Computer Forensics

Søren Debois
May 1, 2017

SECURITY F2017

Lecture 9

Meta

Plan

- Evaluation
- Schedule
- Incident Response
- Computer Forensics
- Ext3

Evaluations

- The course is functioning

- TAs are excellent

- I should work on my articulation

Rest of course

- Monday, May 1st (today):
  Advanced Authentication & Access Control (Jacob)
  Computer Forensics (me)

- Monday, May 8 + Thursday May 11:
  Review workshop

- Monday May 15:
  Guest lecture (Rune Espensen, IBM)
  Questions
  Wrap-up

Review Workshop

- Pick a slot here:
  https://docs.google.com/spreadsheets/d/1MCExhg4j8lb9gLIg_D6RNeKkgF1QygFEwns1lkXOR7Q/edit#gid=0

- Instructions here:
  https://learnit.itu.dk/course/view.php?id=3016559#section-15

Terms

- security incident
  “an illegal or unauthorized action which might involve a computer system or network”

- computer forensics (more generally, digital forensics science)
  “describes a process with the goal of investigating digital media not only but mainly with regard to criminal events”.

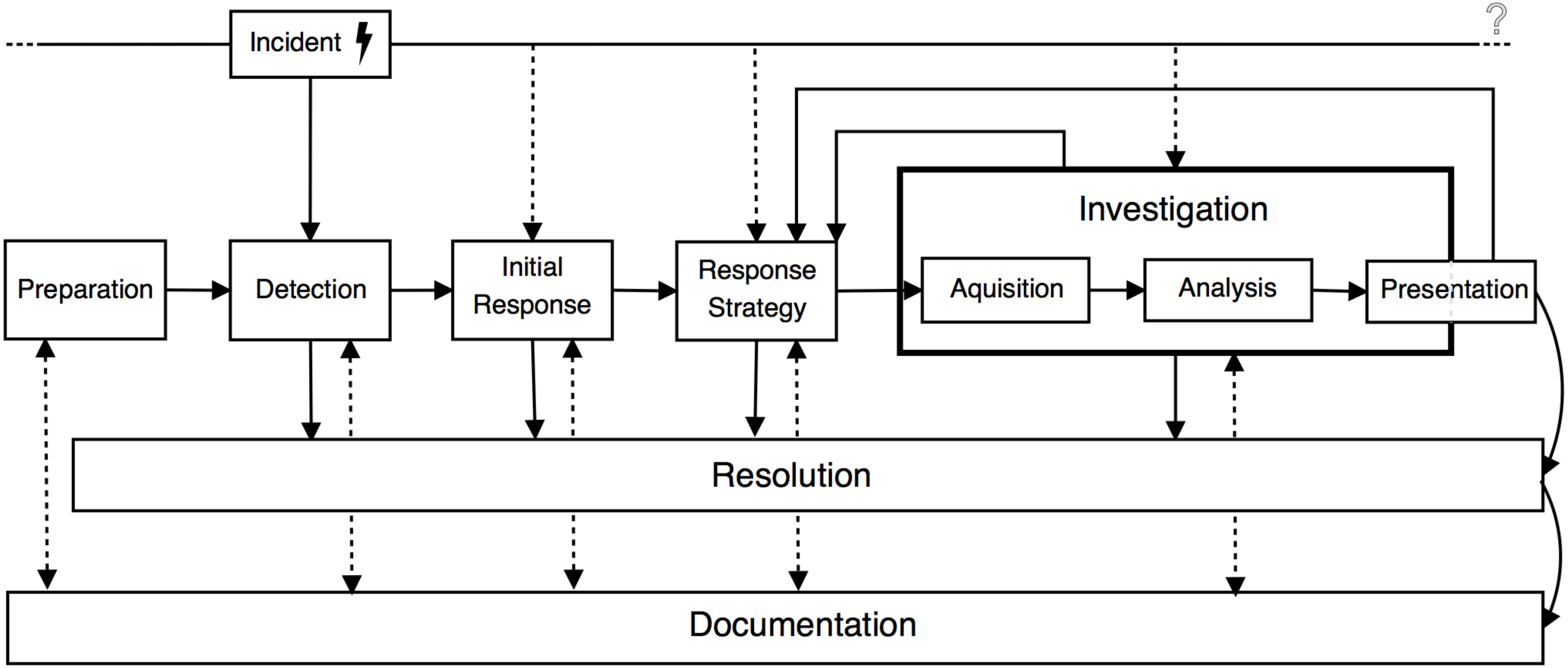
Incidence Response

Preparation

- security incident
  “an illegal or unauthorized action which might involve a computer system or network”

