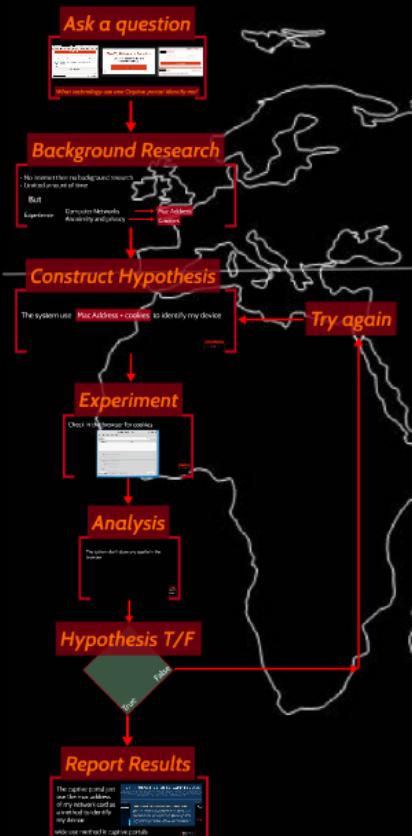


DEFCON GROUP 010



DEFCON GROUP 010



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



Answers 77

h destruction
s new norm

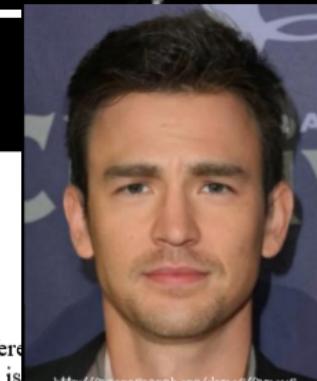
Miguel I Fernandez



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 different 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 this service don't even know that techniques exist or they think these techniques are used just for well-



