

# iOS Forensics a costo zero

HACKINBO SAFE EDITION 2020



14<sup>a</sup> EDIZIONE

# Obiettivi del lab

- ▶ Illustrare il jailbreak di un iPhone con **checkra1n**
- ▶ Effettuare l'acquisizione full file system dell'iPhone con **iOS BFU Triage**
- ▶ Analizzare i dati estratti utilizzando il tool opensource **iLeapp**

# Istruzioni e pre-requisiti

- ▶ Per poter seguire il lab «live» è necessario seguire le istruzioni all'URL  
[https://github.com/mattiaepi/  
HackInBoSafeEdition2020](https://github.com/mattiaepi/HackInBoSafeEdition2020)
- ▶ Se non lo avete fatto prima...oramai è tardi 😊

# checkm8

 Tweet fissato

 **axi0mX**  
@axi0mX

EPIC JAILBREAK: Introducing checkm8 (read "checkmate"), a permanent unpatchable bootrom exploit for hundreds of millions of iOS devices.

Most generations of iPhones and iPads are vulnerable: from iPhone 4S (A5 chip) to iPhone 8 and iPhone X (A11 chip).

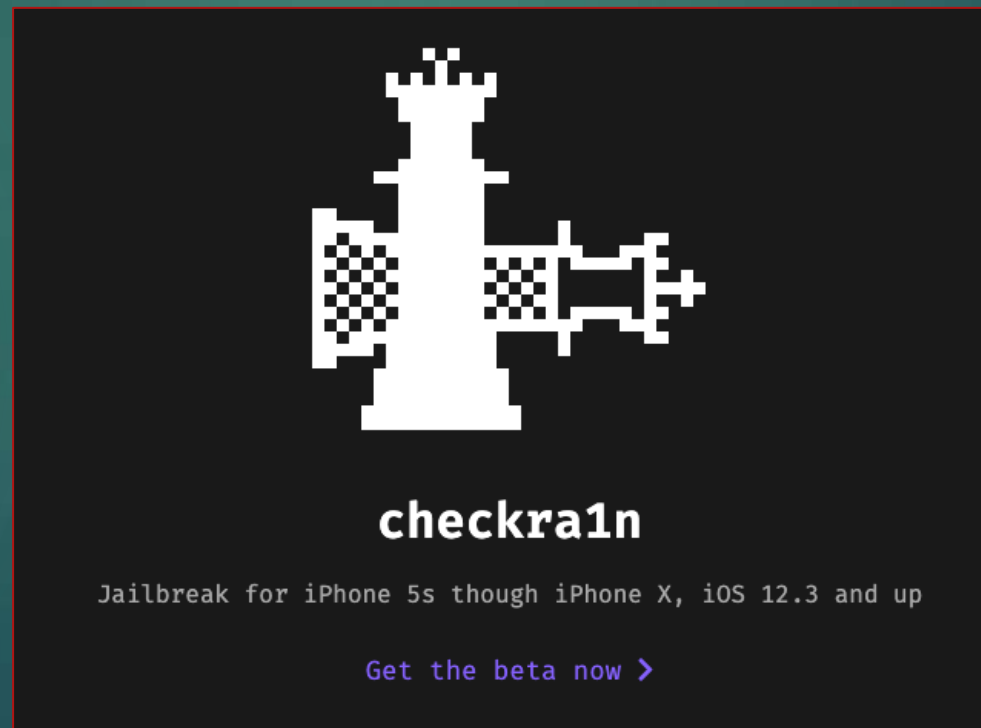


axi0mX/ipwndfu  
open-source jailbreaking tool for many iOS devices -  
axi0mX/ipwndfu  
[github.com](https://github.com)

1:15 PM · 27 set 2019 · [Twitter Web Client](#)

