Live Memory Forensics of Mobile Phones

By: Vrizlynn Thing
Digital Forensics Group
Cryptography and Security Department
Institute for Infocomm Research
Email: vriz@i2r.a-star.edu.sg

A*STAR I²R

Outline of Presentation

- Post-mortem forensics
- Live forensics
- Mobile phone forensics
- Related work
- Our proposed method
- Experiments and results
- Conclusions

Post-Mortem Digital Forensics

- Pull the plug
- Acquire data from static media
- Analyse data
- Correlate data to retrieve relevant evidence
- Forensically sound
- Limitations?

Live Forensic Approach

- Evidence stored (or transferred) off-site
- Static storage media increases in size, so does acquired potential evidence
- Use of encryption and password protection
- More efficient and effective through forensic investigation of system/device's current state

Mobile Phone Forensics

- Volatile information (e.g. application data, conversation histories) often not stored in static storage media
- Current approaches restricted to analysis of static data on SIM, memory cards and internal flash
- Need for live mobile phone forensics (prevent loss of potentially incriminating evidence)

Related Work

Kiley et al. (2008):

- Examined artifacts recovery
- Web-based IM services
- Windows XP system's unallocated hard disk space
- Tools: AccessData Forensic Toolkit and Runtime DiskExplorer
- Results: Very limited chat logs recoverable
- Limitations: short list of unique phrases, experiment parameters not well defined, static memory analysis

Related Work

Husian et al. (2010):

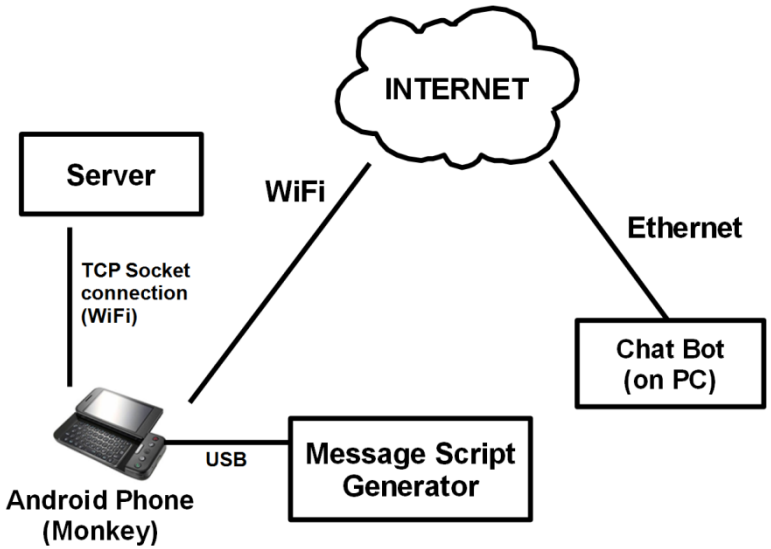
- Investigate possibility of IM related evidence recovery on iPhone
- Logical acquisition through iTunes Backup
- Results: evidence found for client-based IM, no trace found for web-based IM
- Limitation: Only saved logs on static memory could be retrieved

Live Memory Forensics of Mobile Phones

- Main functionality – support communications
- Importance of capability to perform forensic analysis of its interactive based applications
- Our work – An automated system to analyse the dynamic properties of the phone's volatile memory and applications
- Investigate persistency of volatile data and real-time acquisition and analysis

A*STAR I²R

Live Memory Forensics of Mobile Phones



- Message Script Generator (MSG)
- UI/Application Exerciser Monkey
- Chat Bot
- Memory Acquisition Tool
- Memory Dump Analyser (MDA)

A*STAR I²R

Experiments

- Process memory region investigation
  - Identify region where conversations reside
  - 15 rounds of outgoing messages and 15 rounds of incoming messages
  - Results: 1) messages consistently found in shared memory regions; 2) database initialization information and chat session credentials found in heap and stack

