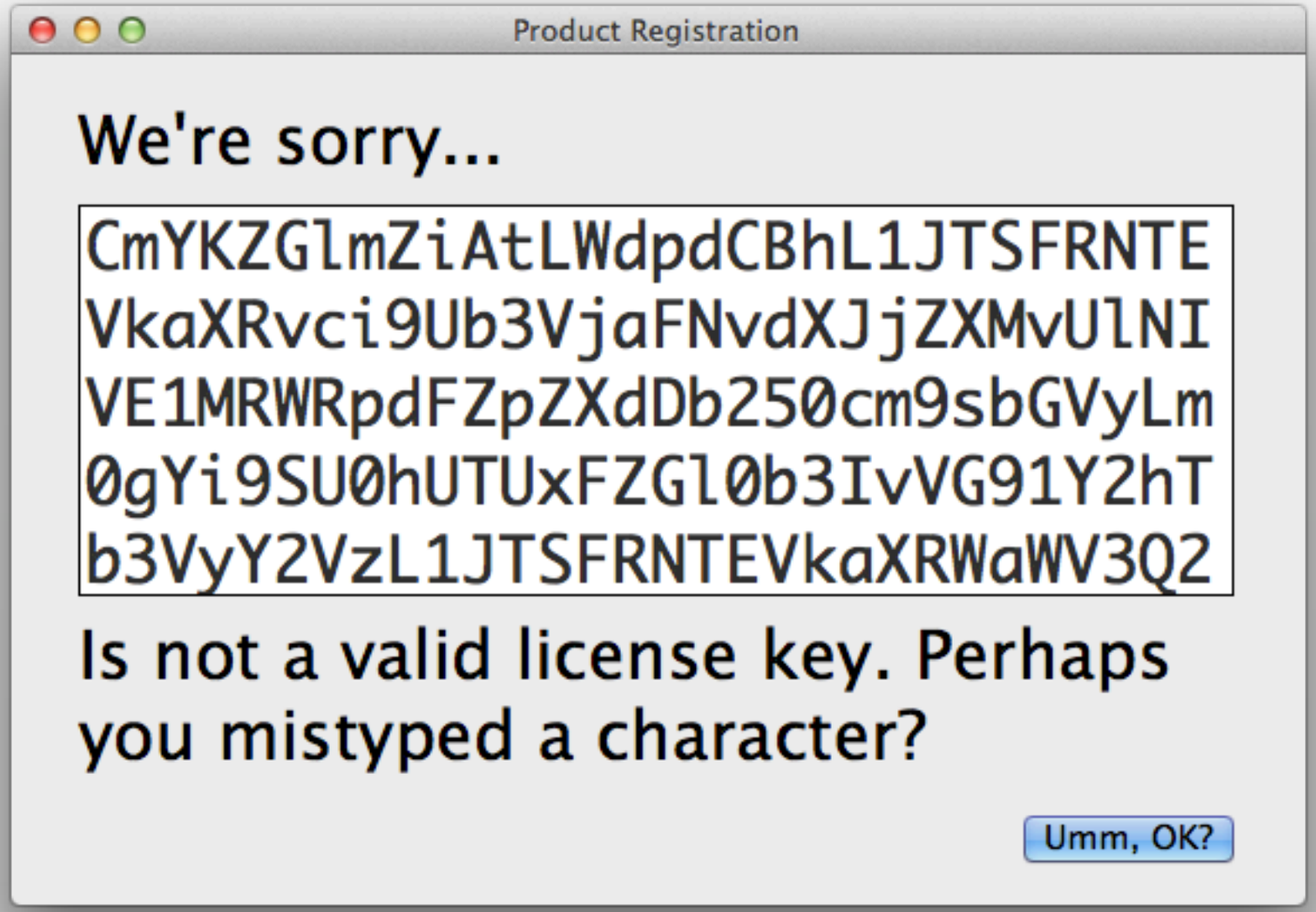
Would You Like A Receipt With That?

Daniel Jalkut | red sweater

Receipt, Brah?


