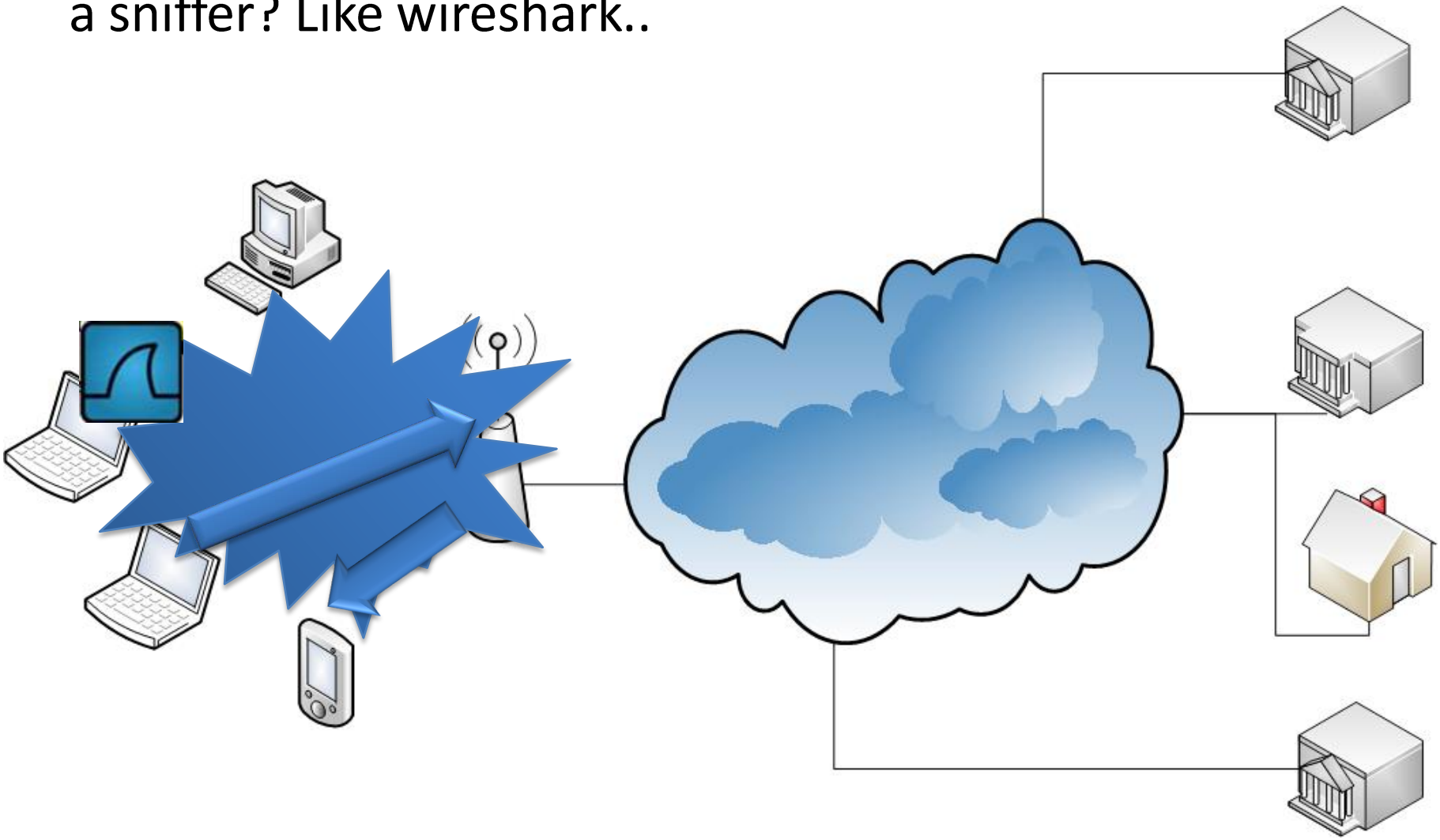
- In fact, this is done via the common access point



