MobileInsight: Extracting and Analyzing Cellular Network Information on Smartphones

http://metro.cs.ucla.edu/mobile_insight/

Yuanjie Li[1], Chunyi Peng[2], Zengwen Yuan[1], Jiayao Li[1], Haotian Deng[2], Tao Wang[3]
[1] University of California, Los Angeles [2] The Ohio State University [3] Peking University

What is MobileInsight?

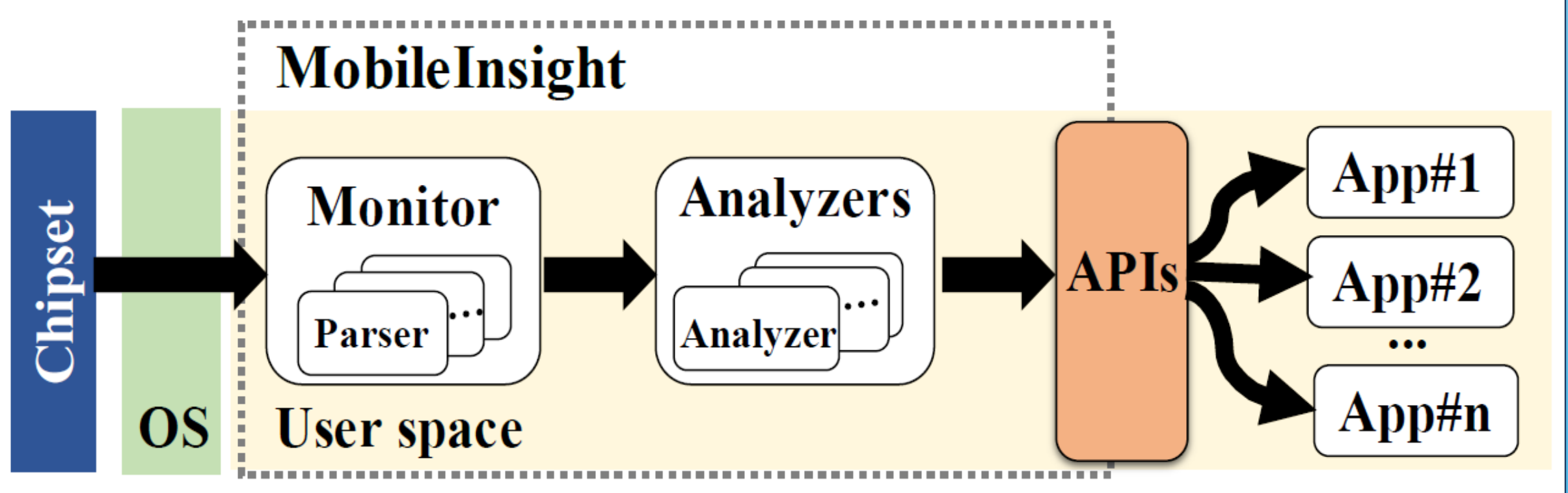
MI is an in-phone software tool that collects, analyzes and exploits runtime fine-grained cellular network information, operations and states over commodity smartphones.

Highlights

- ✓ COTS phones (no extra hardware/PC required)
- ✓ Wide coverage of cellular specific protocols
- ✓ Fine-grained (message-level) granularity
- ✓ Cellular protocol behavior analysis
- ✓ Runtime support
- ✓ APIs provided
- ✓ Downloaded by 36+ groups

