



Calhoun: The NPS Institutional Archive
DSpace Repository

Faculty and Researchers

Faculty and Researchers' Publications

2011-08

Residual Network Data on Android Devices, Presentation

Cardwell, Greg; Beverly, Rob

Monterey, California: Naval Postgraduate School.

<http://hdl.handle.net/10945/39508>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



NAVAL
POSTGRADUATE
SCHOOL

Residual Network Data on Android Devices

LT. Greg Cardwell and Prof. Rob Beverly

Monterey, California

WWW.NPS.EDU



- Consider Implications:
 - Enemy use of COTS Smartphones
 - US DoD Deployed COTS Smartphones
- Intuitively, we believe this is insecure. For many reasons...
- This work examines the extent to which **current and residual network data can be retrieved from Smartphone Flash memory**



- Our Research:
 - Conduct carefully controlled experiments using our own infrastructure to create known ground-truth Smartphone corpus
 - Examine residual network data in corpus
 - We limit our exploration to Android mobile OS



Nexus One Flash Partitions

- mtd0: "misc"
- mtd1: "recovery"
- mtd2: "boot"
- mtd3: "system"
- mtd4: "cache"
- mtd5: "userdata"

Source: Android Forensics: Hoog

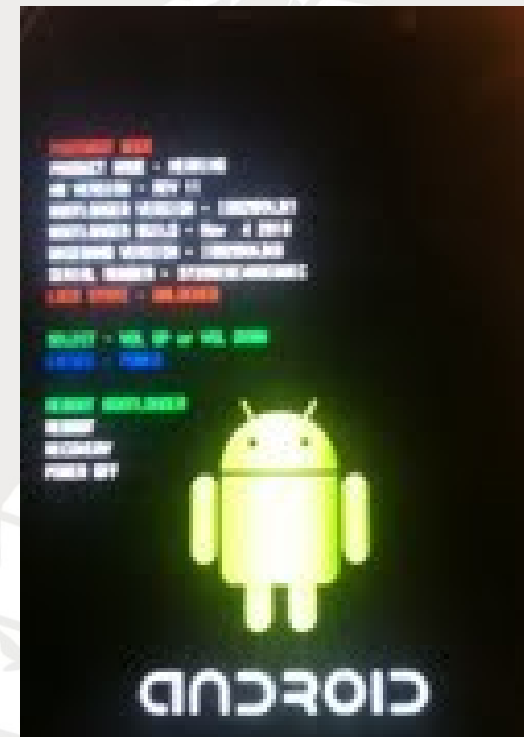
Rooting Tools

- theunlockr.com
 - Adds superuser.apk to mtd3(system)
- Gingerbreak.exe
- superboot

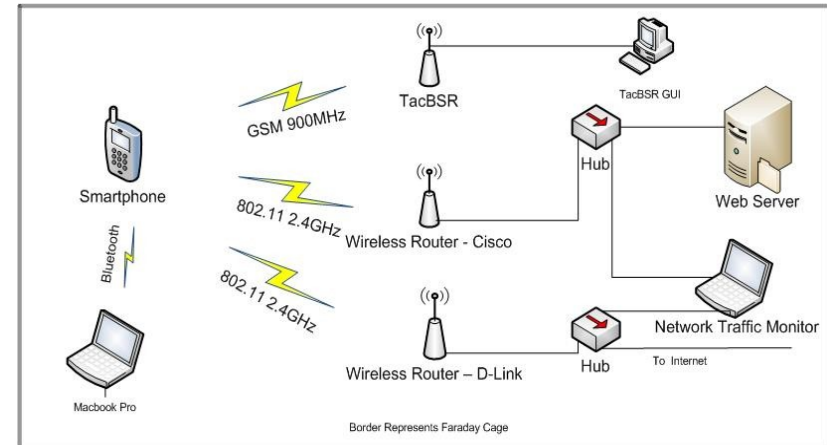
ssh / netcat / dd

ADB Pull

Nandroid



- Clean Android Smartphones
- Performed in Faraday Cage
- Communication. Run our own:
 - GSM BTS
 - 802.11 WiFi
 - Bluetooth
- Different experiments using different communication channels:
 - To our web server/content
- Per-experiment imaging
- Gives us known ground-truth corpus





NAVAL
POSTGRADUATE
SCHOOL

Building the Corpus





Binary IP

Physical dump – 5 instances

0x3A3D7F8	FF FF FF FF FF FF FF FF 02 01 06 00 B3 E8 4F EC 00d.....
0x3A3D809	00 00 00 00 00 00 00 C0 A8 00 64 00 00 00 00 00!U.G6.....
0x3A3D81A	00 00 90 21 55 07 47 36 00 00 00 00 00 00 00 00
0x3A3D82B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D83C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D84D	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D85E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D86F	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D880	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D891	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D8A2	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D8B3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D8C4	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D8D5	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D8E6	00 00 00 00 00 00 63 82 53 63 35 01 05 01 04 FF FFcSc5.....
0x3A3D8F7	FF 00 33 04 00 09 3A 80 03 04 C0 A8 00 01 06 04 C03...:.....
0x3A3D908	A8 00 01 36 04 C0 A8 00 01 00 00 00 00 00 00 006.....
0x3A3D919	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D92A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D93B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D94C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D95D	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D96E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D97F	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D990	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D9A1	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D9B2	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D9C3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D9D4	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D9E5	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3A3D9F6	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Logical dump – 1 instance