- CSIRT
  Computer Security Incident Response Team

- Also known as CERT
  Computer Emergency Response Team


Incident
?
Investigation
Preparation
Detection
Initial Response
Response Strategy
Aquisition
Analysis
Presentation
Resolution
Documentation

Computer forensics

Computer forensics

- computer forensics (more generally, digital forensics science) *“describes a process with the goal of investigating digital media not only but mainly with regard to criminal events”.*

- Focus:
  forensically sound, correct reconstruction of a security incident

- Goal:
  “the acquired data can possibly be used for law enforcement”

- Artefacts:
  remnants created during or as a consequence of the event to be investigated
  (not “evidence”)

Process

- Acquisition
- Analysis
- Presentation

Acquisition

- Collect data
- Secure the object under investigation
  (Access control)
- Potentially, collect live data (e.g., system memory)
- Forensic duplication
- NB! Follow legal procedure
  (E.g., logging, 4-eyes)

Analysis

- Forensic analysis

- E.g., Application/OS Analysis, File System Analysis, Volume Analysis and Memory Analysis and Storage Media Analysis

- Level-of-abstraction shift

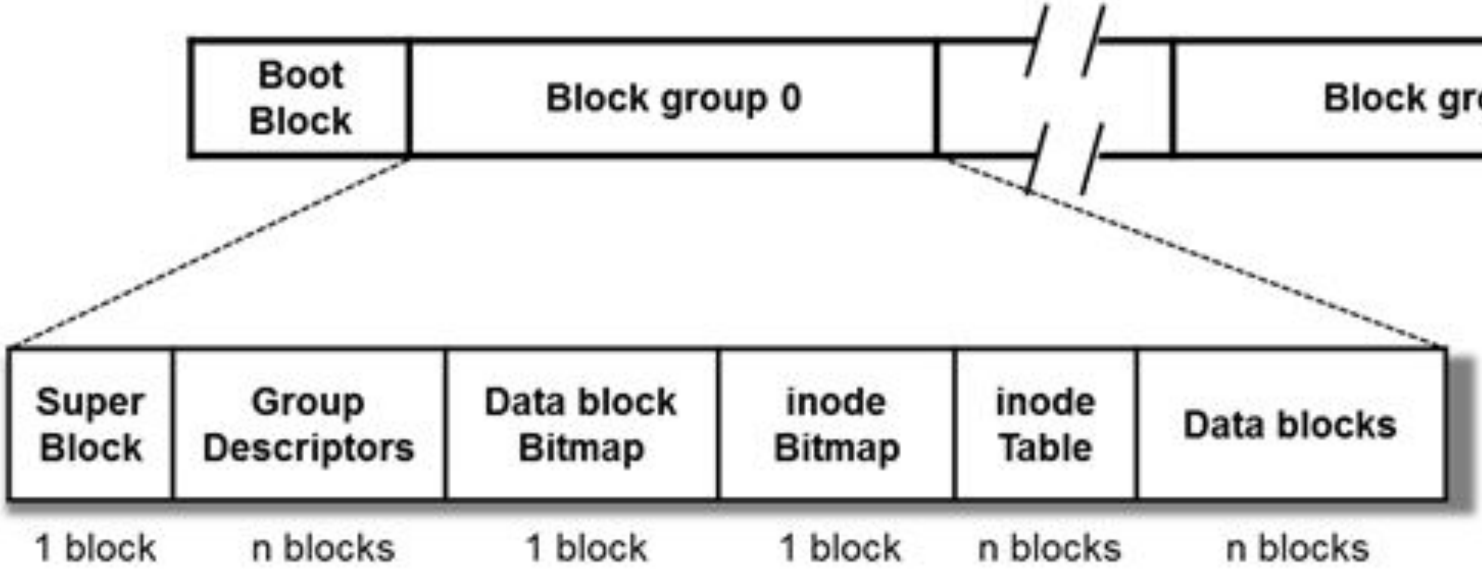
- Note resource/precision tradeoff of analysis

