DEFCON GROUP 010

Try again

Using the scientific method to bypass a captive portal

Through destruction comes new norm
Through grouping comes amplified power

不破不立
不聚不利

questions??

DEFCON GROUP 010

Try again

Using the scientific method to bypass a captive portal

Through destruction comes new norm
Through grouping comes amplified power

不破不立
不聚不利

questions??

Miguel I Fernandez

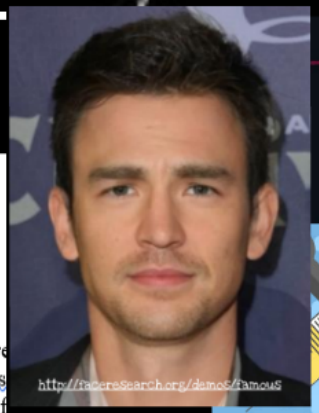
DEFCON GROUP 010 HACKER COMMUNITY

[redacted]

Miguel Ivan Fernandez 伊万–[redacted]
Mfernandezt2@hotmail.com

I. **Introduction**

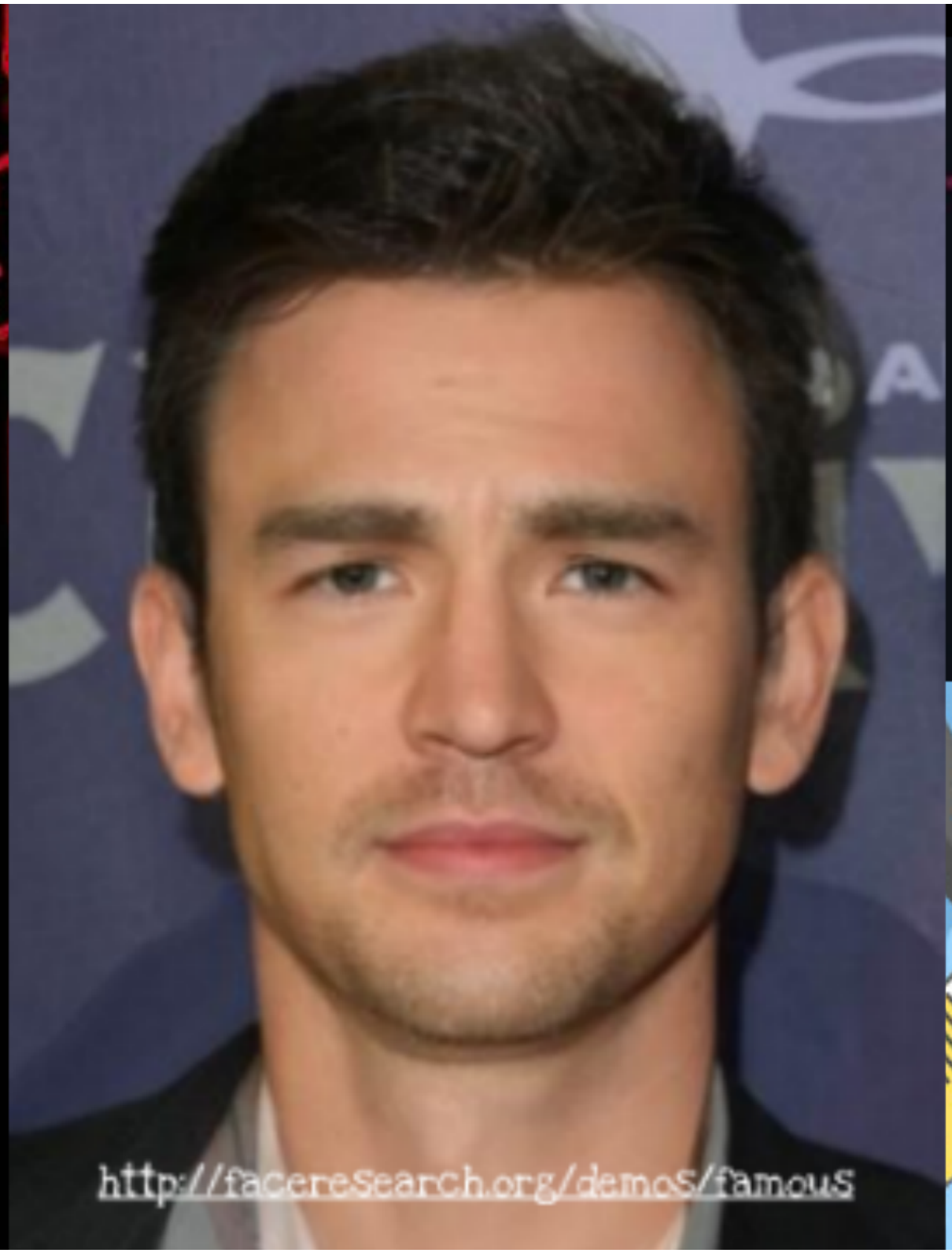
Since the widespread growth of the internet and the email service until nowadays, exist differe techniques and technologies to spy on the users of this service, the problem with that techniques is well known by criminals and they use this in his own sake. On the other hand, most of the users of service don't even know that techniques exist or they think these techniques are used just for well-