Product Registration
We're sorry...
CmYKZGlmZiAtLWdpdCBhL1JTSFRNTE
VkaXRvci9Ub3VjaFNvdXJjZXMvUlNI
VE1MRWRpdFZpZXdDb250cm9sbGVyLm
0gYi9SU0hUTUxFZGl0b3IvVG91Y2hT
b3VyY2VzL1JTSFRNTEVkaXRWaWV3Q2
Is not a valid license key. Perhaps you mistyped a character?
Umm, OK?

“Some Great App” is damaged and can’t be opened. Delete “Some Great App” and download it again from the App Store.

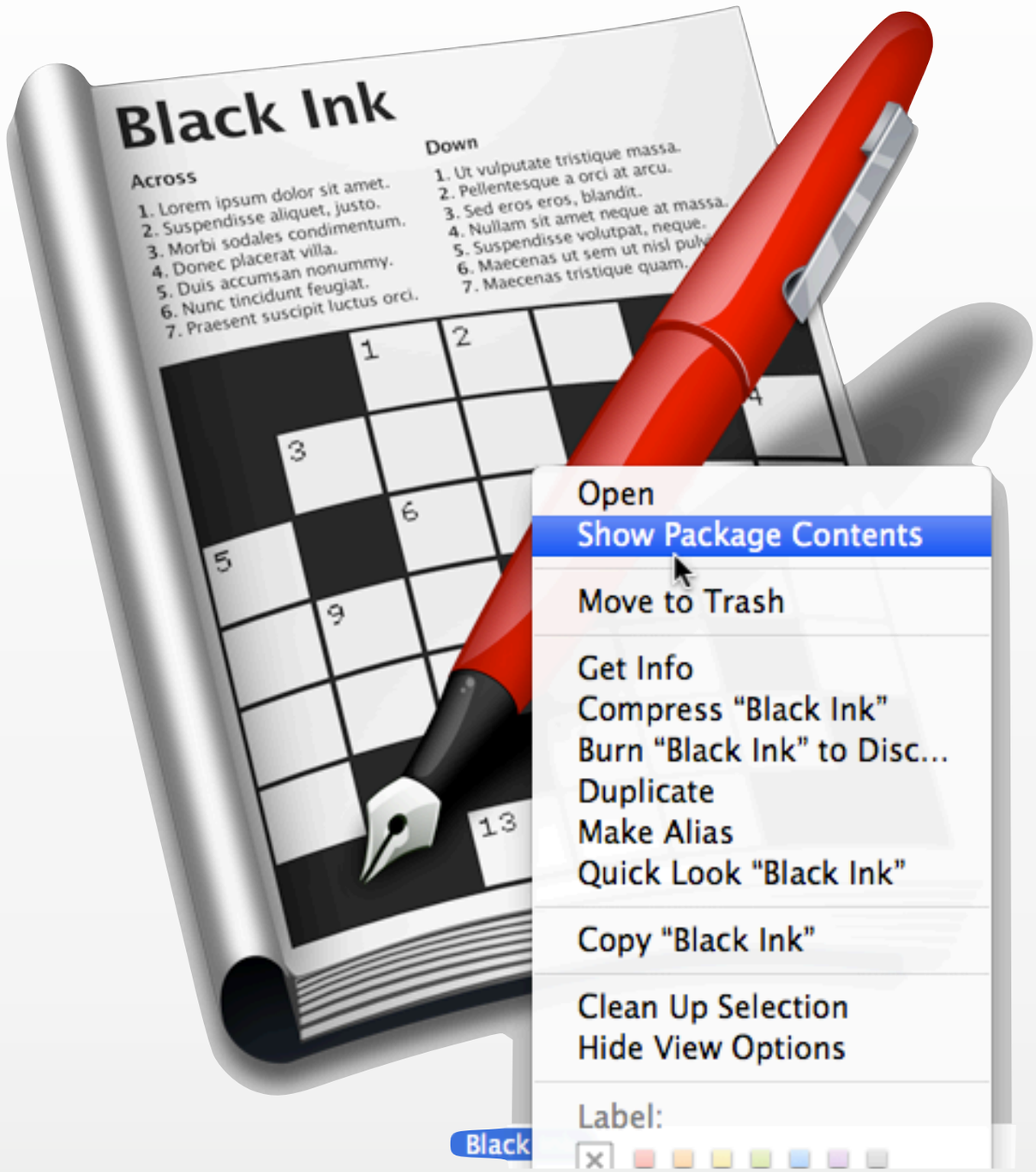
OK

