12th November 2010

ICTR-MCT Team (ICTR-MCT-GCHQ-dl)
MHE Team (MHETeam-GCHQ-dl)
OPDSDHQ ([redacted])
TEA [redacted])
Benhall Records Centre ([redacted])

iPhone target analysis and exploitation with unique device identifiers

Summary

This paper describes standard analysis techniques that have been used to both discover iPhone target end point machines and implant target iPhones directly using the QUANTUM system. It shows that the iPhone Unique Device Identifier (UDID) can be used for target tracking and can be used to correlate with end point machines and target phone. It highlights the exploits currently available and the CNE process to enable further targeting.

[redacted], OPDSDHQ
[redacted]

A. REFERENCES

[a] iPhone applications and privacy issues: An analysis of Application Transmission of iPhone Unique Device Identifiers (UDIDs), [redacted] October 1 2010

[b] CROWN PRINCE – Technique for identifying Apple UDIDs in HTTP traffic – B/7844/5001/1/105, [redacted] – 22/07/10

[c] Strategic Framework Task 4138585 – Report No: 72/09/R/416/C, Roke – October 2009 Issue 2

[d] The Good penetration guide - [redacted]

[e] Current SEPP targets – [redacted]

[f] iPhone target list - [redacted]

B. BACKGROUND

1. Every Apple iPhone, iPad and iPod touch has a unique hardware identifier called the Apple UDID. The UDID is a 40 character hex string (160 bits) that seems to be a SHA-1 hash of the IMEI, serial number and the Bluetooth and WiFi MAC addresses. The UDID is available to developers of applications for these devices, and it is used to identify a given device. As highlighted in [a], the UDID is seen in multiple apps and can be used to allow target tracking or be used to correlate with other personal identifiers.

2. The Mobile Theme has invested a large amount of research into iPhone apps and metadata analysis over the last year accumulating with a detailed report done by [redacted] [c] in October 2009 and 29 SEM rules created by ICTR-MCT [b]. These rules have used to extract iPhone metadata for a number of apps and in particular the Unique Device Identifier (UDID) from any carrier being processed using DEBIT CARDs. Further TDI rules are being developed by GTE that will in the future extract UDID events from carriers processed through the MVR system. The resulting events have then been used to populate both research and corporate QFDs (Query Focused Datasets) such as MUTANT BROTH and AUTOASSOC and will eventually form the basis of mobile correlations in HARD ASSOC.

3. Initially, an exploit was developed by the Joint CNE/TECA Mobile Exploitation Team for iPhone that was to be delivered to the target phone when syncing with an exploited end point machine. This was successful for a BROKER target and resulted in the extraction of SMS, call logs and contact details. After this initial trial, CNE and SD undertook work to discover other single end points seen syncing with iPhones.

4. At HANDEX 2010 (handset exploitation workshop) in August, various aspects of the iPhone OS were investigated for potential vulnerabilities.

12th November 2010

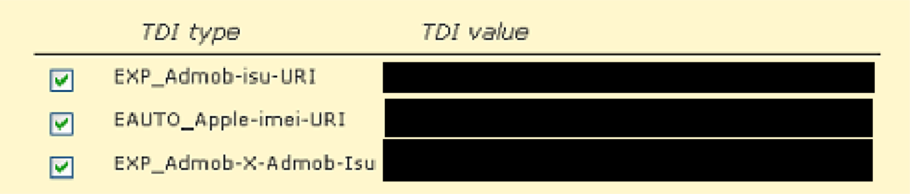
Using an open source PDF vulnerability when using the Safari browser, Joint CNE/TECA Mobile Exploitation Team were able to develop an exploit to deliver a WARRIORPRIDE implant to a target test phone. Further, investigation, liaison and testing with the CNE QUANTUM team resulted in approval for the implant to be deployed against QUANTUM iPhone targets.

C. DESCRIPTION OF ANALYSIS

CNE Endpoint

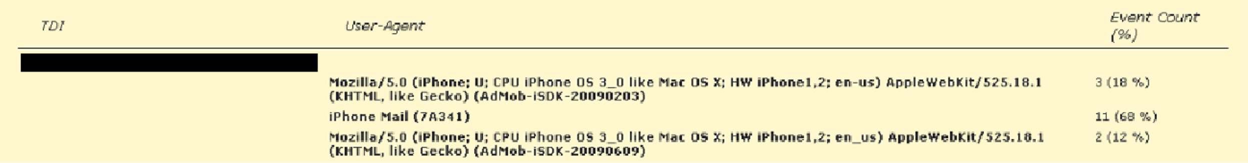
5. As part of the SD Mobile Exploitation theme to identify further end point machines that had been seen syncing with iPhones, a survey was undertaken by CNE and TAO to scan all target end point machines for the appropriate iPhone registry keys. Scanning of all CNE stored single end point (SEPs) registry keys on particular process IDs resulted in 9 CNE endpoints seen this year sync'd with iPhones. The resulting Unique Device Identifiers (UDID) were extracted from the registry keys and ran in MUTANT BROTH and AUTOASSOC, resulting in 6 correlations with either iPhone Safari user agents or the iPhone Mail app seen in passive collection.