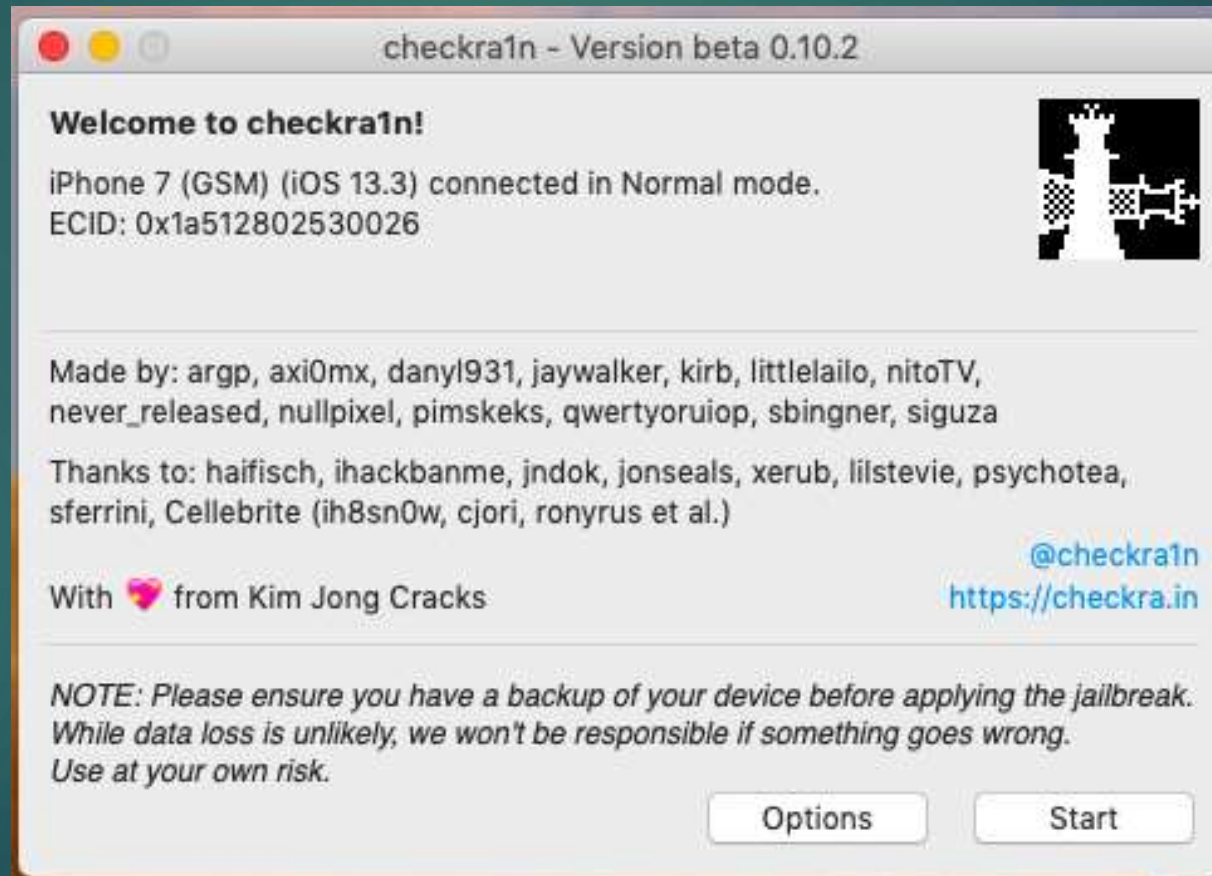
# checkra1n

- ▶ Semi-tethered jailbreak basato su checkm8
- ▶ <https://checkra.in/>



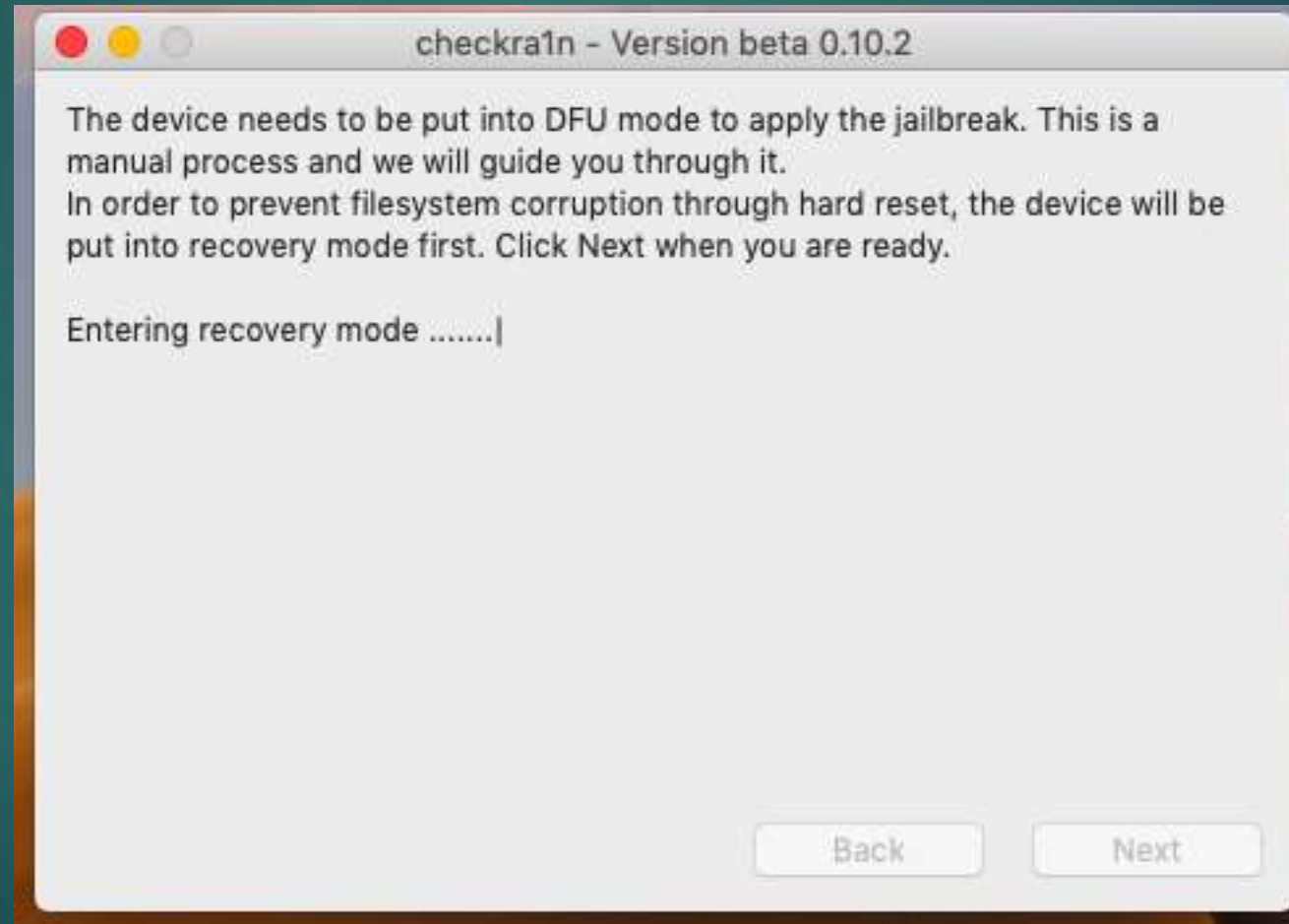