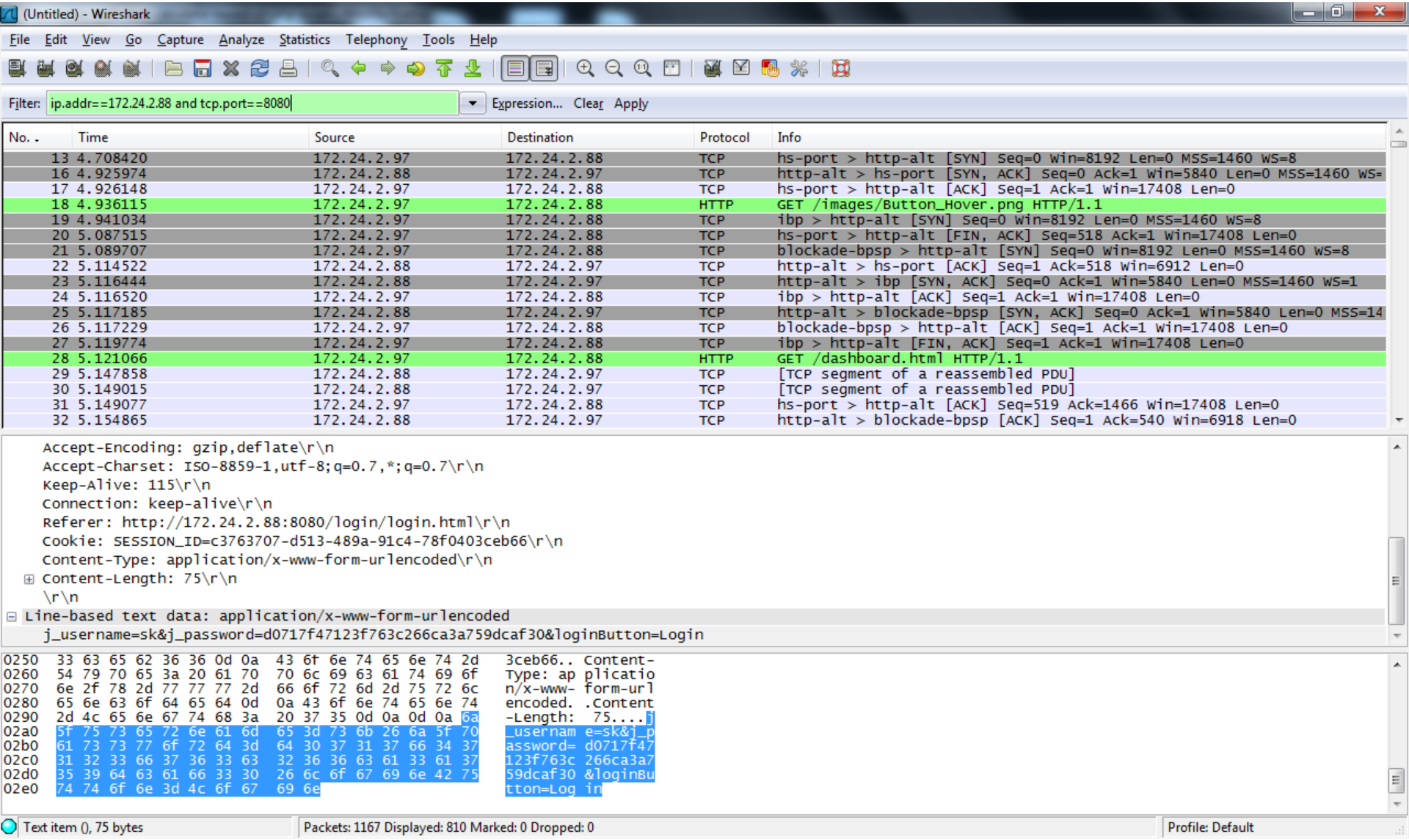
- In fact, this is done via BROADCASTING to the common access point



