

Phone Security Case Study

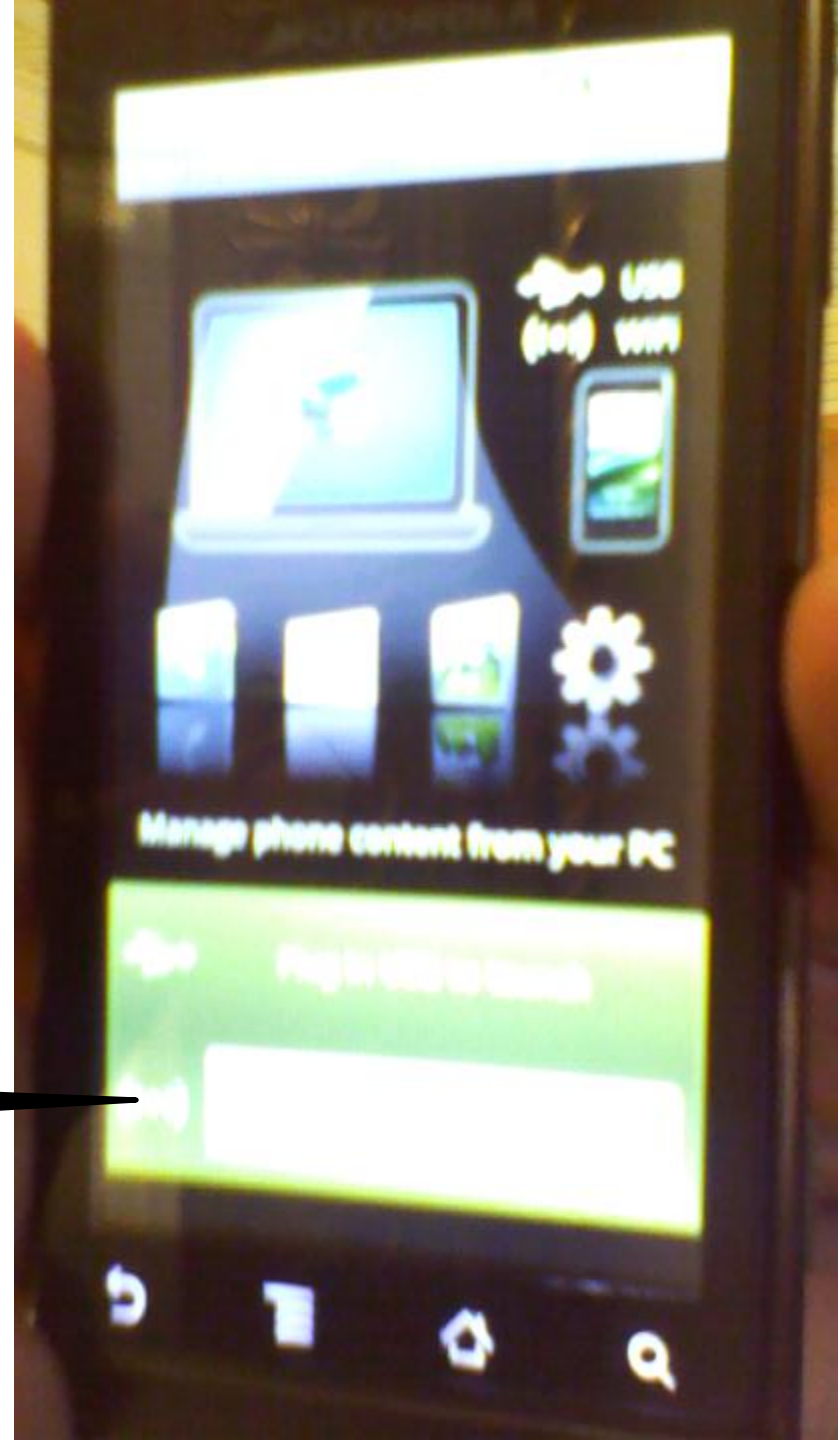
- Milestone
 - Motorola / Android phone
- Can be controlled from your computer
- from any web browser
- The phone does run a web server



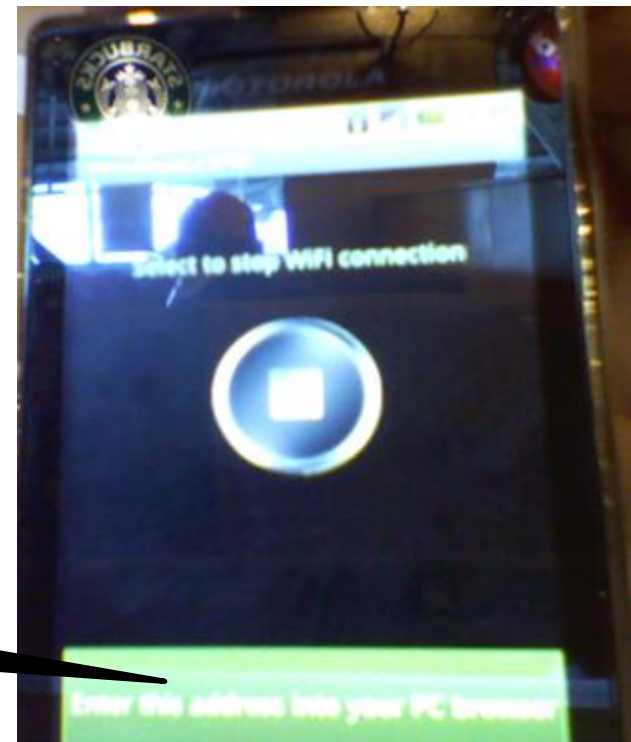
From the Phone

- Enable service over wifi!