mfernandezt2@hotmail.com

exist differe

echniques is



一六

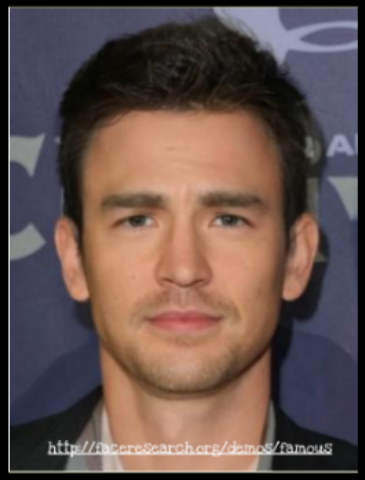
讲解

do you know, when you see one facial composite of some friend you react in positive manner.

what happen if marketers in the future can make personalized commercials using facial composite with your friends face?

+

=



What is the scientific method?

- Methodology
- Research
- Reliable, t(x)
- Impartial
- Accepted by other Fields

Volunteer

DEFCON GR

Using the

Ask a question

What technology use one Captive portal Identify me?

Background Research

- No internet then no background research
- Limited amount of time

But

- Experience
- Computer Networks
- Anonimity and privacy

→ Mac Address
→ Cookies

Construct Hypothesis

The system use Mac Address + cookies to identify my device

Try again

Experiment

Check in the browser for cookies

Analysis

The system don't store any cookie in the browser.

Hypothesis T/F

False

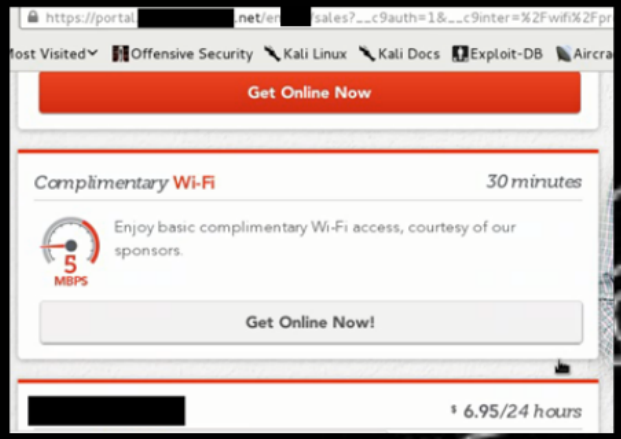
True

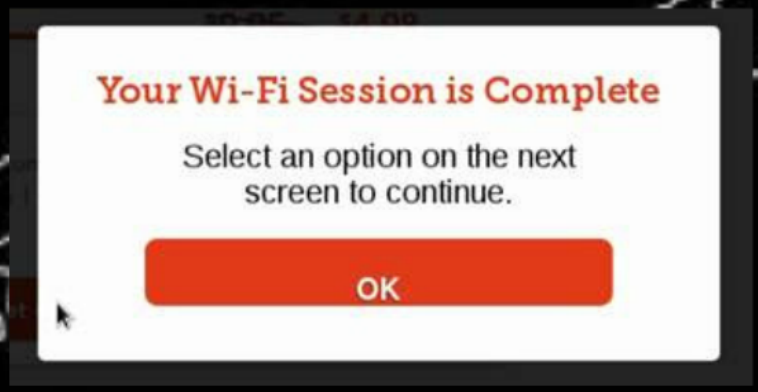
Report Results

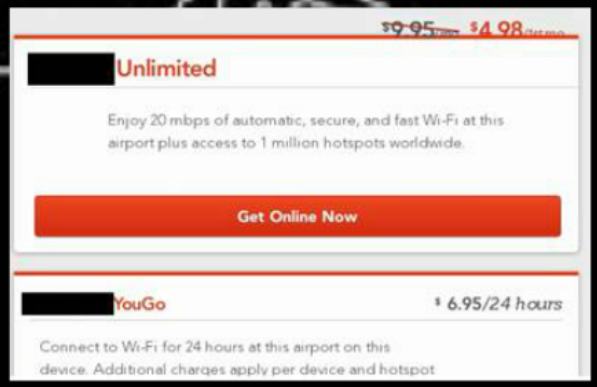
The captive portal just use the mac address of my network card as a method to identify my device.