6. A CNE end point operation against [redacted] (ABSOLINE EPILSON) had resulted in access to a windows end point machine [redacted]). A scan of this machine's registry keys resulted in UDID [redacted]. As can be seen, the UDID has been seen with the Admob SEM rule type and with the Apple-IMEI-URI TDI type. Admob is the largest mobile advertising network allowing games publishers to embed adverts and therefore receive revenue from a number of different brands. The target iPhone OS is 3_0 as shown in the User Agent profile in figure 2.



	TDI type	TDI value
☑	EXP_Admob-isu-URI	[redacted]
☑	EAUTO_Apple-imei-URI	[redacted]
☑	EXP_Admob-X-Admob-Isu	[redacted]

Figure 1 – MUTANT BROTH Matching Identifiers

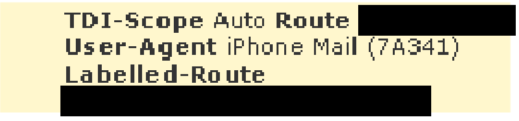


TDI	User-Agent	Event Count (%)
[redacted]		
	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; HW iPhone1,2; en-us) AppleWebKit/525.18.1 (KHTML, like Gecko) (AdMob-iSDK-20090203)	3 (18 %)
	iPhone Mail (7A341)	11 (68 %)
	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; HW iPhone1,2; en_us) AppleWebKit/525.18.1 (KHTML, like Gecko) (AdMob-iSDK-20090609)	2 (12 %)

Figure 2 – [redacted] iPhone UDID User agent profile

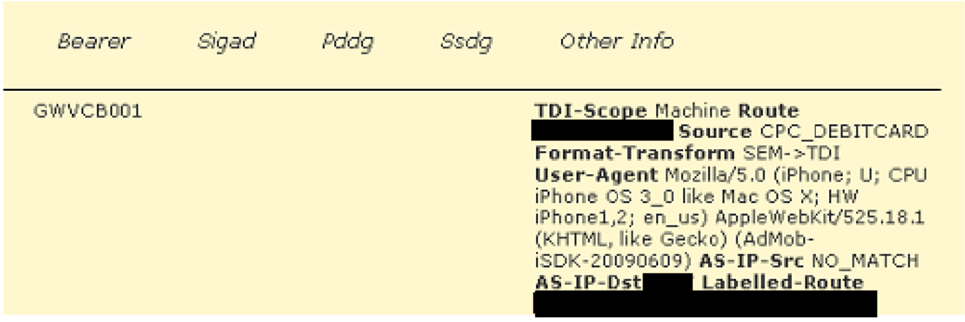
12th November 2010

7. The target UDID can be used track the iPhone seen with ASBOLINE EPILSON end point machine. In this particular case the target UDID has been seen 16 times, the last time off IP [redacted] on the 24/10/10 using the inbuilt iPhone Mail client to access his yahoo account. The user agent for this is shown in Figure 3. In this case the EAUTO_Apple-imei-URI TDI rule was used to extract the specific UDID value.



TDI-Scope Auto **Route** [redacted]
User-Agent iPhone Mail (7A341)
Labelled-Route
[redacted]

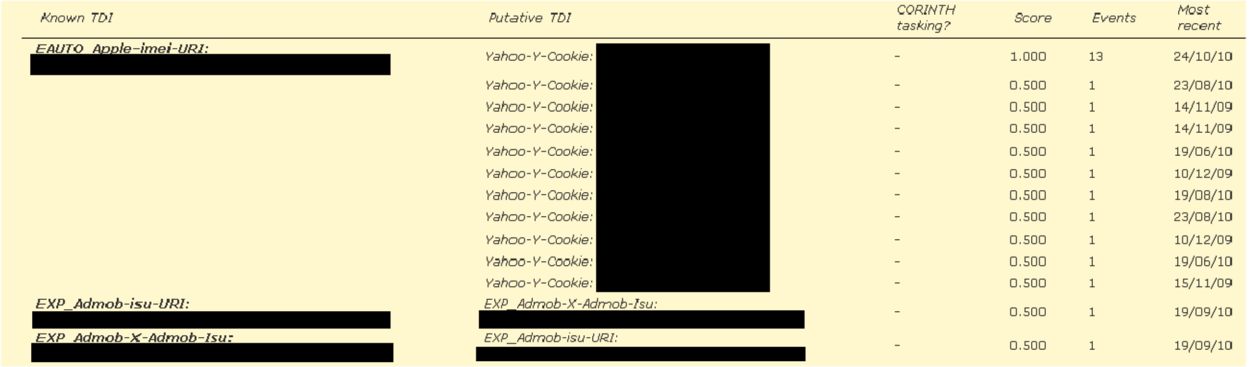
Figure 3 – iPhone Mail client user agent



Bearer	*Sigad*	*Pddg*	*Ssdg*	*Other Info*
GWVCB001				**TDI-Scope** Machine **Route** [redacted] **Source** CPC_DEBITCARD **Format-Transform** SEM->TDI **User-Agent** Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; HW iPhone1,2; en_us) AppleWebKit/525.18.1 (KHTML, like Gecko) (AdMob-iSDK-20090609) **AS-IP-Src** NO_MATCH **AS-IP-Dst** [redacted] **Labelled-Route** [redacted]

Figure 4 – iPhone Admob user agent profile

8. The UDID for all 6 targets were run through AUTOASSOC. The result for [redacted] is shown in Figure 5. As can be seen there is a clear correlation with the [redacted] yahoo-Y-cookie.