Connect with WIFI



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

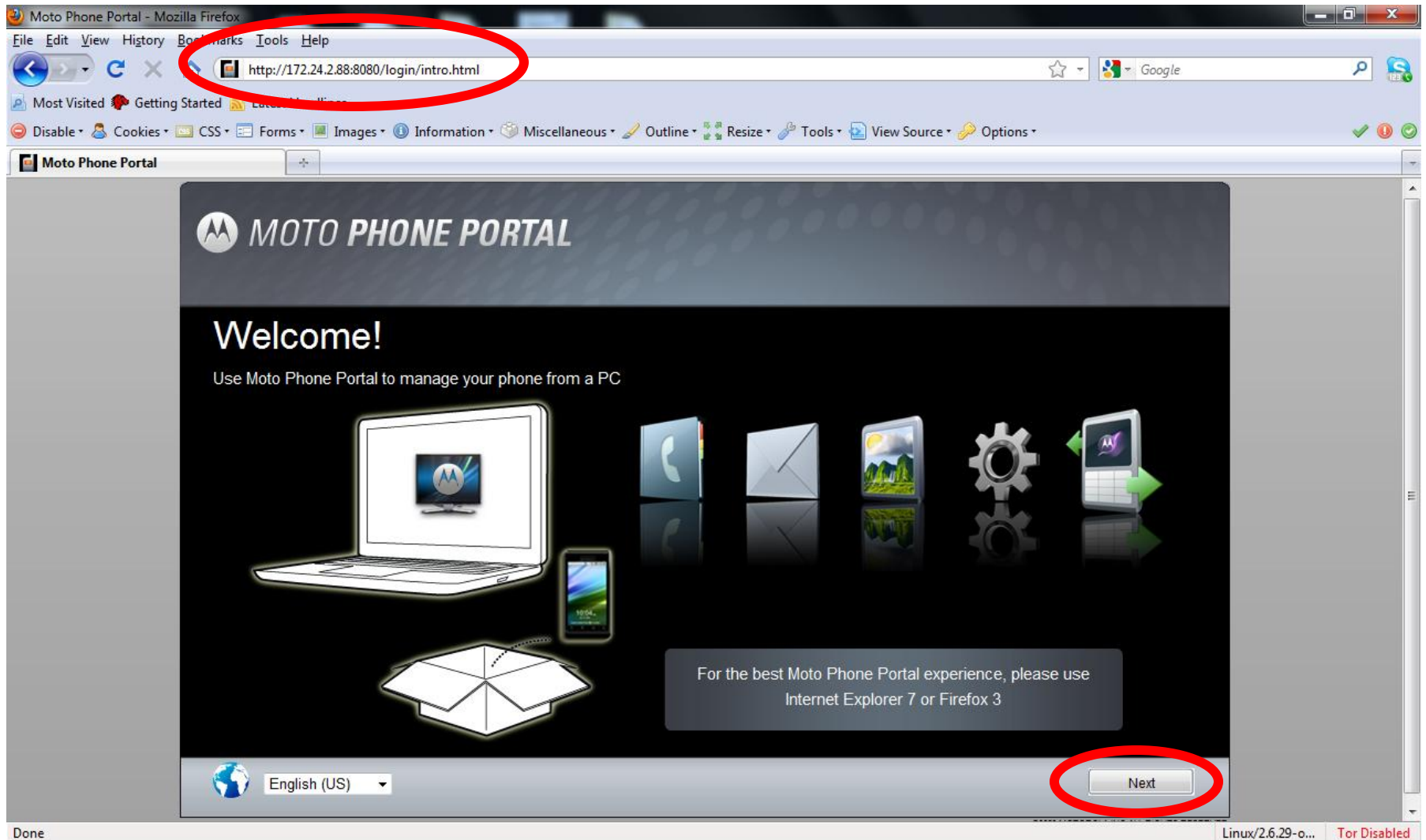


Type

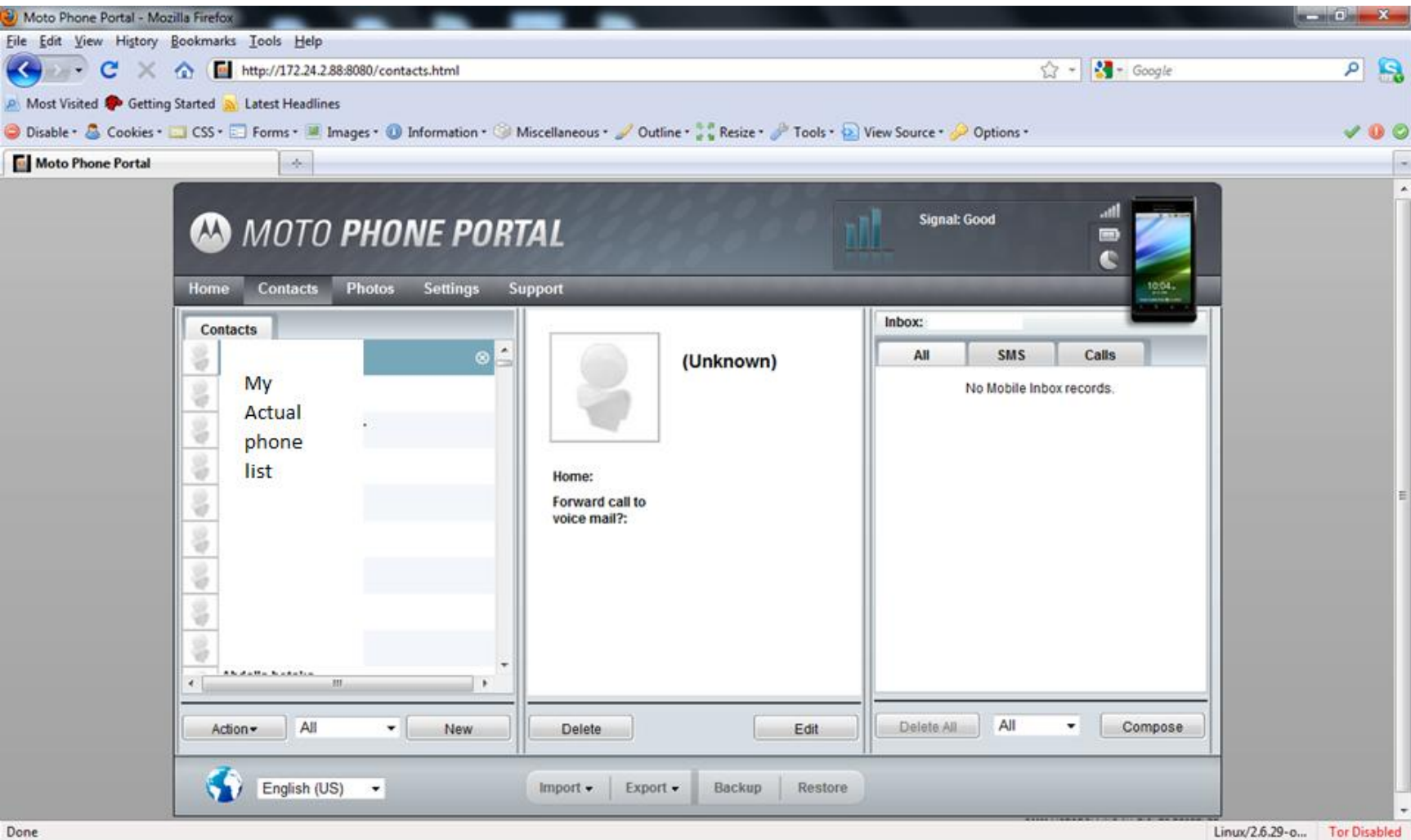