0xDFBF85	FF FF FF FF FF FF FF FF FF FF FF 02 01 06 00 6F C9d.....
0xDFBF86	0E E2 00 00 00 00 00 00 00 00 C0 A8 00 64 00 00 00!U.G6.....
0xDFBF87	00 00 00 00 00 00 90 21 55 07 47 36 00 00 00 00 00
0xDFBF88	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xDFBF89	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xDFC00A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xDFC01B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xDFC02C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xDFC03D	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xDFC04E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xDFC05F	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xDFC070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xDFC081	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xDFC092	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xDFC0A3	00 00 00 00 00 00 00 00 00 00 63 82 53 63 35 01 05 01cSc5.....
0xDFC0B4	04 FF FF FF 00 33 04 00 09 3A 80 03 04 C0 A8 00 013...:.....
0xDFC0C5	06 04 C0 A8 00 01 36 04 C0 A8 00 01 FF FF FF FF FF6.....

Signature – 0x020106
 DHCP ACK-Bootstrap Protocol
 Message Type - 0x02
 Hardware type - 0x01
 Hardware Add len - 0x06
 Hops - 0x00



Cellular Base Stations

User Data Partition – HTC Evo 4G

- Android Location Package
 - Installs cache.cell
 - DB records cell towers
- Unallocated Instances

0x14FBB000	00 01 00 08 00 0B 30 3A 34 30 3A 36 3A 34 37 31 0:40:6:471
0x14FBB010	32 00 00 07 AF 00 00 00 4B 40 42 4B A1 FD 15 69	2...K@BK.i
0x14FBB020	F5 C0 5E 78 F9 B9 94 E1 A4 00 00 01 2F DA B9 B3	^x.../
0x14FBB030	53 00 0E 30 3A 34 31 38 33 3A 38 37 3A 34 39 32	S..0:4183:87:492
0x14FBB040	37 00 00 09 F5 00 00 00 4B 40 42 4C A7 A4 1E 57	7..K@BL W
0x14FBB050	DA C0 5E 78 5E 35 3F 7C EE 00 00 01 2F F0 FD 62	^x^5? .../t
0x14FBB060	11 00 0E 30 3A 34 31 38 33 3A 38 37 3A 34 37 32	...0:4183:87:472
0x14FBB070	38 00 00 0E 23 00 00 00 4B 40 42 74 97 41 D0 84	8...#...K@BtAE
0x14FBB080	E8 C0 5E 71 B7 6F 6D 76 25 00 00 01 2F F0 E4 02	^qomv%.../.
0x14FBB090	85 00 0B 30 3A 34 30 3A 36 3A 34 39 36 35 00 00	. 0:40:6:4965..
0x14FBB0A0	0A ED 00 00 00 4B 40 42 4C 7D 24 18 0D 3D C0 5E	...K@BL}\$. =^
0x14FBB0B0	78 BB 38 4F D2 A6 00 00 01 2F F5 69 2D 35 00 0B	x@Bn.../i-5.
0x14FBB0C0	30 3A 34 30 3A 36 3A 34 34 35 36 00 00 08 3A 00	0:40:6:4456....:
0x14FBB0D0	00 00 4B 40 42 4C E3 0C AA 32 6E C0 5E 78 81 DC	.K@BL 2n^x
0x14FBB0E0	0D B2 70 00 00 01 2F FA AF EE F0 00 0E 30 3A 34	p.../...0:4
0x14FBB0F0	31 38 33 3A 38 37 3A 34 39 32 38 00 00 06 C2 00	183:87:4928....
0x14FBB100	00 00 4B 40 42 4B DC 8B 86 B1 60 C0 5E 78 FA 82	.K@BK ^x
0x14FBB110	E8 7D 2C 00 00 01 30 06 53 AA 01 00 0E 30 3A 34	},...0.S...0:4
0x14FBB120	31 38 33 3A 38 37 3A 34 36 37 32 00 00 06 89 00	183:87:4672....
0x14FBB130	00 00 4B 40 42 4C 73 DE 1E 2D E8 C0 5E 78 9B 8C	.K@BLs -^x
0x14FBB140	B8 E0 87 00 00 01 30 09 BB CC AE 00 0D 33 31 30	...0 . 310
0x14FBB150	3A 30 3A 38 37 3A 34 36 37 32 FF FF FF FF 00 00	:0:87:4672....



IP and MAC

User Data Partition – Nexus One

<u>Count</u>	<u>IP Address</u>
80	3.0.0.5
8	193.113.200.195
8	192.168.192.192
8	192.168.77.1
4	1.8.8.1
4	1.4.0.1
3	192.168.251.150
3	200.142.130.104
3	2.6.32.9
3	139.7.24.1
2	213.158.194.226
2	210.241.199.199
2	194.182.251.158
2	212.53.51.143
2	200.192.230.142
2	149.254.201.135
.	
.	