Known TDI	*Putative TDI*	*CORINTH tasking?*	*Score*	*Events*	*Most recent*
EAUTO_Apple-imei-URI: [redacted]	*Yahoo-Y-Cookie:* [redacted]	-	1.000	13	24/10/10
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	23/08/10
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	14/11/09
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	14/11/09
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	19/06/10
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	10/12/09
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	19/08/10
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	23/08/10
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	10/12/09
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	19/06/10
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	15/11/09
EXP_Admob-isu-URI: [redacted]	*EXP_Admob-X-Admob-Isu:* [redacted]	-	0.500	1	19/09/10
EXP_Admob-X-Admob-Isu: [redacted]	*EXP_Admob-isu-URI:* [redacted]	-	0.500	1	19/09/10

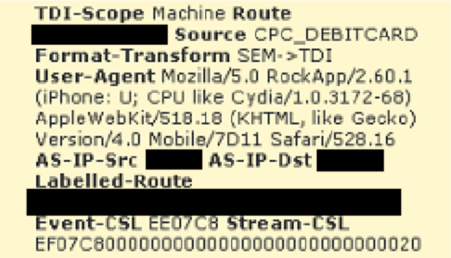
Figure 5 – AUTOASSOC results for ABSOLINE EPSILON

9. The IP address, identifier type, bearer and user agent type for all 6 targets was extracted and formed the basis of further target development work. Running the resulting 6 UDIDs through AUTOASSOC, resulted in two correlations with a high enough score. These were [redacted] and [redacted] and confirmed to be correct after discussing with

the [redacted]. Checking BROADOAK tasking revealed that both targets had known associated iPhone IMEIs already tasked.

10. A recent rescan of all currently active CNE SEPs resulted in only 5 of the 9 identified CNE machines actually being available for exploit. The other 4 implants having been removed. Of these five UDIDs, four returned with correlated UDIDs that had recently been seen in passive collection. These are contained in the iPhone target list [f].

11. Analysis of all TAO SEPs resulted in 116 UDIDs being identified. Of these UDIDs, 15 were correlated with iPhone user agents and the resulting identifier type, project name, case notation and IP noted. A full list is available in the iPhone target list [f]. Of these four had the Cydia user agent as shown in Figure 6 indicating the target had jailbroken their phone. All four end points were located in [redacted].

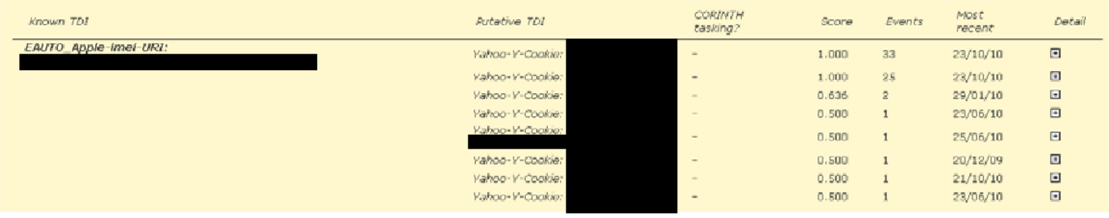


```
TDI-Scope Machine Route
[redacted] Source CPC_DEBITCARD
Format-Transform SEM->TDI
User-Agent Mozilla/5.0 RockApp/2.60.1
(iPhone: U; CPU like Cydia/1.0.3172-68)
AppleWebKit/518.18 (KHTML, like Gecko)
Version/4.0 Mobile/7D11 Safari/528.16
AS-IP-Src [redacted] AS-IP-Dst [redacted]
Labelled-Route
[redacted]
Event-CSL EE07C8 Stream-CSL
EF07C800000000000000000000000020
```

Figure 6 – iPhone jailbroken user agent in MUTANT BROTH

12. The same 15 TAO UDIDs were run through AUTOASSOC and resulted in three good correlations with yahoo selectors –[redacted] [redacted] and [redacted] These were in turn confirmed to be correct correlations with TAO target end points and two showed associated target iPhone IMEIs. Further, analysis of the Yahoo mail used via the Safari browser clearly showed the resulting UDID was transmitted in traffic.

13. One of these TAO end point machines, SOLARSHOCK116 ([redacted] [redacted]– Iranian), has been seen syncing with iPhone UDID –[redacted], was correlated with [redacted] and [redacted] using AUTOASSOC. The UDID was last seen on 23/10/10 at 03:46:36z on [redacted] using the EAUTO_Apple-imei-URI TDI.



Known TDI	Putative TDI	CORINTH tasking?	Score	Events	Most recent	Detail
EAUTO_Apple-imei-URI: [redacted]	Yahoo-Y-Cookie: [redacted]	-	1.000	33	23/10/10	⊡
	Yahoo-Y-Cookie: [redacted]	-	1.000	25	23/10/10	⊡
	Yahoo-Y-Cookie: [redacted]	-	0.636	2	29/01/10	⊡
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	23/06/10	⊡
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	25/06/10	⊡
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	20/12/09	⊡
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	21/10/10	⊡
	Yahoo-Y-Cookie: [redacted]	-	0.500	1	23/06/10	⊡