<http://172.24.2.88:8080/>

In your PC browser

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

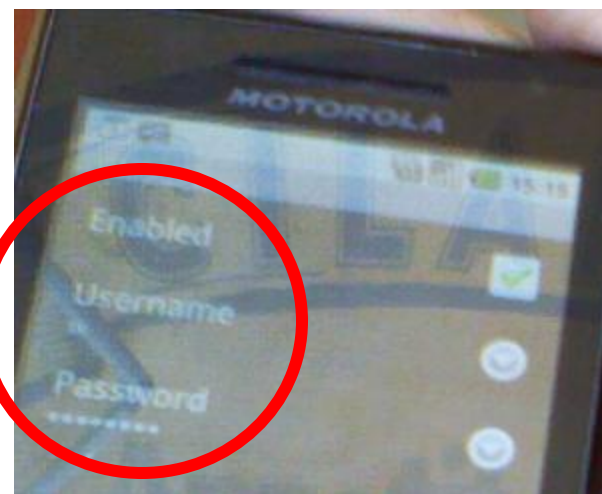
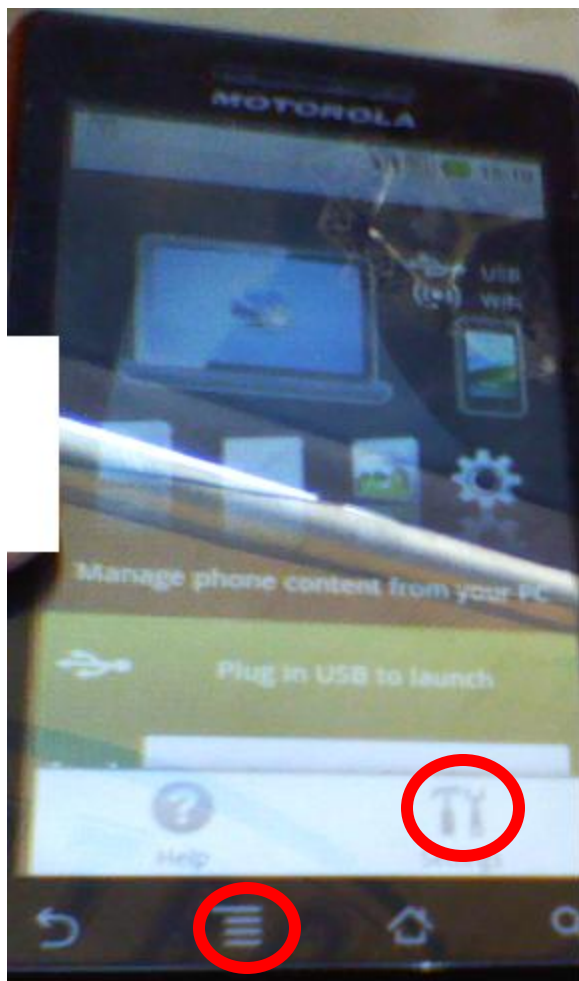


