Use of Machine Learning Classification Techniques to Detect Atypical Behavior in Medical Applications

Terrence M. Ziemniak, CISSP
tmziemniak@yahoo.com

Finding the Good Stuff

- Information Security
- Physical Security
  - Loss prevention
  - Teenagers don't act like that
- Automate this analysis?

Health Care's Problem

- Compliance
- Detect Inappropriate behavior
  - Snooping
  - Shared Credentials
  - Incorrect/Inappropriate access rights
  - Data Loss

Complexities Impede Security

- Open by design
- Outsourcing
- Nurses
- Hospital Services
- Practice Management
- Residents and Students
- EHR

Current Solutions

- High/Low Activity
- Geography
- Spot Check
- VIP
- Matching last name
- Specific event (break the glass)
- Allegation

Proposed Solution

- No attempt to define bad event
- Compare activity of peers
- Pharmacists don't act like that

Machine Learning

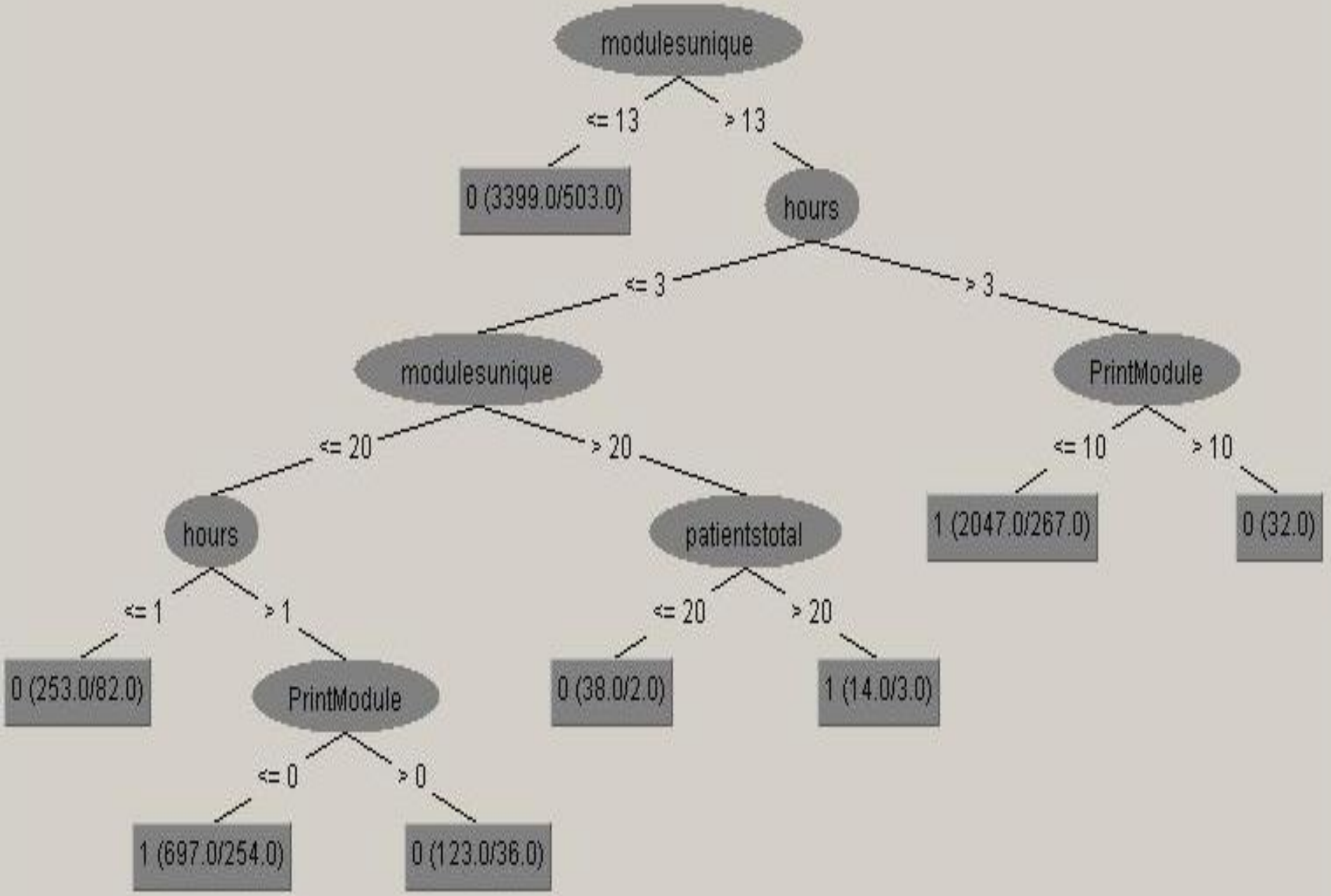
- Speech Recognition
- Game Play
- Computer Vision
- Spam
- Fraud Detection
- Computer Recommendations