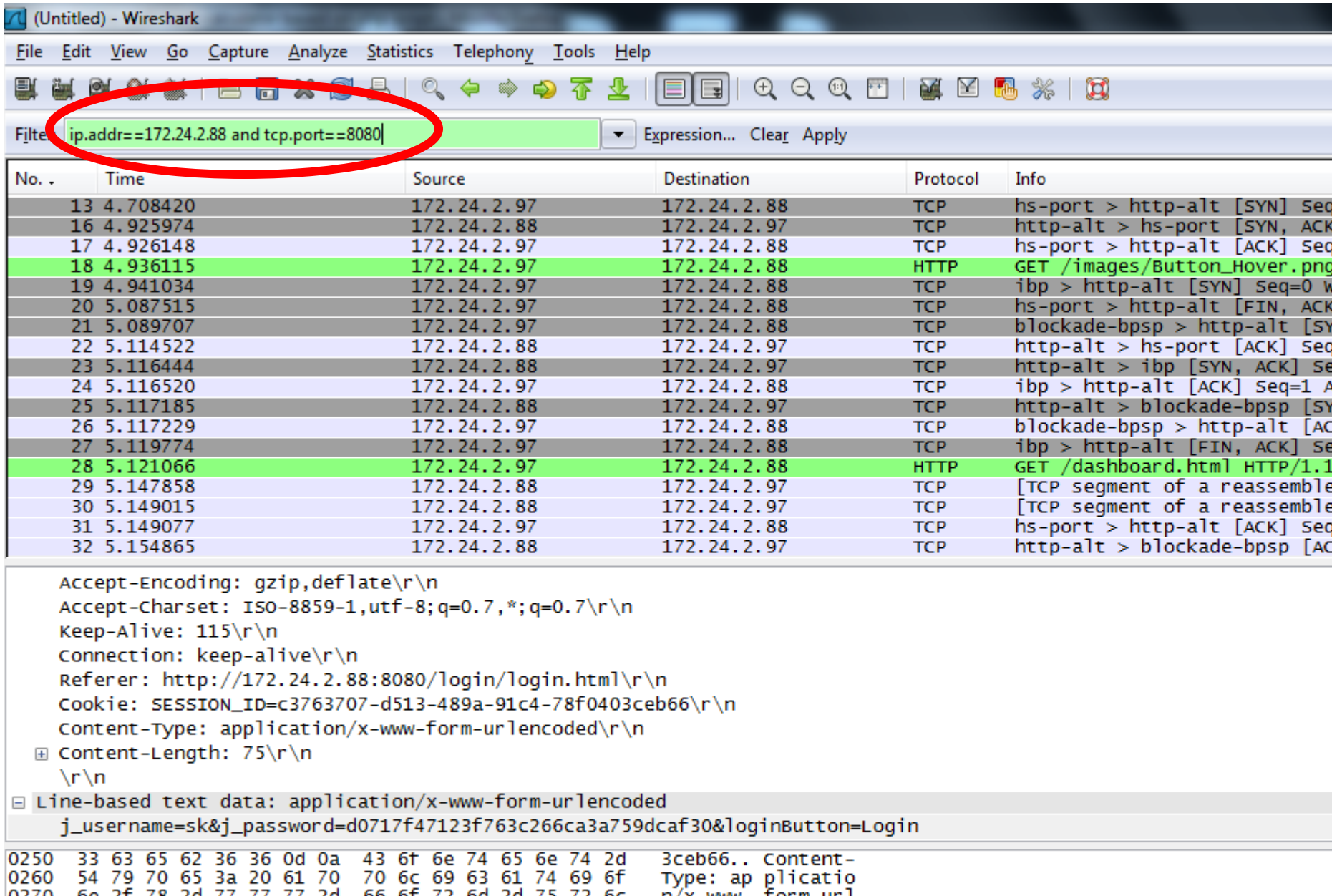
- What if someone happens to be running a sniffer? Like wireshark..



