

Digital Forensic on MTK-based Shanzhai Mobile Phone with NAND Flash

Mengfei He, Junbin Fang, Zoe L. Jiang, S.M. Yiu, K.P. Chow,
Xiamu Niu

Joint work

Harbin Institute of Technology Shenzhen Graduate School, China
The University of Hong Kong, Hong Kong
Jinan University, Guangzhou, China

Agenda

Introduction

- **Chinese Shanzhai mobile phone market**
- **Shanzhai Mobile phone forensics**

Overview on MTK-based Shanzhai phone flash memory

Digital forensics procedure

- **Storage structure**
- **Procedure analysis**

Conclusion

Introduction-Chinese Shanzhai mobile phone market

Shanzhai refers to Chinese imitation and pirated brands and goods - wikipedia



A real iphone?

- More than hundreds of different types of Shanzhai phones

e.g. "iphone 4" :

- Very cheap US\$60 for a cheaper version;
US\$130 for a more comprehensive version.
- A really big business

Shanzhai phone factory



Pictures from [1]

* Photos taken by an insider

Where to buy these phones?



Pictures from [1]

Where to buy these phones?



Pictures from [1]

Shanzhai Mobile phone forensics



More crimes involve mobile phones

More and more Shanzhai phones found to be involved in crime cases – **NOT ONLY in CHINA, but also TAIWAN, US** etc.

Shanzhai phone forensics becomes important. But, little published research on Shanzhai phone forensics due to the **lack of system manuals and knowledge of the memory layout**



Agenda

Introduction

- **Chinese Shanzhai mobile phone market**
- **Shanzhai Mobile phone forensics**

Overview on MTK-based Shanzhai phone flash memory

Digital forensics procedure

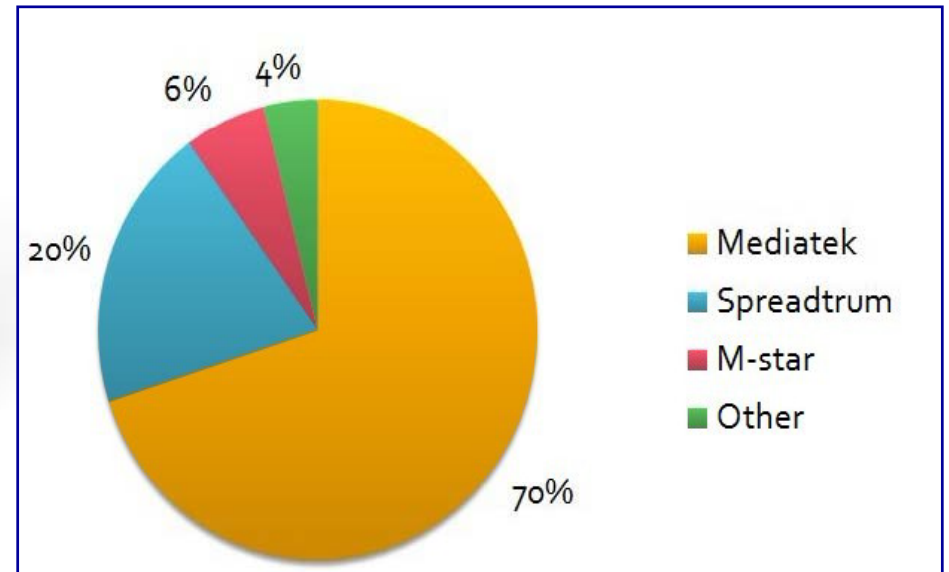
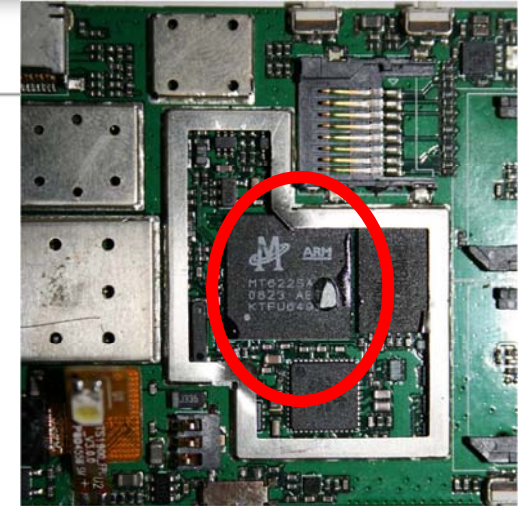
- **Storage structure**
- **Procedure analysis**