- Now you'll get access to phone functions

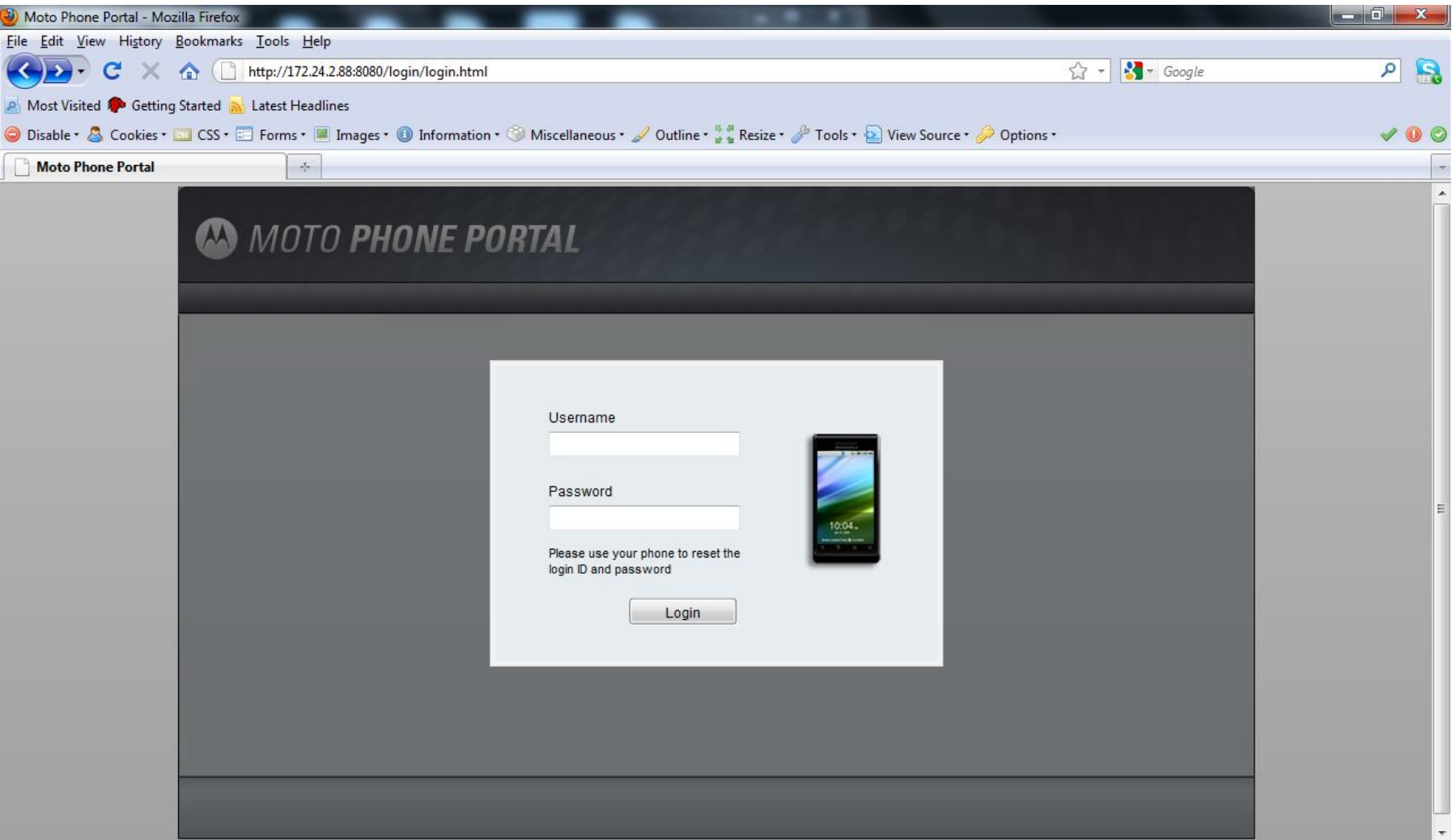


- Notice:
 - It didn't ask for a password!
 - There is no authentication
 - Not such a great default
 - What might work for the USB cable doesn't seem right for wifi!

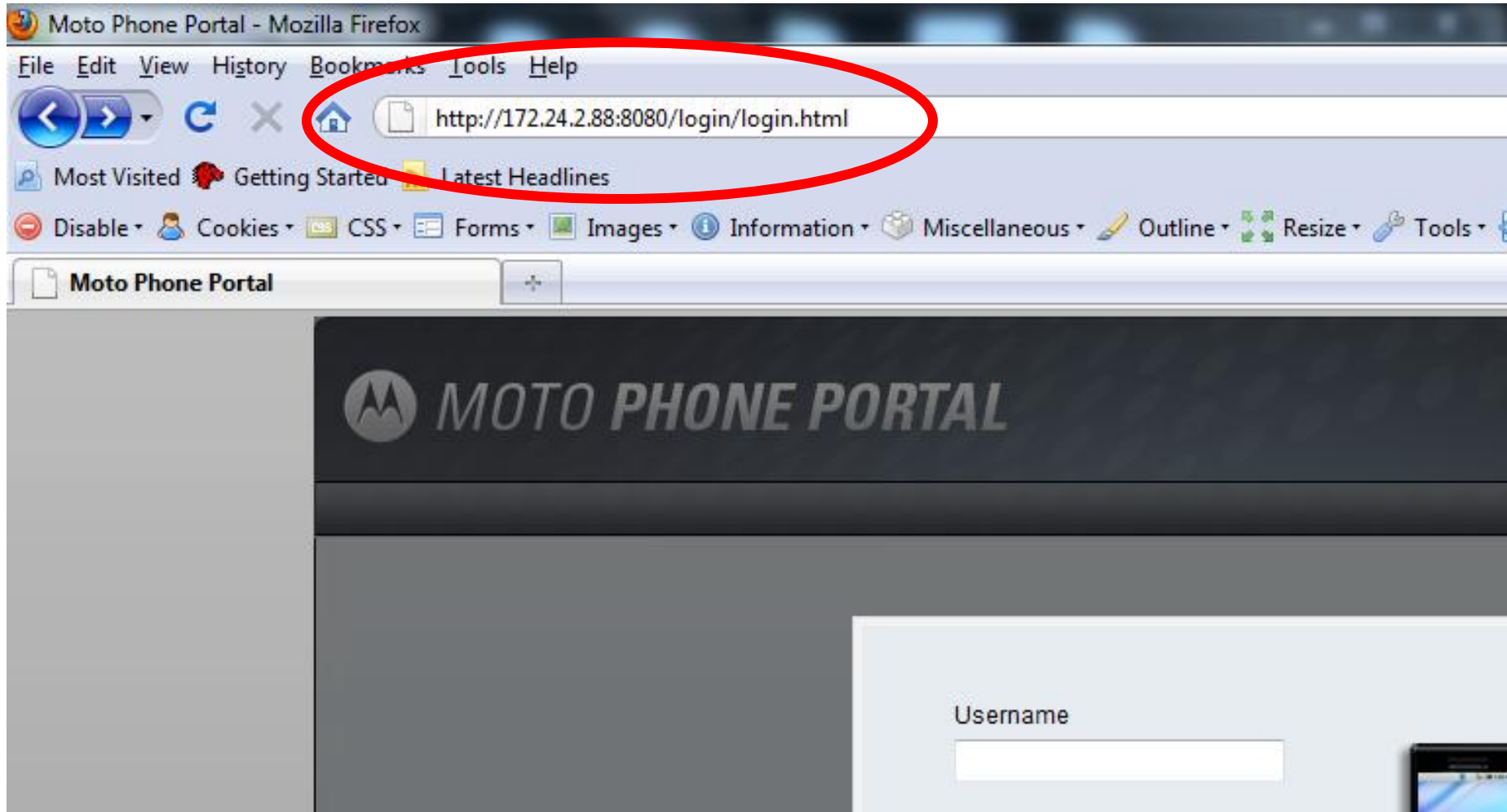
- Configure it properly
- Add Secure username and password



- Much better!

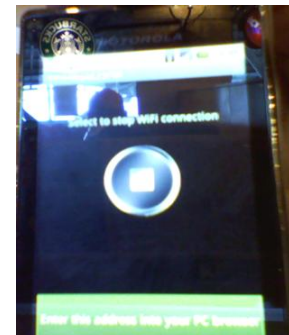
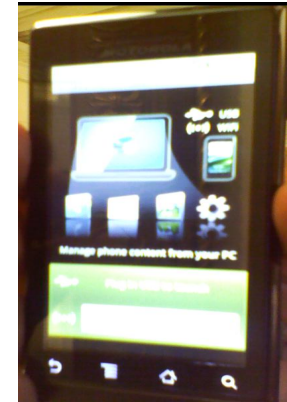


- but wait
- No SSL/TLS
- How can this be a secure password!

