Digital Witness
Remote Method for Volunteering
Digital Evidence on Mobile Devices

Nigel Campbell, Evan Stuart, Trevor Goodyear, Winston Messer, and James Fairbanks
$ whoami

- Research Scientist @ GTRI
- Software Developer
- MSCS Student
Overview

https://www.army.mil/article/39356/evidence_collection_course_helps_ips_close_cases
Overview

- Problem and State of the Art
- Security and Threat Model
- Mobile App
- Custody Control
- Officer Facing Application
- Conclusions and Future Work
State of the Art

- Witness or Victim has digital evidence
- They report to police officers
- Officers take an image of entire phone using forensic software such as Cellebrite or FTK Imager.
- Officers then take image and analyze it within their forensics suite of tools (E.g. Autopsy, EnCase)
Cellebrite Devices give the impression of selective capture
Introduction

- Working with the DeKalb County Police Department we observed a typical forensic capture time of a mobile phone of approximately 2 hours.
- Plus time traveling to and from the police station
- Plus time spent waiting for a device to clear the evidence backlog.
Quis custodiet ipsos custodes?

- Without FOSS forensics tools, police themselves can’t verify privacy policies
- FBI vs Apple
- Cellebrite
- Greybox
Current Workflow is Problematic

- Takes too long to extract information
- Consumes PD resources
- Valid privacy concerns
- Office time spent identifying relevant information
Solution

Solution Architecture
Open Source
github.com/DigitalWitness
Physical Evidence Submission

- Evidence must be tracked with the case it belongs to.
- Pen and Paper evidence locker
- Evidence is checked in and out, these operations is need to be translated
- Chain of Custody is a sequence of:

  (item, name, date)
Digital Evidence Submission

- Lawful Authority: warrant, court order ...
- No rigorous chain of custody available for Digital Evidence
- Our custody component brings this process up to date
Threat Model

- Our threat model is not one of full trust or skepticism
- Police and courts trust the software
- Users want to minimize data exposed to police
- Police want to verify authorship of data revealed to them
- Courts and interest groups (e.g., ACLU) want to verify police assertions
- Human factors of witnesses and victims is important
Security Model

- Authorities must prove that they are collecting only the information that they claim to collect
- PKI Encryption is used:
  - Mobile devices must generate their own private keys
  - Mobile devices must deliver the public parts to the authorities
Disclosing Specific Evidence: Mobile App

- The Disclose app allows Android and iOS users to upload evidence
- Permissions are minimally invasive and time out after submission
- Witnesses and Victims can authenticate with existing accounts, convenient and helpful to authorities
Disclose: Account Creation

- On signup, device specific ECDSA public/private keys are generated.
- Public key is submitted to the custody server process.
- Private key is subsequently used to generate digital signatures for evidence.
Disclose: Evidence Selection and Submission
Disclose: Digital Signature Creation

- During submission
  - Signature is created via the ECDSA private key
  - Verified by the custody server (using previously submitted public key).
- Ensures authenticity and message integrity.
Officer Facing Application

Officers can view all the evidence submitted including Geolocation and Metadata. Integrity of this information is protected by chain of custody.
Maintaining the “digital” chain of custody

- Creation of distinct identities (witnesses/victims)
- Recording signatures (for evidence submissions)
- The digital ledger
# Custody Ledger

<table>
<thead>
<tr>
<th>id</th>
<th>message</th>
<th>signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>parent:null Upload Image 1</td>
<td>ef2110</td>
</tr>
<tr>
<td>2</td>
<td>parent:ef2110 View Image 1</td>
<td>ff1122</td>
</tr>
<tr>
<td>3</td>
<td>parent:ff1122 Submit Image 1</td>
<td>aa33dd</td>
</tr>
</tbody>
</table>
Custody Control

- Identities hold the user information
- Ledge tracks the messages
- Each entry in the Ledger has a parent and a signature that can be used to verify the integrity of the message
- By incorporating the signature of the parent entry into the message of the next entry, the ledger protects against evidence fabrication
Why not blockchain

- We don’t need a distributed ledger
- There is a central broker anyway, the federal court system
- No way to incentivise people to supply compute power for verification
- We can get what we need with Merkle Trees and PKI
Merkle Trees

The custody component contains a merkle tree implementation for validating the chain of custody.

Given a piece of evidence (message) and the Top Hash (from the custody service). Watchdogs can verify that the evidence was collected in the order the Officers say it was.
Future Work

- Field deployment and evaluation
- Analytics of media collected
- Crime forecasting
- Identification of underserved areas and situational awareness
Conclusions

- Evidence submitted through Disclose can be verified and tracked
- Actions by officers using the web app can be audited for privacy violations and warrant requirements
- ECDSA PKI and Merkle Trees are sufficient for providing these guarantees
GTPD COP
Demo