# Step 1

## Collegare iPhone



# Step 2

Il dispositivo viene riavviato in Recovery mode



# Step 3

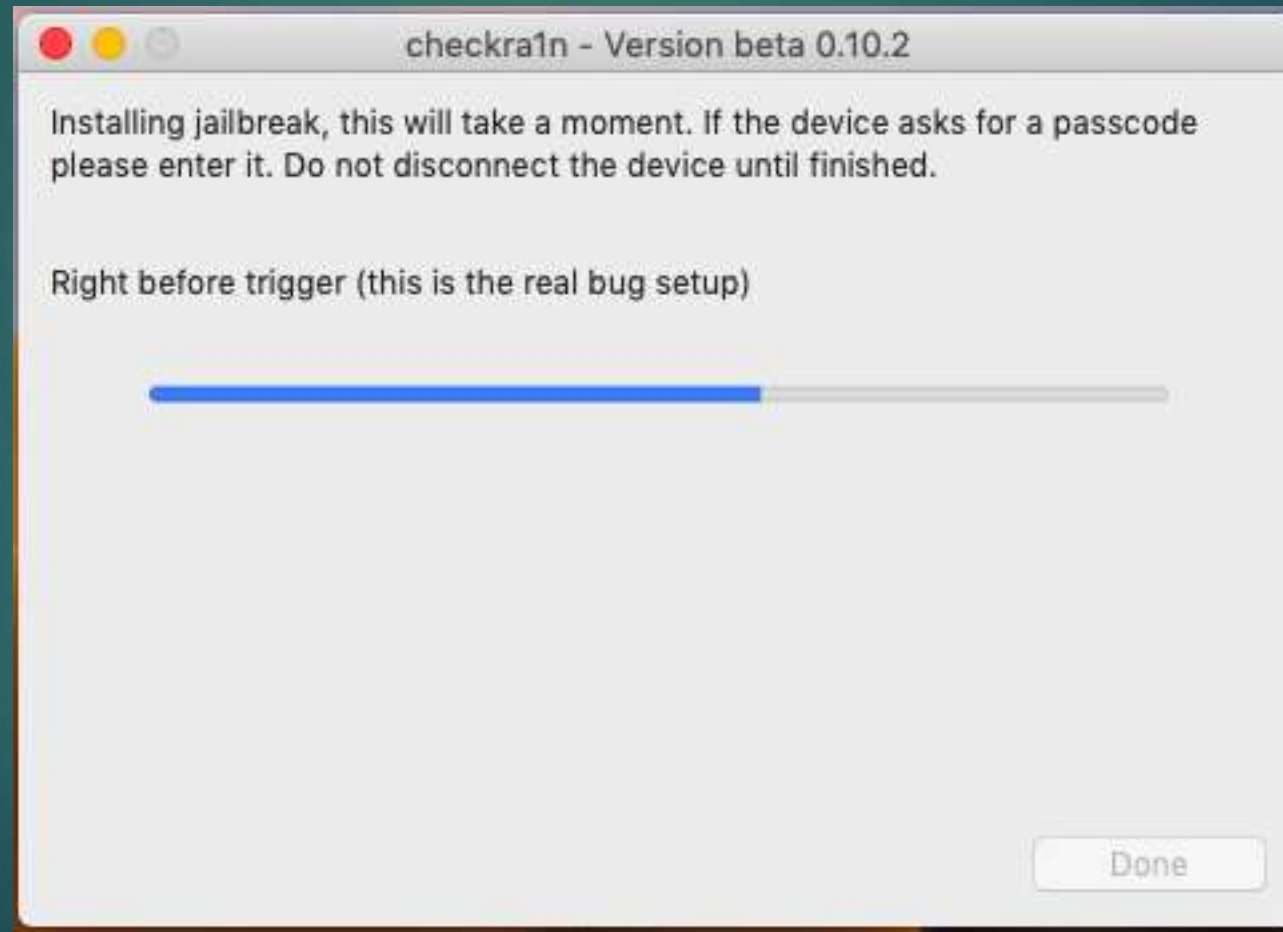
Seguire le istruzioni per avviare il dispositivo in DFU Mode