wide use method in captive portals

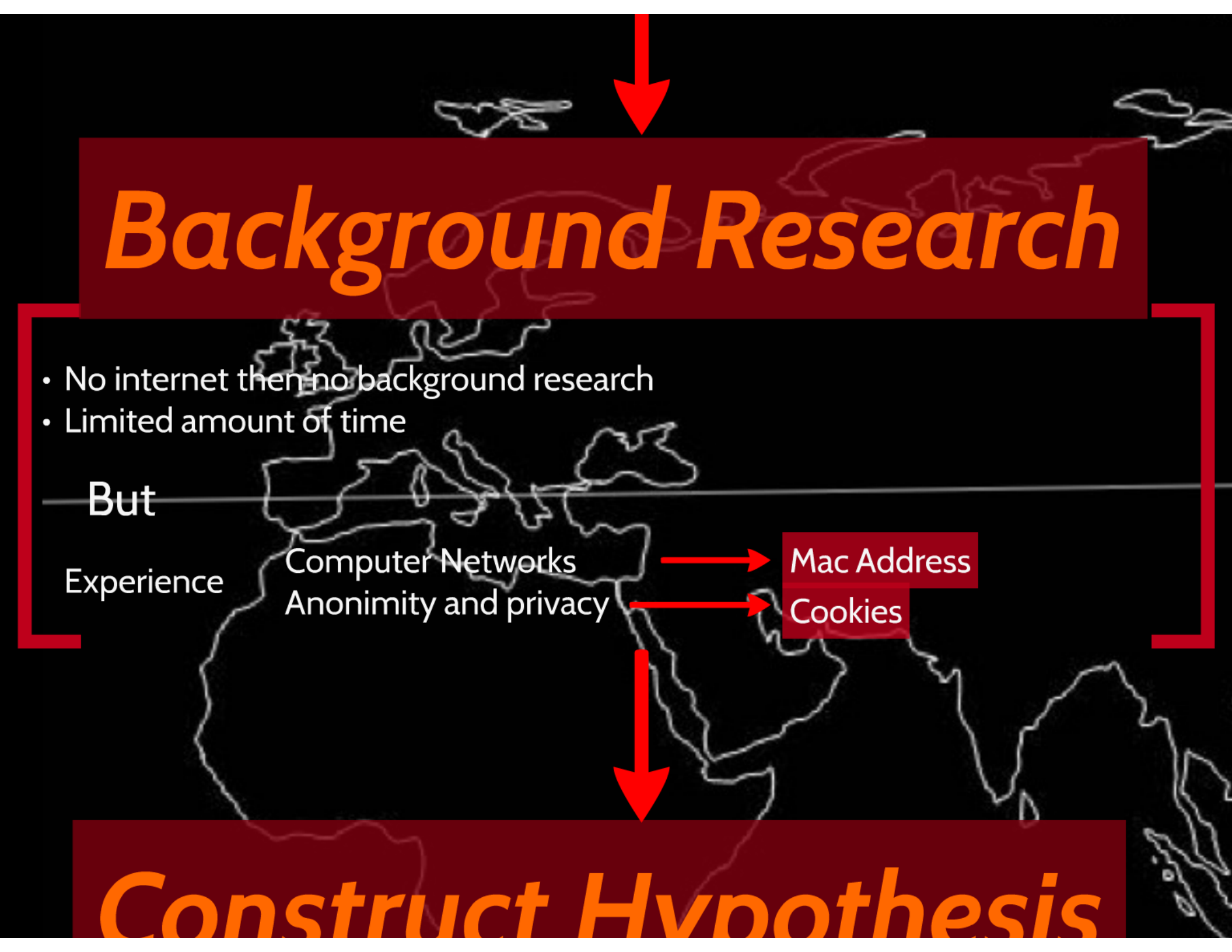
Ask a question







What technology use one Captive portal identify me?


Background Research
• No internet then no background research
• Limited amount of time
But
Experience
Computer Networks
Anonimity and privacy
Mac Address
Cookies
Construct Hypothesis