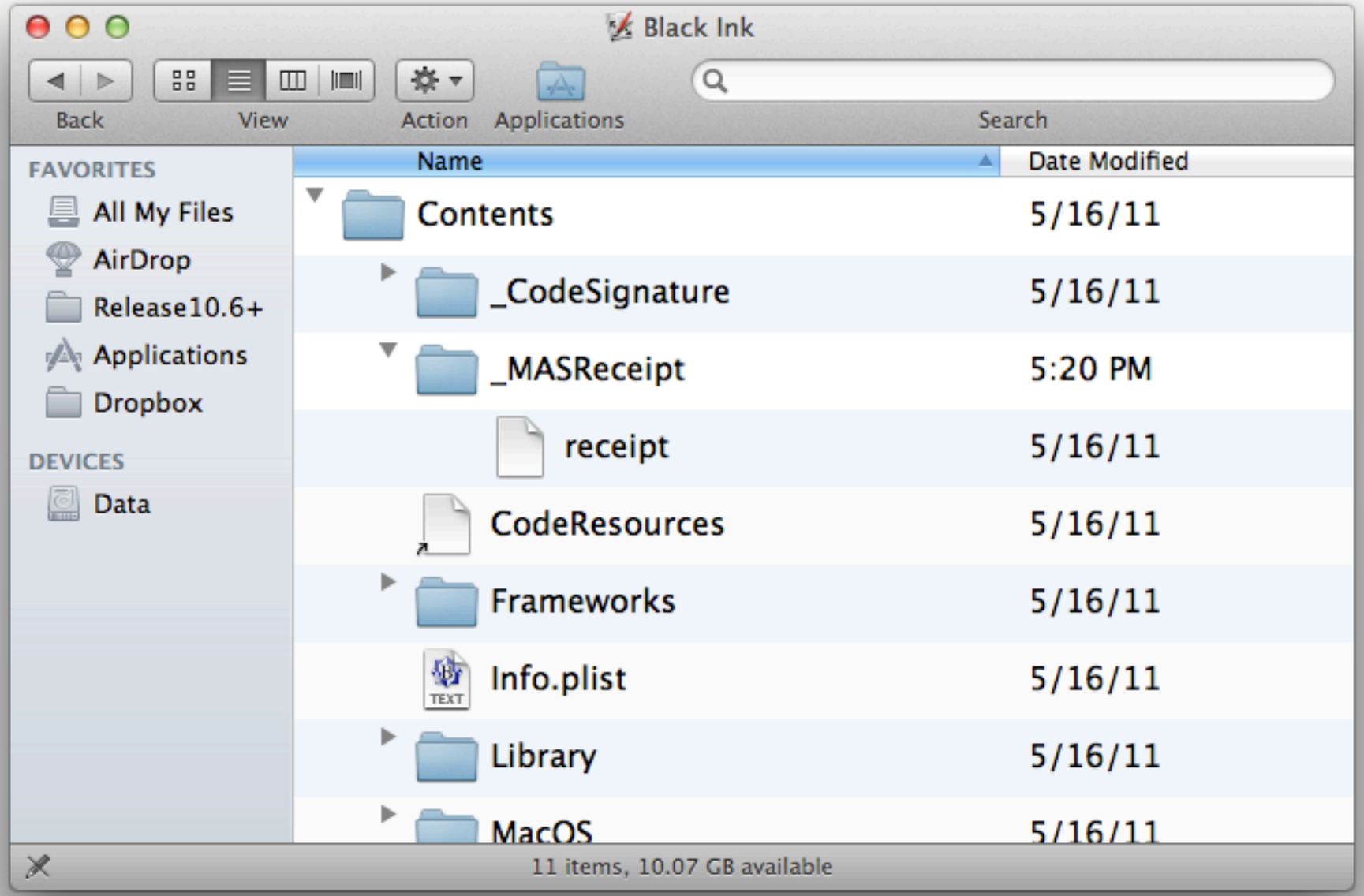
App Store Receipts

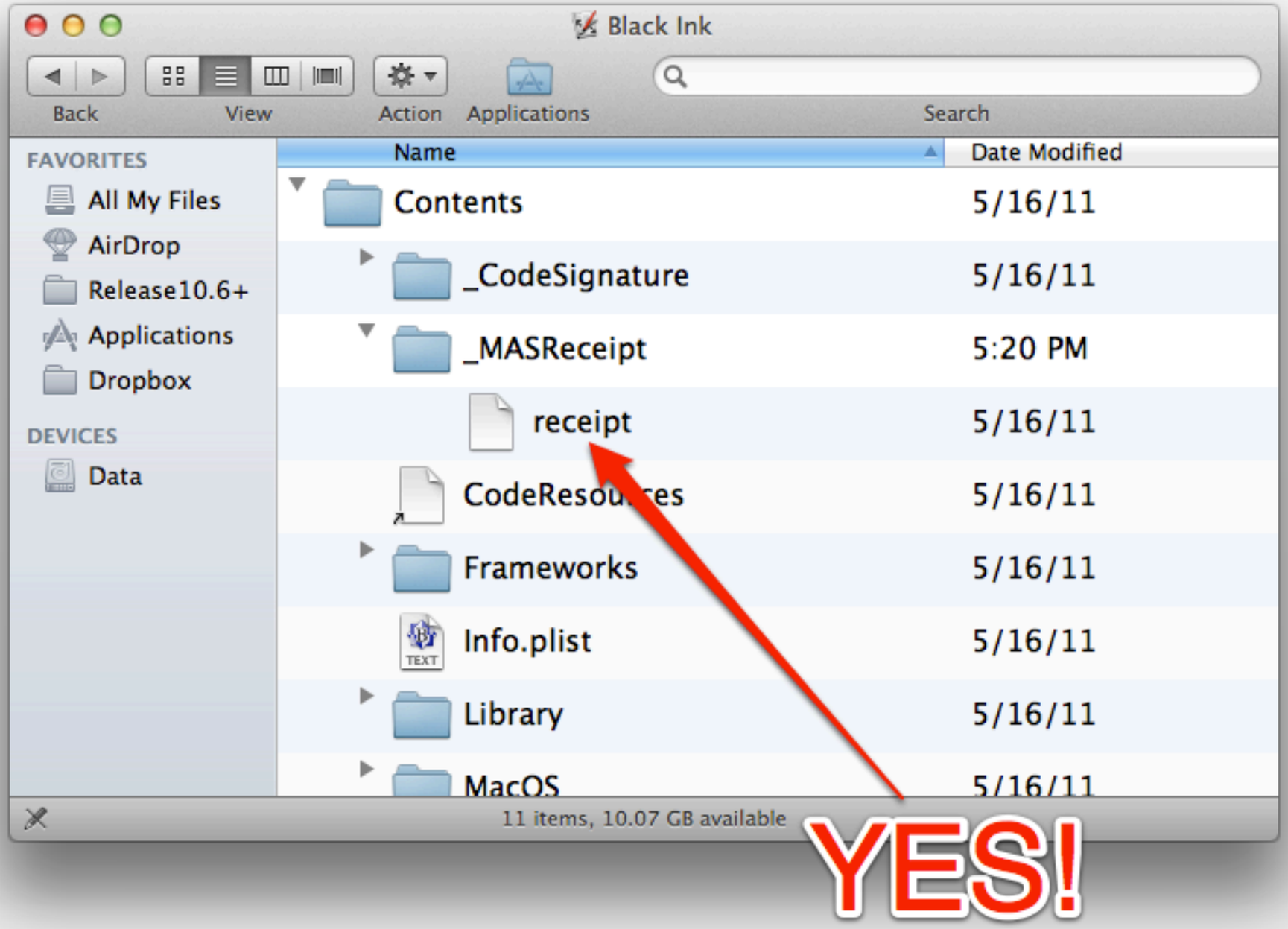
- Proof-of-purchase from Apple
- Identify the permitted product and machine
- Delivered on-the-fly by the Mac App Store