Figure 7- SOLARSHOCK116 UDID AUTOASSOC correlations

QUANTUM EXPLOIT

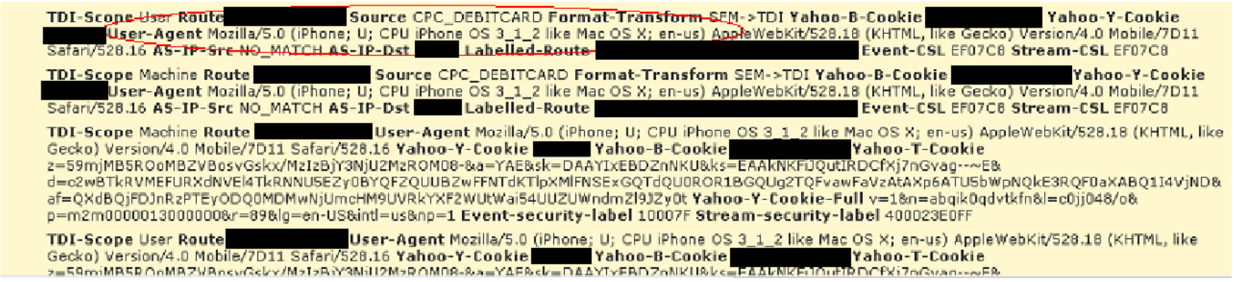
14. After extensive testing of the QUANTUM tipping and redirection to the SHORTSHEET exploitation server by the Joint CNE/TECA Mobile Exploitation Team, further target development work was needed to identify iPhone targets recently seen active on the appropriate user agents. Bulk extraction of targets over a three-week period from BLACKHOLE by ICTR resulted in a large number of iPhone targets and further queries in Xkeyscore resulted in others. Others were passed from discussions with various IPTs and two were also passed from TAO contacts.

15. In total 44 selectors were checked to verify that the correct user agent was present. Of these 44 selectors, 41 were yahoo selectors and 3 gmail selectors. Of these 26 were seen with a valid iPhone Safari user agent as shown in Figure 8. A summary of OS versions seen with target phones is shown in Table 1 with OS highlighted in red currently exploited. These are 3_1_2, 3_1_3 and 4_0_1. In all 26 cases, the target analysts were contacted with details regarding their targets use of an exploitable iPhone.

iPhone OS	Number
3_0	4
3_1	2
3_1_2	6
3_1_3	15
4_0	3
4_0_1	5
4_0_2	1

Table 1 – iPhone target OS summary

24. One particular case was a [redacted] target, [redacted] with yahoo selector [redacted], that was seen active on a iPhone OS 3_1_2, as shown in Figure 8. The resulting Yahoo-B cookie is [redacted] and as can be seen the target has been active off [redacted]). Running the resulting Yahoo-B cookie through MUTANT BROTH resulted in 171 events primarily on case notations GWUKG005, GWVCB003 and IRUKC036. The resulting information was then forwarded to the analysts in the [redacted] team for tasking by the standard CNE process as outlined in the *Good Penetration Guide* [d].



```
TDI-Scope User Route [redacted] Source CPC_DEBITCARD Format-Transform SEM->TDI Yahoo-B-Cookie [redacted] Yahoo-Y-Cookie
[redacted] User-Agent Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_1_2 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7D11
Safari/528.16 AS-IP-Src NO_MATCH AS-IP-Dst [redacted] Labelled-Route [redacted] Event-CSL EF07C8 Stream-CSL EF07C8

TDI-Scope Machine Route [redacted] Source CPC_DEBITCARD Format-Transform SEM->TDI Yahoo-B-Cookie [redacted] Yahoo-Y-Cookie
[redacted] User-Agent Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_1_2 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7D11
Safari/528.16 AS-IP-Src NO_MATCH AS-IP-Dst [redacted] Labelled-Route [redacted] Event-CSL EF07C8 Stream-CSL EF07C8

TDI-Scope Machine Route [redacted] User-Agent Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_1_2 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like
Gecko) Version/4.0 Mobile/7D11 Safari/528.16 Yahoo-Y-Cookie [redacted] Yahoo-B-Cookie [redacted] Yahoo-T-Cookie
z=59mjMB5ROoMBZVBosvGskx/MzIzBjY3NjU2MzROM08-&a=YAE&sk=DAAYIxEBDZnNKU&ks=EAAkNKFiJQutIRDCfXj7nGvag--~E&
d=c2wBTkRVMEFURXdNVEl4TkRNNU5EZy0BYQFZQUUBZwFFNTdKTlpXMlFNSExGQTdQU0ROR1BGQUg2TQFvawFaVzAtAXp6ATU5bWpNQkE3RQF0aXABQ1I4VjND&
af=QXdBQjFDJnRzPTEyODQ0MDMwNjUmcHM9UVRkYXF2WUtWai54UUZUWndmZl9JZy0t Yahoo-Y-Cookie-Full v=1&n=abqik0qdvtkfn&l=c0jj048/o&
p=m2m0000013000000&r=89&lg=en-US&intl=us&np=1 Event-security-label 10007F Stream-security-label 400023E0FF

TDI-Scope User Route [redacted] User-Agent Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_1_2 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like
Gecko) Version/4.0 Mobile/7D11 Safari/528.16 Yahoo-Y-Cookie [redacted] Yahoo-B-Cookie [redacted] Yahoo-T-Cookie
z=59mjMB5ROoMBZVBosvGskx/MzIzBjY3NjU2MzROM08-&a=YAE&sk=DAAYIxEBDZnNKU&ks=EAAkNKFiJQutIRDCfXj7nGvag--~E&
```

Figure 8 –Valid iPhone Safari user agent in MB ([redacted]<yahoo>)

25. The target [redacted] with target selector [redacted] was seen active on different iPhone OS and more recently on an iPad. Three other targets were seen active on iPads and two others on iPods but with no other associated iPhone device. Of the 44 targets seen, 16 were seen using the iPhone Mail client that comes by default with all OS. A total of 7 targets were seen using the Yahoo Mobile Messenger app.