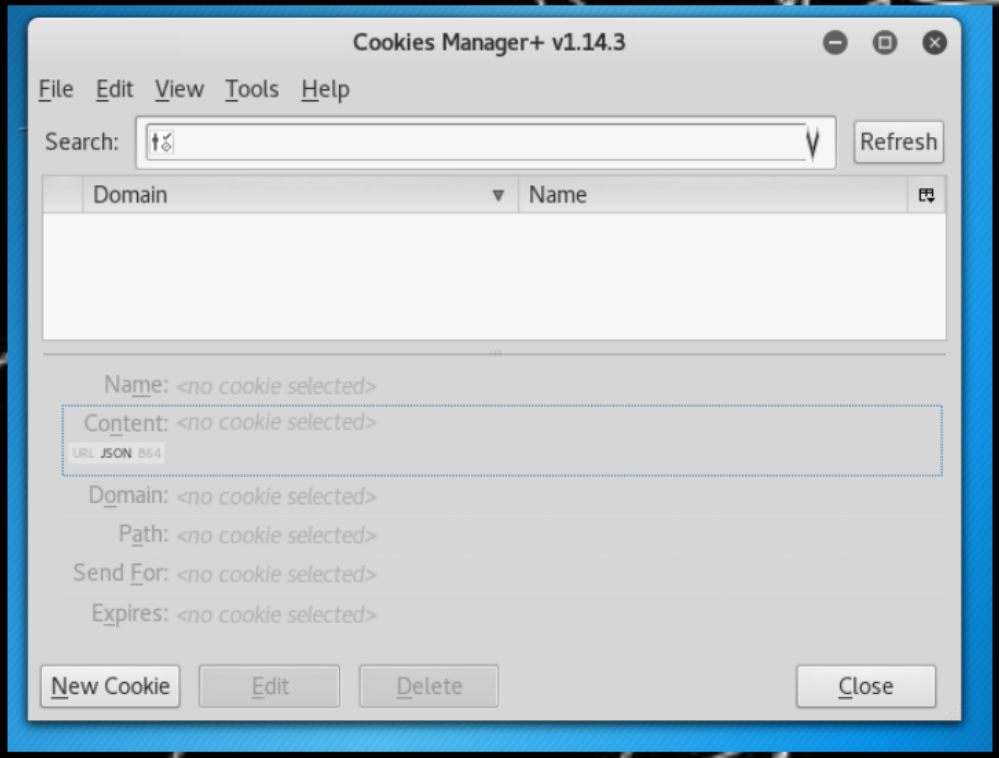
Construct Hypothesis

The system use Mac Address + cookies to identify my device

Experiment

Experiment

Check in the browser for cookies



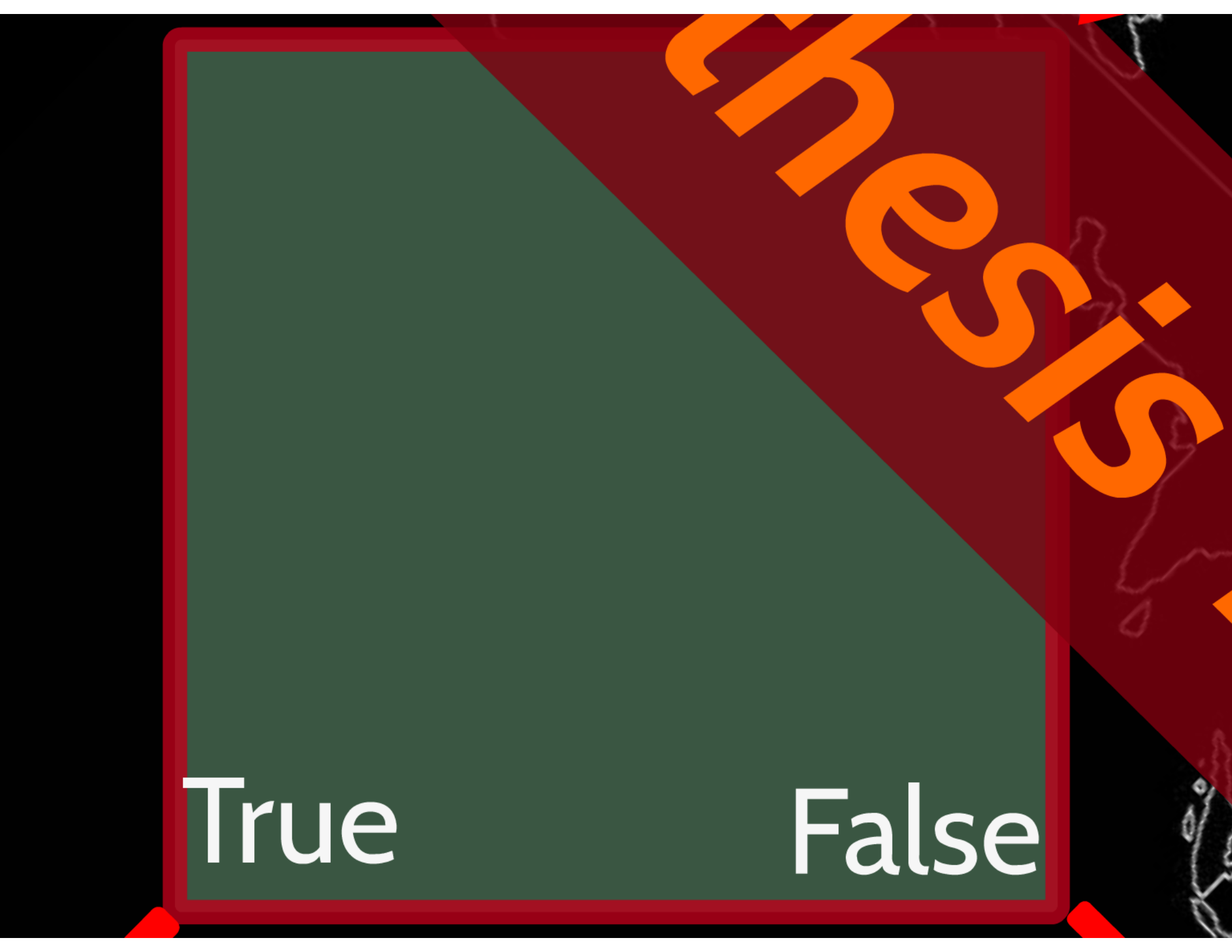
Analysis

The system don't store any cookie in the browser.

