ZPETv2

The iOS Zero-Pin Extraction Toolkit

Build ID **16807**

DuffyAPP-IT
@J_Duffy01

ZPETv2 Application

ZPET is designed to allow for the analysis of iDevices in Before First Unlock (**BFU**) Mode. **ZPET** will allow for the extraction of various pieces of information which may be considered sensitive in some environments.

Examples include Installed **Application Identifiers**, **WiFi Access Point Information**, **Apple ID** & Other **Accounts** on-device.

Other than the built-in Modules, the community has the option to **create their own Modules** for **ZPET**.

This will allow for the functionality of **ZPET** to be expanded and support extra third party applications such as **Twitter** (WIP), **WhatsAPP**, **Facebook**, **Signal** and more.

Requirements

Hardware Requirements:

- macOS Device running 10.13 or later
- Lightning - USB-A Cable

Software Requirements:

- **Brew Package Manager** (https://brew.sh)
- **libimobiledevice** (brew install libimobiledevice)
- **Checkra1n binary** (obtained via https://checkra.in)

The software is delivered as a compiled binary to be executed directly from the macOS terminal.
No proprietary or specialist hardware is required to operate ZPETv2.

Launch Instructions

To launch ZPETv2, follow these instructions:

- Use Checkra1n to boot the iOS Device. The device does not have to be unlocked.
- Modify '**module-loader**' (inside the **Modules** directory) to load the modules you have added to the 'Modules' directory.
- Launch the macOS terminal
- 'cd' to the directory of the extracted ZPET Build ZIP.

  for example '**cd ~/Downloads/ZPETv2-16807**'
- Execute **ZPET** on the macOS Host using the following command '**sudo ./ZPETv2**'

Common Issues

Error	Solution
`ZPET component 'moduleloader' is missing!`	The binary was possibly double-clicked, instead of being launched directly from the terminal. This problem is caused by macOS default behaviour (which is to execute binaries from the users 'home' folder if double-clicked).
`prerequisites not fulfilled!`	The installation of libimobiledevice is likely to be corrupt - try manually re-installing using the terminal command: '**brew reinstall libimobiledevice**'
`Module Could Not Execute - iosRecieve Failed...`	Is the connected device booted with checkra1n and connected via USB?

Module Specification / Development Process

Developing a module for ZPETv2 has been designed specifically with ease of the development, testing and release process in mind.

Each ZPETv2 Module is comprised of 5-8 lines of text in a file - nothing complex here. Build it in **nano**, TextEdit or really any editor of choice.

Module Design

Line#	Contains…	Example…
1	**Module Name*** - What's your module going to display?	Installed iOS Applications
2	**Module Description*** - Roughly a single line - provides a little more clarity to the data-source	Fetch Installed iOS User Applications from FrontBoard
3	**Module Author*** - Website, Blog, Twitter Handle? :-)	DuffyAPP_IT
4	**Source File*** - The File/Folder 'Of Interest' - Automatically retrieved from the connected device (**tar** support in the future)	/var/mobile/Library/FrontBoard/applicationState.db
5	**Parse Type*** - **sqlite, plist, exec** (JSON support in a future update)	sqlite
6	**Specific Value*** - This value's meaning changes based on the parse type. In the case of a SQL database, this value will contain the Query. In the case of a plist, this will contain the 'Key' of the data you're retrieving.	SELECT DISTINCT Application_identifier FROM kvs_debug LIMIT 8
7	**Exec End** - This value is often used where a 'second operation' is required to fulfil the functionality of the module. Completely optional, but supported.	Echo 'COMPLETE'
8	**Pipe-Init-Process** - This value can be used for a variety of purposes - for example, piping the SQL Query or plist **stdout** to 'grep' or another CLI utility of choice.	grep description | cut -f2- -d':' | sort --unique

It's worth noting that if you require **Pipe-Init-Process**, but not **Exec End**, you are able to replace line 7 with a blank line.

Complete Modules