Conclusion

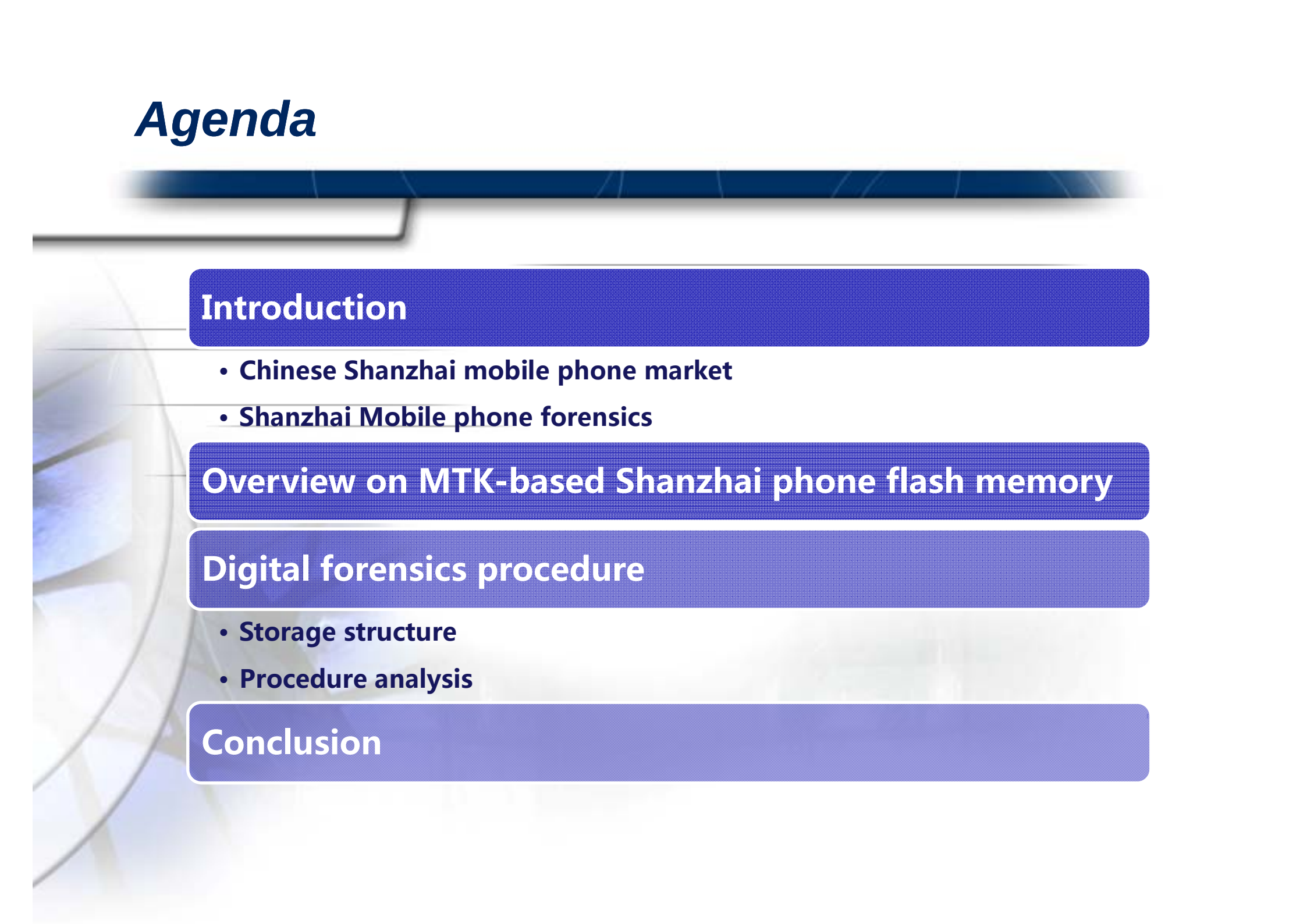
Overview on MTK-based Shanzhai phone flash memory