26. For all target selectors seen with valid Safari user-agents, further MUTANT BROTH, AUTOASSOC and MARINA queries were performed to discover any other possible OS versions seen with the selector. MARINA profile queries were performed resulting in the OS version being returned within the MachineID field. The resulting user-agents, time/date, bearer, IP and any other associated selectors are shown in the iPhone target list [f]. Associated selectors are either from MUTANT BROTH, AUTOASSOC or seen directly as stated in BROADOAK. All Yahoo B-cookies as shown in Figure 8 were run in MUTANT BROTH to confirm their uniqueness with the iPhone and target yahoo selectors.

D. OPERATIONAL OUTCOME

27. The QUANTUM redirect and PDF Safari browser exploit was developed to work against 3_1_2, 3_1_3 and 4_0_1 Safari OS versions. Of the 26 targets seen with valid exploitable OS version, 5 were added to the QUANTUM system for targetting.

28. Once notified, GCHQ IPTs either added the target to existing CNE section 7 warrants as defined in [e] or developed targetting aids as defined in [d] and wrote the appropriate warrant. The resulting section 7 warrants were approved by IPT team leaders and signed off by the CNE Legal Team. Three NSA targets were discovered and were added by CNE Legal Team to the Partner Agreement Forms to allow exploitation.

29. Initially, [redacted] yahoo selector ([redacted]) and B-cookie was put on cover on QUANTUM. [redacted] was not seen active recently on a iPhone Safari browser to access his yahoo account, preferring instead to use the inbuilt iPhone Mail client or his iPad. Three QUANTUM attempts resulted in no redirect to SHORTSHEET server for

[redacted] and after further analysis it was discovered that this selector was not [redacted] but an associate. It was removed from tasking.

30. Target analysis and warrant was completed for a further five targets and a successful QUANTUM redirect and the PDF exploit was delivered for [redacted] (**URN PFVT658**) on the 30th of October. The resulting WARRIORPRIDE install was also performed and beaconed on the 2nd of November. The target phone was shown to be jailbroken and on the 3rd of November content was successfully extracted from the phone and was available in Looking Glass. This is highlighted in Appendix B with the resulting iPhone directory structure presented how it appears in Looking Glass. The WARRIORPRIDE exploit has resulted in extraction of the target's address book, sms, call logs, notes, WLAN logs, bookmarks, map query history, Safari browsing history and some images. Detailed analysis of extracted files will be covered in a further report.

31. A successful redirect to [redacted] in October was performed but due to what is believed to be Javascript being disabled on the phone the firmware type of the phone could not be confirmed to enable the first stage implant. This initial survey of the firmware type has now been removed after discussions within CNE but the target has not been seen recently on his iPhone for exploitation. The two other targets tasked for QUANTUM have failed to be seen recently in collect.

32. Currently, there are four CNE Single End Point machines that have been identified with recently sync'd iPhone targets. The most recent being an OVERLIT target seen on 29/09/10. These targets are being monitored by CNE and will have the SLIDE exploit installed to allow implant of WARRIORPRIDE when the iPhone is sync'd with the existing SEP machine.

E. CONCLUSION

33. With the analysis of the UDIDs on target machines and correlation in passive collection with known target yahoo selectors, the UDID can be used to correlate iPhone handset to end point sync machine and tasked yahoo selectors. The UDID can be used for realtime tracking of target iPhones and could in theory be used as a selector for QUANTUM events where other traditional selectors (yahoo-Y/B cookie etc) are not present. Of course an exploit for the application would have to be written which is not trivial.

34. It is not possible at this time to take the UDID and reverse engineer the SHA-1 HASH to discover the IMEI, MAC addresses and serial number.

35. Further work is ongoing to identify targets of interest that are suitable for the QUANTUM exploitation. Development and monitoring of current identified targets is still being done. Discovery of an associated IMEI for [redacted] will help in firmware identification and exploitation of this target.

36. CNE are now conducting monthly surveys of all target machines registry keys for iPhone UDIDs. A similar tipping mechanism for all BROADOAK hits needs to be completed using a XKS workflow. Hopefully, other targets will be added for QUANTUM exploitation or discovered on new CNE SEPs in the future and a successful exploit of a target phone performed.

F. FURTHER WORK

37. Analysis of three PRESTON accesses has resulted in the identification of a number of iPhone targets. Development work against at least three target sets is needed with extraction of appropriate UDIDs and iTunes XDSID values. Suitable section 5 warrants need to be in place to pursue these end point machines, once CNE have gained access and the resulting target iPhones have been discovered.

38. With further work being undertaken by BSS and TECA on the WHIPSAW redirect and exploitation server, it should be possible in the coming months to implant directly the target iPhone. However, the WHIPSAW exploit is only available via the tasked ADSL line.