- Note similarities to the situation of the adversary

Presentation

- Report
- Recovered artefacts
- Objective interpretation of artefacts

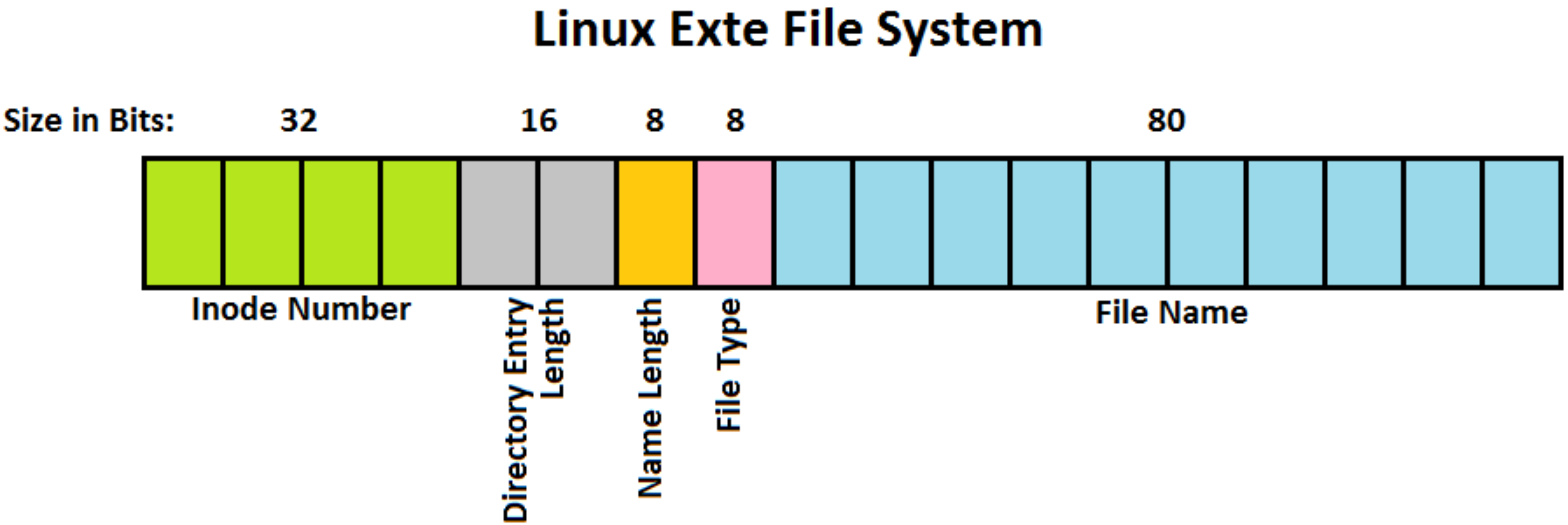
ext3


Boot Block
Block group 0
Block group n
Super Block
Group Descriptors
Data block Bitmap
inode Bitmap
inode Table
Data blocks
1 block
n blocks
1 block
1 block
n blocks
n blocks