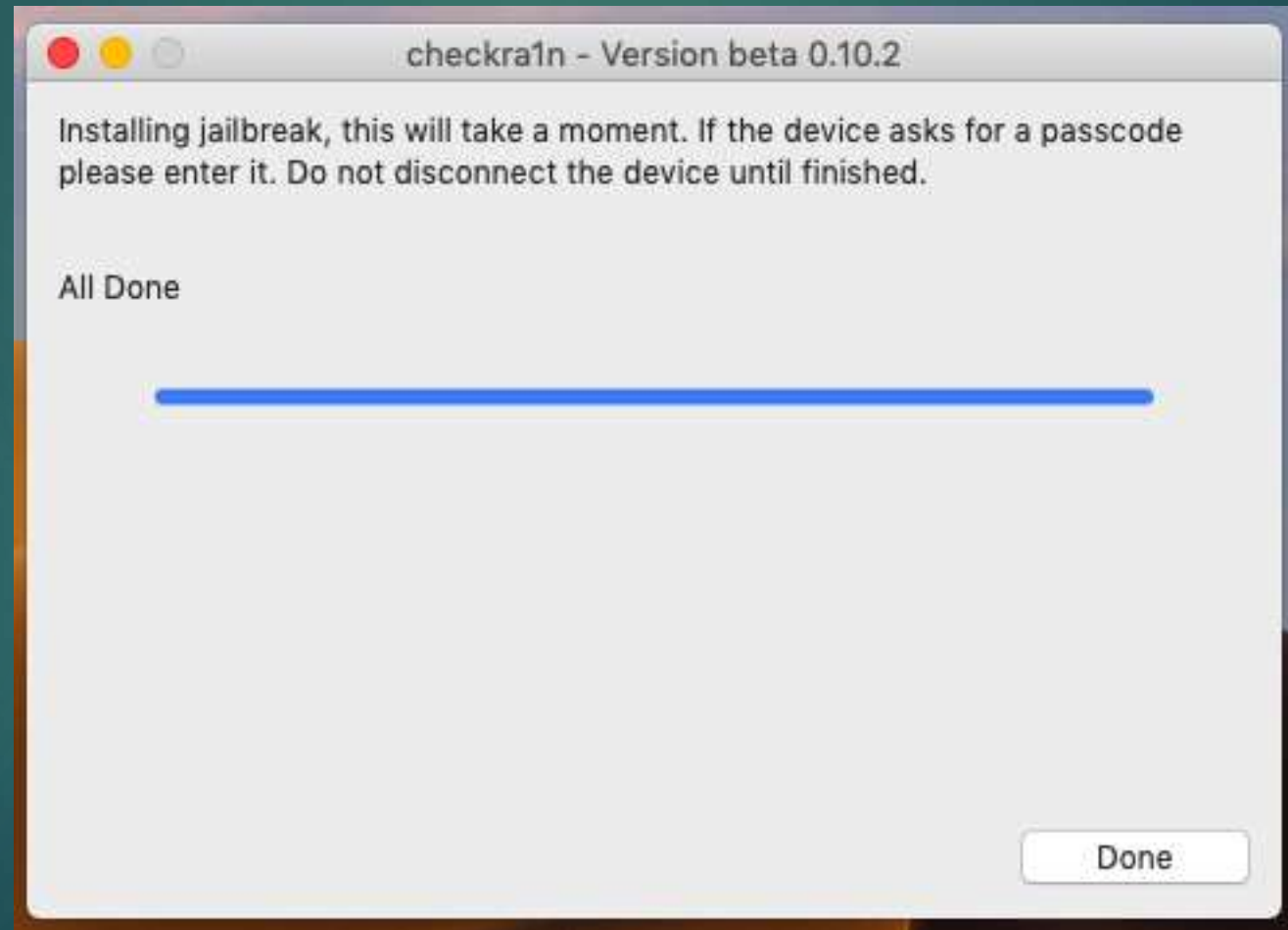
# Step 4

## Jailbreak!






# Step 4

## Jailbreak!




# Post su [blog.digital-forensics.it](http://blog.digital-forensics.it)

 [blog.digital-forensics.it](http://blog.digital-forensics.it)


 **ZENA FORENSICS** 

## Checkra1n Era - Ep 5 - Automating extraction and processing (aka "Merry Xmas!")

By Mattia Epifani - December 23, 2019




After my third post on [how to automate an extraction BFU](#), my great friend, colleague and fellow citizen Giovanni 'sug4r' Rattaro, [Tsurugi Linux](#) team leader and core developer, wrote me a message saying: "Belin Mattia! You had a great idea! But we can quickly improve your script!" And I answered: "Yes, why not. How is it going for you in the next couple of weeks? Do you have time?". And ...