Locating Receipts

- Inside App Bundle
- _MASReceipt folder
- appStoreReceiptURL Cocoa method in 10.7


Black Ink
Across
1. Lorem ipsum dolor sit amet.
2. Suspendisse aliquet, justo.
3. Morbi sodales condimentum.
4. Donec placerat villa.
5. Duis accumsan nonummy.
6. Nunc tincidunt feugiat.
7. Praesent suscipit luctus orci.
Down
1. Ut vulputate tristique massa.
2. Pellentesque a orci at arcu.
3. Sed eros eros, blandit.
4. Nullam sit amet neque at massa.
5. Suspendisse volutpat, neque.
6. Maecenas ut sem ut nisl pul
7. Maecenas tristique quam.
Open
Show Package Contents
Move to Trash
Get Info
Compress “Black Ink”
Burn “Black Ink” to Disc...
Duplicate
Make Alias
Quick Look “Black Ink”
Copy “Black Ink”
Clean Up Selection
Hide View Options
Label:
Black


Black Ink
Back
View
Action
Applications
Search
FAVORITES
All My Files
AirDrop
Release10.6+
Applications
Dropbox
DEVICES
Data
Name
Date Modified
Contents
5/16/11
_CodeSignature
5/16/11
_MASReceipt
5:20 PM
receipt
5/16/11
CodeResources
5/16/11
Frameworks
5/16/11
Info.plist
5/16/11
Library
5/16/11
MacOS
5/16/11
11 items, 10.07 GB available


Black Ink
Back
View
Action
Applications
Search
FAVORITES
All My Files
AirDrop
Release10.6+
Applications
Dropbox
DEVICES
Data
Name
Date Modified
Contents
5/16/11
_CodeSignature
5/16/11
_MASReceipt
5:20 PM
receipt
5/16/11
CodeResources
5/16/11
Frameworks
5/16/11
Info.plist
5/16/11
Library
5/16/11
MacOS
5/16/11
11 items, 10.07 GB available
YES!

