IOS 탈옥

91613777 연호준
91613662 김효성

Table of Contents

- 탈옥이란? 그리고 왜 탈옥인가?
- 역사 및 원리
- 탈옥 해보기
- 소스를 이용해 트윅사용하기
- 탈옥 활용하기
- 후기

1. 탈옥이란?

탈옥 (jailbreak)이란 애플과 앱스토어에서 막아놓은 컨텐츠들을 기기의 최고권한을 부여하여 사용할수 있게 만드는 작업입니다.

탈옥이란 용어는 애플과 앱스토어에서 막아놓고 제한적인 사용을 마치 감옥에 가둔것과 같다. 라고 표현하며

최고권한을 주어 제한된 기능들을 사용가능하게 하는것은 감옥에서 탈출하는것과 같다고 표현하여 탈옥이라 불리게 되었습니다

역사 및 원리

1.IOS 1

탈옥이란 IOS의 첫 시작이라 볼수있는 IOS 1.1.1 에서 부터 시작되었다. 사용자들은 아이팟에서 버그를 발견하였고 탈옥계발팀인 아이폰 데브팀이 버그를 이용해 탈옥에 성공했지만 재부팅시에 오류와 함께 강제 복원을 해야한다는 불편함이 있었다.

2.IOS 2~3

IOS 2 서부터 현재까지 쓰이는 Cydia 가 존재했기 시작했고 현재와는 다르게 installer가 따로 존재했다. Cydia에는 각종 트윅이 존재했고 installer에는 각종 테마와 게임이 존재했다,

• IOS 4

IOS 4 부터가 정말 탈 할 고
많은 기능을 부여할 다.

redsn0w, greenpois0 필 e탈
옥툴도 배포됐으며 다양

홈화면의 스크롤 애니 터 로고
도 바꿀수가 있을만큼 가 되었
습니다.