Analysis

when i change the mac address and go to the captive portal i can see the 30 minutes of complimentary wifi

the system just use mac address to identify if one device is allow to have complimentary wifi or not


thesis
True
False

DEFCON GR

Using the

Ask a question

What technology use one Captive portal Identify me?

Background Research

- No internet then no background research
- Limited amount of time

But

- Experience
- Computer Networks
- Anonimity and privacy

→ Mac Address
→ Cookies

Construct Hypothesis

The system use Mac Address + cookies to identify my device

Try again

Experiment

Check in the browser for cookies

Analysis

The system don't store any cookie in the browser.

Hypothesis T/F

False

True

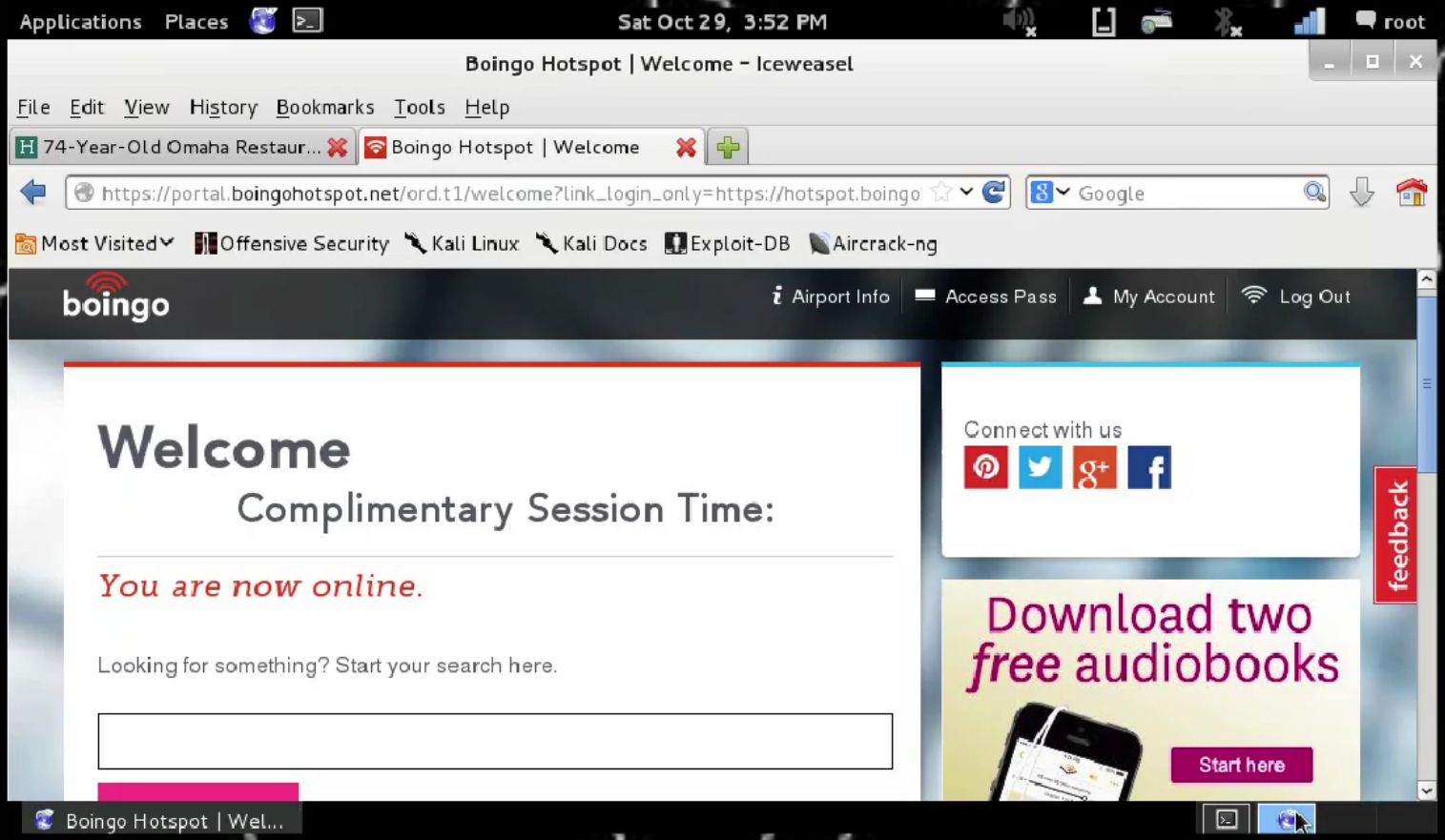
Report Results

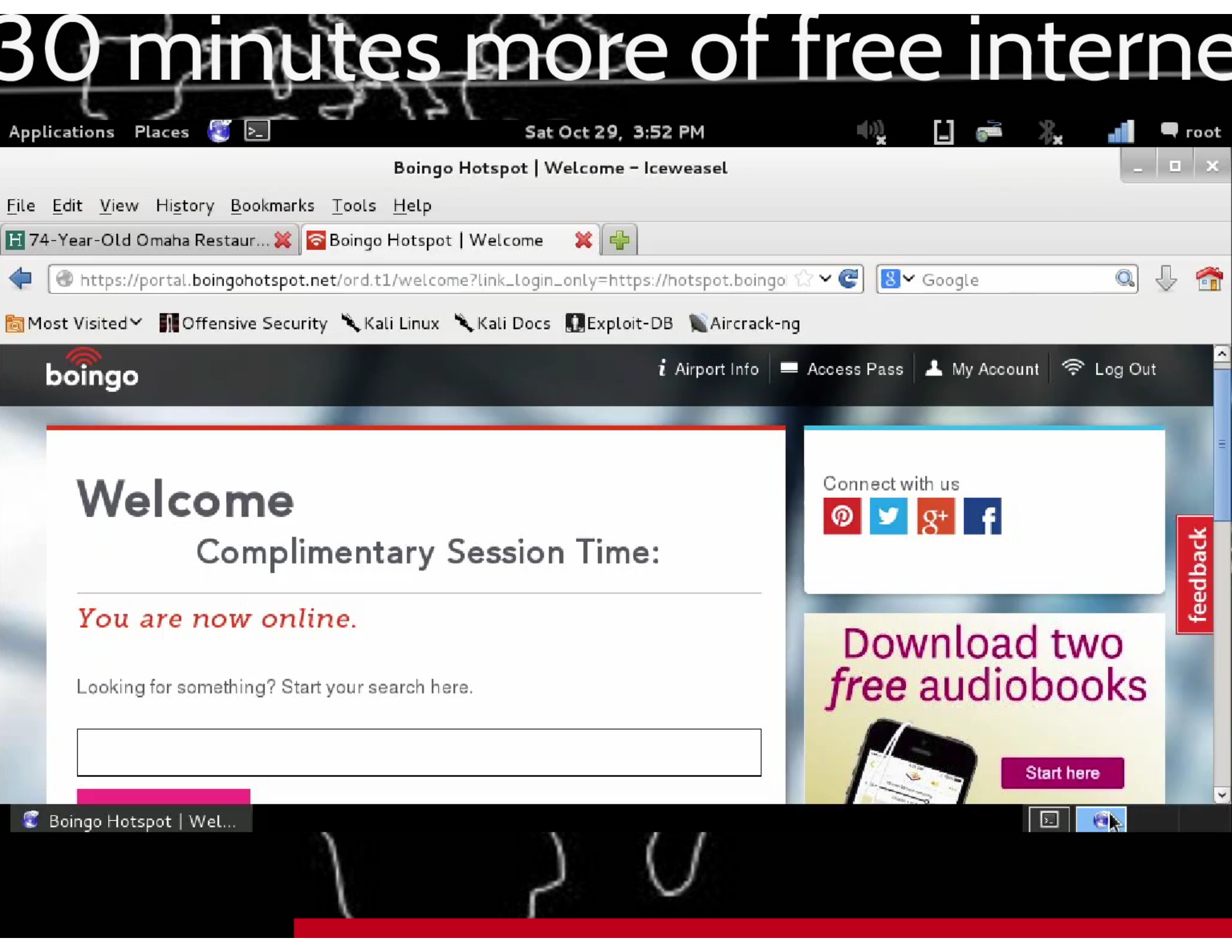
The captive portal just use the mac address of my network card as a method to identify my device.