- 六个角度 -
讲解人性漏洞

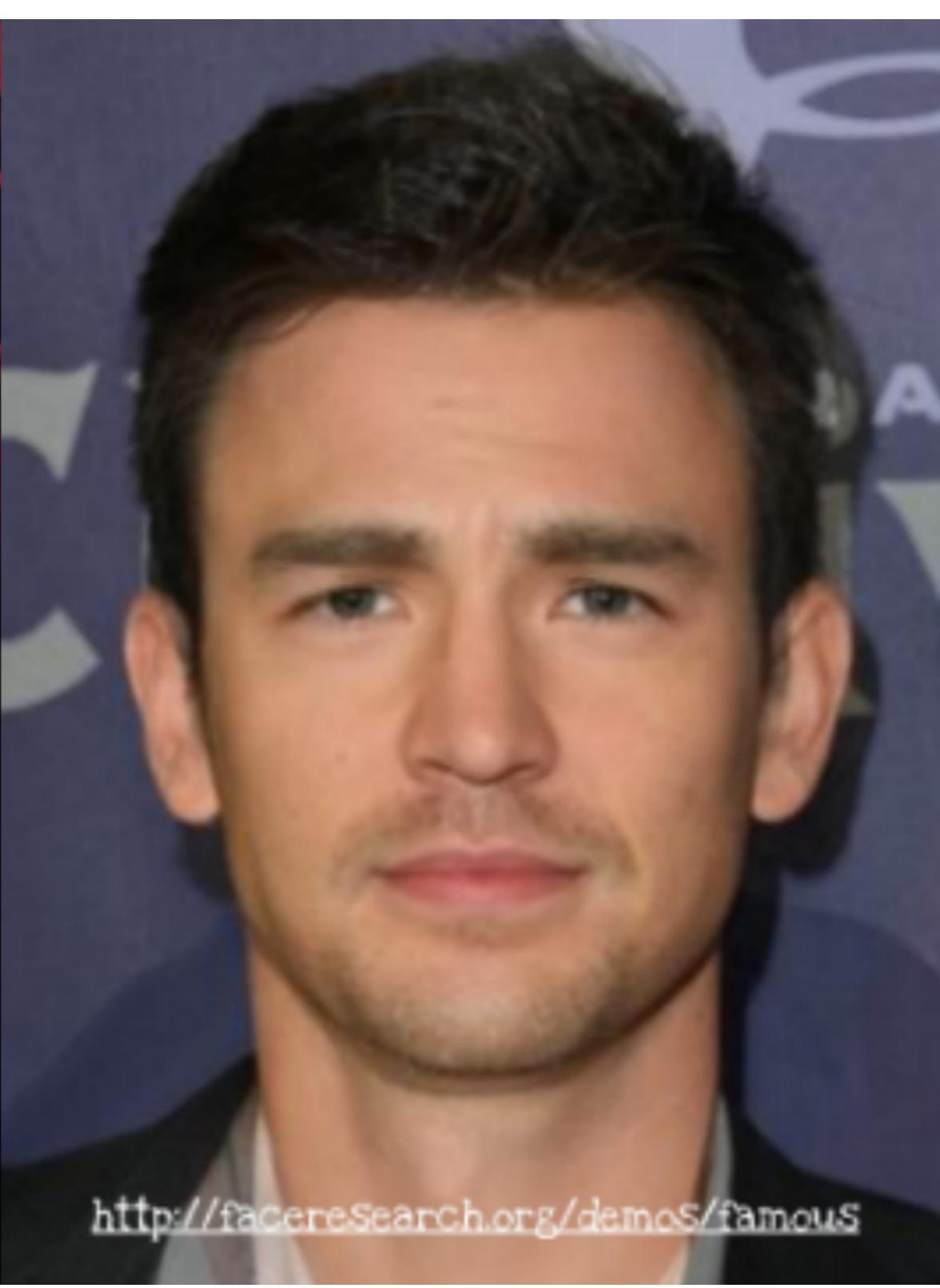
渗透工具



mfernandezt2@hotmail.com

exist different
techniques is
the usage of

<http://facereSearch.org/demos/famous>



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