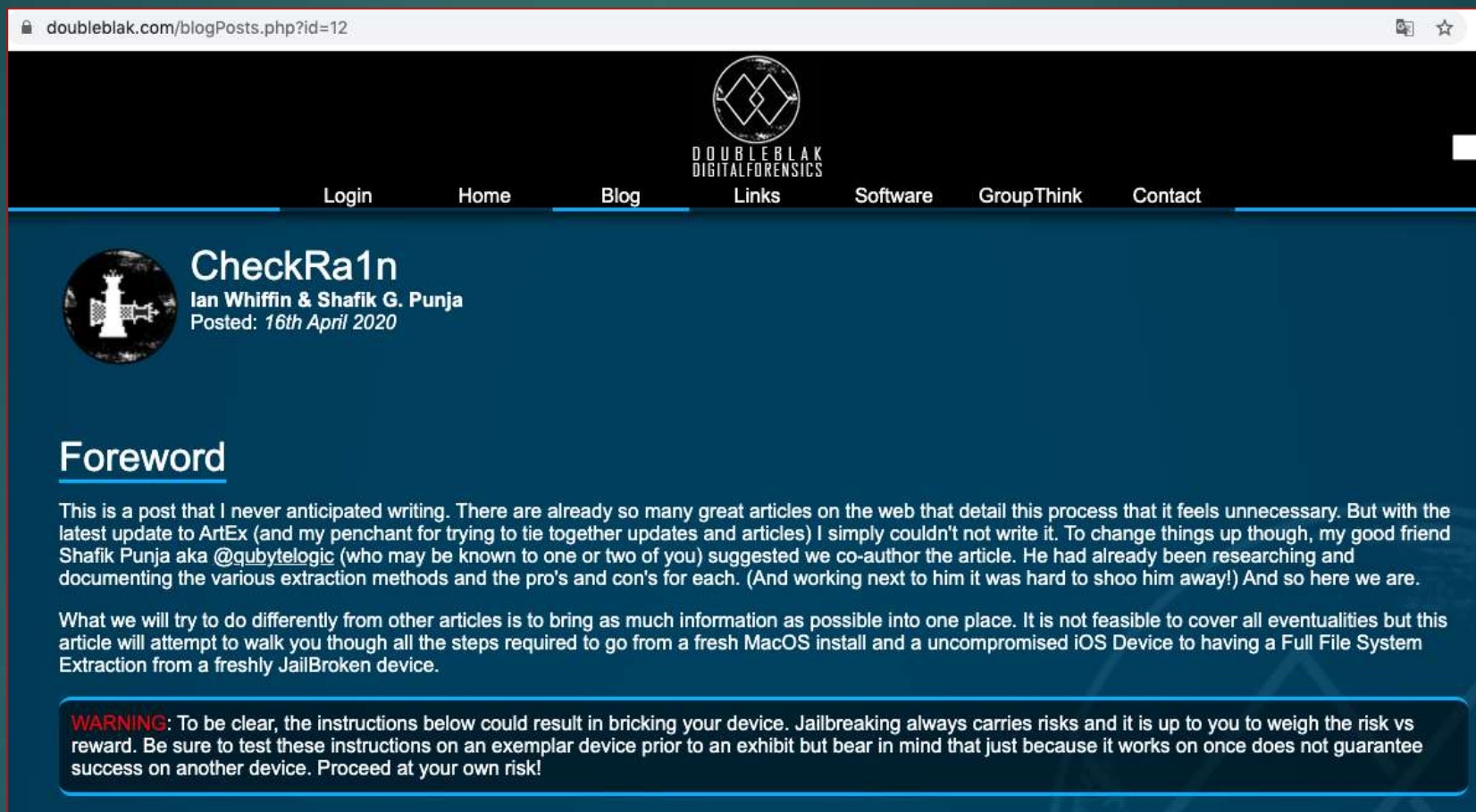


KEEP READING

## Checkra1n Era - Ep 4 - Analyzing extractions "Before"



# Post su Doubleblak.com



The method we are going to focus on however is the method developed by fellow foreniscator Mattia Epifani available at [https://github.com/RealityNet/ios\\_bfu\\_triage](https://github.com/RealityNet/ios_bfu_triage) which is a free and awesome tool that is also pretty straight forward to use once the preperation steps are completed.

I should state pretty early on for anyone who isn't familiar.

# Step 5

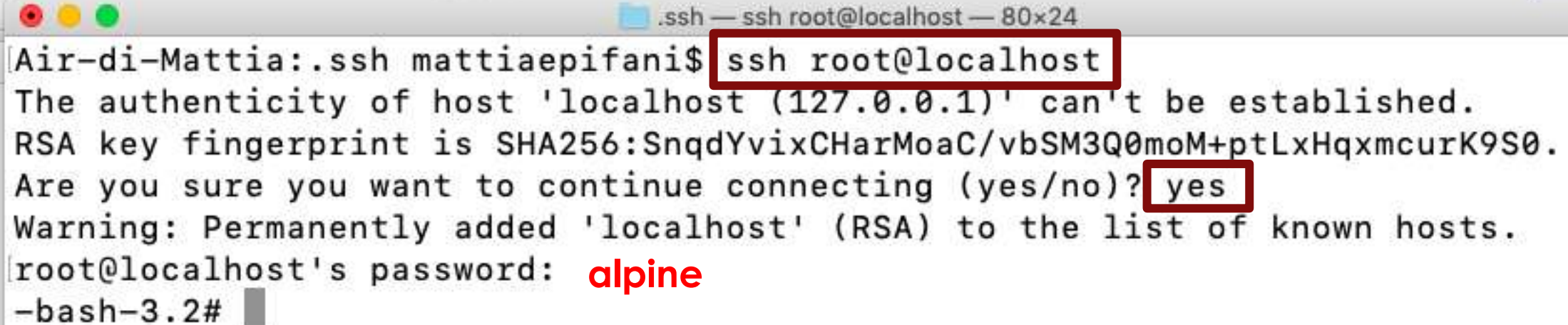
Eseguire iproxy Libimobiledevice.org

```
mattiaepifani — iproxy + sudo — 80x24
Last login: Sat May 30 09:48:29 on ttys000
Air-di-Mattia:~ mattiaepifani$ sudo iproxy 22 44
Password:
waiting for connection
accepted connection, fd = 4
waiting for connection
Number of available devices == 1
Requesting connecion to device handle == 2 (serial: 4a3251cf16913c1e99bd49e0ada5
6c24e13f0918), port 44
run_ctos_loop: fd = 4
run_stoc_loop: fd = 4
```