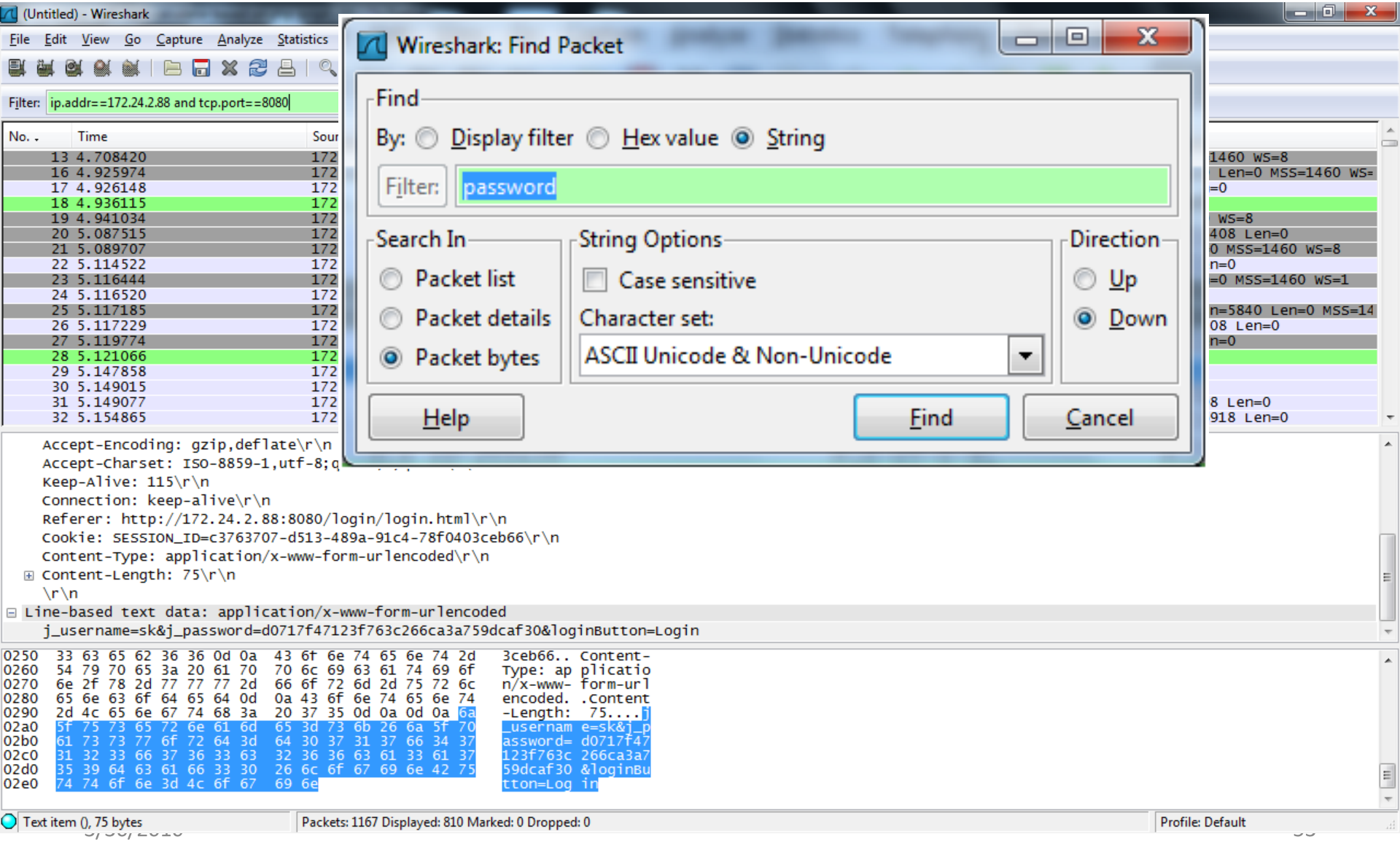
- they'd be getting a copy of all the traffic
- and they can read the contents