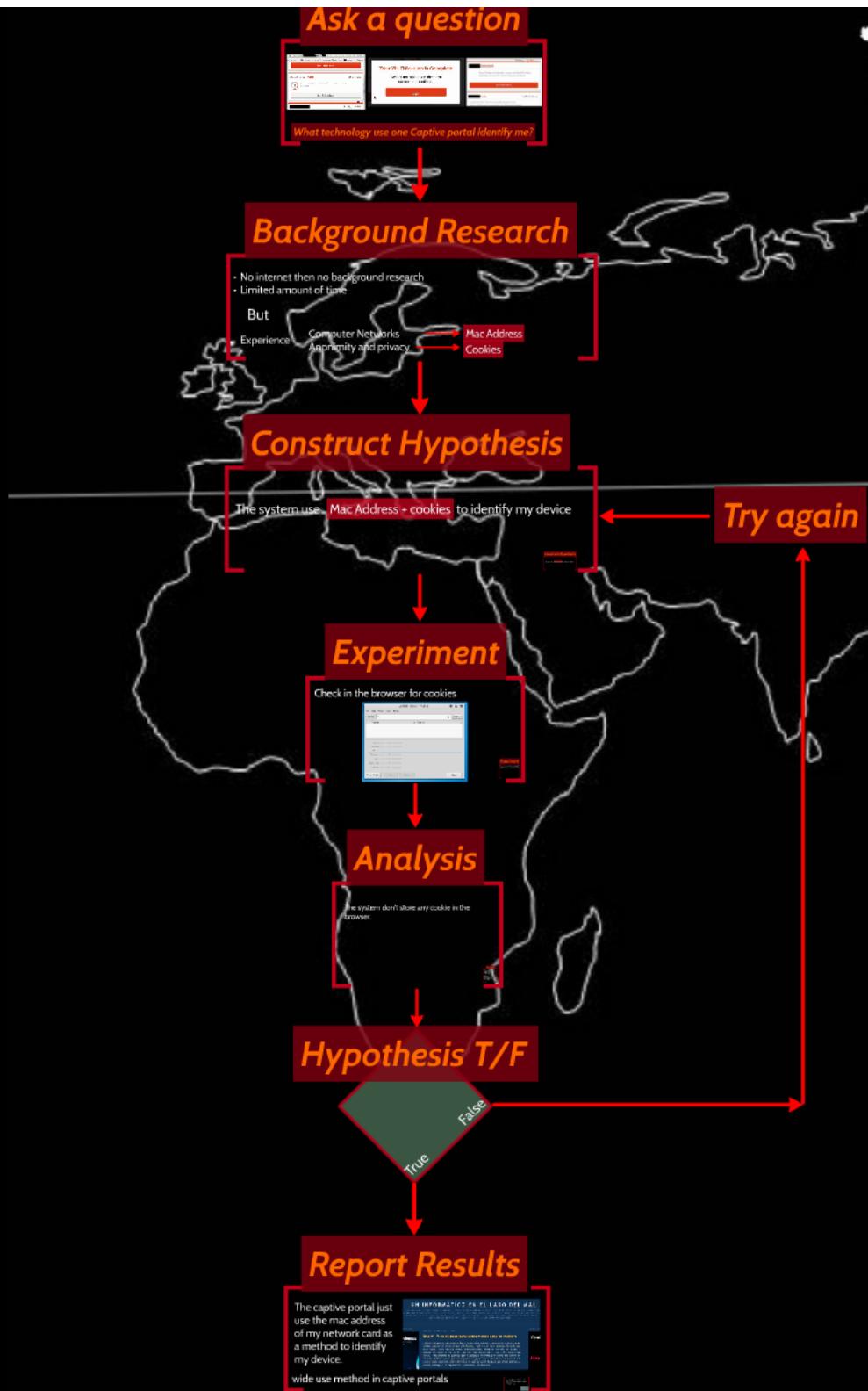


Through destruction comes new life
Through growth comes amplification

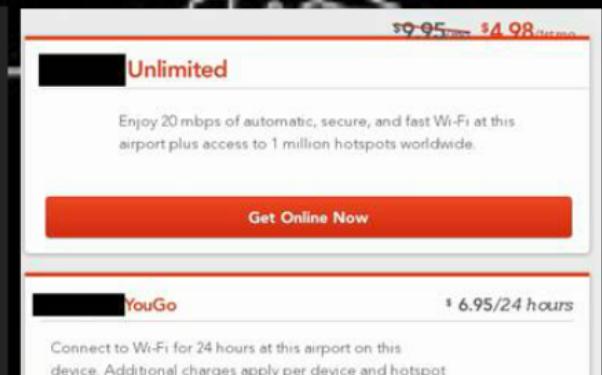
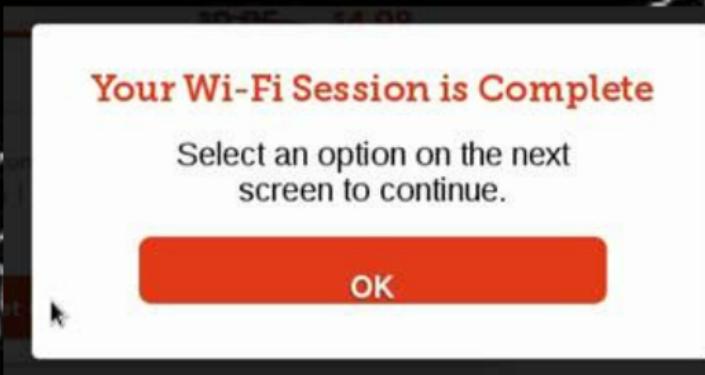
不破不立
无毁无成