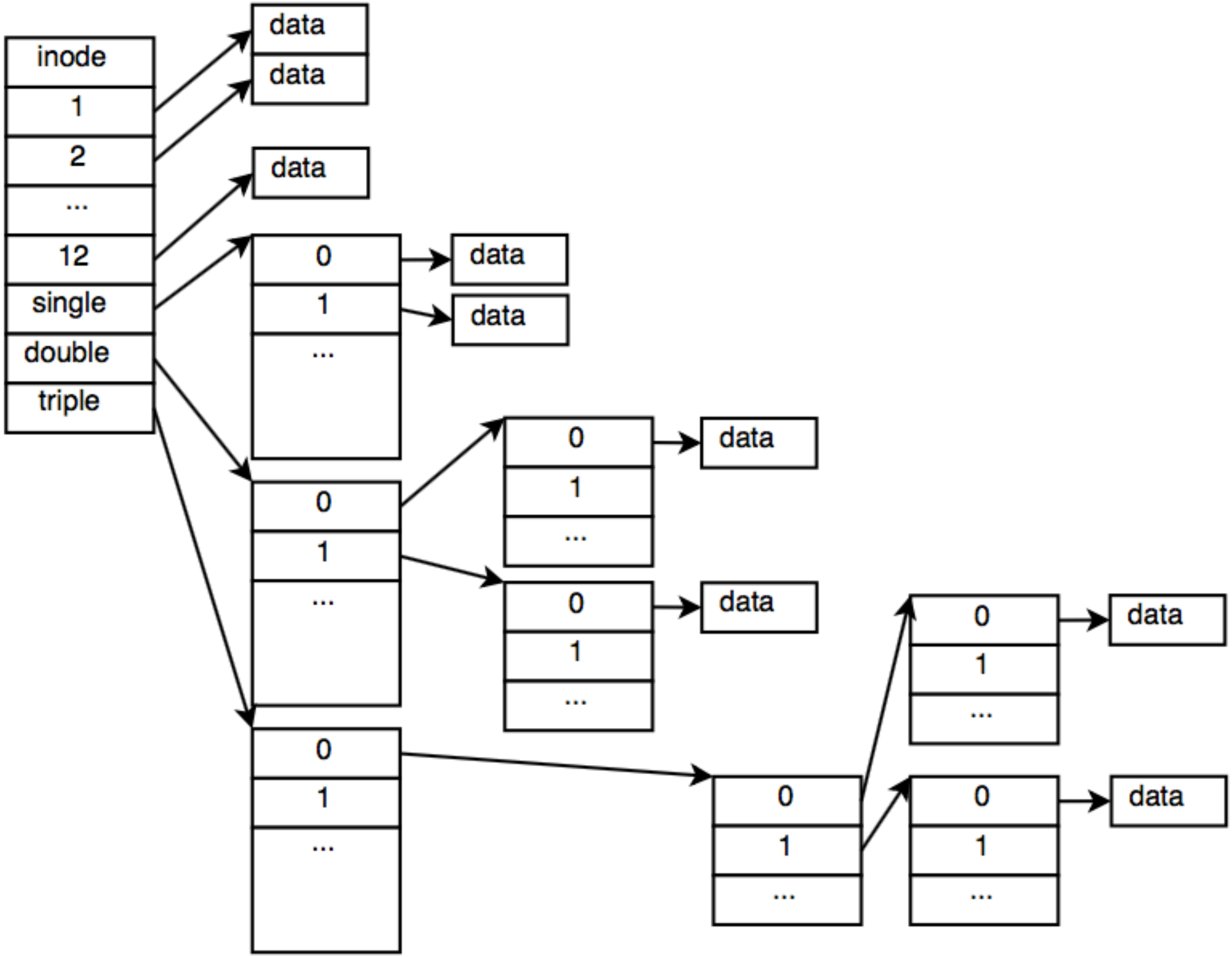
Superblock

- At bytes 1024–2048
- Block and inode allocation information such as
  - Block size
  - Total number of blocks
  - Total number of inodes
- Metadata which indicates the last time the file system was mounted or read
- Enabled FS features
- Backup copies of the superblock in each *block group*. (Usually.)

Directory entry



http://web.cs.ucla.edu/classes/winter16/cs111/scribe/12d/img/Ext3_Dir_Entry.png


inode
1
2
...
12
single
double
triple
data
data
data
0
1
...
data
data
0
1
...
0
1
...
data
0
1
...
data
0
1
...
0
1
...
0
1
...
data
0
1
...
data

Questions?