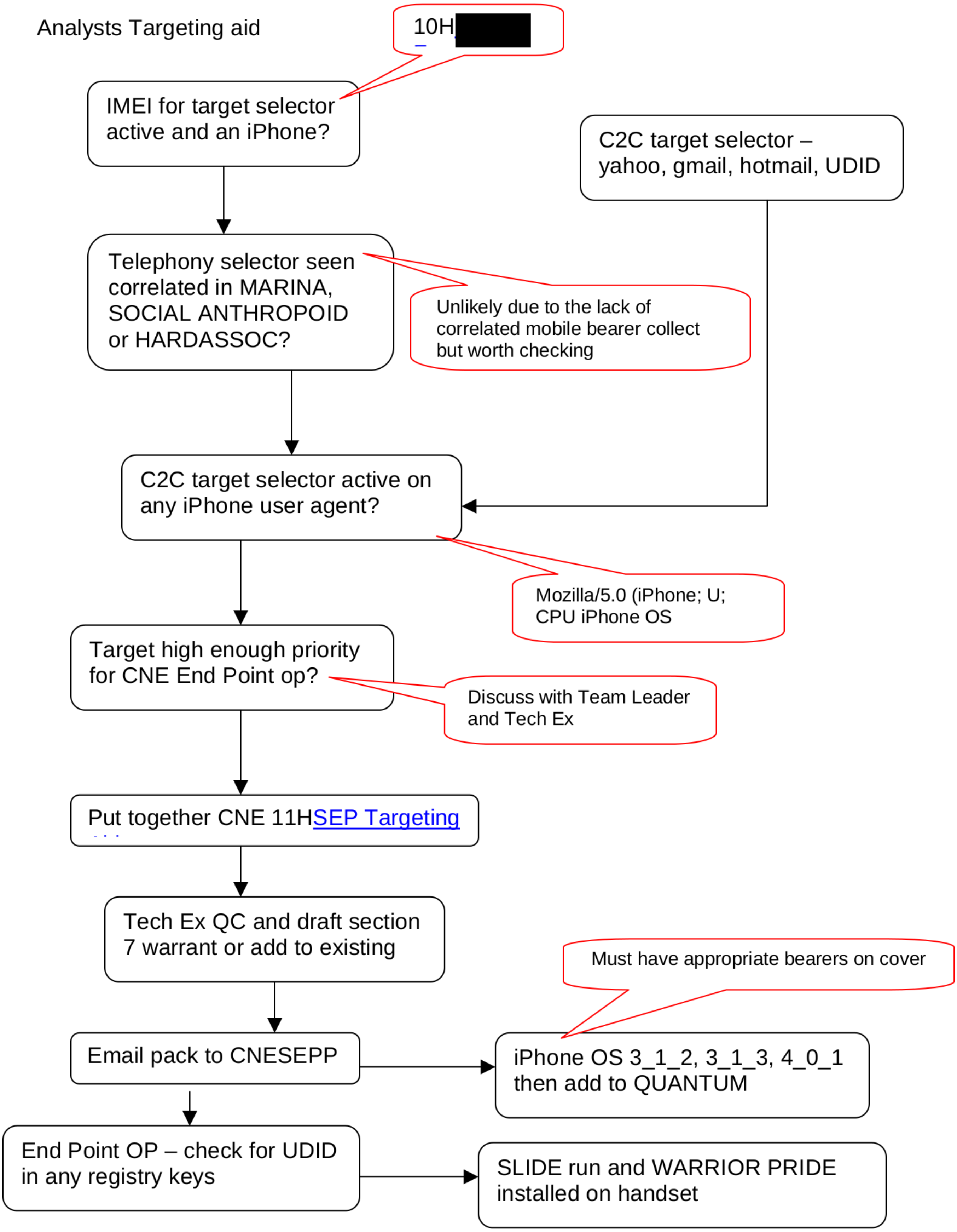
39. An automatic implantation of SLIDE on to an iPhone is needed. Currently this is manual process requiring a CNE operator to be connected to the endpoint machine whilst the target is syncing the end point machine and iPhone.

40. A larger number of iPhone TDIs need to be written to allow further events to be populated into the QFDs allowing correlations with other target selectors. This will also enable further real-time tracking of target identifiers.

12th November 2010

APPENDIX A

Analysts Targeting aid



10H[redacted]

IMEI for target selector active and an iPhone?

Telephony selector seen correlated in MARINA, SOCIAL ANTHROPOID or HARDASSOC?

Unlikely due to the lack of correlated mobile bearer collect but worth checking

C2C target selector – yahoo, gmail, hotmail, UDID

C2C target selector active on any iPhone user agent?

Mozilla/5.0 (iPhone; U; CPU iPhone OS

Target high enough priority for CNE End Point op?