IOS 5~8

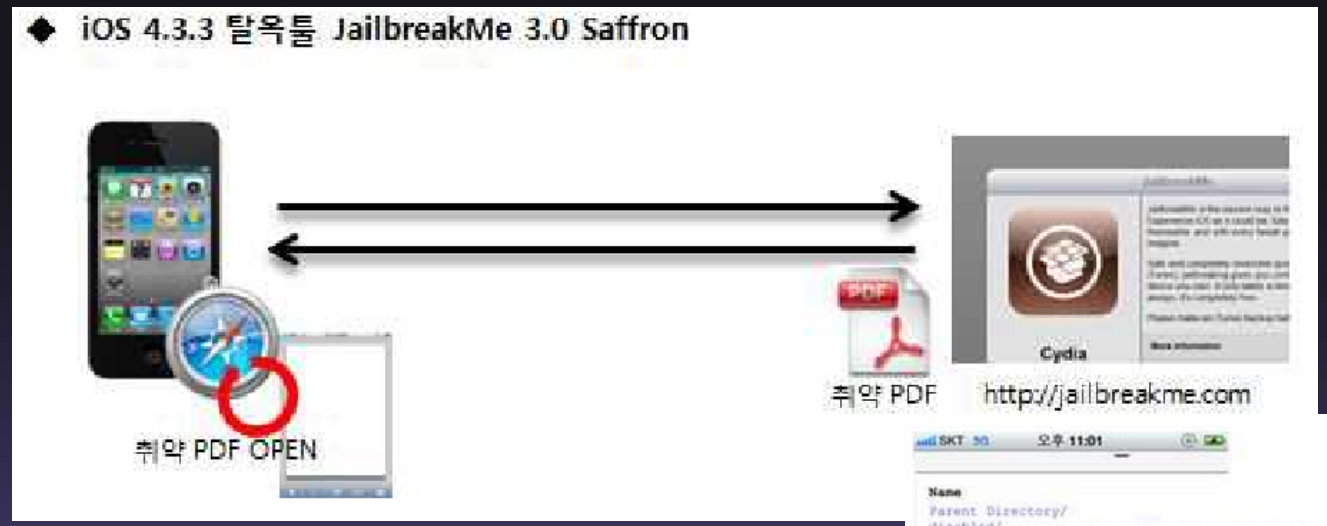
탈옥계발팀인 redsn0w가 나머지 탈옥을 맡았습니다

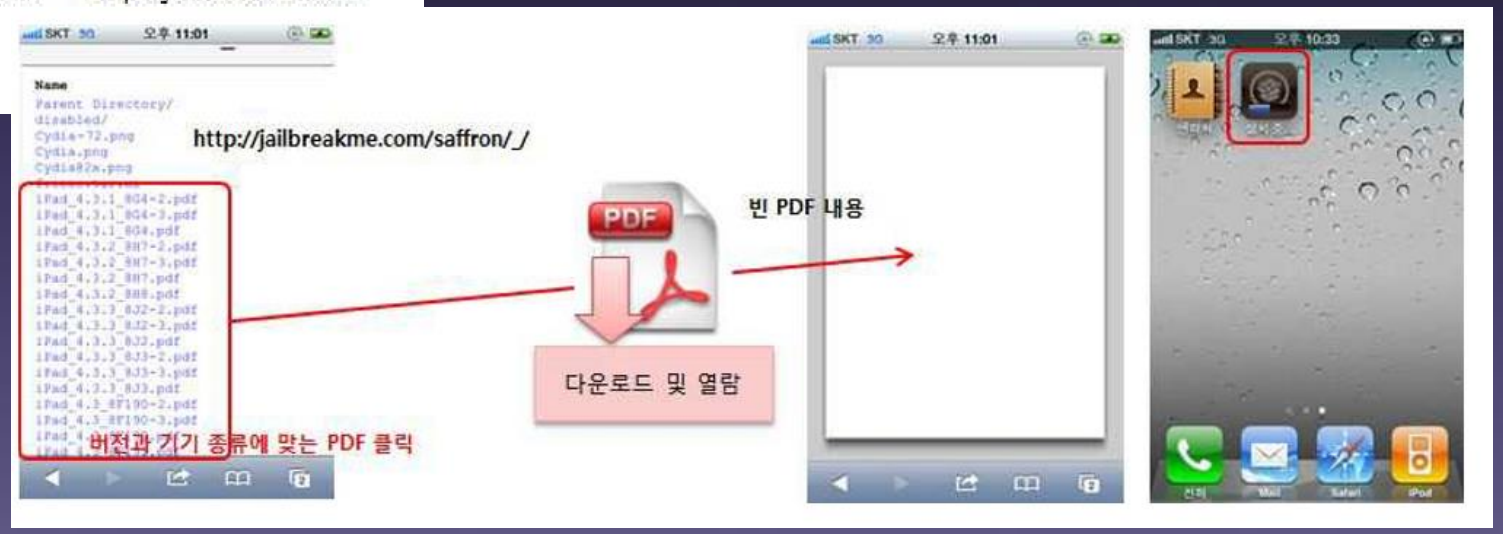
IOS 9

중국의 탈옥팀인 Pangu 현재 9.1버젼까지 탈옥을 만들었습니다.