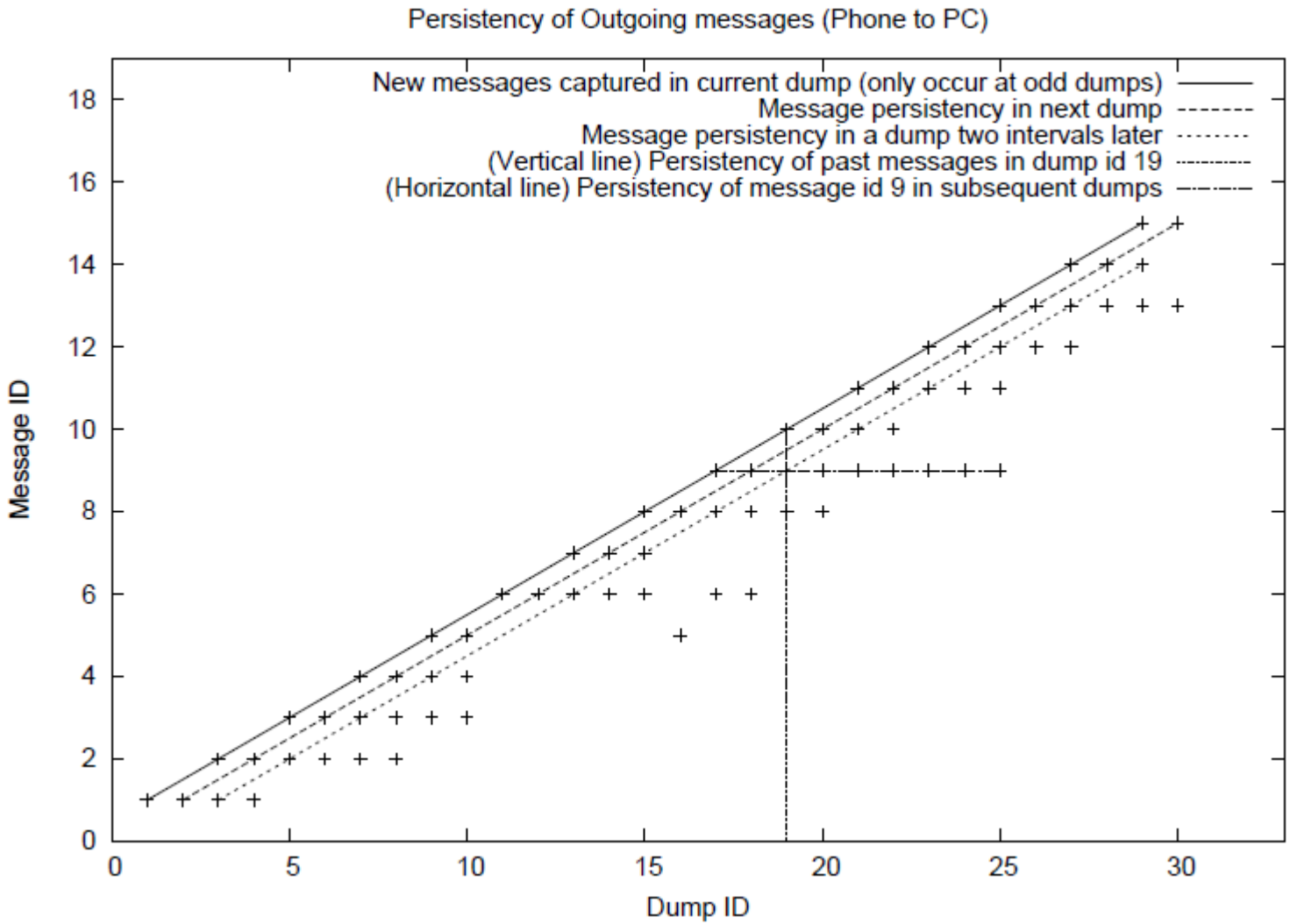
Experiments

- Cached data examination
  - Examine browser cached data to investigate information retrieval possibility
  - 15 rounds of outgoing messages and 15 rounds of incoming messages
  - Results: cached data stored in SQLite databases; contains bookmarks, searches, images, javascripts, formdata, cookies, etc. but no trace of conversation found