Most, if not all, Shanzhai phones use chips manufactured by **MediaTak (MTK)** - a Taiwan chipset company

MT6225	} low-end chips with NOR flash
MT6223	
MT6253	
MT6235	} high-end chips with NAND flash
MT6238	
MT6228	
MT6230	



Agenda



Introduction

- **Chinese Shanzhai mobile phone market**
- **Shanzhai Mobile phone forensics**

Overview on MTK-based Shanzhai phone flash memory

Digital forensics procedure

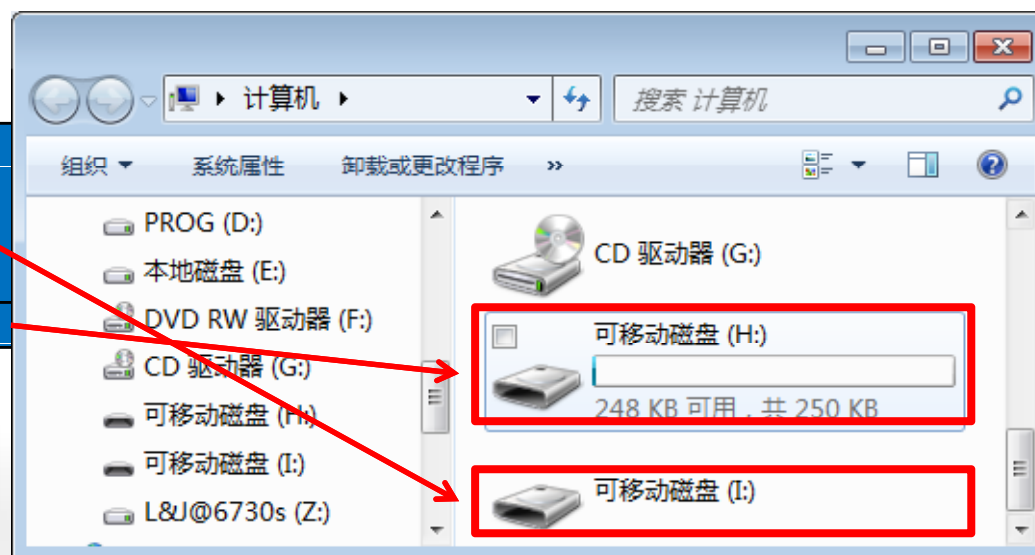
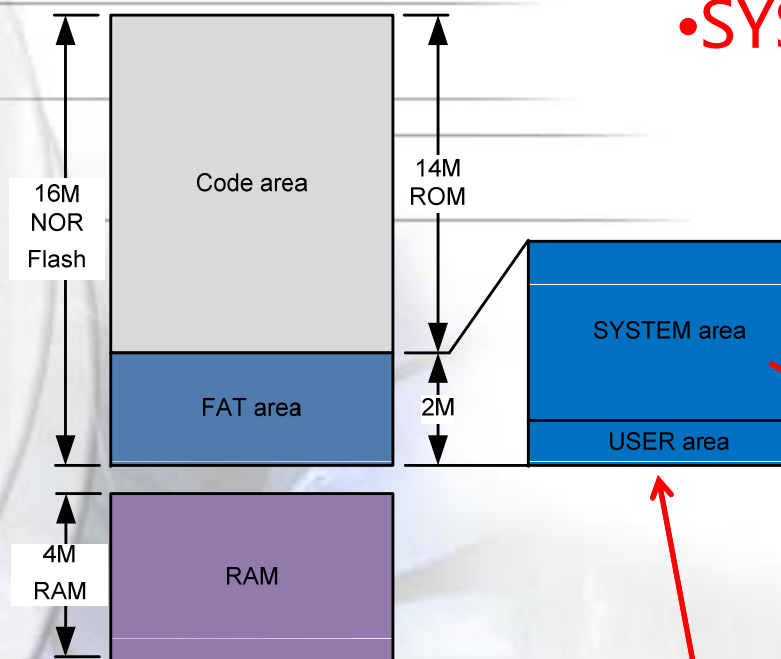
- **Storage structure**
- **Procedure analysis**