Machine Learning

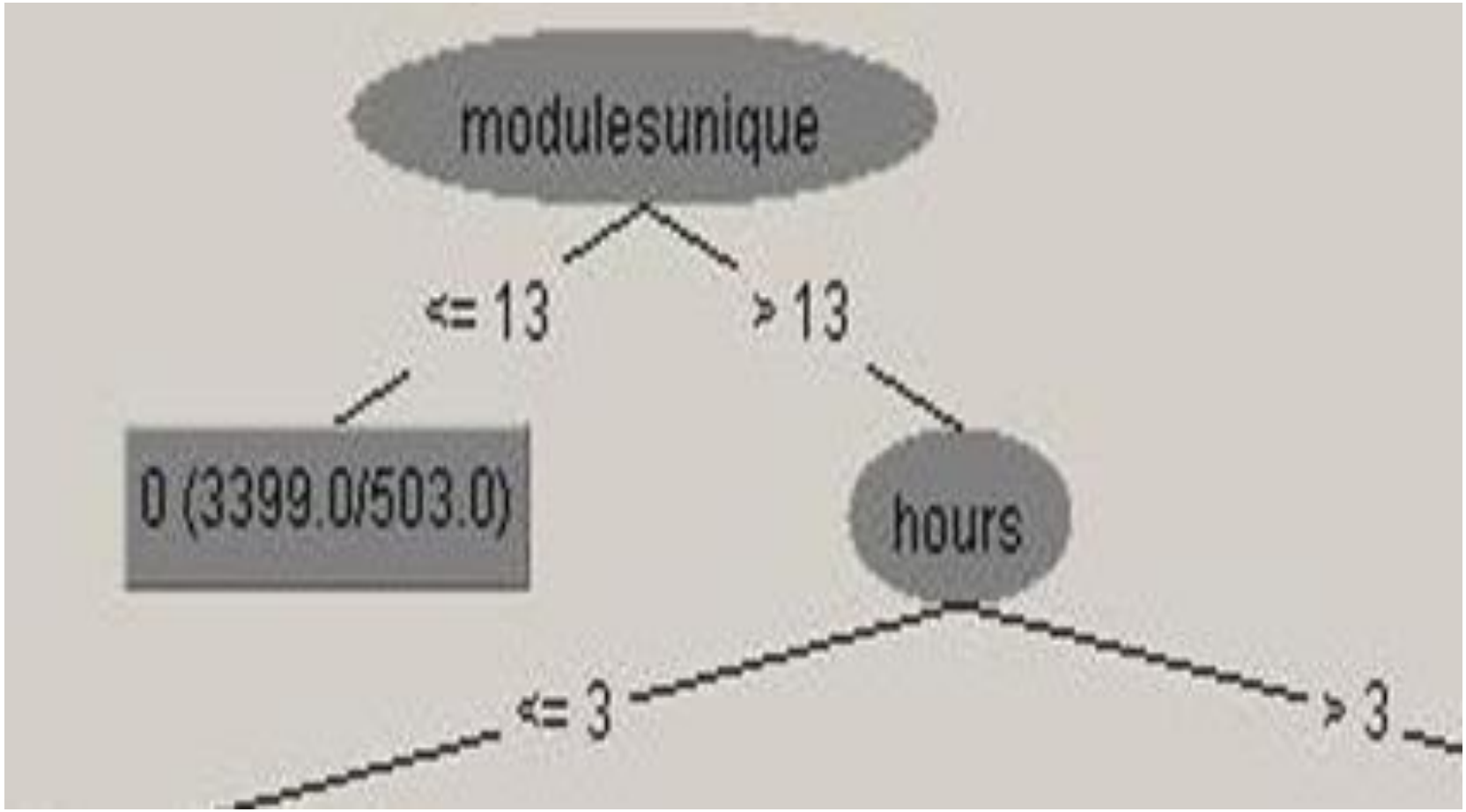
- The core objective of a Machine Learning algorithm is to generalize from its experience, i.e. to provide a model that captures the overall characteristics and interactions of the dataset it has been trained on (Alpaydin, 2004)
- How apply to our problem?