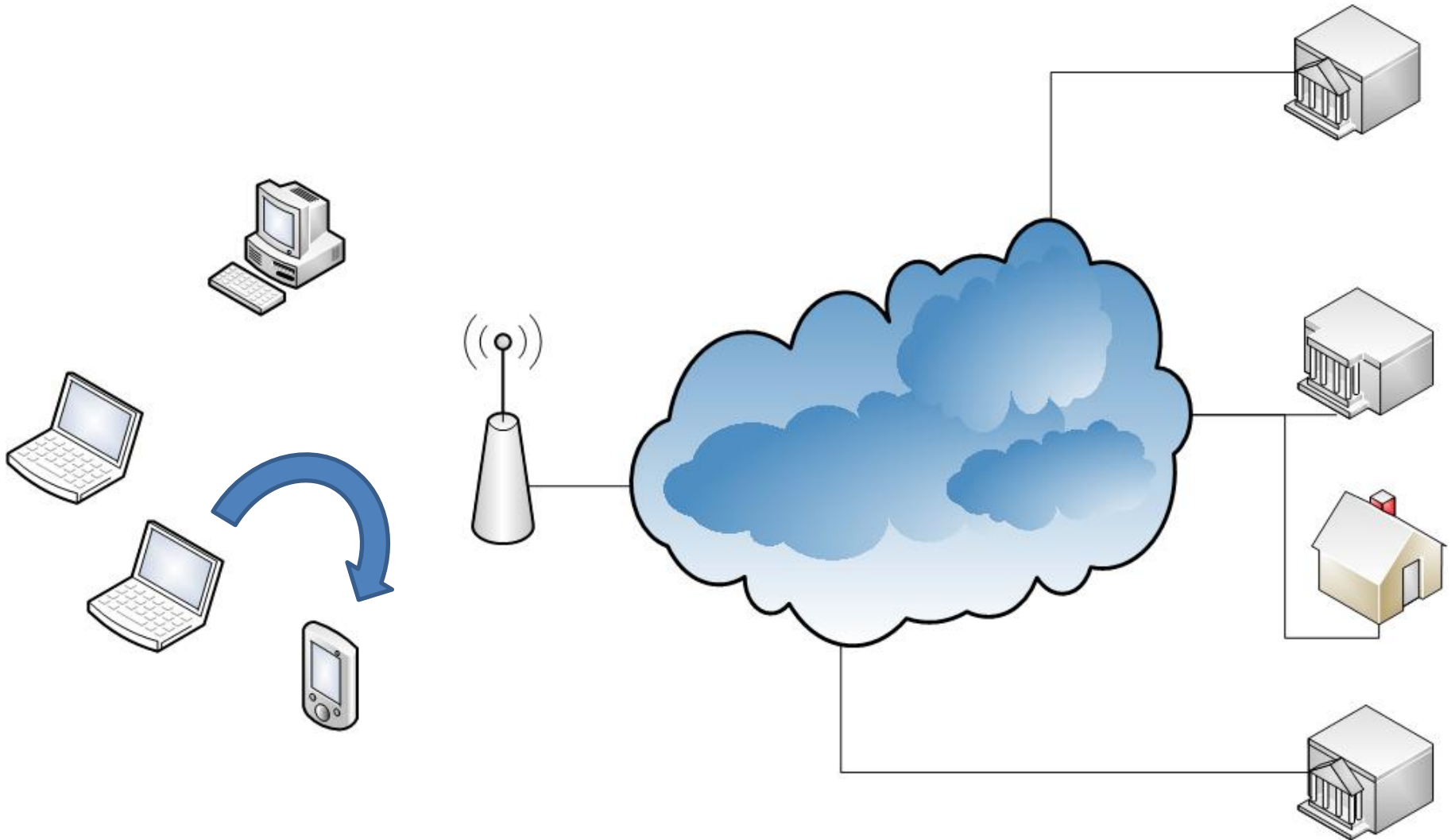


the attack

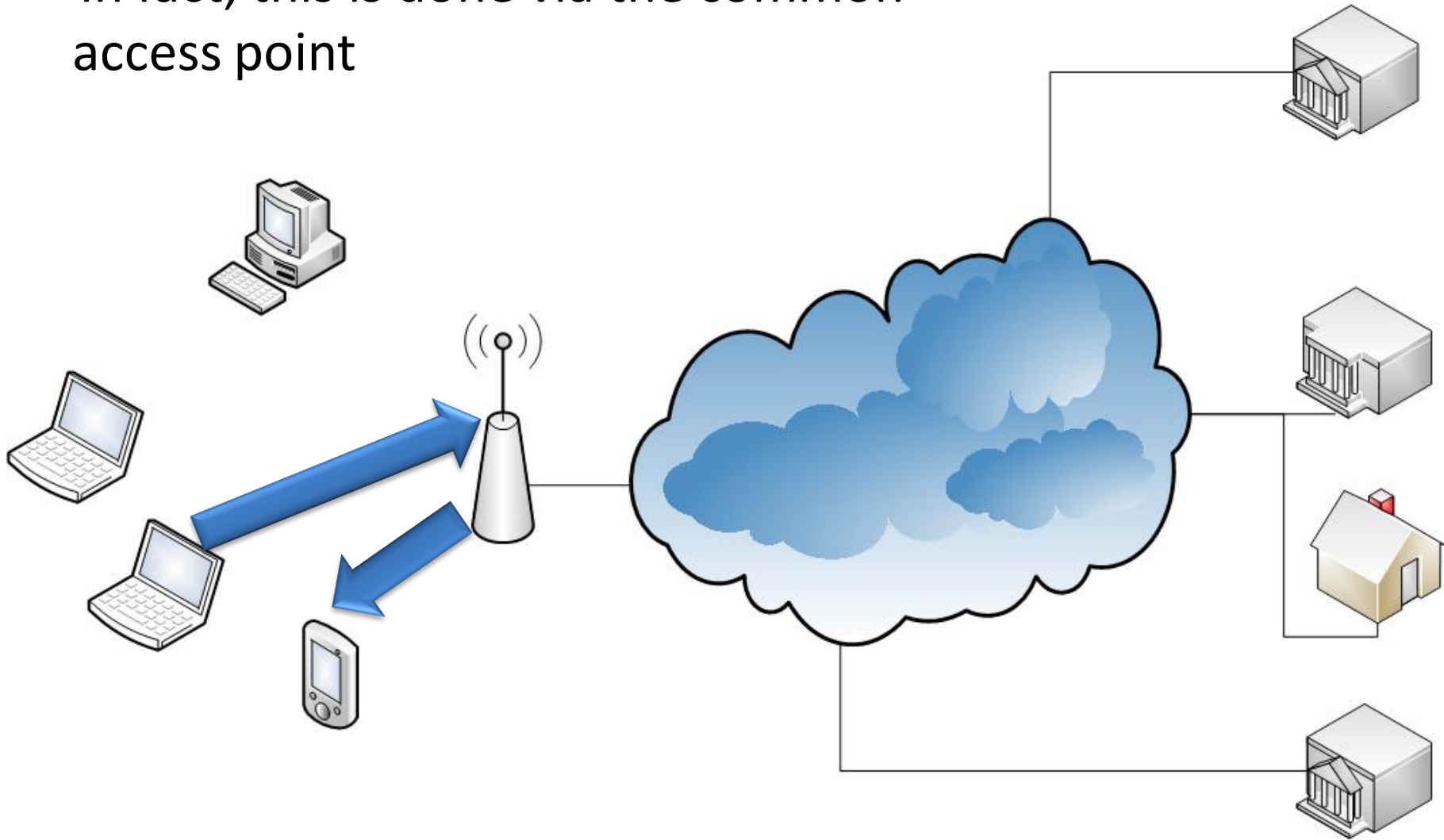
- In the coffee shop and decide to use phone's portal feature