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

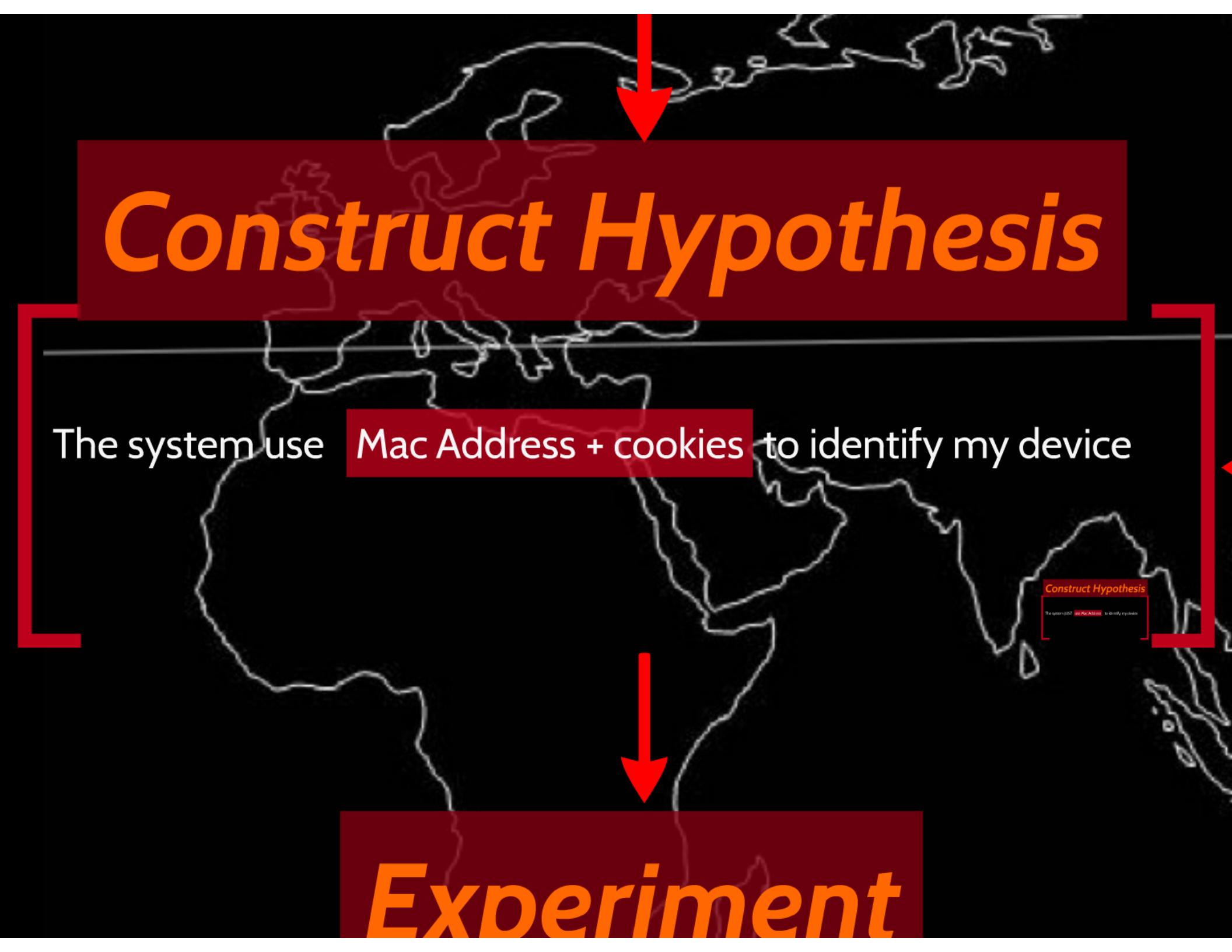
Computer Networks

Anonymity and privacy

Mac Address

Cookies

Construct Hypothesis



Construct Hypothesis

