NTNU

Norwegian University of Science and Technology

IoT forensics

Jens-Petter Sandvik

Faculty of Information Technology and Electrical Engineering, NTNU
Department of Information Security and Communication Technology
NTNU Digital Forensics Group

2018-05-08 / Finse / COINS Winter School

NTNU

Me, myself and I

- Cand.scient. UiO, Institure of Informatics, 2005
- Programmer of antivirus software
  - Scanning engine
- Digital forensics in Kripos since 2006
- Chapter author in textbook
  - “Mobile and embedded forensics”
  - Andre Årnes (ed.), “Digital forensics”, Wiley, 2017
- PhD reserach project: IoT forensics
  - Supervisors:
    - Katrin Franke (NTNU)
    - Habtamu Abie (NR)
    - Andre Årnes (Telenor/ NTNU)

NTNU

What exactly is *Internet of Things*?

- 1999: Things tracked by RFID over the Internet
- Now: Physical and virtual *things* with processing, sensing and actuating functionality connected over internet, together with the infrastructure
  - M2M
- Estimated number of things in 2020: 20 billion to 200 billion
- Things can have limitations to resource usage, bandwidth, connection reliability
- New and existing protocols, architecture and technology
- Many application areas
  - Smart homes
  - Smart infrastructure
  - Industrial IoT/ Industrie 4.0
  - Intelligent Transportation Systems
  - etc

NTNU

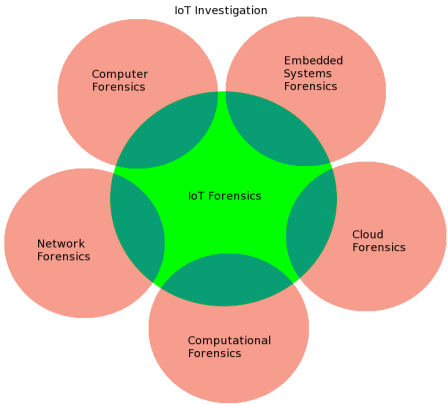
What exactly is *Digital Forensics*?

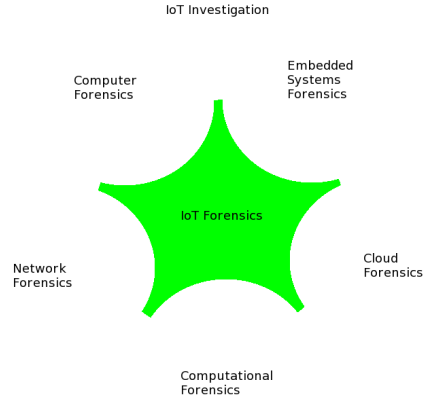
Definition

Forensic science refers to the application of scientific methods to establish factual answers to legal problems both in criminal and civilian cases. Digital forensics refers to forensic science as applied to digital media.

- Types of digital forensics:
  - Computer forensics
  - Mobile device forensics
  - Embedded system forensics
  - Database forensics
  - Network forensics
  - +++
- Pragmatically named
  - No strict taxonomy
- Forensic process:
  - Identify, collect, examine, analyze, report
  - Forensic readiness / proactive forensics

IoT forensics





NTNU

IoT and forensics - what is new?

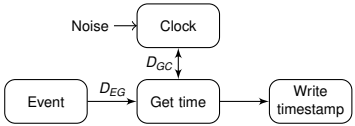
- More devices
  - Time consuming
  - Resource consuming
- More data
  - Cloud
  - On thing
  - Somewhere between
- New types of devices
- Volatile data
- Edge computing/ Fog computing
- Dynamic systems
- Failing devices

The Reliability of Clocks as Digital Evidence under Low Voltage Conditions

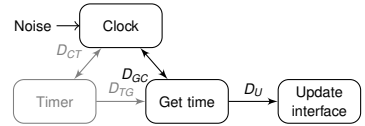
- Tested 4 different devices
- Hypotheses:
  - H_0: Clock can be adjusted by low voltage on battery
  - H_a: Clock goes either (close to) correct, or is being reset when voltage is low
- One phone was automatically adjusted 8-12 years into the future when voltage was held at 2.03 - 2.10 V for 9-10 s
- All tested methods for documenting time had a precision better than 4 s.
  - max(devices, 3rd - 1st quartile) $\leq$ 0.59 s
- A model for delays and noise in clocks
  - Based on Willasen (2008)
  - $c(t) = b(t) + d(t) + \sum_X D_X(t)$

Delay model

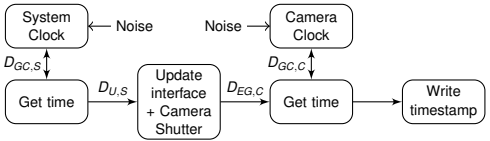
Event triggering writing a timestamp



Updating an interface

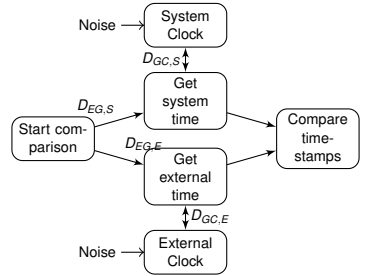


Documenting time with a photo



$$d_s(t) - d_c(t) + \sum D_s(t) + \sum D_c(t)$$

Documenting time with app



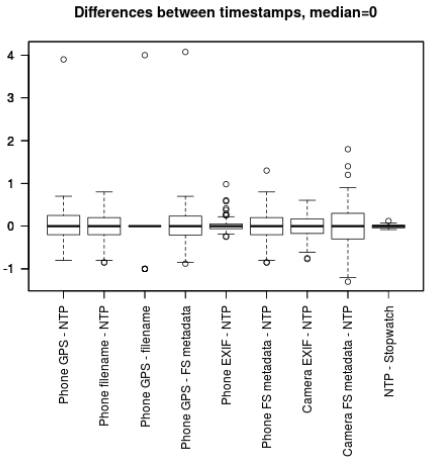
$$d_S(t) - d_E(t) + \sum D_S(t) - \sum D_E(t)$$