How MI Works

Overview

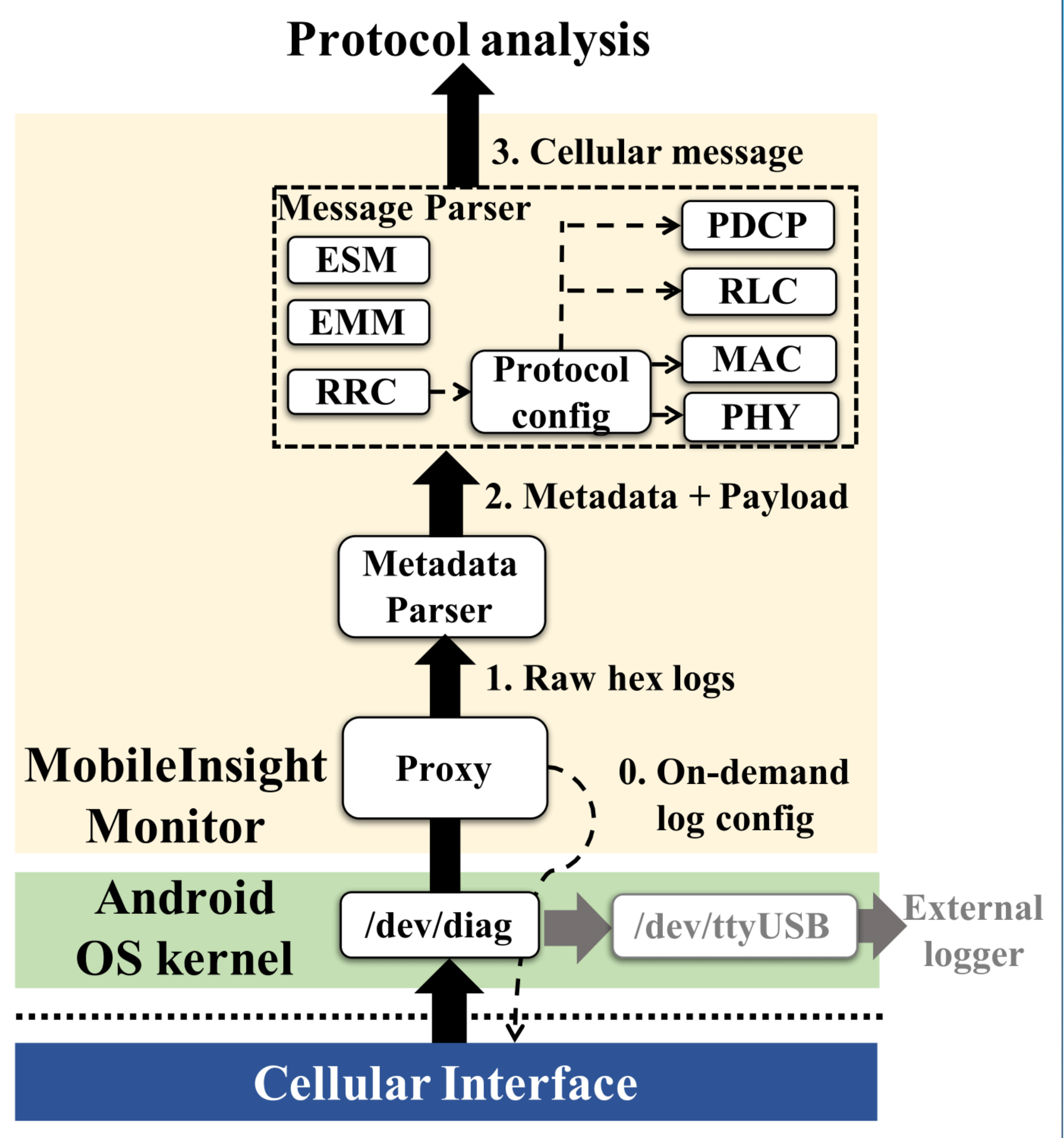


- In-device runtime monitor
- Cellular protocol analyzers
- MobileInsight APIs

In-Device Runtime Monitor

It extracts raw cellular logs from the chipset to device user-space, and parses them into protocol messages.