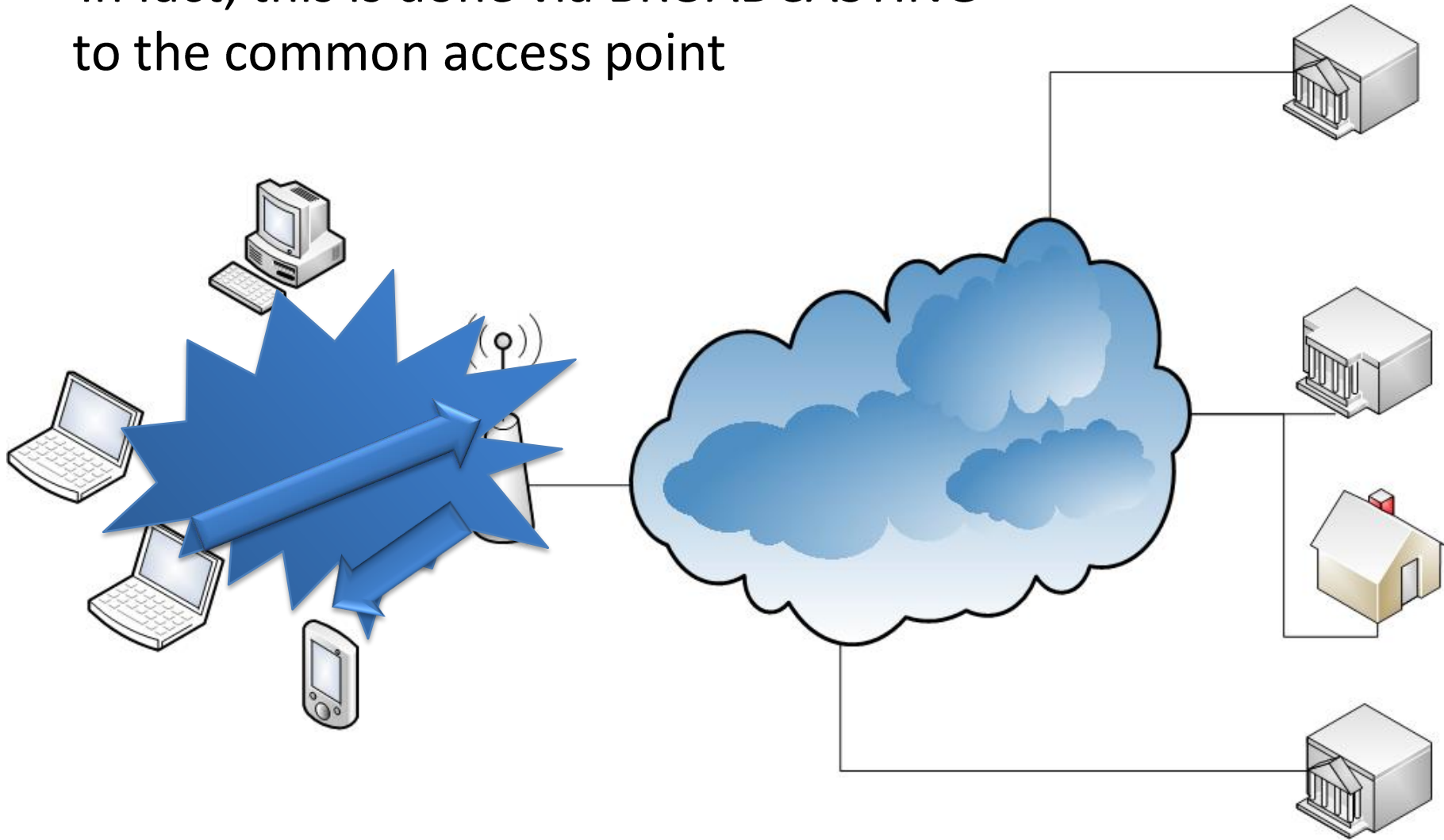
- It might seem that the computer is connecting to the phone directly