Conclusion

Digital forensics procedure-Storage structure

Internal flash memory of Shanzhai phone

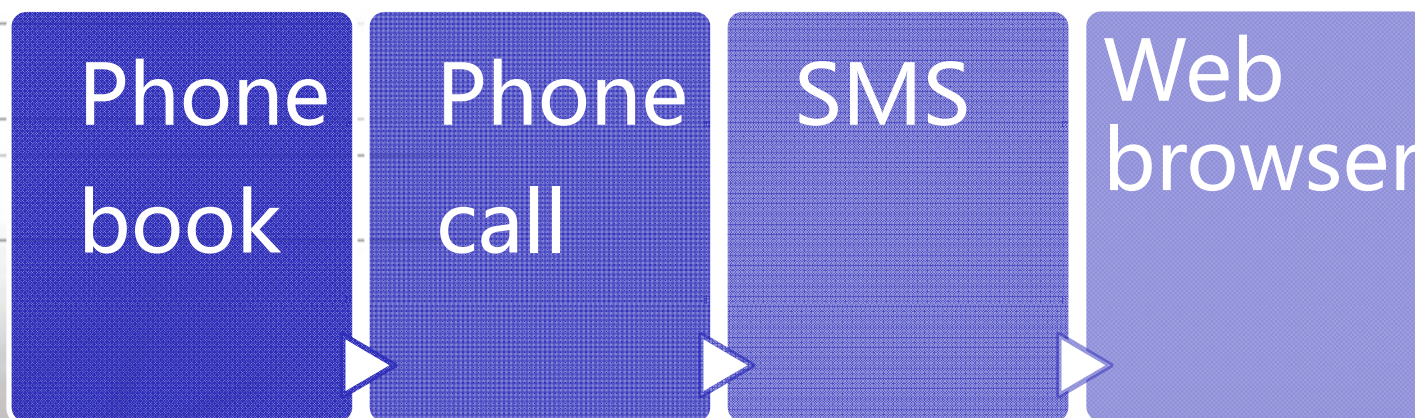
- USER area is accessible via USB connection with Windows OS
- SYSTEM area is invisible to user



* Note that this is only the logical distribution of the two areas. Physically, the blocks in flash for the two areas are mixed and not separated as clear as this figure.

Digital forensics procedure-Procedure analysis

a MediaTek MT6235 processor and a 132MB NAND flash chip



Phone book-Storage structure

073198E0	00 00 00 00 00 00 04 A4	41 00 4E 00 44 00 59 00	N.D.Y.
073198F0	31 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	1.....
07319900	00 00 00 00 00 00 00 00	38 39 37 36 33 35 37 00	8976357.
07319910	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
07319920	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
07319930	00 00 36 A4 00 00 00 00	00 00 00 00 00 00 00 00	..6?.....

Phone book-Forensic experiment design

Step	Operation	Name	Phone #
1	Add one entry	Andy	8976356
2	Add one entry	Andy1	8976357
3	Add one entry	Andy2	8976358
4	Delete one entry	Andy1	8976357
5	Add one entry	Andy3	8976359