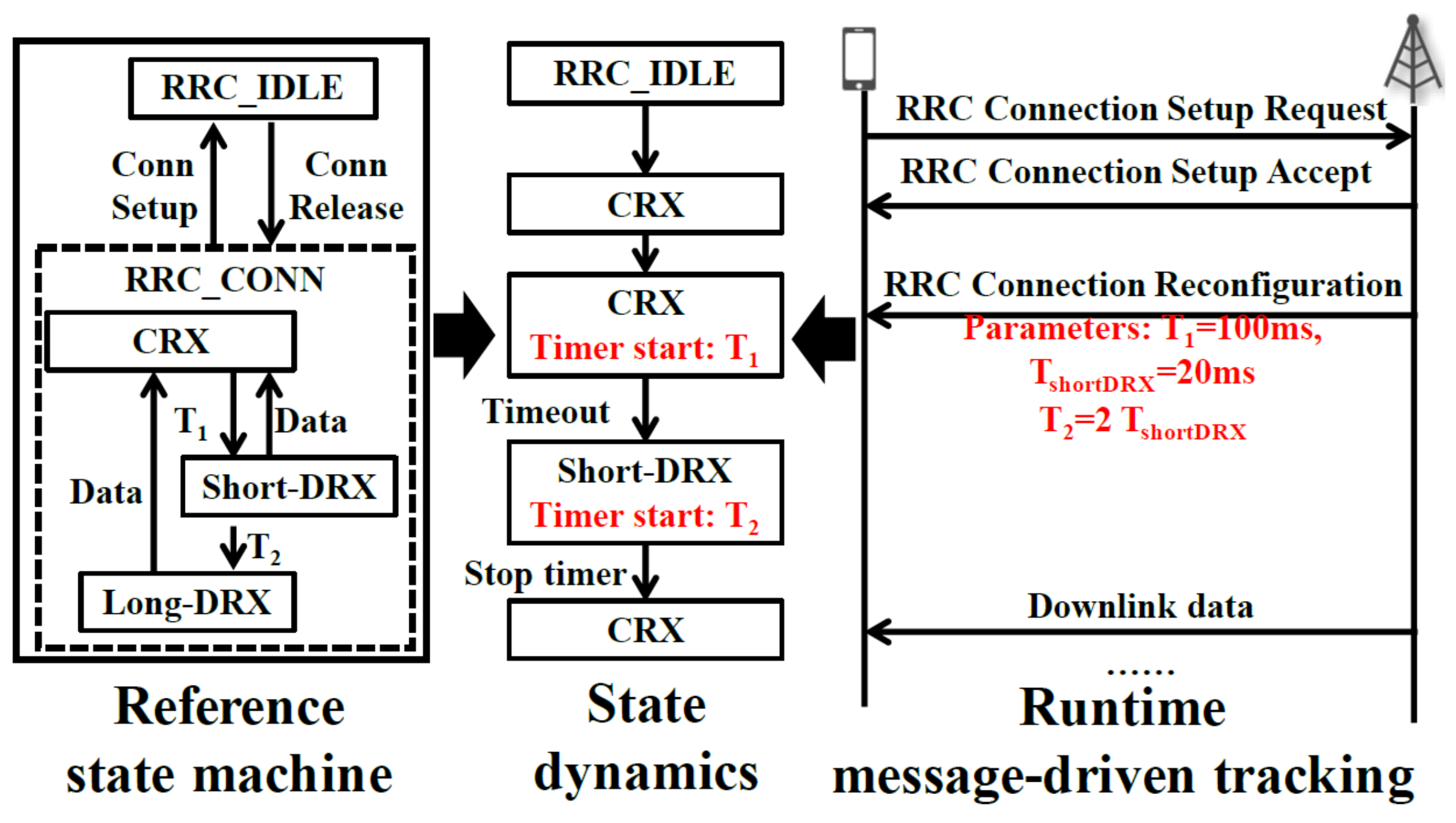
- Extraction from side channel
  (virtual device /dev/diag/)
- Two-level parser
  (metadata + 3GPP protocol messages)
- Optimization via on-demand mode
  (dynamic configuration/parsing)