NTNU

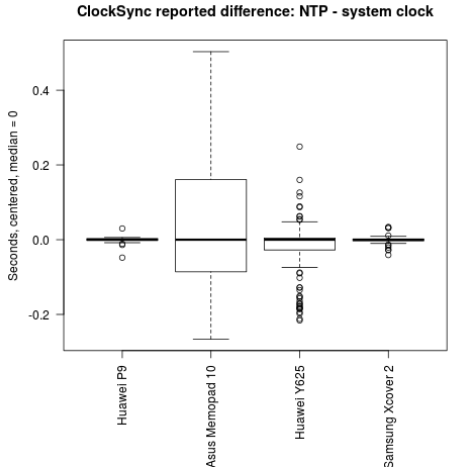
Methods of measuring precision

- Equipment:
  - Two cameras (Huawei P9 Phone + Canon 60D DSLR)
  - Stopwatch
  - Computer running NTP client
- Comparing timestamps from photos with NTP and stopwatch
- Finding $\sum_X D_X(t)$ in $c(t) = b(t) + d(t) + \sum_X D_X(t)$
- Also testing app running on phones: ClockSync
  - NOT FORENSICALLY SOUND!
  - ...But very convenient for testing

Results of measuring precision, comparing camera timestamps



Camera documentation

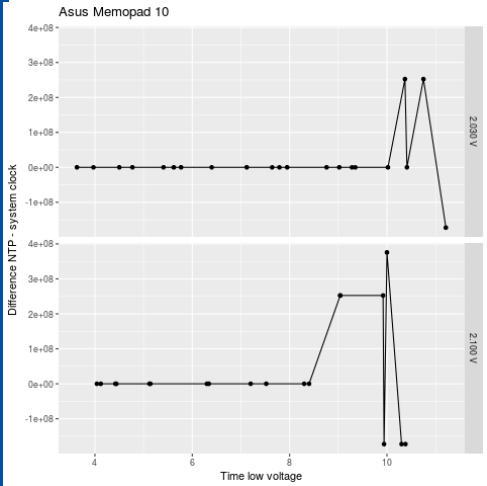


ClockSync app

Method of testing clocks under low voltage

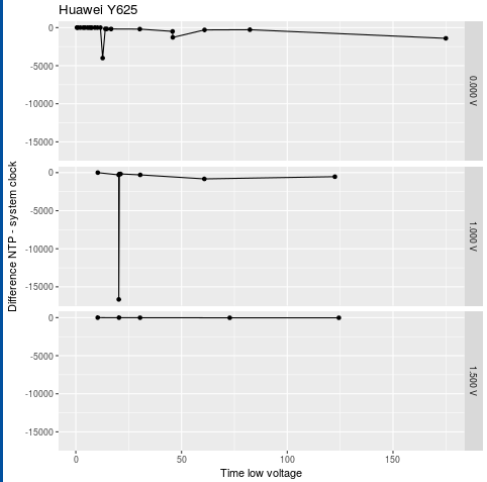
- 4 devices tested:
  - 2 Android phones – Huawei Y625 & Samsung Xcover 2
  - 1 Android tablet – Asus Memopad 10
  - 1 Windows phone – Nokia Lumia 830
- Android phones were tested using ClockSync app, Windows phone by photo
  - Documenting time before and after low power
- Connected power supply to battery pads, turned down voltage with OS running
  - Operating voltage on battery is 3.8 V
  - Low voltage (approx 2 V) was not sufficient to run the OS
  - Some batteries needed to connect thermistor or battery size indicator
- Find the time-voltage combinations where clock was reset
- See whether clock invalidated the alternative hypothesis
  - Decide if $d(t)$ is affected in $c(t) = b(t) + d(t) + \sum_X D_X(t)$

Results: ASUS Memopad 10 tablet



- At 2.030 or 2.100 V, and $\sim$ 10*s*, clock jumped forward
- 2025-07-20 and 2029-06-18
- 252 460 800 s, 252 460 816 s, 375 831 104 s
- 0x0F0C3F00, 0x0F0C3F10, 0x1666BA40
- Epoch was 1970-01-02 00:00:00Z
- After 30-60 s, time adjusted to normal time
  - SSL error for Google checkin service
  - Device clock outside validity period of certificate

Results: Huawei Y625-U21 mobile phone



— Clock stops or lags before being reset
— Epoch is right before the clock shuts down
  - Seems to be updating the time reset value regularly
— Did not see jumps in time apart from this

NTNU

What now?

- Forensic examination of fused data
- Dependability and forensic examinations
- Forensic challenges of opportunistic networks
- Car forensics
- Simulation of IoT systems
  - Forensic readiness assessment
  - Synthetic datasets
- From deterministic to stochastic system models in digital forensics(?)