# Step 6

## Collegarsi al dispositivo via ssh



A screenshot of a terminal window titled ".ssh — ssh root@localhost — 80x24". The prompt is "Air-di-Mattia:~\$". The user has entered "ssh root@localhost", which is highlighted with a red box. The terminal displays the following text: "The authenticity of host 'localhost (127.0.0.1)' can't be established. RSA key fingerprint is SHA256:SnqdYvixCHarMoaC/vbSM3Q0moM+ptLxHqxmcurK9S0. Are you sure you want to continue connecting (yes/no)?", where "yes" is highlighted with a red box. Below this, it says "Warning: Permanently added 'localhost' (RSA) to the list of known hosts." and "root@localhost's password: alpine", with "alpine" in red. The prompt changes to "-bash-3.2#".

```
Air-di-Mattia:~$ ssh root@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
RSA key fingerprint is SHA256:SnqdYvixCHarMoaC/vbSM3Q0moM+ptLxHqxmcurK9S0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
root@localhost's password: alpine
-bash-3.2#
```

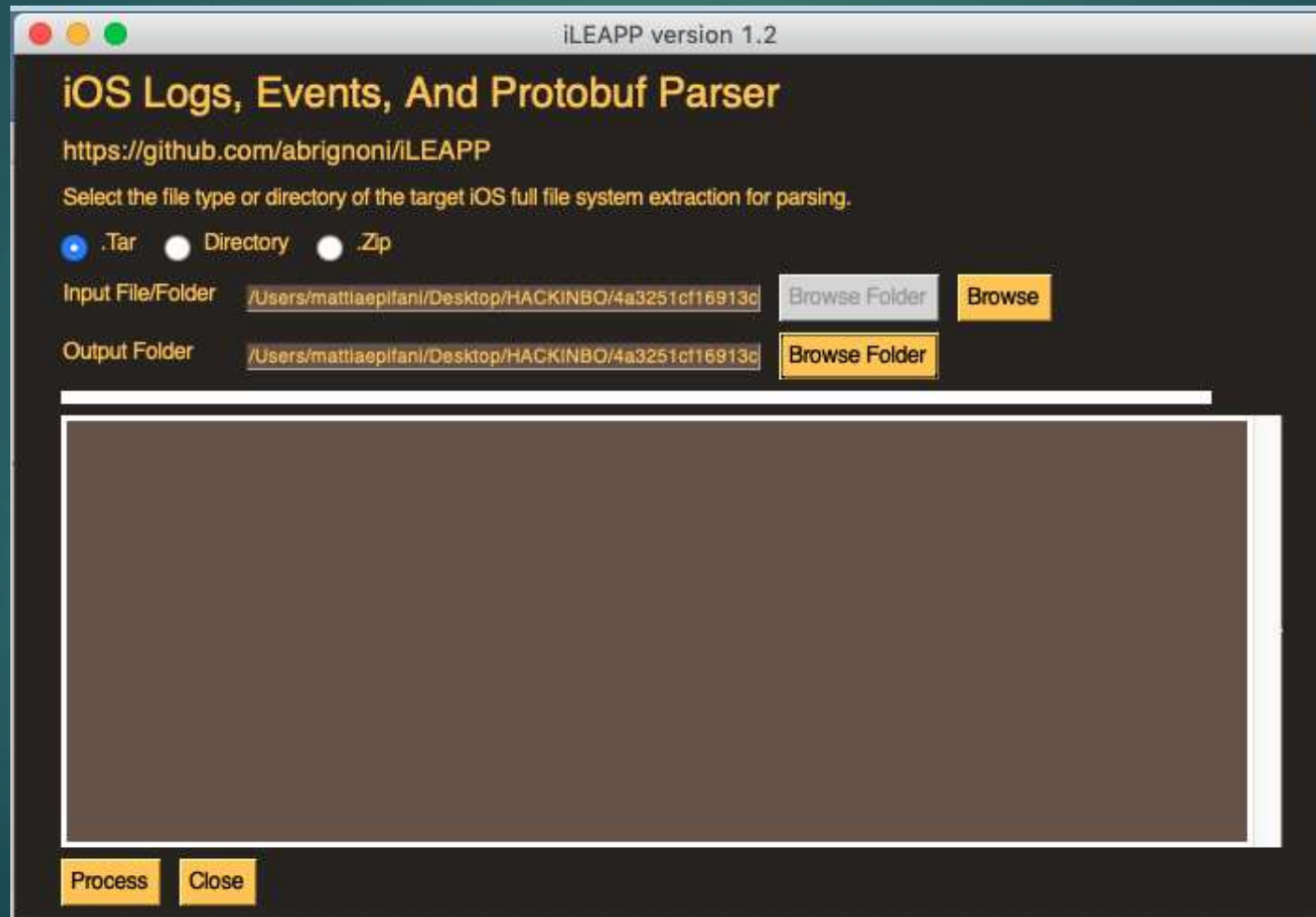