Cellular Protocol Analyzer

1. Extract protocol state dynamics

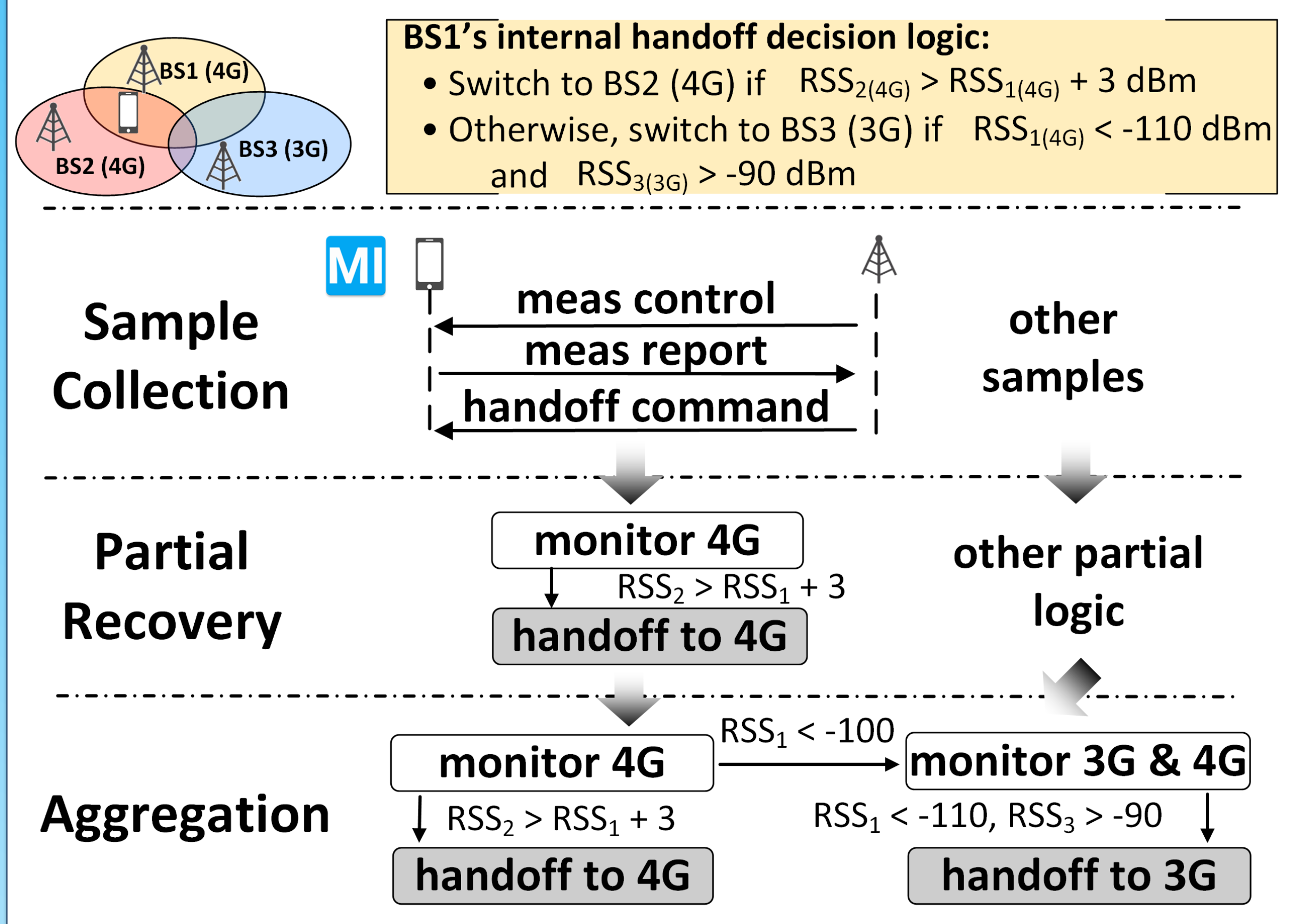
- Construct reference state machine
  (based on 3GPP standards)
- Track state transitions from runtime message parsing
- Extract states and state-relevant configurations



2. Infer network operation logics

(Use handoff as an example)

- Model handoff decision logic
- Perform online inference
  - Collect samples
  - Recover the logic partially
  - Aggregate