Experiments

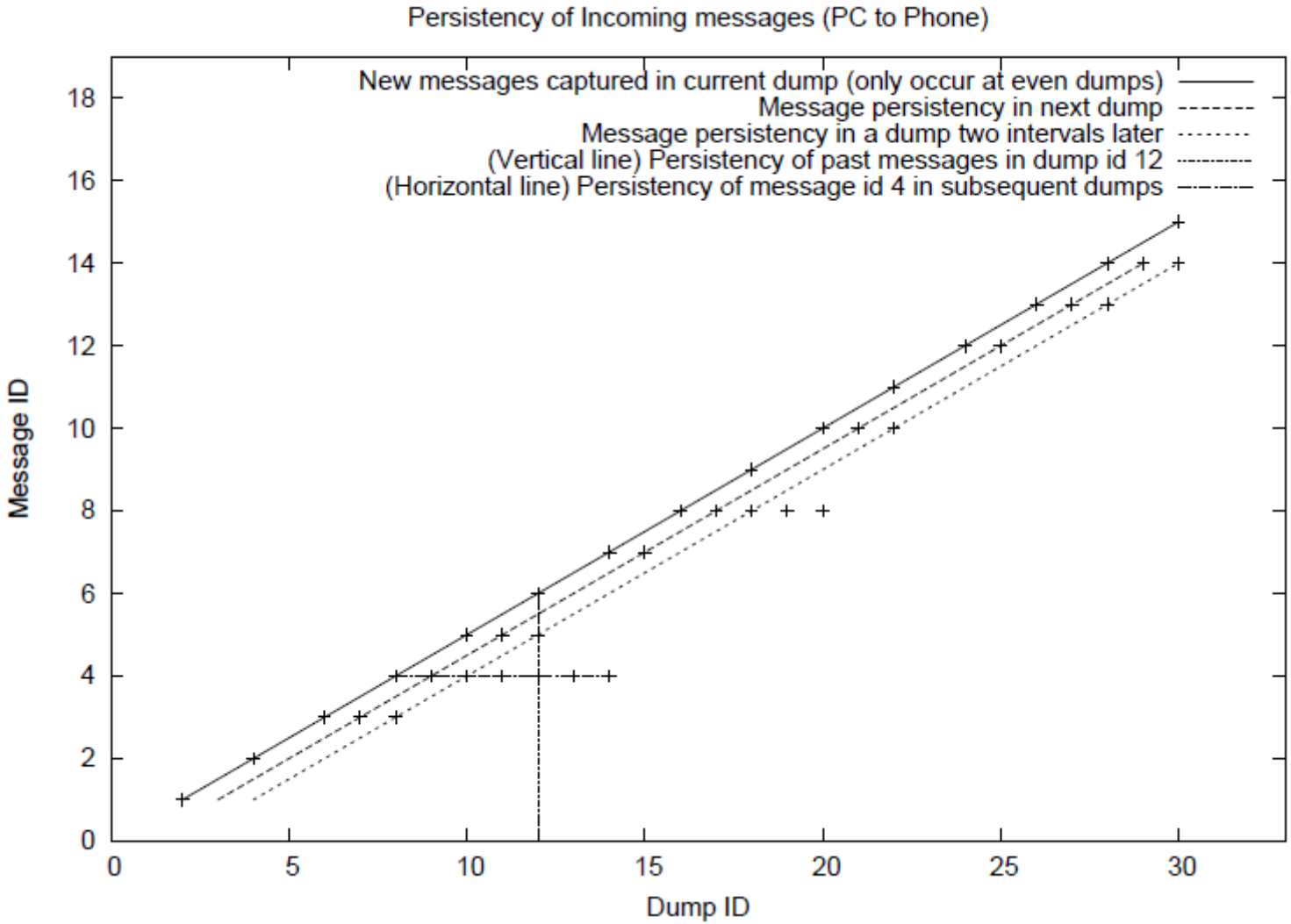
- Volatile data persistency investigation
  - Determine realistic set of parameters
  - Interval between keypresses: 500ms
  - Character set: standardise one key press = one character in memory
  - Message length: 75, 150, 225 characters
  - 15 rounds of outgoing messages and 15 rounds of incoming messages