원리

JailbreakMe

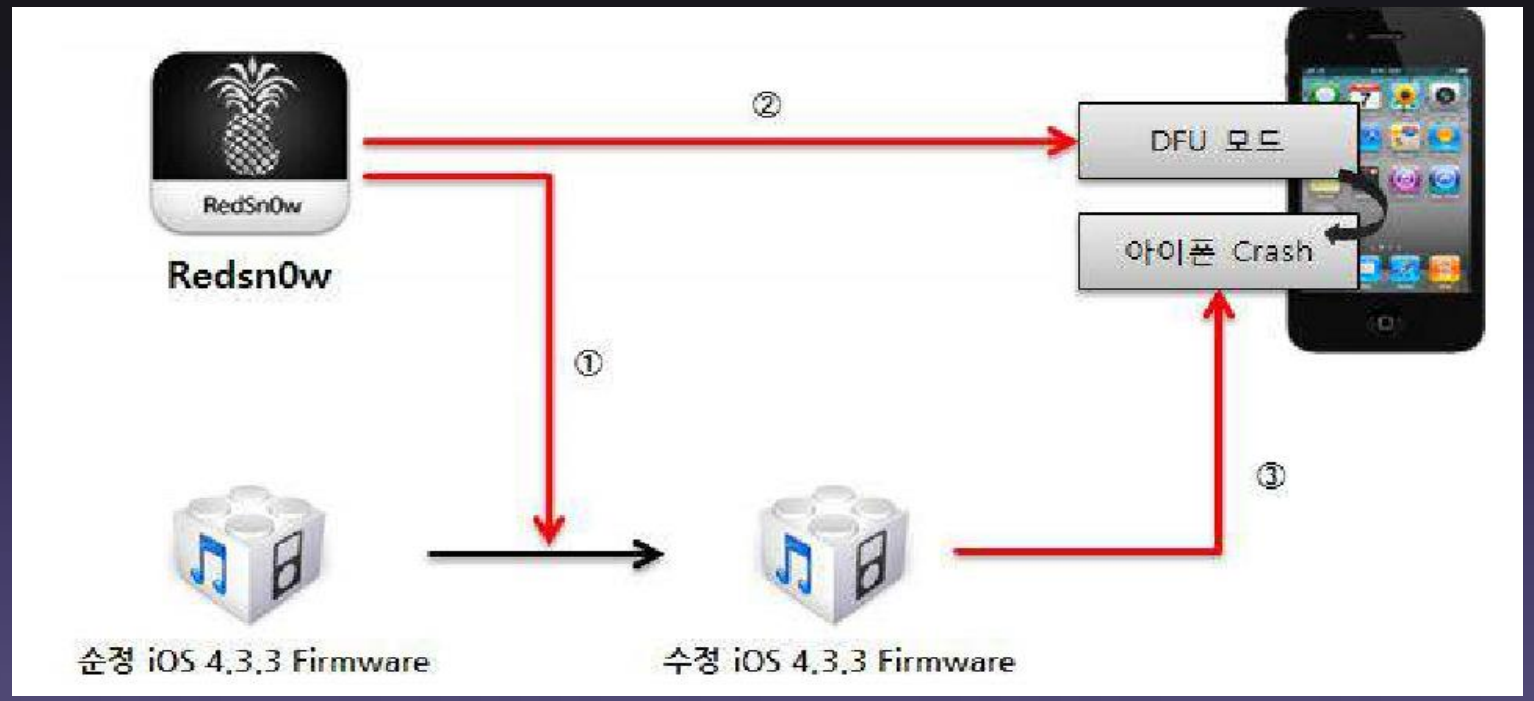




Jailbreakme

IOS 4.X는 PDF 파일을 여는 부분에서 취약점이 있었다.
탈옥 계발자들은 이 취약점을 이용해 빈 PDF를 이용해 탈옥에 필요한 파일을 공격하여 수정할수가 있었다.

Greenpois0n 과 Redsn0w



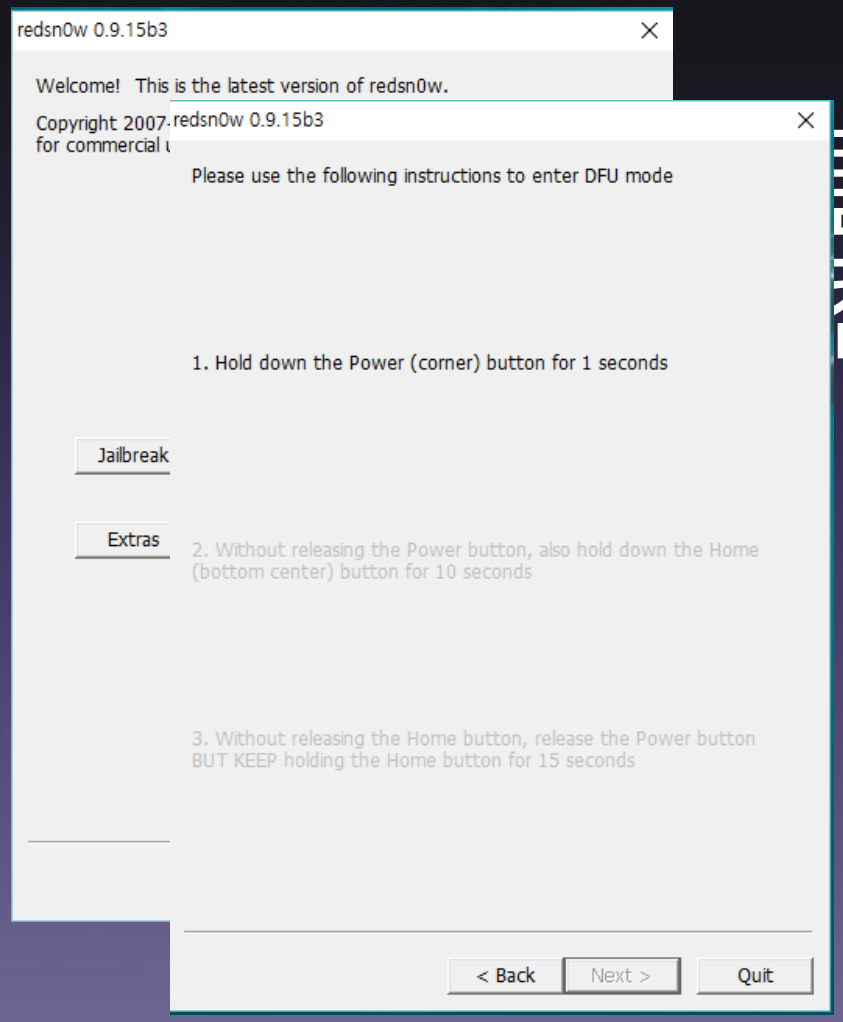
Readsn0w와 greenpois0n 은 순정 .ipsw 펌웨어 파일을 수정하여 dfu모드에 들어가있는 아이폰을 Crash 하여 수정된 펌웨어로 업데이트를 하는 방식이다.