MobileInsight APIs

- APIs for *Monitor()* and *Analyzer()*

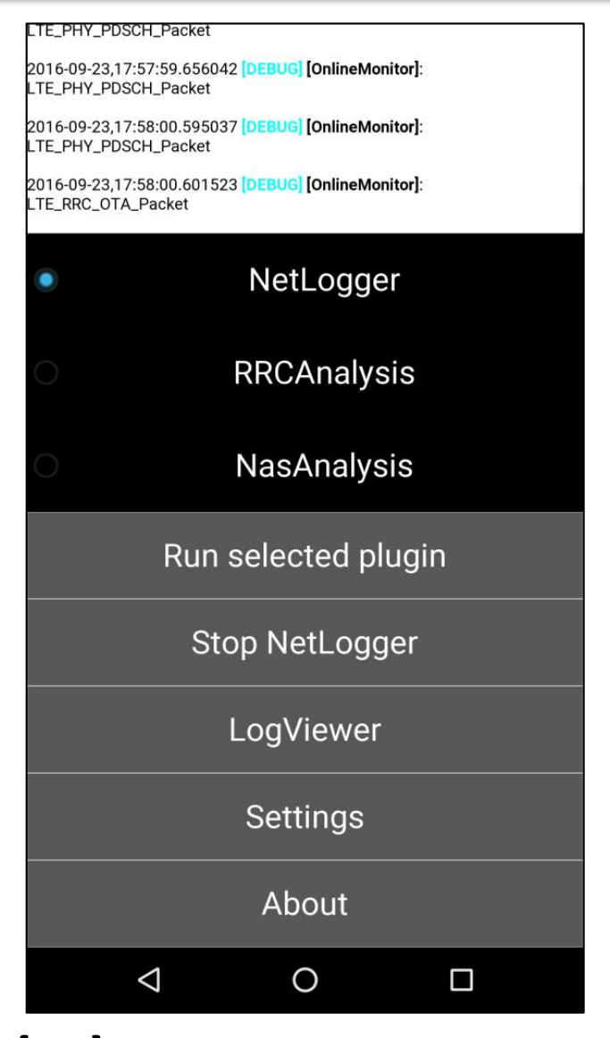
```
# A simple example on how to track 3G/4G RRC protocol
# Initialize an in-device monitor
src = OnlineMonitor()
# Declare cellular protocol analyzers
lte_rrc_analyzer = LteRrcAnalyzer() #4G RRC
wcdma_rrc_analyzer = WcdmaRrcAnalyzer() #3G RRC
# Bind analyzers to the monitor
lte_rrc_analyzer.set_source(src)
wcdma_rrc_analyzer.set_source(src)
# Start processing
src.run()
```

Check more examples and tutorials on our website.

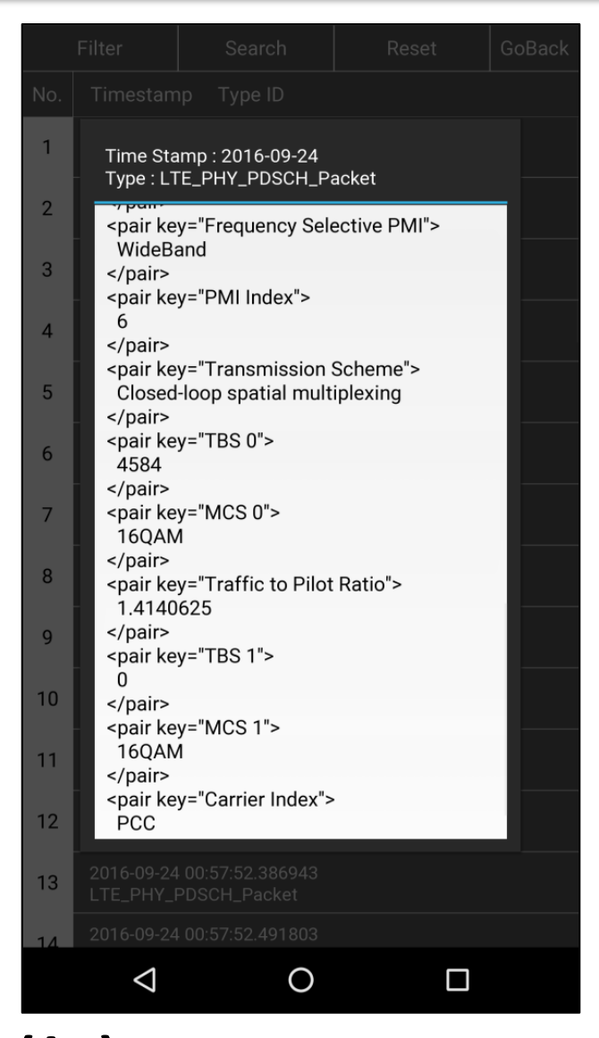
What MI Achieves?