Dataset

- Health Care Application
- 8 Hospitals
- 15,000 Employees
- 2 Month period
- Events into Instances
- 11 Attributes


modulesunique
<= 13
> 13
0 (3399.0/503.0)
hours
<= 3
> 3
modulesunique
PrintModule
<= 20
> 20
<= 10
> 10
hours
patientstotal
1 (2047.0/267.0)
0 (32.0)
<= 1
> 1
<= 20
> 20
0 (253.0/82.0)
PrintModule
0 (38.0/2.0)
1 (14.0/3.0)
<= 0
> 0
1 (697.0/254.0)
0 (123.0/36.0)

Classification Tree - Detail

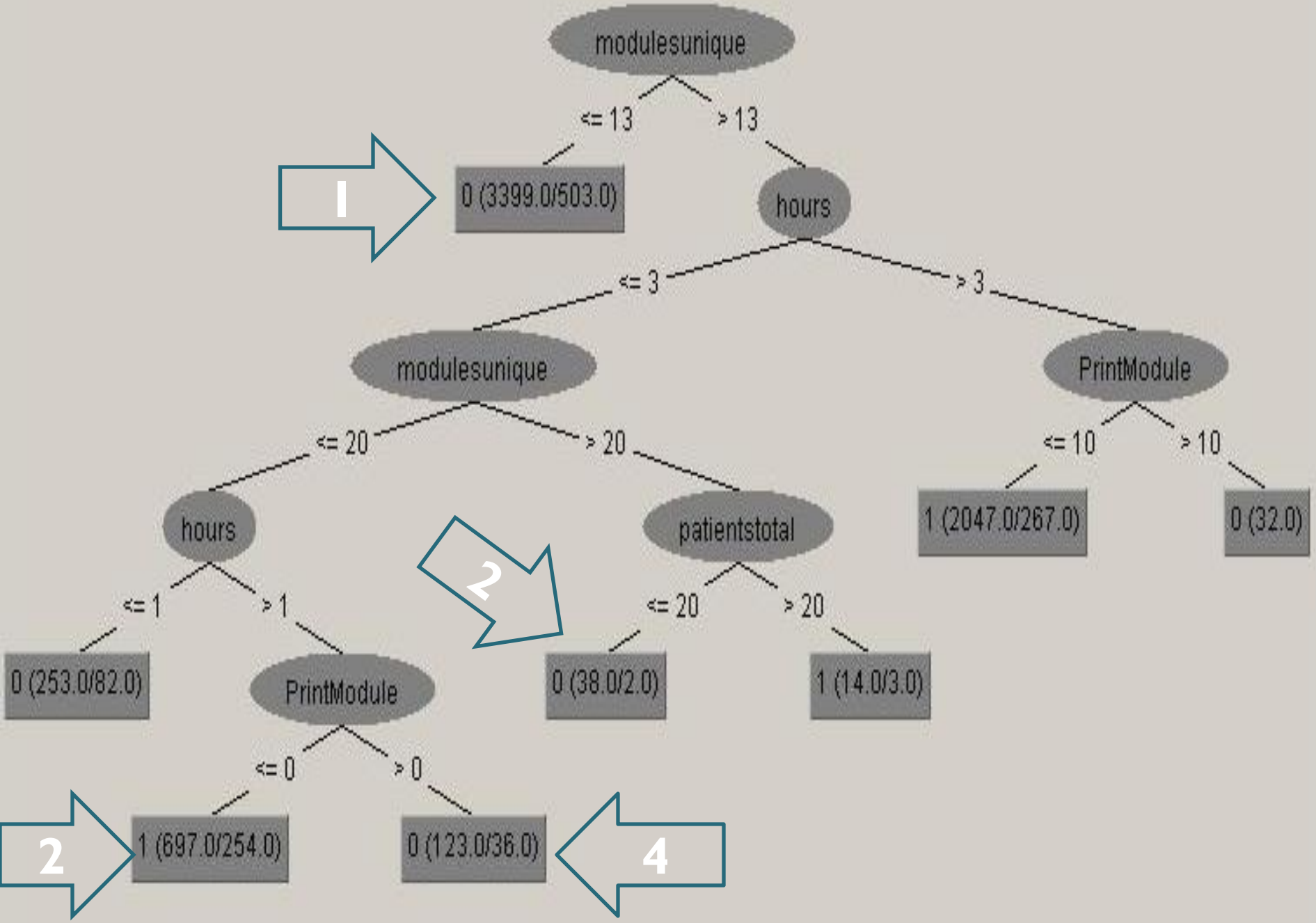


System

- ML detect unusual activity
  - Classify
- Unusual trimmed Suspicious
  - Exercise