3.탈옥해보기

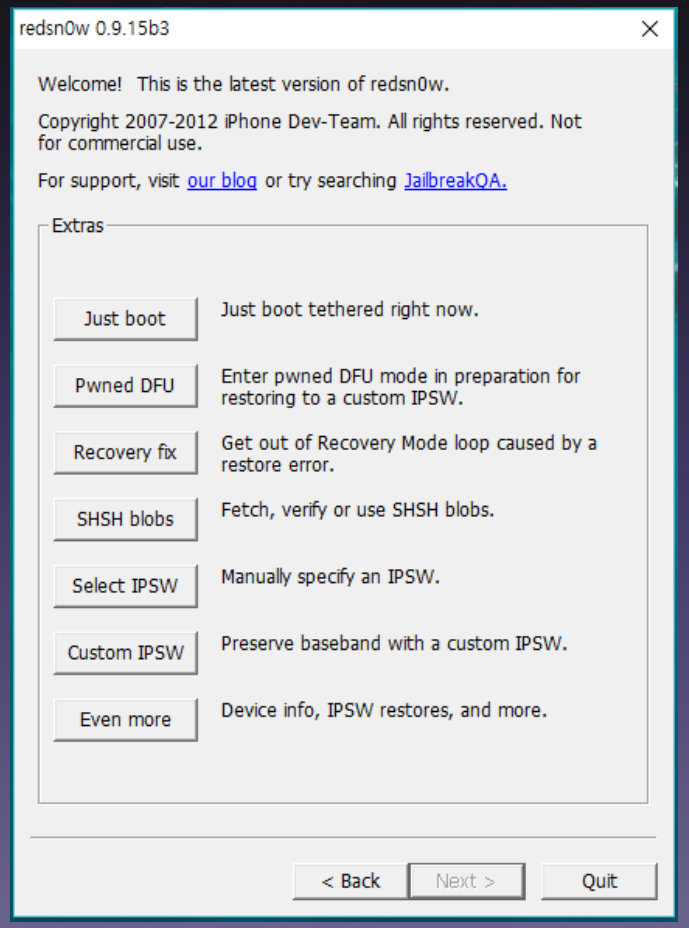
탈옥 기기 정보

기기:아이팟 4세대

펌웨어 정보:IOS 6.1.6

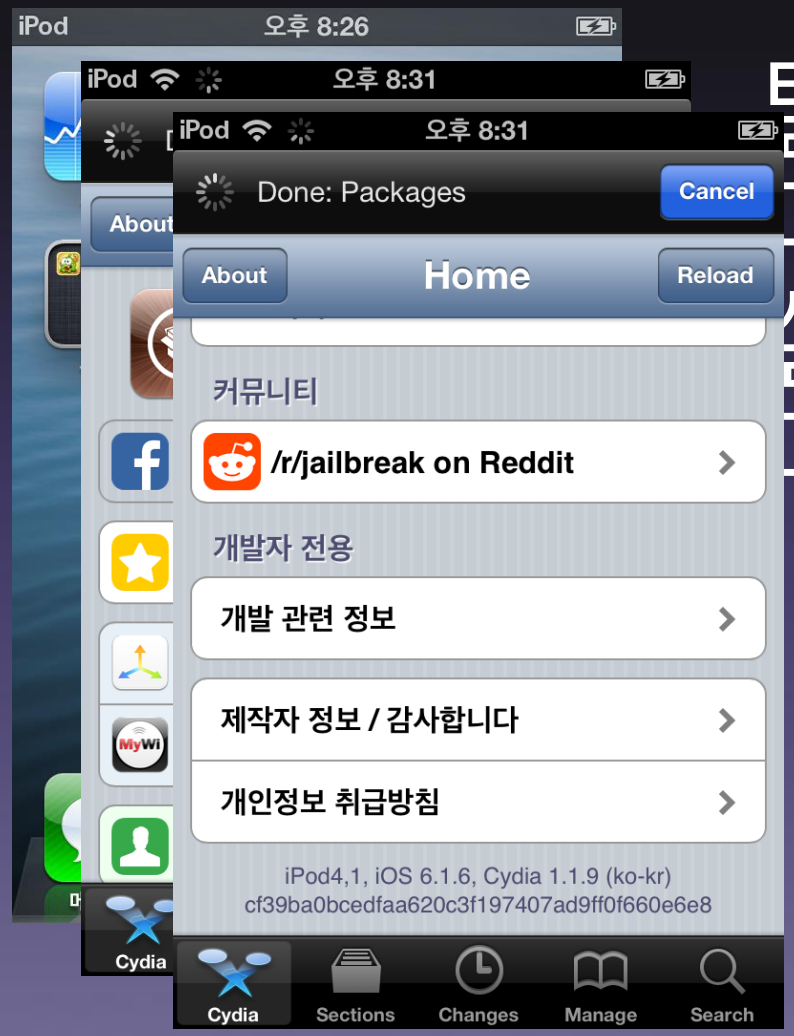


탈옥툴인 redsn0w를 실행시
킨 모습입니다.