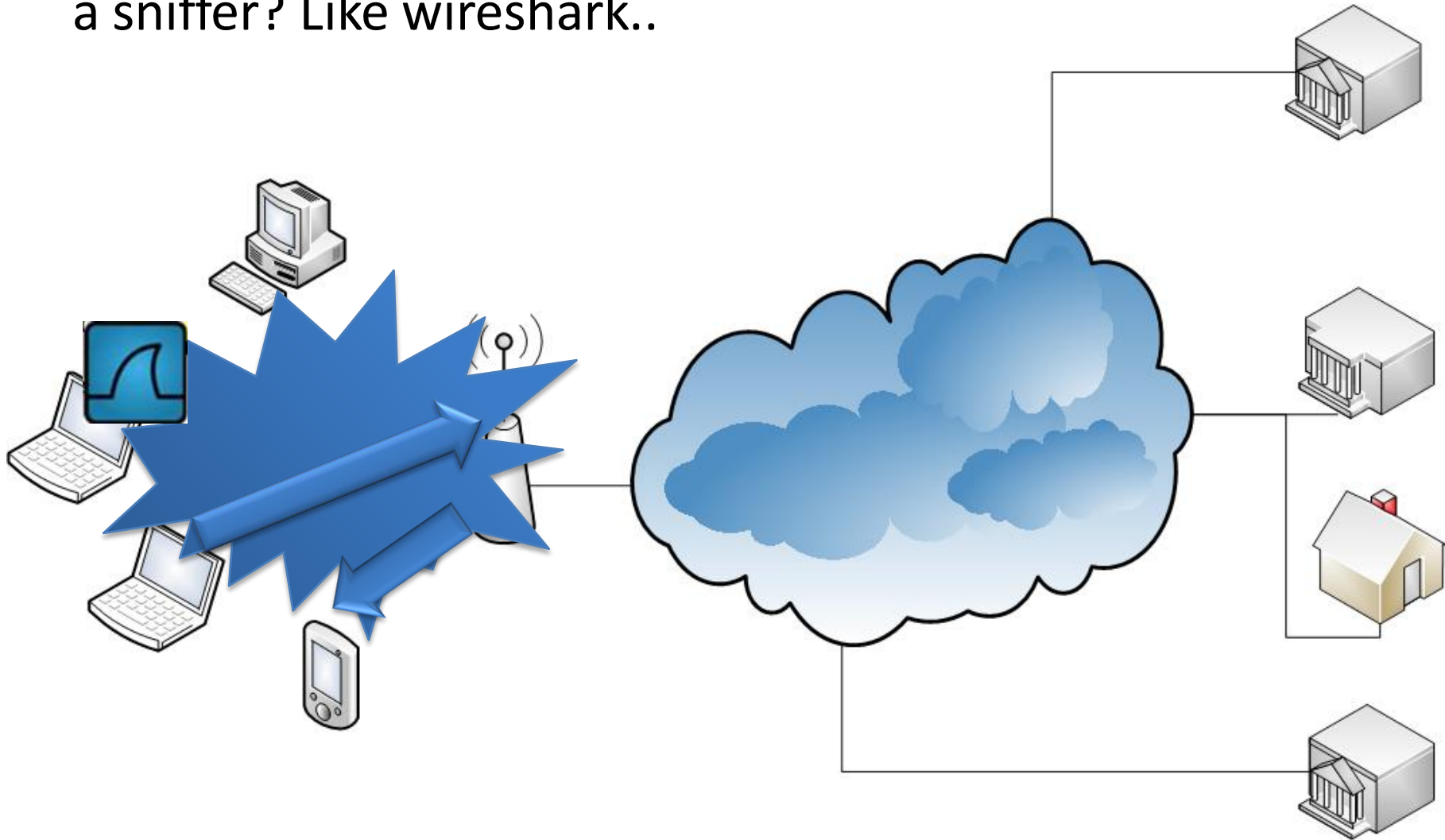
- In fact, this is done via the common access point



- 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

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: ip.addr==172.24.2.88 and tcp.port==8080

No.	Time	Source	Destination	Protocol	Info
13	4.708420	172.24.2.97	172.24.2.88	TCP	hs-port > http-alt [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8
16	4.925974	172.24.2.88	172.24.2.97	TCP	http-alt > hs-port [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 WS=
17	4.926148	172.24.2.97	172.24.2.88	TCP	hs-port > http-alt [ACK] Seq=1 Ack=1 win=17408 Len=0
18	4.936115	172.24.2.97	172.24.2.88	HTTP	GET /images/Button_Hover.png HTTP/1.1
19	4.941034	172.24.2.97	172.24.2.88	TCP	ibp > http-alt [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8
20	5.087515	172.24.2.97	172.24.2.88	TCP	hs-port > http-alt [FIN, ACK] Seq=518 Ack=1 win=17408 Len=0
21	5.089707	172.24.2.97	172.24.2.88	TCP	blockade-bpsp > http-alt [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8
22	5.114522	172.24.2.88	172.24.2.97	TCP	http-alt > hs-port [ACK] Seq=1 Ack=518 win=6912 Len=0
23	5.116444	172.24.2.88	172.24.2.97	TCP	http-alt > ibp [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 WS=1
24	5.116520	172.24.2.97	172.24.2.88	TCP	ibp > http-alt [ACK] Seq=1 Ack=1 win=17408 Len=0
25	5.117185	172.24.2.88	172.24.2.97	TCP	http-alt > blockade-bpsp [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=14
26	5.117229	172.24.2.97	172.24.2.88	TCP	blockade-bpsp > http-alt [ACK] Seq=1 Ack=1 win=17408 Len=0
27	5.119774	172.24.2.97	172.24.2.88	TCP	ibp > http-alt [FIN, ACK] Seq=1 Ack=1 win=17408 Len=0
28	5.121066	172.24.2.97	172.24.2.88	HTTP	GET /dashboard.html HTTP/1.1
29	5.147858	172.24.2.88	172.24.2.97	TCP	[TCP segment of a reassembled PDU]
30	5.149015	172.24.2.88	172.24.2.97	TCP	[TCP segment of a reassembled PDU]
31	5.149077	172.24.2.97	172.24.2.88	TCP	hs-port > http-alt [ACK] Seq=519 Ack=1466 win=17408 Len=0
32	5.154865	172.24.2.88	172.24.2.97	TCP	http-alt > blockade-bpsp [ACK] Seq=1 Ack=540 win=6918 Len=0

Accept-Encoding: gzip,deflate\r\n
 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
 Keep-Alive: 115\r\n
 Connection: keep-alive\r\n
 Referer: http://172.24.2.88:8080/login/login.html\r\n
 Cookie: SESSION_ID=c3763707-d513-489a-91c4-78f0403ceb66\r\n
 Content-Type: application/x-www-form-urlencoded\r\n
 Content-Length: 75\r\n
 \r\n

Line-based text data: application/x-www-form-urlencoded
 j_username=sk&j_password=d0717f47123f763c266ca3a759dcaf30&loginButton=Login