Discuss with Team Leader and Tech Ex

Put together CNE 11HSEP Targeting

Tech Ex QC and draft section 7 warrant or add to existing

Must have appropriate bearers on cover

Email pack to CNESEPP

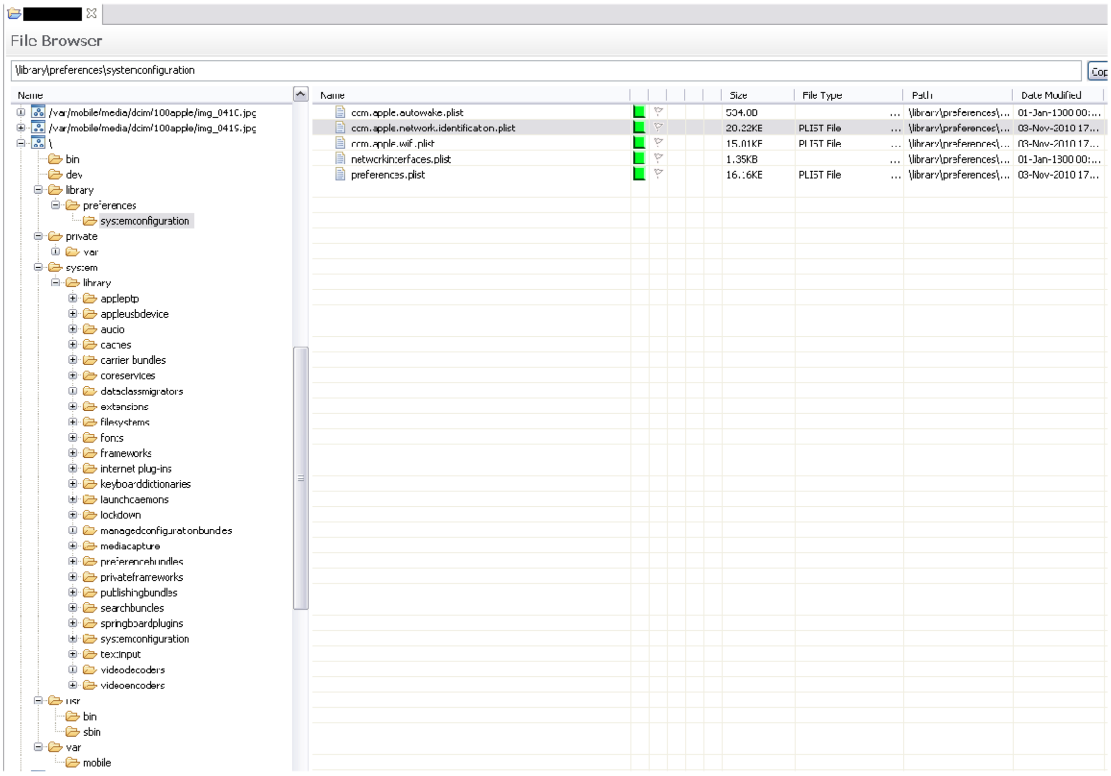
iPhone OS 3_1_2, 3_1_3, 4_0_1 then add to QUANTUM