Extra 버튼을 누르면 일명 '반탈' 을 위한 부팅 버튼과 복원된 shsh를 통해 탈옥된 펌웨어 파일을 만드는 shsh blobs 등이 있습니다

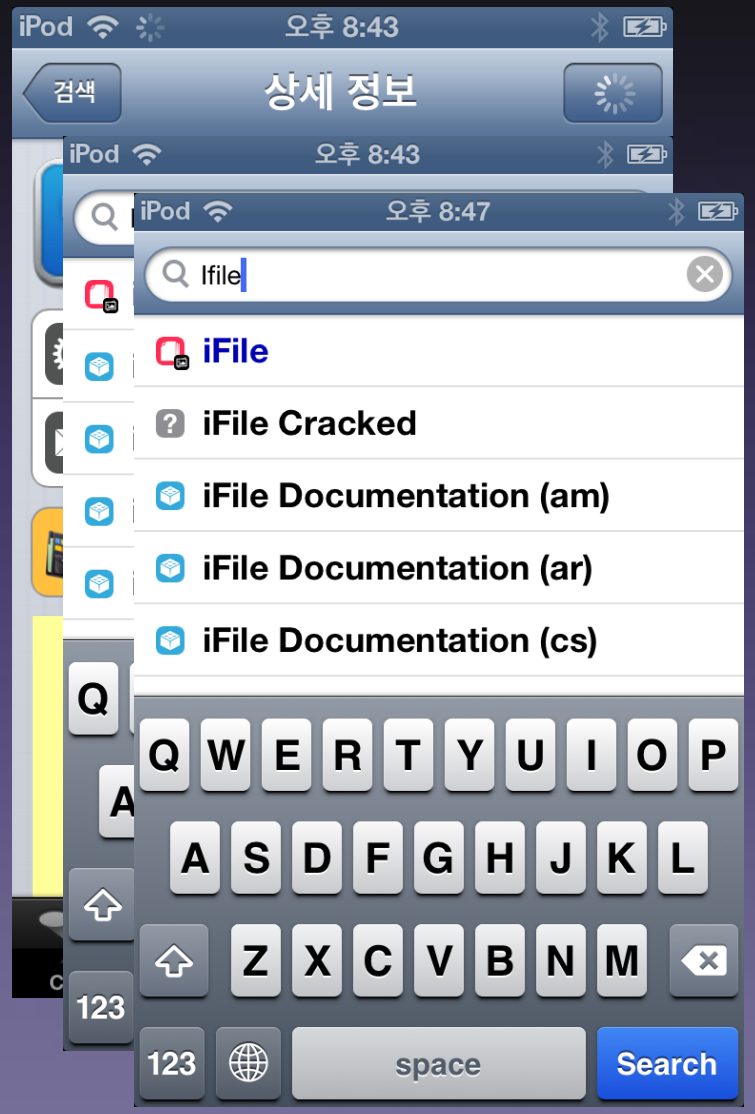
하지만 저는 IOS 6만을 위한 아주 간편한 탈옥 툴인 p0sixsqwn을 이용하여 탈옥을 하였습니다.