We acquire the images after each step
Only one snapshot can be found

Phone book-Forensic analysis

073CF090	00 00 00 00 00 00 00 00	00 00 A1 00 41 00 4E 00	 ?A. N. I
073CF0A0	44 00 59 00 00 00 00 00	00 00 00 00 00 00 00 00	D. Y.....
073CF0B0	00 00 00 00 00 00 00 00	00 00 00 00 38 39 37 36	 8976
073CF0C0	33 35 36 00 00 00 00 00	00 00 00 00 00 00 00 00	356.....
073CF0D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
073CF0E0	00 00 00 00 00 00 04 A4	00 00 4E 00 44 00 59 00	 ? . N. D. Y.
073CF0F0	31 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	1.....
073CF100	00 00 00 00 00 00 00 00	00 39 37 36 33 35 37 00	 976357.
073CF110	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
073CF120	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
073CF130	00 00 BD A4 41 00 4E 00	44 00 59 00 32 00 00 00	.. 钱A. N. D. Y. 2...
073CF140	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
073CF150	00 00 00 00 38 39 37 36	33 35 38 00 00 00 00 00	 8976358.....
073CF160	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
073CF170	00 00 00 00 00 00 00 00	00 00 00 00 00 00 38 A4	 8

0740CE90	00 00 00 00 00 00 00 00	00 00 A1 00 41 00 4E 00	 ?A. N.
0740CEA0	44 00 59 00 00 00 00 00	00 00 00 00 00 00 00 00	D. Y.....
0740CEB0	00 00 00 00 00 00 00 00	00 00 00 00 38 39 37 36	 8976
0740CEC0	33 35 36 00 00 00 00 00	00 00 00 00 00 00 00 00	356.....
0740CED0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0740CEE0	00 00 00 00 00 00 04 A4	41 00 4E 00 44 00 59 00	 N. D. Y.
0740CEF0	33 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	3.....
0740CF00	00 00 00 00 00 00 00 00	38 39 37 36 33 35 39 00	 8976359.
0740CF10	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0740CF20	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0740CF30	00 00 3A A4 41 00 4E 00	44 00 59 00 32 00 00 00	.. : . N. D. Y. 2...
0740CF40	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0740CF50	00 00 00 00 38 39 37 36	33 35 38 00 00 00 00 00	 8976358.....
0740CF60	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0740CF70	00 00 00 00 00 00 00 00	00 00 00 00 00 00 38 A4	 8

Phone book-Forensic analysis

- Deleted phonebook entry will not be overwritten until a new phonebook entry is added
- Newly added phonebook entry is stored just behind the previously added entries
- Any modification on phonebook will lead it to update its storing position and the previous one will be emptied. We do not find any snapshot related to our historical operation

Phone call-Forensics experiment design

Step	Operation	Name	Phone #
1	Dial a call	Andy1	8976357
2	Dial a call	Andy2	8976358
3	Dial a call	Andy3	8976359
4	Delete a call record	Andy2	8976358
5	Dial a call	Andy4	8976360

We acquire the images after each step
Only one snapshot can be found

Phone call-Forensic analysis

- When deleting one phone call record, all other below it will be moved up one position
- Newly added phone call record will be placed to the topmost
- Any change to the phone call record will lead the entire call log change its storage position and the previous one will become empty. Similar to the phonebook, no snapshot appears in our experiment.

SMS-Storage structure

0733EA50	03 08 91 68 31 08 70 55 05 F0 24 0D 91 68 51 18	.. 慇1.pU. ?. 慇Q.
0733EA60	55 94 84 F9 00 00 21 70 10 90 94 93 23 07 7A F3	U顛?. !p. 悵?. z
0733EA70	19 BD 36 E7 01 FF FF FF FF FF FF FF FF FF FF	. ??
0733EA80	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	
0733EA90	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	
0733EAA0	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	
0733EAB0	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	
0733EAC0	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	
0733EAD0	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	
0733EAE0	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	
0733EAF0	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	
0733EB00	00 00 00 00 86 C2 00 00 00 00 00 00 00 00 00	 噲.....