wide use method in captive portals


Construct Hypothesis
The system JUST use Mac Address to identify my device

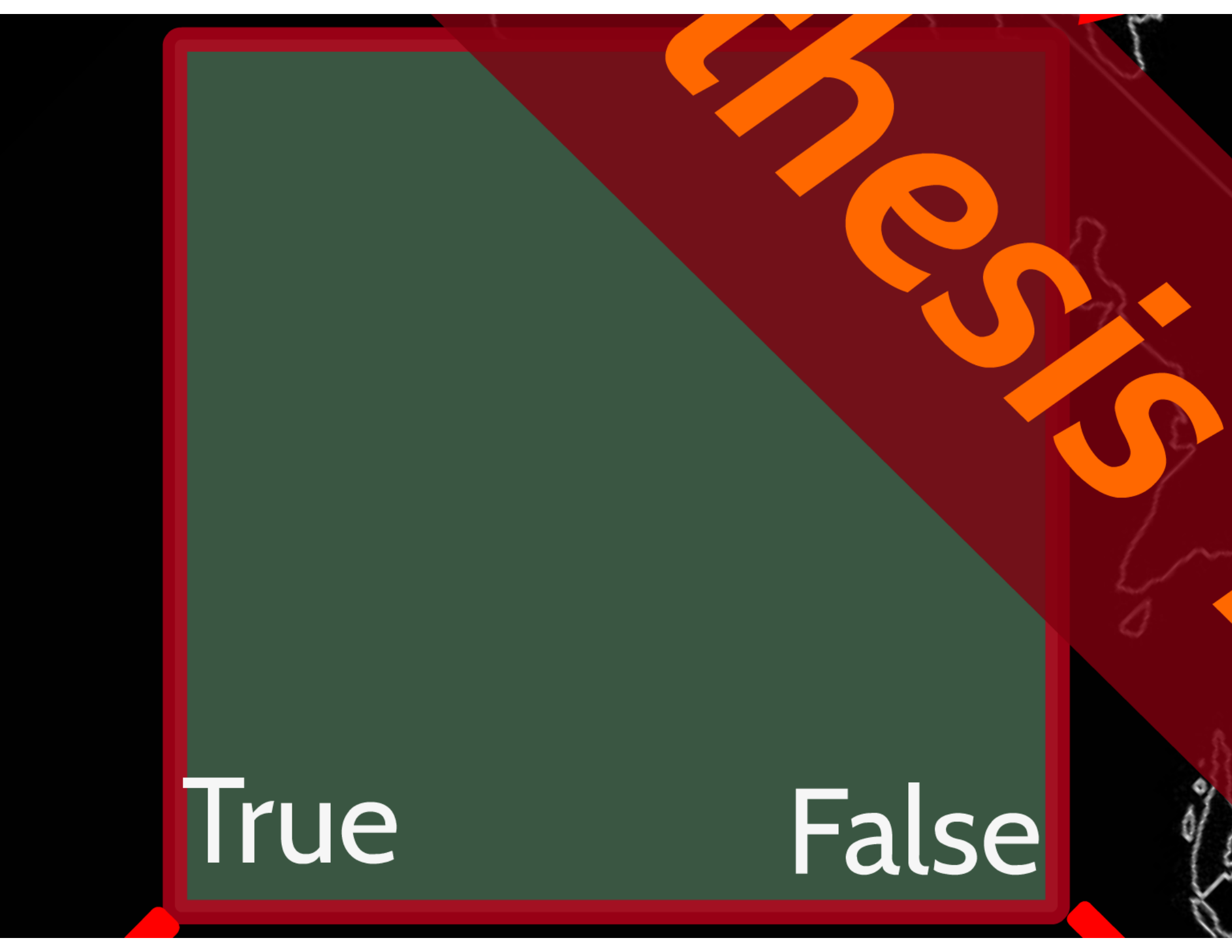
Change the mac address and see if i can get 30 minutes more of free internet.




30 minutes more of free interne
Applications Places
Sat Oct 29, 3:52 PM
root
Boingo Hotspot | Welcome - Iceweasel
File Edit View History Bookmarks Tools Help
74-Year-Old Omaha Restaur...
Boingo Hotspot | Welcome
https://portal.boingohotspot.net/ord.t1/welcome?link_login_only=https://hotspot.boingo
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng
boingo
Airport Info
Access Pass
My Account
Log Out
Welcome
Complimentary Session Time:
You are now online.
Looking for something? Start your search here.
Connect with us
feedback
Download two free audiobooks
Start here
Boingo Hotspot | Wel...

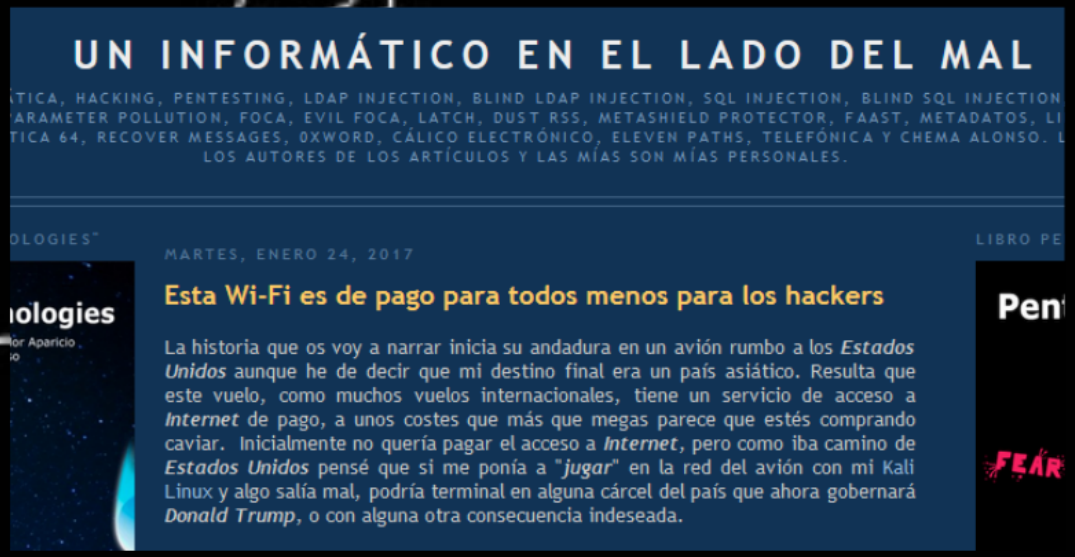
when i change the mac address and go to the captive portal i can see the 30 minutes of complimentary wifi