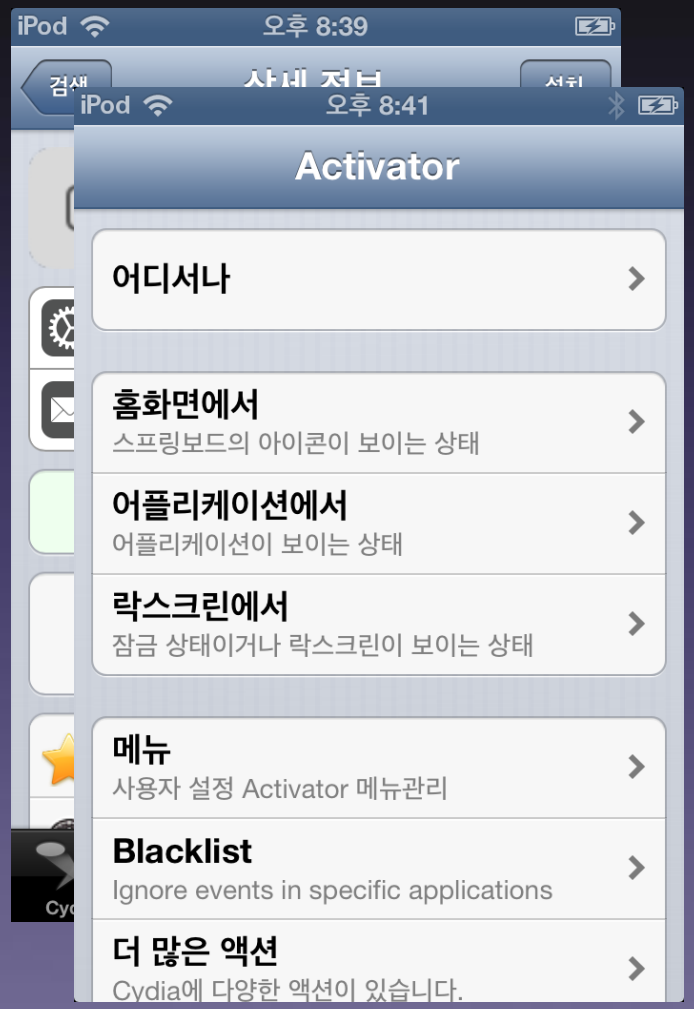
탈옥이 끝나니 탈옥이 완료되었다는것을 인증해주는 Cydia가 설치가 되있는것을 알수있습니다

Cydia의 실행화면입니다

소스 탭을 누른 모습입니다.
이곳에서 소스를 추가한다면
트윅을 무궁무진하게 받을수
있습니다.