SMS-Forensic experiment design

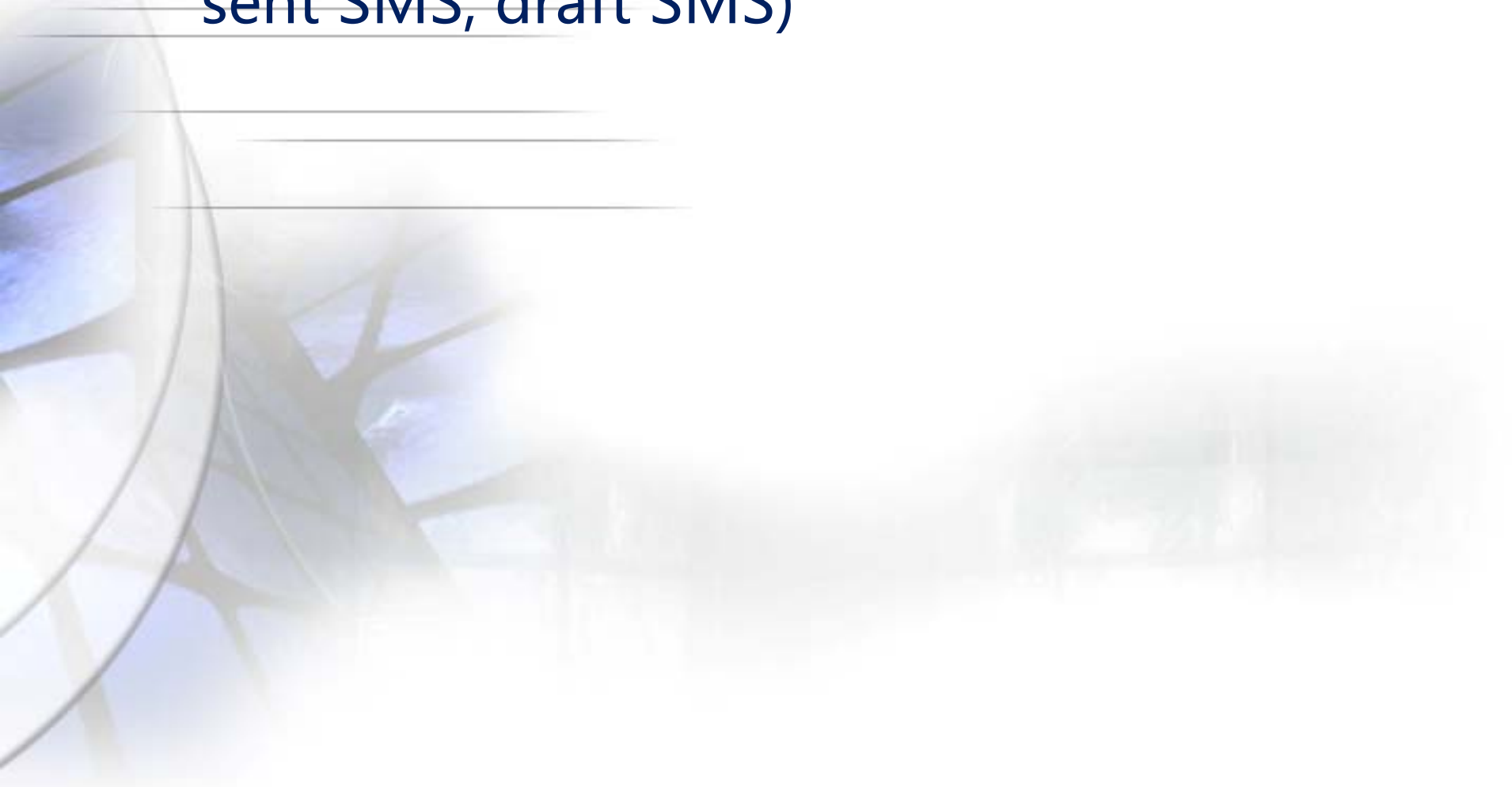
Step	Operation	Phone #
1	Receive an SMS	15815549489
2	View an SMS	15815549489
3	Receive an SMS	1065712035030104
4	Receive an SMS	10086
5	Delete an SMS	1065712035030104
6	Receive an SMS	18718672692
7	Send an SMS	15815549489

We acquire the images after each step
Only one snapshot can be found

SMS-Forensic analysis



All the SMS are stored together (received SMS,
sent SMS, draft SMS)



Web browser-Storage structure

07491FD0	68 74 74 70 3A 2F 2F 57 57 57 2E 42 41 49 44 55	http://WWW.BAIDU
07491FE0	2E 43 4F 4D 00 00 00 00 00 00 00 00 00 00 00 00	.COM.....