<u>Count</u>	<u>MAC Address</u>	<u>Pre</u>	<u>Post</u>
1479	00:26:08:BC:D4:14	0x01	0x00
18	00:26:08:BC:D4:14	0xff0x20	
15	00:26:08:BC:D4:14	0x0a	0x23
12	90:21:55:2C:4D:67	0xff	0x00
11	00:26:08:BC:D4:14	0x5f	0x31
1	c0:c1:c0:40:cd:ac	0x11	0xff
1	00:11:95:39:13:d1	0x11	0xff
	- cache.wifi		

- Associated to a wireless access point
 - wpa_supplicant.conf
 - 3 Instances
 - 1 currently allocated

0x3A23FFF	FF 63 74 72 6C 5F 69 6E 74 65 72 66 61 63 65 3D 65 74 68	ctrl_interface=eth
0x3A24012	30 0A 75 70 64 61 74 65 5F 63 6F 6E 66 69 67 3D 31 0A 0A	update_config=1
0x3A24025	6E 65 74 77 6F 72 6B 3D 7B 0A 09 73 73 69 64 3D 22 4E 50	network={ ssid="NP
0x3A24038	53 22 0A 09 6B 65 79 5F 6D 67 6D 74 3D 4E 4F 4E 45 0A 09	S" key_mgmt=NONE
0x3A2404B	70 72 69 6F 72 69 74 79 3D 33 0A 7D 0A 0A 6E 65 74 77 6F	priority=3 } netwo
0x3A2405E	72 6B 3D 7B 0A 09 73 73 69 64 3D 22 41 6E 64 72 6F 69 64	rk={ ssid="Android
0x3A24071	46 6F 72 65 6E 73 69 63 73 22 0A 09 70 73 6B 3D 22 6E 70	Forensics" psk="np
0x3A24084	73 70 61 73 73 77 6F 72 64 22 0A 09 6B 65 79 5F 6D 67 6D	spassword" key_mgm
0x3A24097	74 3D 57 50 41 2D 50 53 4B 0A 09 70 72 69 6F 72 69 74 79	t=WPA-PSK priority
0x3A240AA	3D 32 0A 7D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00	=2 }



User Data Partition – Nexus One

- CheckInService.xml
 - 1 Currently Allocated
- Current IMSI

- 29 - 915050000000122
- 01 - 915050000000122



Bluetooth Data

User Data Partition – Nexus One

- Btopp.db
- Settings.db

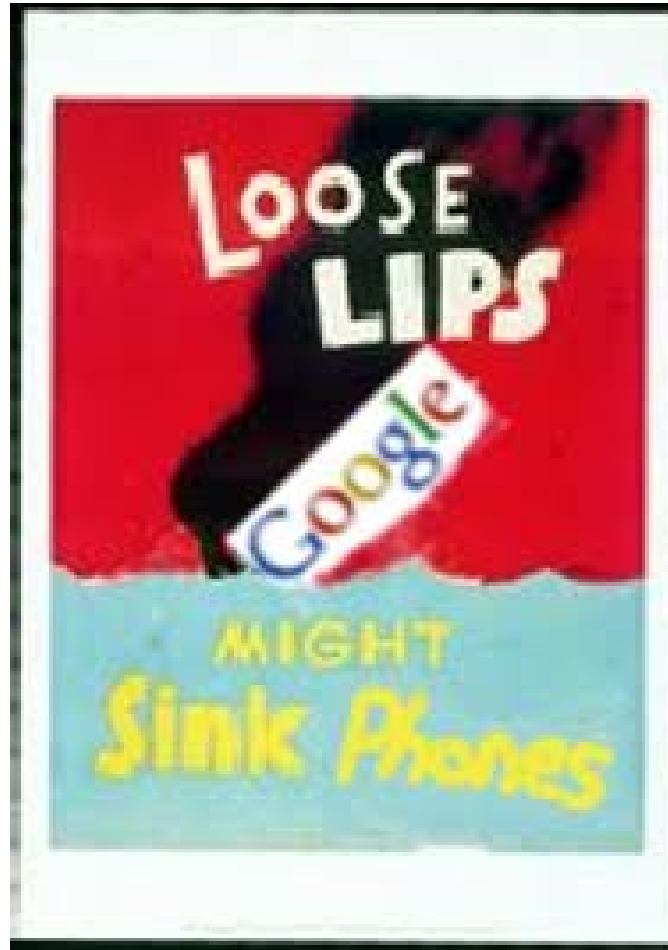
- 1479 - 00:26:08:BC:D4:14 0x01 0x00
- 18 - 00:26:08:BC:D4:14 0xff 0x20
- 15 - 00:26:08:BC:D4:14 0x0a 0x23
- 11 - 00:26:08:BC:D4:14 0x5f0x31



- MAC Address Database
- YAFFS Forensic Tools
- Mobile RAM Capture



Questions ??????????????



Source: precentral.net