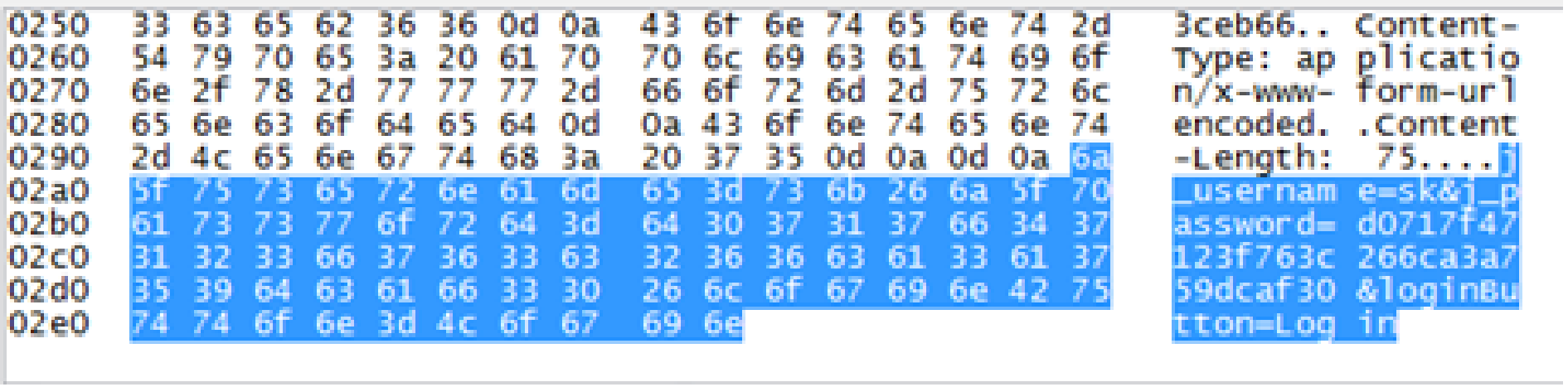
- Say they single out the phone connection



- Or just search for a common word. Like:
  password



- They'd get something like:



```
0250  33 63 65 62 36 36 0d 0a  43 6f 6e 74 65 6e 74 2d   3ceb66.. Content-
0260  54 79 70 65 3a 20 61 70  70 6c 69 63 61 74 69 6f   Type: ap plicatio
0270  6e 2f 78 2d 77 77 77 2d  66 6f 72 6d 2d 75 72 6c   n/x-www- form-url
0280  65 6e 63 6f 64 65 64 0d  0a 43 6f 6e 74 65 6e 74   encoded. .Content
0290  2d 4c 65 6e 67 74 68 3a  20 37 35 0d 0a 0d 0a 6a   -Length:  75....j
02a0  5f 75 73 65 72 6e 61 6d  65 3d 73 6b 26 6a 5f 70   _usernam e=sk&j_p
02b0  61 73 73 77 6f 72 64 3d  64 30 37 31 37 66 34 37   assword= d0717f47
02c0  31 32 33 66 37 36 33 63  32 36 36 63 61 33 61 37   123f763c 266ca3a7
02d0  35 39 64 63 61 66 33 30  26 6c 6f 67 69 6e 42 75   59dcaf30 &loginBu
02e0  74 74 6f 6e 3d 4c 6f 67  69 6e                    tton=Log in
```

- Which contains:

`j_username=` **sk**

`j_password=` **d0717f47123f763c266ca3a759dcaf30**

- But that's not so bad is it?
- Looks like the password is Encrypted?

- Or is it just hashed?
- MD5 maybe?

- a quick “view source” finds:

```
function encodePassword(a){var b=$.md5(a);return b}
```

- So the attacker won’t find the password.
- But does it matter?
- The PC browser send the hashed password to the phone.
- The attacker has the hashed password.
- The attacker can send the hashed password to the phone.

FYI

```
MD5(“soso”)= d0717f47123f763c266ca3a759dcaf30
```

Conclusion

- Do not run a web server on your phone unless you know what you're doing!
- What works for a cable might not work for wifi:
  - Context matters!
- Security is difficult
- Scrutiny is essential