The system use **Mac Address + cookies** to identify my device

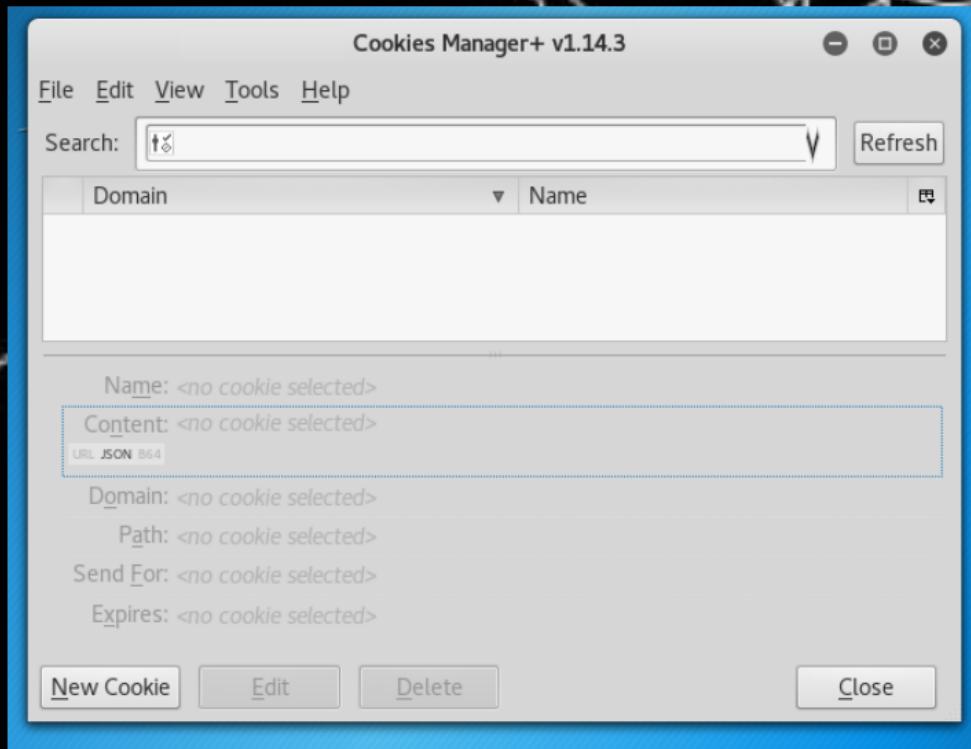
Construct Hypothesis

The system use **Mac Address** to identify my device

Experiment

Experiment

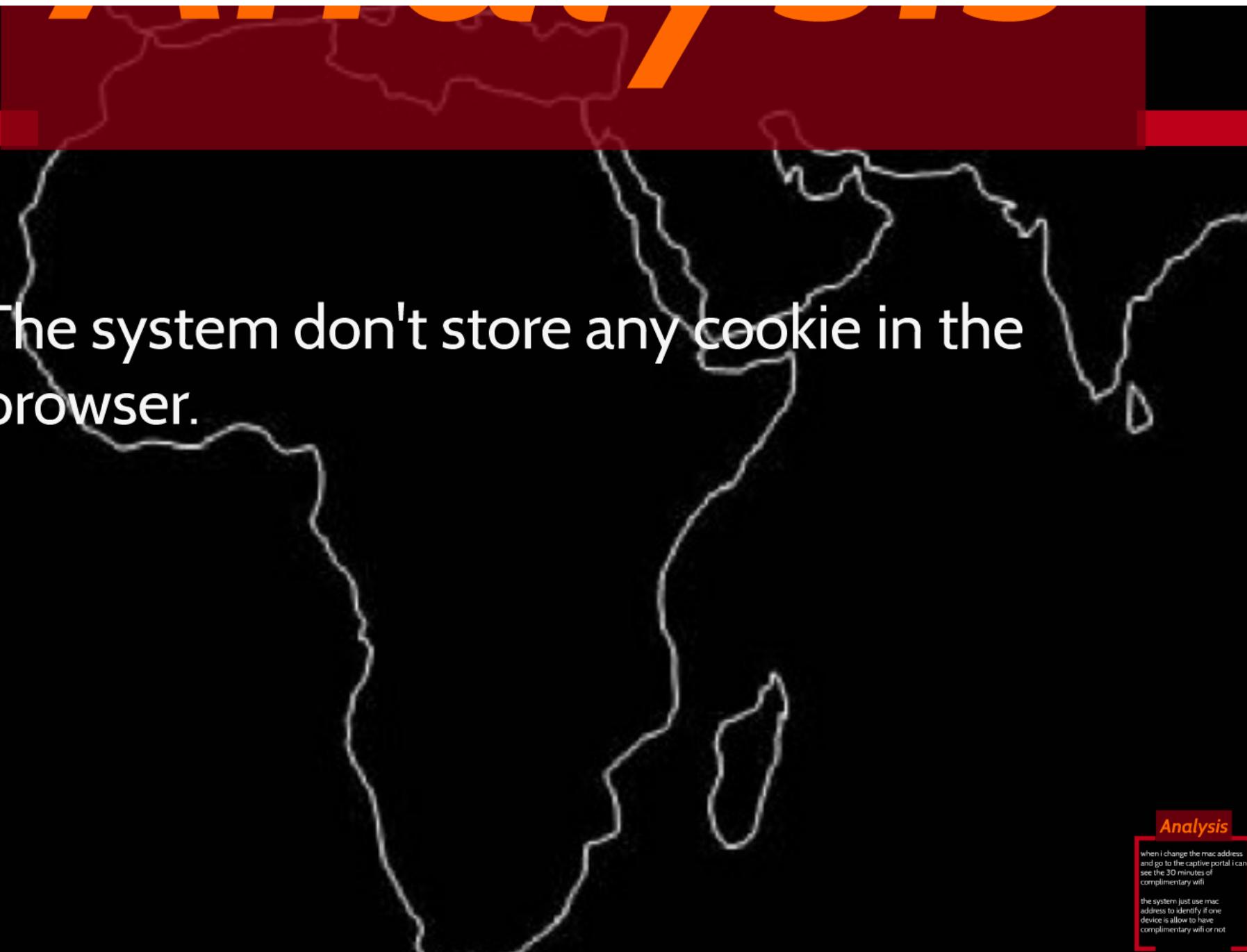
Check in the browser for cookies



Experiment

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





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 allowed to have complimentary wifi or not.