Experiments



A*STAR I²R

Experiments

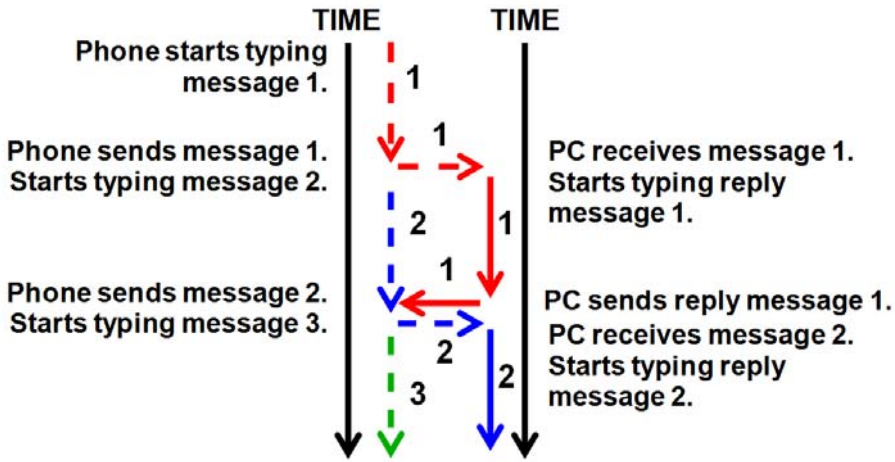


A*STAR I²R

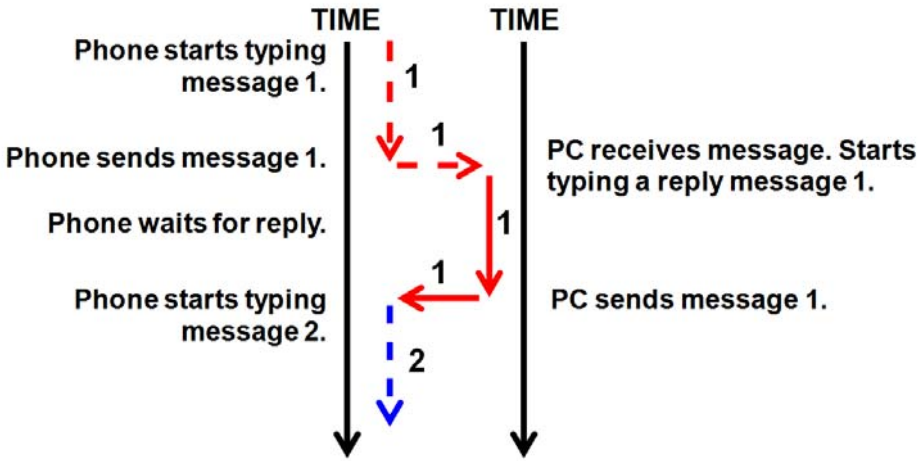
Experiments

- Memory dump interval investigation
  - No-wait scenario (worst case)
  - Waiting scenario
  - Intervals of 5, 10, 20, 30 seconds for no-wait
  - Intervals of 40, 60 seconds for waiting
  - 15 rounds of outgoing messages and 15 rounds of incoming messages

Experiments



No-wait Scenario



Waiting Scenario

A*STAR I²R

Experiments

Message Length (Chars)	Dump Interval			
	40 secs		60 secs	
	Outgoing Msgs	Incoming Msgs	Outgoing Msgs	Incoming Msgs
75	15/15	15/15	15/15	13/15
150	15/15	15/15	15/15	15/15
225	15/15	14/15	15/15	15/15

- Waiting scenario
- 100% of outgoing messages acquired and detected successfully
- Avg. acquisition rate: 97.8% for 40-sec interval and 95.6% for 60-sec interval

A*STAR I²R

Experiments

Message Length (Chars)	Dump Interval			
	5 secs		10 secs	
	Outgoing Msgs	Incoming Msgs	Outgoing Msgs	Incoming Msgs
75	15/15	15/15	15/15	13/15
150	15/15	15/15	15/15	13/15
225	15/15	15/15	15/15	13/15

Message Length (Chars)	Dump Interval			
	20 secs		30 secs	
	Outgoing Msgs	Incoming Msgs	Outgoing Msgs	Incoming Msgs
75	15/15	11/15	15/15	12/15
150	15/15	13/15	15/15	13/15
225	15/15	10/15	15/15	13/15

- No-wait scenario
- 100% of outgoing messages acquired and detected successfully
- Avg. acquisition rate: 100%, 86.7%, 75.6% and 84.4% for 5, 10, 20 and 30-sec interval, respectively

A*STAR I²R

Conclusions

- Identified the need for live memory forensic analysis for mobile phones
- Proposed a method and system to analyse dynamic properties of mobile phones' volatile memory and perform real-time evidence acquisition, automatically and systematically in different communication scenarios
- Current system capable of optimizing acquisition parameters to improve efficiency

A*STAR I²R

Thank you!

Vrizlynn Thing
vriz@i2r.a-star.edu.sg

A*STAR I²R