End Point OP – check for UDID in any registry keys

SLIDE run and WARRIOR PRIDE installed on handset

APPENDIX B

[redacted] Looking Glass iPhone directory structure



[redacted] ☒

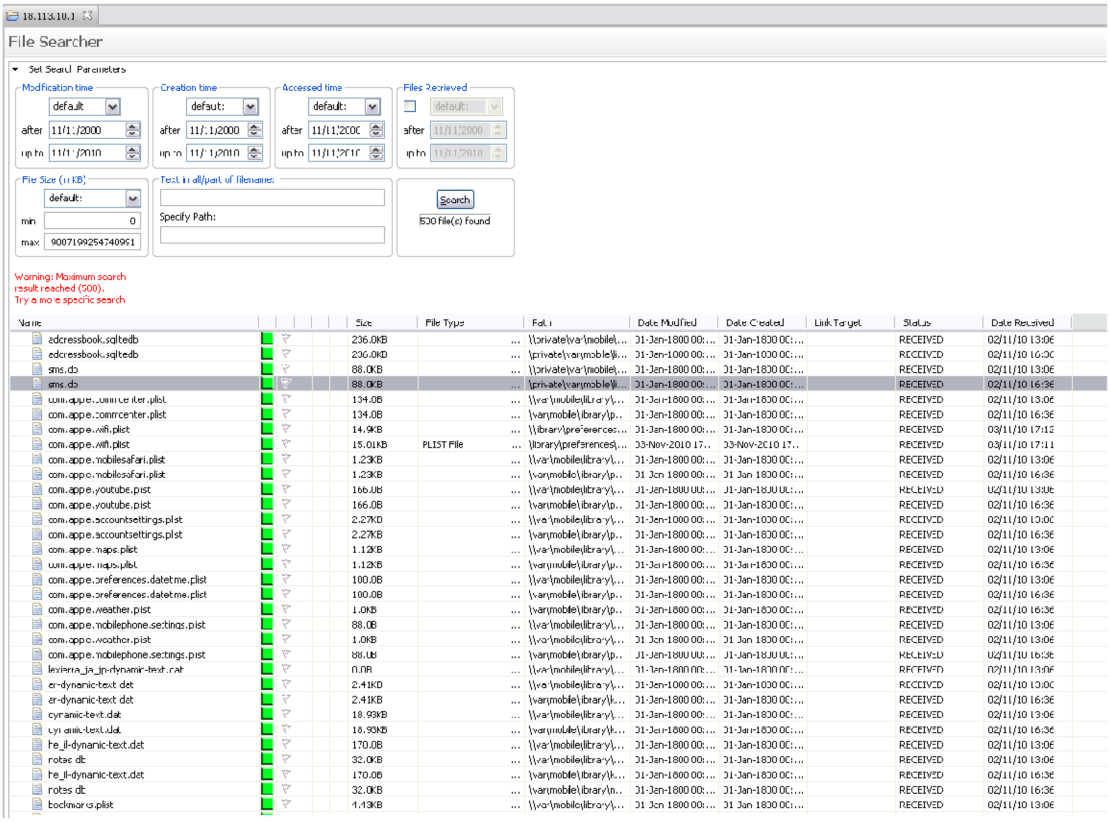
File Browser

\library\preferences\systemconfiguration

```
Name
⊞ /var/mobile/media/dcim/100apple/img_0410.jpg
⊞ /var/mobile/media/dcim/100apple/img_0419.jpg
⊟ \
    bin
    dev
  ⊟ library
    ⊟ preferences
        systemconfiguration
  ⊟ private
    ⊞ var
  ⊟ system
    ⊟ library
      ⊞ appleptp
      ⊞ appleusbdevice
      ⊞ audio
      ⊞ caches
      ⊞ carrier bundles
      ⊞ coreservices
      ⊞ dataclassmigrators
      ⊞ extensions
      ⊞ filesystems
      ⊞ fonts
      ⊞ frameworks
      ⊞ internet plug-ins
      ⊞ keyboarddictionaries
      ⊞ launchdaemons
      ⊞ lockdown
      ⊞ managedconfigurationbundles
      ⊞ mediacapture
      ⊞ preferencebundles
      ⊞ privateframeworks
      ⊞ publishingbundles
      ⊞ searchbundles
      ⊞ springboardplugins
      ⊞ systemconfiguration
      ⊞ textinput
      ⊞ videodecoders
      ⊞ videoencoders
  ⊟ usr
      bin
      sbin
  ⊟ var
      mobile
```

Name		Size	File Type	Path	Date Modified
ccm.apple.autowake.plist	🟩	534.0B		... \library\preferences\...	01-Jan-1300 00:...
ccm.apple.network.identification.plist	🟩	20.22KB	PLIST File	... \library\preferences\...	03-Nov-2010 17...
ccm.apple.wifi.plist	🟩	15.01KB	PLIST File	... \library\preferences\...	03-Nov-2010 17...
networkinterfaces.plist	🟩	1.35KB		... \library\preferences\...	01-Jan-1300 00:...
preferences.plist	🟩	16.16KB	PLIST File	... \library\preferences\...	03-Nov-2010 17...

[redacted] returned files



18.113.10.1 ☒

File Searcher

▾ Set Search Parameters

Modification time: default; after 11/11/2000; up to 11/11/2010

Creation time: default; after 11/11/2000; up to 11/11/2010

Accessed time: default; after 11/11/2000; up to 11/11/2010

Files Retrieved: □ default; after 11/11/2000; up to 11/11/2010

File Size (in KB): default; min 0; max 9007199254740991

Text in all/part of filename:

Specify Path:

500 file(s) found

Warning: Maximum search result reached (500). Try a more specific search

Name		Size	File Type	Path	Date Modified	Date Created	Link Target	Status	Date Received
addressbook.sqlitedb	🟩	236.0KB		... \\private\var\mobile\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
addressbook.sqlitedb	🟩	236.0KB		... \private\var\mobile\li...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
sms.db	🟩	88.0KB		... \\private\var\mobile\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
sms.db	🟩	88.0KB		... \private\var\mobile\li...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
com.appe.commcenter.plist	🟩	134.0B		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
com.appe.commcenter.plist	🟩	134.0B		... \var\mobile\library\p...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
com.appe.wifi.plist	🟩	14.9KB		... \\library\preferences...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	03/11/10 17:12
com.appe.wifi.plist	🟩	15.01KB	PLIST File	... \library\preferences\...	03-Nov-2010 17..	03-Nov-2010 17..		RECEIVED	03/11/10 17:11
com.appe.mobilesafari.plist	🟩	1.23KB		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
com.appe.mobilesafari.plist	🟩	1.23KB		... \var\mobile\library\p...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
com.appe.youtube.plist	🟩	166.0B		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
com.appe.youtube.plist	🟩	166.0B		... \var\mobile\library\p...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
com.appe.accountsettings.plist	🟩	2.27KB		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
com.appe.accountsettings.plist	🟩	2.27KB		... \var\mobile\library\p...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
com.appe.maps.plist	🟩	1.12KB		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
com.appe.maps.plist	🟩	1.12KB		... \var\mobile\library\p...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
com.appe.preferences.datetime.plist	🟩	100.0B		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
com.appe.preferences.datetime.plist	🟩	100.0B		... \var\mobile\library\p...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
com.appe.weather.plist	🟩	1.0KB		... \var\mobile\library\p...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
com.appe.mobilephone.settings.plist	🟩	88.0B		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
com.appe.weather.plist	🟩	1.0KB		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
com.appe.mobilephone.settings.plist	🟩	88.0B		... \var\mobile\library\p...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
lexicon_ja_jp-dynamic-text.dat	🟩	0.0B		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
ar-dynamic-text.dat	🟩	2.41KB		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
ar-dynamic-text.dat	🟩	2.41KB		... \var\mobile\library\k...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
dynamic-text.dat	🟩	18.93KB		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
dynamic-text.dat	🟩	18.93KB		... \var\mobile\library\k...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
he_il-dynamic-text.dat	🟩	170.0B		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
notes.db	🟩	32.0KB		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06
he_il-dynamic-text.dat	🟩	170.0B		... \var\mobile\library\k...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
notes.db	🟩	32.0KB		... \var\mobile\library\n...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 16:36
bookmarks.plist	🟩	1.43KB		... \\var\mobile\library\...	01-Jan-1800 00:...	01-Jan-1800 00:...		RECEIVED	02/11/10 13:06