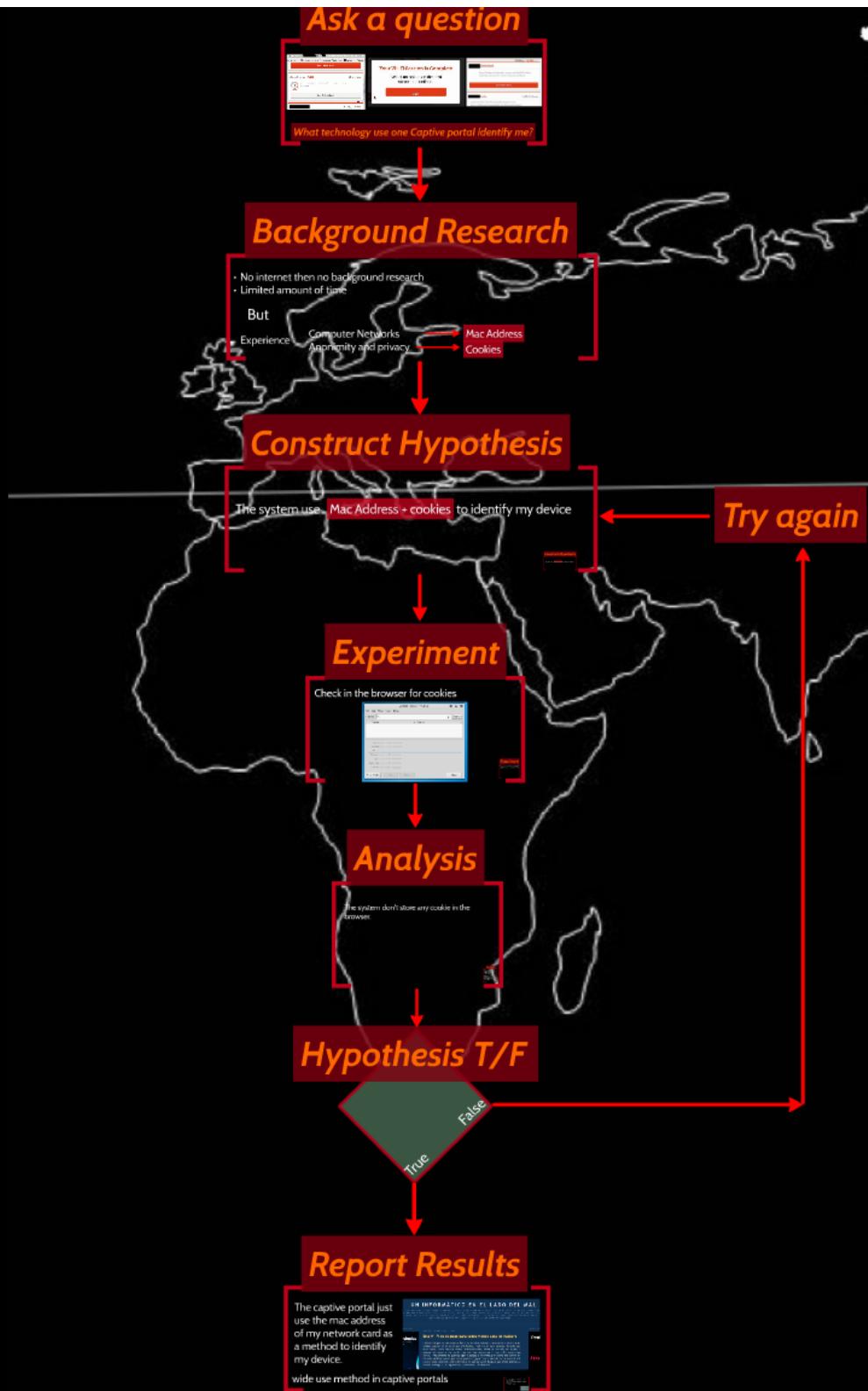
True

False

thesis

DEFCON GR

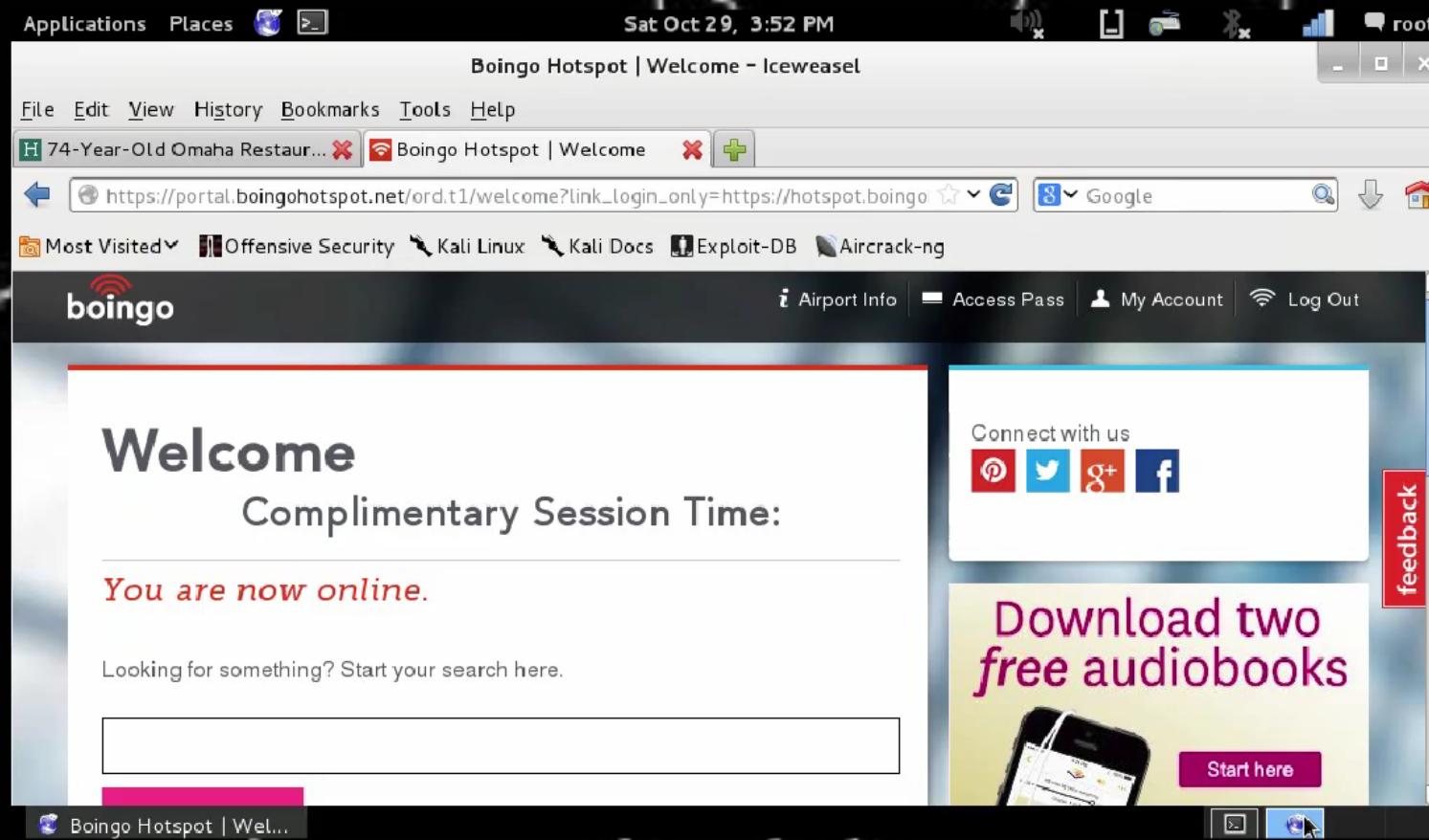
Using the



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

H 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 Docs Aircrack-ng

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

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

True

False

thesis

Report Results

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

UN INFORMÁTICO EN EL LADO DEL MAL

ITICA, HACKING, PENTESTING, LDAP INJECTION, BLIND LDAP INJECTION, SQL INJECTION, BLIND SQL INJECTION, PARAMETER POLLUTION, FOCA, EVIL FOCA, LATCH, DUST RSS, METASHIELD PROTECTOR, FAAST, METADATOS, LISTA 64, RECOVER MESSAGES, OXWORD, CÁLICO ELECTRÓNICO, ELEVEN PATHS, TELEFÓNICA Y CHEMA ALONSO. LOS AUTORES DE LOS ARTÍCULOS Y LAS MÍAS SON MÍAS PERSONALES.

MARTES, ENERO 24, 2017

LIBRO PE

Pen

FEAR

Esta Wi-Fi es de pago para todos menos para los hackers

La historia que os voy a narrar inicia su andadura en un avión rumbo a los *Estados Unidos* aunque he de decir que mi destino final era un país asiático. Resulta que este vuelo, como muchos vuelos internacionales, tiene un servicio de acceso a *Internet* de pago, a unos costes que más que megas parece que estés comprando caviar. Inicialmente no quería pagar el acceso a *Internet*, pero como iba camino de *Estados Unidos* pensé que si me ponía a "jugar" en la red del avión con mi Kali Linux y algo salía mal, podría terminar en alguna cárcel del país que ahora gobernará *Donald Trump*, o con alguna otra consecuencia indeseada.

wide use method in captive portals

The results are not important as the positive
methodology.
• We don't have to accept the result of our research
because of yes.
• Considerate 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.

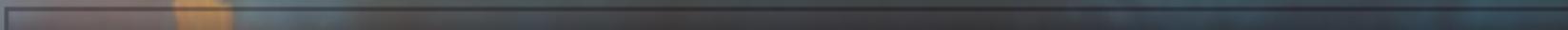




- The negative results are important as the positive results; Publish them.
- We don't have to accept the result of on research because of yes.
- Corroborate the results.



GOING NEW DIRECTIONS
Through grouping



立 利

questions??



mfernandezt2@hotmail.com