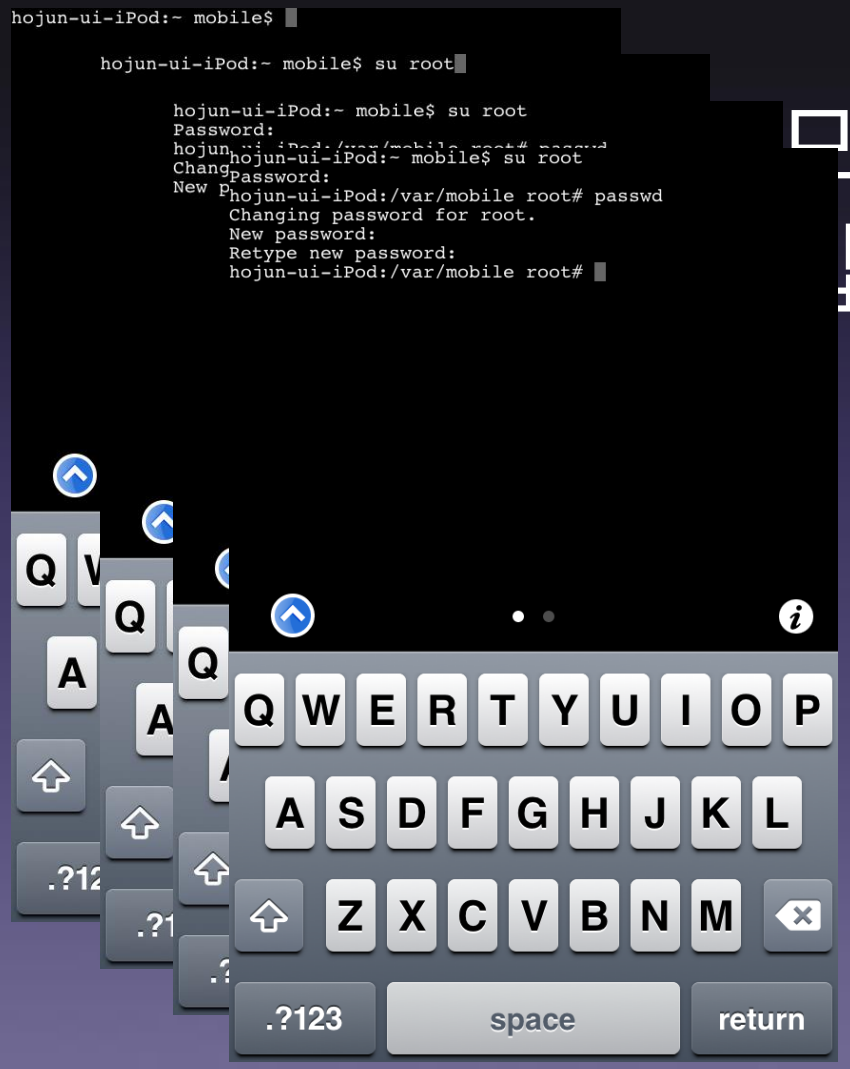


아이폰의 파일 탐색기인 ifile은 유료 트윅입니다.
하지만 일정 소스를 추가한다면
무료로 받을수가있습니다



또다른 트윅중 하나는 activator입니다.
이 트윅은 잠금화면의 시계를 두번 탭한다는 등 일정 행동을 하면 설정해놓은 기능을 실행시켜주는 트윅입니다.

저희는 정보보호학개론 강의때 교수님이 알려주신 아이폰 터미널의 비밀번호를 바꾸어 보았습니다.



모바일 터미널 실행화면입니다.

리눅스 처럼 su root 를 입력했습니다.

그다음 passwd를 입력하자 새로운 비밀번호를 입력하라는 글이 나왔습니다.

새로운 비밀번호를 입력하고 return 을 누르자 새로운 비밀번호가 설정되었습니다.

이뿐만 아니라 간편 설정창과 앱스토어 안의 유료어플들을 다운받을수있는 트윅, 그리고 인앱 구매를 무료로 바꿔주는 트윅들도 존재합니다.

인앱 구매에서 구매인증 단계를 건너뛰어 무료로 구매를 하는 모습입니다.

스와이프 애니매이션을 바꿀수있는 Barrel 트윅입니다.

후기

- 정말 IOS 4에서부터 6까지는 탈옥 트윅의 종류도 다양하고 사용도 편리했지만 점점 보안이 업데이트 되어가는 펌웨어에 탈옥툴의 출시도 늦어져가고 트윅들도 지원을 하지않아 탈옥의 의미를 잃어 버렸습니다.
- 하지만 구버전의 펌웨어를 쓴다면 정말 세상에 단 하나밖에 없는 기기를 만들수도 있다는 생각에 탈옥 후 에는 무궁무진한 가능성을 가졌다는것을 알수있게 되었습니다.

Q&A