Receipt Content

- Signed by Apple
- PKCS #7 container, defined RFC 2315
- Payload attributes encoded ASN.1

```
 0 = NSData 19 bytes:    0C 11 50 72 6F 64 75 63 74 69 6F 6E 52 65 63 65 | ..ProductionRece
                         69 70 74                                        | ipt;
 1 = NSData 6 bytes:     02 04 17 FB C6 21                               | .....!;
 2 = NSData 38 bytes:    0C 24 63 6F 6D 2E 72 65 64 2D 73 77 65 61 74 65 | .$com.red-sweate
                         72 2E 6D 61 72 73 65 64 69 74 2E 6D 61 63 61 70 | r.marsedit.macap
                         70 73 74 6F 72 65                               | pstore;
 3 = NSData 7 bytes:     0C 05 33 2E 33 2E 35                            | ..3.3.5;
 4 = NSData 6 bytes:     02 04 01 32 D1 2E                               | ...2..;
 5 = NSData 20 bytes:    A5 05 5B BE 6E 97 CB 11 E7 26 1B B0 AD 9F 7E FE | ..[.n....&....~.
                         05 C4 AD B5                                     | ....;
 6 = NSData 77 bytes:    95 05 3D C8 71 31 43 67 E3 45 43 0F 04 9A 3D 87 | ..=.q1Cg.EC...=.
                         DD 1A A7 A6 6B 39 4D 13 0D 82 89 AB A2 63 AA 78 | ....k9M......c.x
                         88 59 37 D8 C4 56 5B DD DA 4C EA 8A 7A C4 97 AA | .Y7..V[..L..z...
                         22 8D F9 AC EC 08 E5 F0 D6 54 78 06 DB 31 27 10 | ".........Tx..1'.
                         78 7C F9 B4 4F 24 5C 59 6D 0D 4F 37 B6          | x|..O$\Ym.O7.;
 7 = NSData 65 bytes:    75 DD B1 63 28 85 D3 7C 4D A1 87 4A CE 22 90 C6 | u..c(..|M..J."..
                         2D F3 77 F7 B8 AE D1 06 CB 8B E6 E3 E2 E8 25 01 | -.w...........%.
                         35 5B 51 47 DD 74 5F 9B 74 54 EF 9C 43 A1 DE 1F | 5[QG.t_.tT..C...
                         44 2A 93 E7 5C 10 FA 6B F9 B1 00 15 0E 68 E3 D7 | D*..\..k.....h..
                         47                                              | G;
 8 = NSData 22 bytes:    16 14 32 30 31 31 2D 31 30 2D 32 36 54 31 39 3A | ..2011-10-26T19:
                         34 32 3A 30 35 5A                               | 42:05Z;
 9 = NSData 6 bytes:     02 04 50 32 30 33                               | ..P203;
 10 = NSData 4 bytes:    16 02 34 2B                                     | ..4+;
 11 = NSData 4 bytes:    02 02 26 EA                                     | ..&.;
 12 = NSData 22 bytes:   16 14 32 30 31 31 2D 31 30 2D 32 36 54 31 39 3A | ..2011-10-26T19:
                         34 32 3A 30 35 5A                               | 42:05Z;
13 = NSData 4 bytes:     02 02 27 76                                     | ..'v;
14 = NSData 3 bytes:     02 01 01                                        | ...;
15 = NSData 8 bytes:     02 06 14 03 18 3B 0C BA                         | .....;..;
16 = NSData 5 bytes:     02 03 46 00 3B                                  | ..F.;;
```

Supported Attributes

- Application Version
- Bundle Identifier
- Opaque Value (“Special Sauce”)
- Hash: 20-byte SHA-1 digest

Unsupported Attributes

- Receipt Type (0)
- Misc Dates (8 and 12)
- Age Rating (10)
- Wish I Knew more!

Validation

- Finder launches app
- App evaluates receipt
- Bad receipt? Exit with status 173
- System prompts “App Damaged”

Inspecting Receipts

* **OpenSSL**
* **asn1c code generator**
  - http://bit.ly/asn1c
* **Common Crypto**
* **MyCrypto**
  - http://bit.ly/mycrypto

In-App Validation

- **Verify Apple signature**
- **Check Bundle ID, App Version**
- **Compare Hash with GUID & Opaque Value**
- **Validating App Store Receipts**
  - http://bit.ly/appleval

Drawbacks

* **Non-unique, unlimited**
* **Non-transferable**
* **Lack of detail**
* **Apps worthless without receipt**

App Store Lock-In

- Apple owns customer relationship
- Licenses generated by Apple, for Apple
- Only latest version of an App Store app is ever available to users

Developer Flexibility?

- Non-Apple Receipt Signatures
- Relaxed GUID validation
- Relaxed version validation

Application Archives

- **Save every version**
- **Code signed by Apple**
  - codesign -dvvv /Applications/YourApp.app
- **If the receipt doesn't fit ...**

Receipt Archives

- Only Apple can issue receipts
- Apps and receipts are signed by Apple
- Safety in saving signed apps and receipts

App-Driven Archives

- **Organize by Mac, app, version**
- **Save to a well-known location**
- **This App Is Your App**
  - http://bit.ly/rsyourapp

Admin-Driven Archives

* Every user
* Every version
* Every Mac

User-Driven Archives

* Every version
* Every Mac
* I'm afraid that's it

Brave New World

- In Apple's Hands
- Fend for ourselves
- Forge ahead

This App Is Your App - Red Sweater Blog

http://bit.ly/rsyourapp

Validating App Store Receipts - Apple Developer Center

http://bit.ly/appleval

asn1c - Open Source asn1 decoder

http://bit.ly/asn1c

MyCrypto - Jens Alfke

http://bit.ly/mycrypto