the system just use mac address to identify if one device is allow to have complimentary wifi or not


thesis
True
False

Report Results

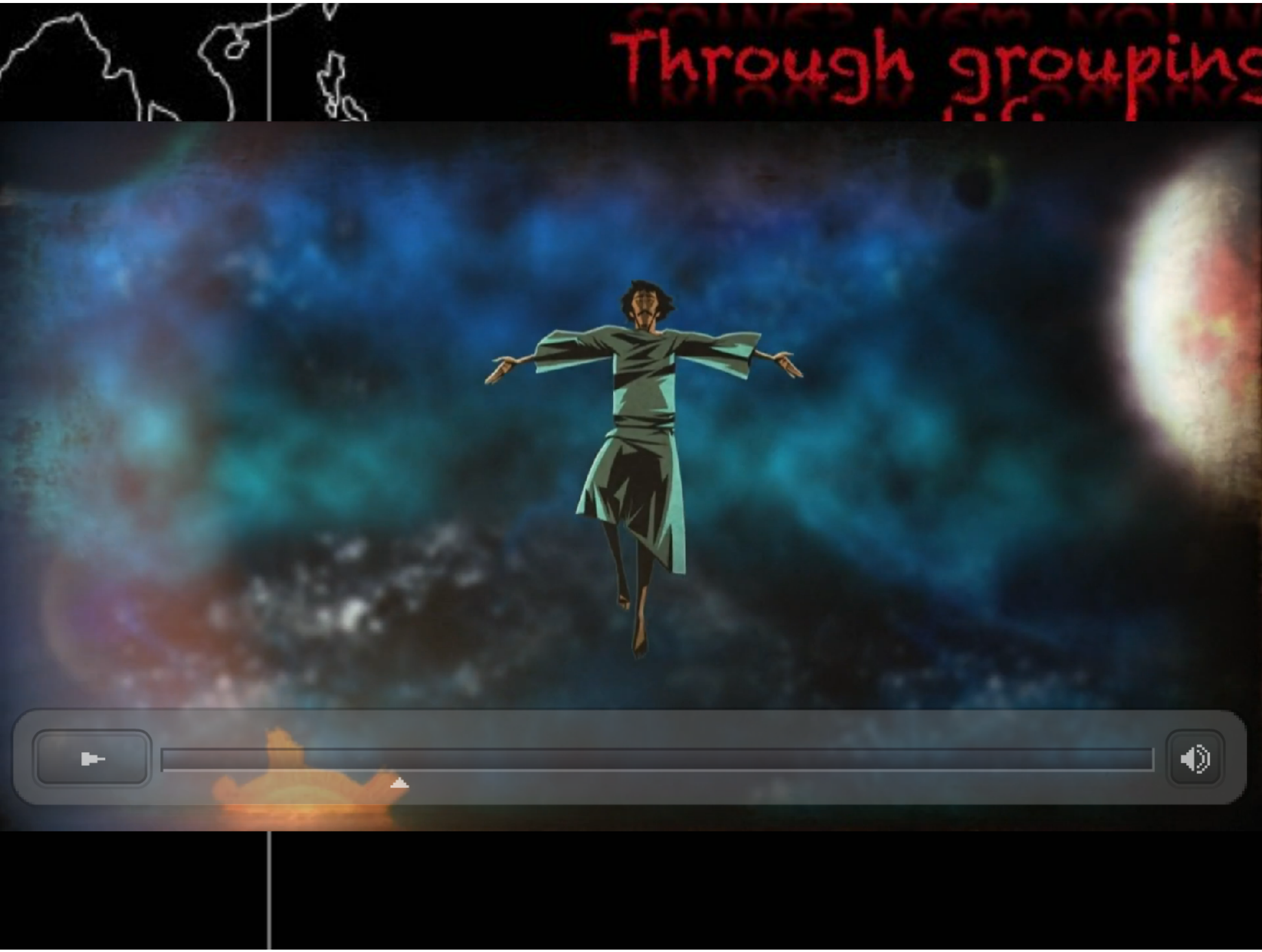
The captive portal just use the mac address of my network card as a method to identify my device.



wide use method in captive portals

- The negative results are important as the positive results; Publish them.
- We don't have to accept the result of on research because of yes.
- Corroborate the results.

- The negative results are important as the positive results; Publish them.
- We don't have to accept the result of on research because of yes.
- Corroborate the results.


Through groupings

questions??

mfernandezt2@hotmail.com