# Step 7

## Esequire iOS BFU Triage



# Step 8

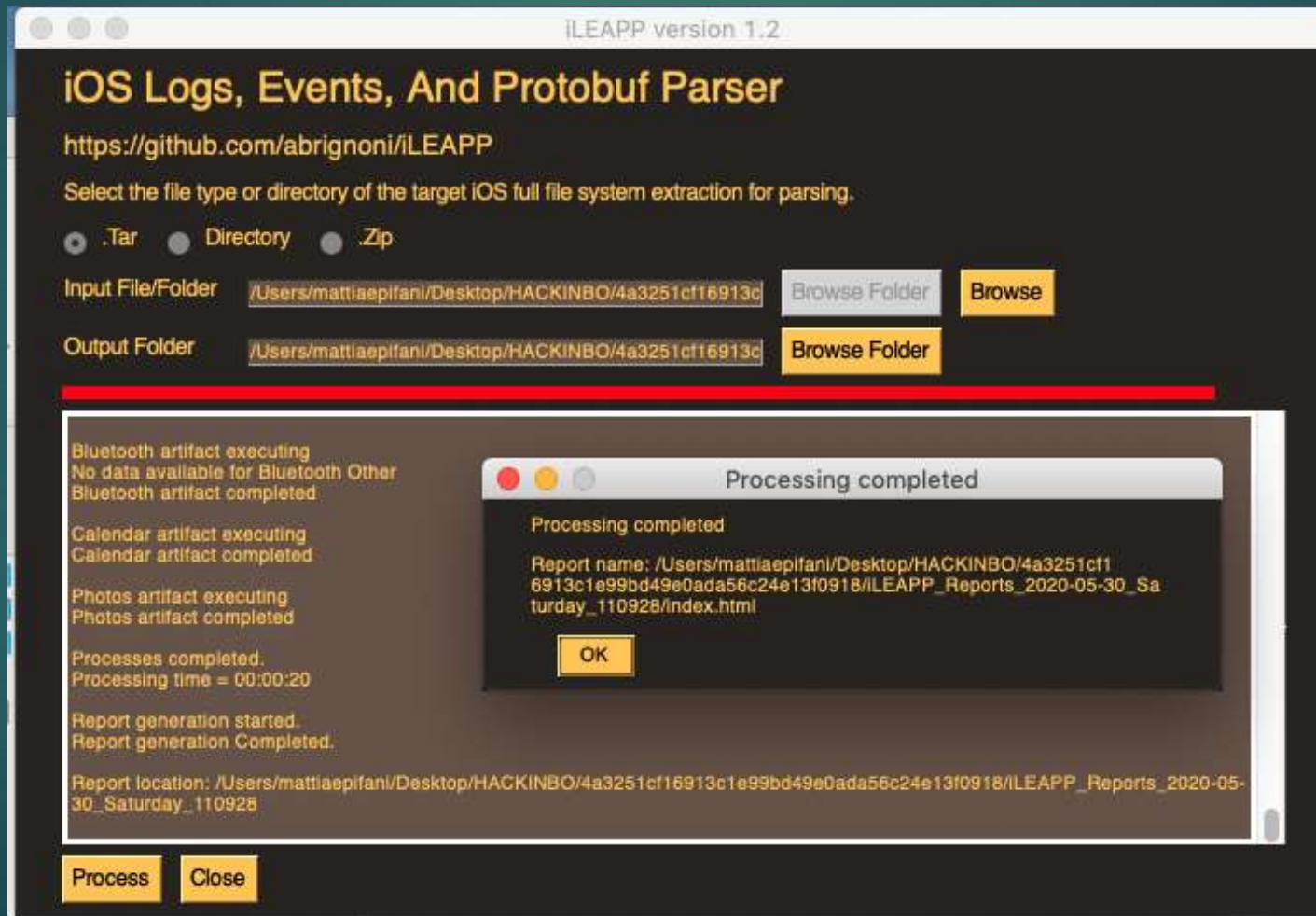
## Esequire iLEAPP





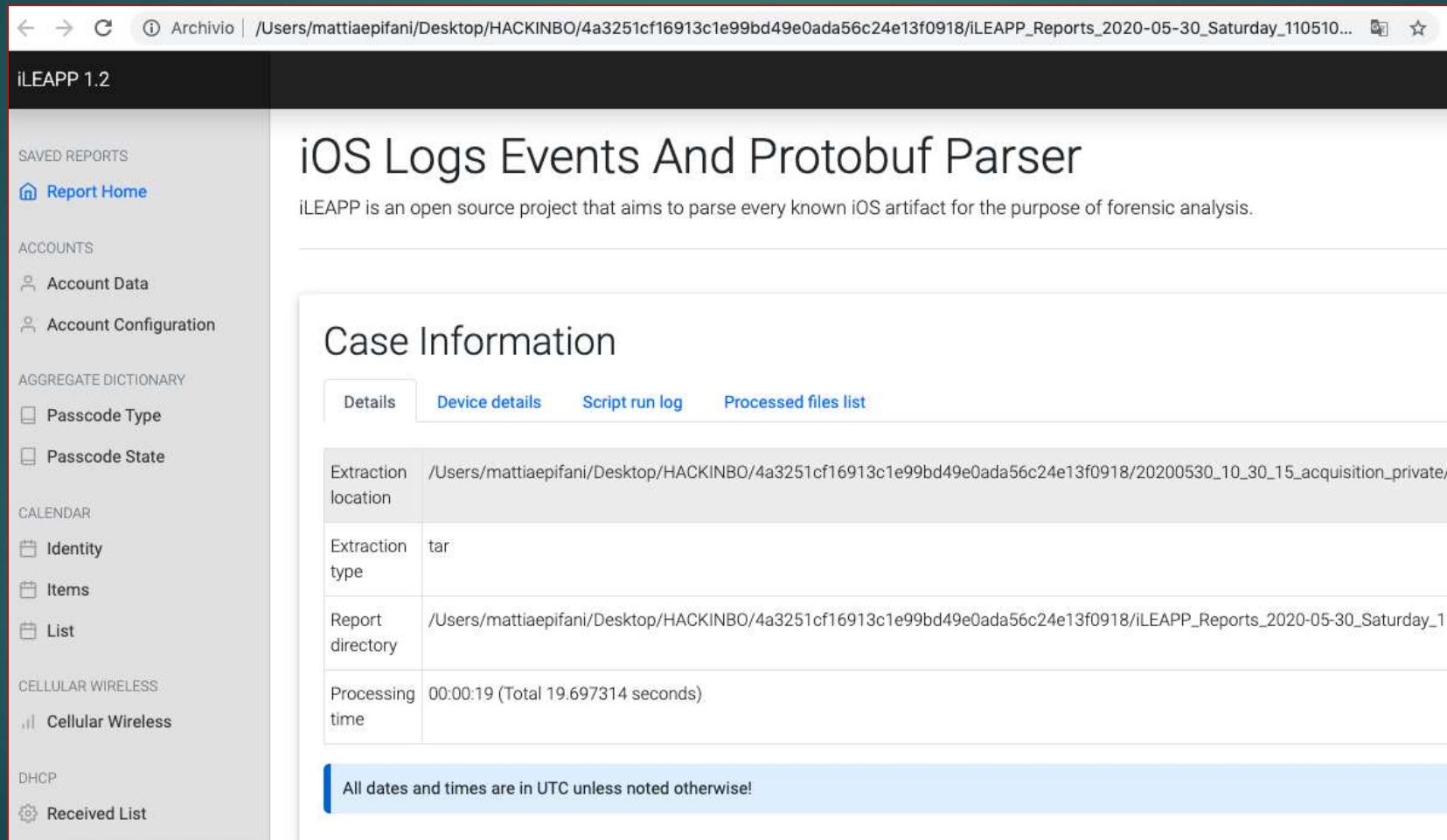
# Step 8

## Esequire iLEAPP



# Step 9

## Analizzare il risultato



The screenshot displays the iLEAPP 1.2 web application. The browser's address bar shows the URL: `/Users/mattiaepifani/Desktop/HACKINBO/4a3251cf16913c1e99bd49e0ada56c24e13f0918/iLEAPP_Reports_2020-05-30_Saturday_110510...`. The application's header is dark with the text "iLEAPP 1.2".

The left sidebar contains several sections of navigation links:

- SAVED REPORTS**: [Report Home](#)
- ACCOUNTS**: [Account Data](#), [Account Configuration](#)
- AGGREGATE DICTIONARY**: [Passcode Type](#), [Passcode State](#)
- CALENDAR**: [Identity](#), [Items](#), [List](#)
- CELLULAR WIRELESS**: [Cellular Wireless](#)
- DHCP**: [Received List](#)

The main content area is titled "iOS Logs Events And Protobuf Parser" and includes a subtitle: "iLEAPP is an open source project that aims to parse every known iOS artifact for the purpose of forensic analysis." Below this is a "Case Information" section with four tabs: "Details" (selected), "Device details", "Script run log", and "Processed files list".

Field	Value
Extraction location	/Users/mattiaepifani/Desktop/HACKINBO/4a3251cf16913c1e99bd49e0ada56c24e13f0918/20200530_10_30_15_acquisition_private/
Extraction type	tar
Report directory	/Users/mattiaepifani/Desktop/HACKINBO/4a3251cf16913c1e99bd49e0ada56c24e13f0918/iLEAPP_Reports_2020-05-30_Saturday_110510...
Processing time	00:00:19 (Total 19.697314 seconds)

A blue banner at the bottom of the Case Information section states: "All dates and times are in UTC unless noted otherwise!"

# Riferimenti

- ▶ <https://github.com/mattiaepi/HackInBoSafeEdition2020>
- ▶ <https://checkra.in/>
- ▶ <https://blog.digital-forensics.it/>
- ▶ <https://doubleblak.com/blogPosts.php?id=12>
- ▶ <https://github.com/abrignoni/iLEAPP>

# CREDITS AND CONTACTS

## **RN Team**

Mattia Epifani

Francesco Picasso

Fabio Massimo Ceccarelli

Claudia Meda

Silvia Spallarossa

## **iOS BFU Triage**

Giovanni Rattaro

**mattia.epifani@realitynet.it**  
**@mattiaep**