- **A variety of devices supported**
  - ✓ 13+ phone models tested
  - ✓ Android (4.3.0-7.0.0), iOS (feasibility)
  - ✓ Chipsets: Qualcomm Snapdragon, MediaTek/Intel (ongoing)
- **Wide coverage of protocols/msgs**
  - ✓ Full set of 4G/3G control-plane protocols (RRC, MM,ESM/SM/CM…)
  - ✓ Most 4G data-plane protocols + partial 3G support
  - ✓ 240 message types supported
  - ✓ 3GPP releases 7-12
- **Responsive and effective**
  - ✓ Processing time within 0.8ms (99+%)
  - ✓ Used to identify/analyze handoff (mis)configurations, security loopholes, failures/degrades, …
- **Acceptable overhead**
  - ✓ CPU: 1-3% @S5,6P, RAM: <30 MB, Power: 11-58mw (average)

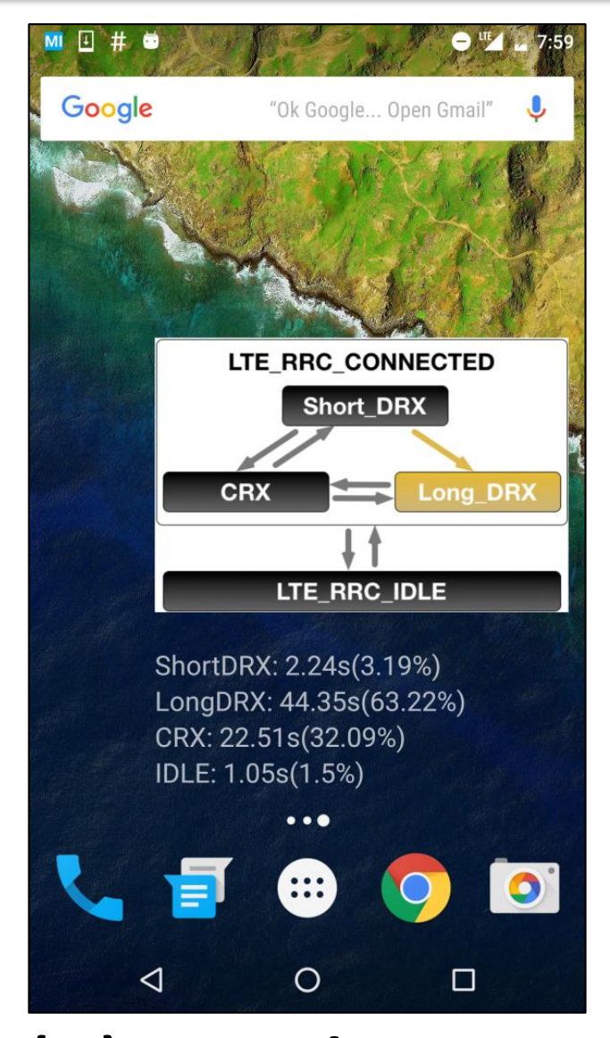
Demos



(a) Monitor: NetLogger



(b) Monitor: Logview



(c) Analyzer (Ex: 4G-RRC)

(d) DASH video streaming (speed booster)

Toward a Community Tool

- ✓ Downloaded by 36+ groups
  (from US, China, Korea, UK, Germany, ..)
- ✓ 245+GB dataset available
  (13+ months, 8+ carriers, 30+ users, …)

Download MI and Explore More!