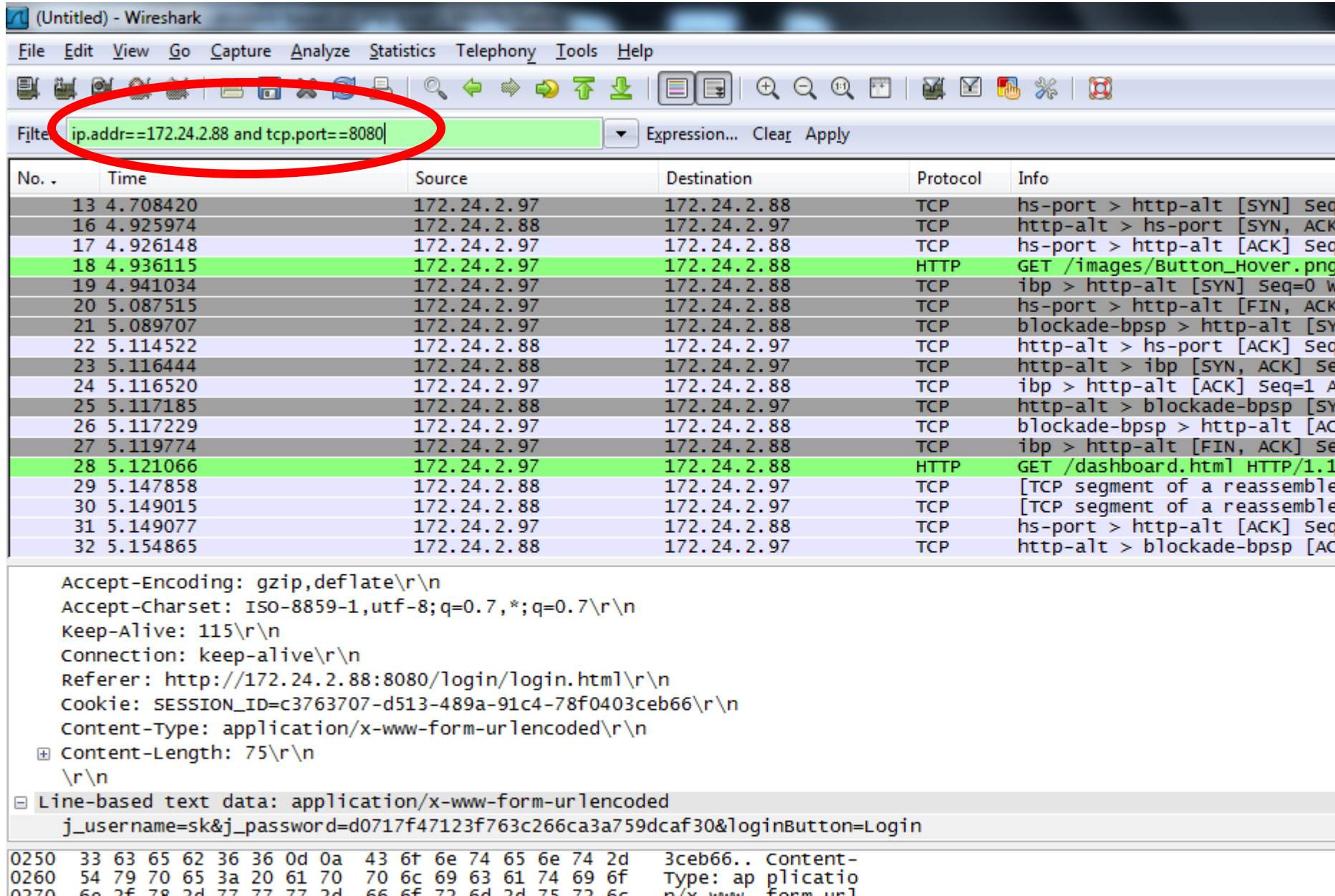
0250	33 63 65 62 36 36 0d 0a 43 6f 6e 74 65 6e 74 2d	3ceb66.. Content-
0260	54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f	Type: ap plicatio
0270	6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c	n/x-www- form-ur l
0280	65 6e 63 6f 64 65 64 0d 0a 43 6f 6e 74 65 6e 74	encoded. .Content
0290	2d 4c 65 6e 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	_user nam 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

Text item (0), 75 bytes

Packets: 1167 Displayed: 810 Marked: 0 Dropped: 0

Profile: Default

- Say they single out the phone connection



The image shows the Wireshark network protocol analyzer interface. The title bar reads "(Untitled) - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. The toolbar contains various icons for file operations, navigation, and analysis. The filter bar at the top contains the expression `ip.addr==172.24.2.88 and tcp.port==8080`, which is circled in red. Below the filter bar is a table of captured packets. Packet 18 is highlighted in green. The packet details pane shows the following information:

```
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 115\r\n
Connection: keep-alive\r\n
Referer: http://172.24.2.88:8080/login/login.html\r\n
Cookie: SESSION_ID=c3763707-d513-489a-91c4-78f0403ceb66\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 75\r\n
\r\n
Line-based text data: application/x-www-form-urlencoded
j_username=sk&j_password=d0717f47123f763c266ca3a759dcaf30&loginButton=Login
```

The packet bytes pane at the bottom shows the raw data for the selected packet, including hex and ASCII representations.

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

The screenshot shows the Wireshark interface with a packet capture window and a search dialog box. The packet capture window displays a list of packets, with packet 28 highlighted. The search dialog box is titled "Wireshark: Find Packet" and has the following settings:

- Find By: Display filter Hex value String
- Filter: password
- Search In: Packet list Packet details Packet bytes
- String Options: Case sensitive
- Character set: ASCII Unicode & Non-Unicode
- Direction: Up Down

The packet capture window shows the following packets:

No.	Time	Source
13	4.708420	172
16	4.925974	172
17	4.926148	172
18	4.936115	172
19	4.941034	172
20	5.087515	172
21	5.089707	172
22	5.114522	172
23	5.116444	172
24	5.116520	172
25	5.117185	172
26	5.117229	172
27	5.119774	172
28	5.121066	172
29	5.147858	172
30	5.149015	172
31	5.149077	172
32	5.154865	172

The packet details pane shows the following information for packet 28:

- Accept-Encoding: gzip, deflate\r\n
- Accept-Charset: ISO-8859-1, utf-8; q=0.5\r\n
- Keep-Alive: 115\r\n
- Connection: keep-alive\r\n
- Referer: http://172.24.2.88:8080/login/login.html\r\n
- Cookie: SESSION_ID=c3763707-d513-489a-91c4-78f0403ceb66\r\n
- Content-Type: application/x-www-form-urlencoded\r\n
- Content-Length: 75\r\n
- Line-based text data: application/x-www-form-urlencoded
- j_username=sk&j_password=d0717f47123f763c266ca3a759dcaf30&loginButton=Login

The packet bytes pane shows the following hex and ASCII data:

```
0250 33 63 65 62 36 36 0d 0a 43 6f 6e 74 65 6e 74 2d 3c3eb66.. Content-
0260 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f  Type: applicatio
0270 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c  n/x-www- form-ur
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 42 75 74 74 6f 6e 3d 4c 6f 67 69 6e  tton=Log in
```

- 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: applicatio
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	_username=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