P1. User typed website

07448BC0	BC 8C E4 BD A0 E5 B0 B1 E7 9F A5 E9 81 93 00 FF	紆浣豺氨鏂ラ厶.
07448BD0	30 36 4C 54 BA 3A 68 74 74 70 3A 2F 2F 57 57 57	.6LT?http://WWW
07448BE0	2E 42 41 49 44 55 2E 43 4F 4D 2F 00 E7 99 BE E5	.BAIDU.COM/.鐳惧
07448BF0	BA A6 E4 B8 80 E4 B8 8B EF BC 8C E4 BD A0 E5 B0	害涓€涓�紆浣豺
07448C00	B1 E7 9F A5 E9 81 93 00 FE 16 B5 FF FF FF FF FF	辯鍵閫???

P2. Both user typed website and the hyperlink user went through
header, website and caption

Web browser-Forensic experiment design

Step	Operation	Website
1	Visit	http://www.baidu.com
2	Visit	http://www.soso.com:80/?t=04964
3	Visit	http://wap.sogou.com/sogou/?fr=s-sogou&clk=s-sogou
4	Delete	http://www.soso.com:80/?t=04964
5	Visit	http://dh.sogou.com/guide?m=cla&nid=1&cl=soxs&from=sogou&v=2&uID=JkmvQBdk299yhm9h

074131C0	BC 8C E4 BD A0 E5 B0 B1 E7 9F A5 E9 81 93 00 FF	紆浣豺氨鏂ﻝ.
074131D0	00 36 4C 54 BA 3A 68 74 74 70 3A 2F 2F 57 57 57	.6LT?http://www
074131E0	2E 42 41 49 44 55 2E 43 4F 4D 2F 00 E7 99 BE E5	.BAIDU.COM/. 鍋惧
074131F0	BA A6 E4 B8 80 E4 B8 8B EF BC 8C E4 BD A0 E5 B0	害涓€涓嶻紆浣豺
07413200	B1 E7 9F A5 E9 81 93 00 FE 00 34 4C 54 B9 3B 68	辯燧閫??4LT?h豺
07413210	74 74 70 3A 2F 2F 77 77 77 2E 73 6F 73 6F 2E 63	ttp://www.soso.c
07413220	6F 6D 3A 38 30 2F 3F 74 3D 30 34 39 36 34 00 E6	om:80/?t=04964.
07413230	90 9C E6 90 9C E6 9B B4 E6 87 82 E4 BD A0 00 FF	眞鏄ﻝ滄ﻝ鏄ﻝ備絳.
07413240	00 62 4C 54 B9 3F 68 74 74 70 3A 2F 2F 77 61 70	.bLT?http://wap
07413250	2E 73 6F 67 6F 75 2E 63 6F 6D 2F 73 6F 67 6F 75	.sogou.com/sogou
07413260	2F 3F 66 72 3D 73 2D 73 6F 67 6F 75 26 63 6C 6B	/?fr=s-sogou&clk
07413270	3D 73 2D 73 6F 67 6F 75 00 E6 90 9C E7 8B 97 E6	=s-sogou.鏄ﻝ滅娌
07413280	90 9C E7 B4 A2 E5 BC 95 E6 93 8E 20 2D 20 E4 B8	眞綯(-)紆鏄ﻝ?- 涓
07413290	8A E7 BD 91 E4 BB 8E E6 90 9C E7 8B 97 E5 BC 80	娉綉涓嶻眞鏄ﻝ楸紆
074132A0	E5 A7 8B 00 FF 00 5D 4C 54 B9 5B 68 74 74 70 3A	濮? .]LT?http:

074A37C0	BC 8C E4 BD A0 E5 B0 B1	E7 9F A5 E9 81 93 00 FF	紆浣豺氨鏹ヲ込.
074A37D0	00 36 4C 54 BA 3A 68 74	74 70 3A 2F 2F 57 57 57	.6LT?http://www
074A37E0	2E 42 41 49 44 55 2E 43	4F 4D 2F 00 E7 99 BE E5	.BAIDU.COM/. 鍋惧
074A37F0	BA A6 E4 B8 80 E4 B8 8B	EF BC 8C E4 BD A0 E5 B0	害涓€涓�嬭紆浣豺
074A3800	B1 E7 9F A5 E9 81 93 00	FE 00 34 4C 54 B9 3B 68	辯燧閭??4LT?ho.c
074A3810	74 74 70 3A 2F 2F 77 77	77 2E 73 6F 73 6F 2E 63	ttp://www.soso.c
074A3820	6F 6D 3A 38 30 2F 3F 74	3D 30 34 39 36 34 00 E6	om:80/?t=04964.
074A3830	90 9C E6 90 9C E6 9B B4	E6 87 82 E4 BD A0 00 FF	眞鏹滄垮鏹備絳.
074A3840	00 62 4C 54 B9 3F 68 74	74 70 3A 2F 2F 77 61 70	.bLT?http://wapu
074A3850	2E 73 6F 67 6F 75 2E 63	6F 6D 2F 73 6F 67 6F 75	.sogou.com/sogouI
074A3860	2F 3F 66 72 3D 73 2D 73	6F 67 6F 75 26 63 6C 6B	/?fr=s-sogou&clk
074A3870	3D 73 2D 73 6F 67 6F 75	00 E6 90 9C E7 8B 97 E6	=s-sogou.鏹滅娑 Y
074A3880	90 9C E7 B4 A2 E5 BC 95	E6 93 8E 20 2D 20 E4 B8	眞綯(-)鉄鏹?- 涓不
074A3890	8A E7 BD 91 E4 BB 8E E6	90 9C E7 8B 97 E5 BC 80	娑綉浣庯眞鏹耦紆
074A38A0	E5 A7 8B 00 FF 00 5D 4C	54 B9 5B 68 74 74 70 3A	濮? .]LT等http:
074A38B0	2F 2F 64 68 2E 73 6F 67	6F 75 2E 63 6F 6D 2F 67	//dh.sogou.com/gz
074A38C0	75 69 64 65 3F 6D 3D 63	6C 61 26 6E 69 64 3D 31	uide?m=cla&nid=1b
074A38D0	26 63 6C 3D 73 6F 78 73	26 66 72 6F 6D 3D 73 6F	&cl=soxs&from=so,
074A38E0	67 6F 75 26 76 3D 32 26	75 49 44 3D 4A 6B 6D 76	gou&v=2&uID=Jkmvy
074A38F0	51 42 44 4B 32 39 39 79	68 6D 39 68 00 E5 B0 8F	QBDK299yhm9h.灑
074A3900	E8 AF B4 00 FF 00 3B 4C	54 B9 87 68 74 74 70 3A	璇? .;LT鏹http:..

Web browser-Forensic analysis

- When we delete a web browser record, only its first byte is replaced with 0xFE
- The newly generated web browser record is just placed in the bottom
- Any operation could lead all the record in P2 change its location and no snapshot is generated

Conclusion

- MT6235 does not generate snapshots
- The investigation will be helpful when we encounter to this type of chip during forensic investigation
- Future work includes
 - trying to get a more detailed allocation architecture of the system for phone calls, phone book entries, SMS, and other related information
 - further analysis on the Spreadtrum-based Shanzhai phone which is another popular platform for Shanzhai phone.

Reference

- [1] Junbin Fang, Zoe Jiang, Kam-Pui Chow, Siu-Ming Yiu, Lucas Hui and Gang Zhou. MTK-based Chinese Shanzhai Mobile Phone Forensics, *Eighth Annual IFIP WG 11.9 International Conference on Digital Forensic*, 2012, pp. 1-9.

Thanks !



caven20studios

BzDap.com