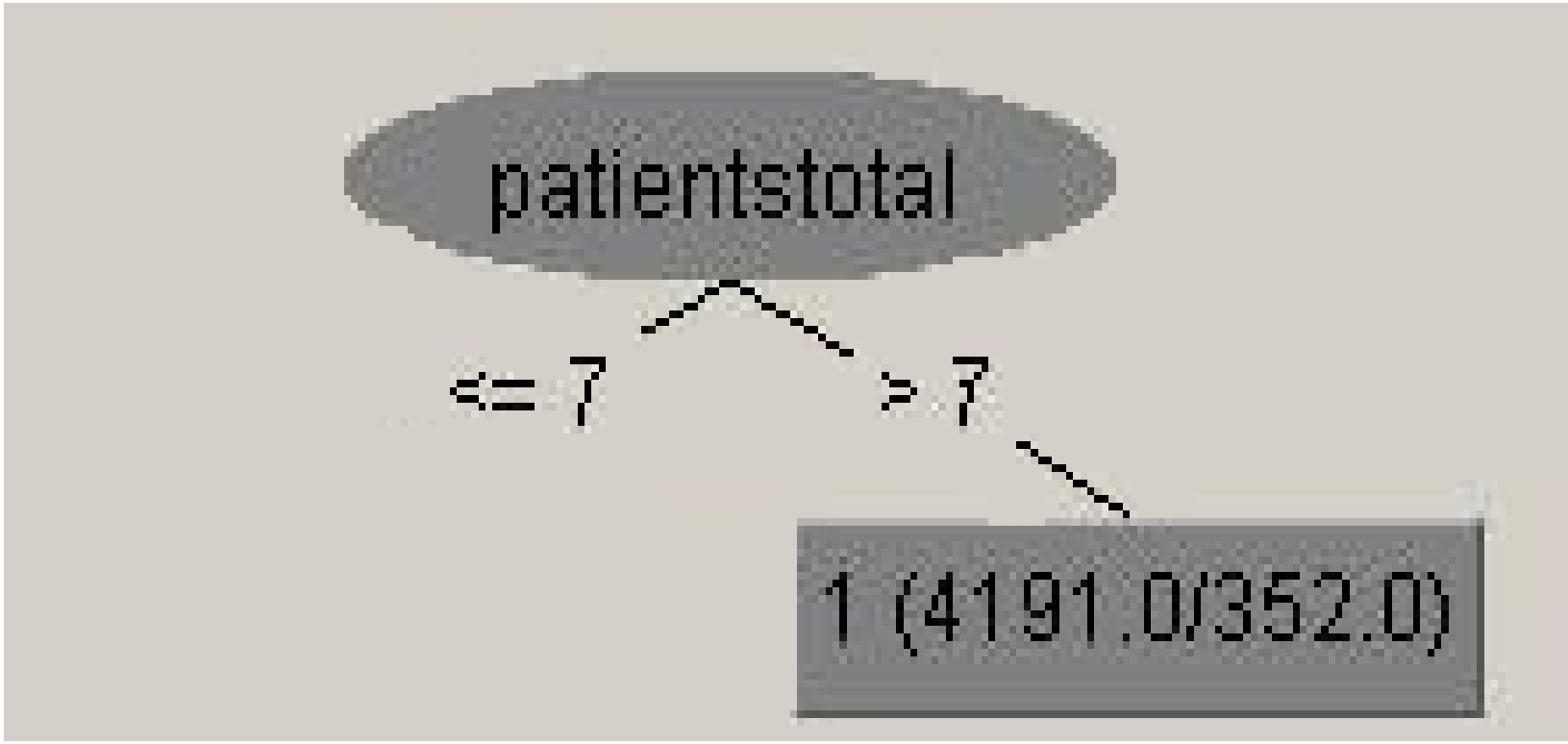
Unusual to Suspicious

- Ad-hoc
  - Intuition
- Depth
  - Short
  - Long
- Outlying


modulesunique
<= 13
> 13
0 (3399.0/503.0)
hours
<= 3
> 3
modulesunique
PrintModule
<= 20
> 20
<= 10
> 10
hours
patientstotal
1 (2047.0/267.0)
0 (32.0)
<= 1
> 1
<= 20
> 20
0 (253.0/82.0)
PrintModule
0 (38.0/2.0)
1 (14.0/3.0)
<= 0
> 0
1 (697.0/254.0)
0 (123.0/36.0)
1
2
2
4

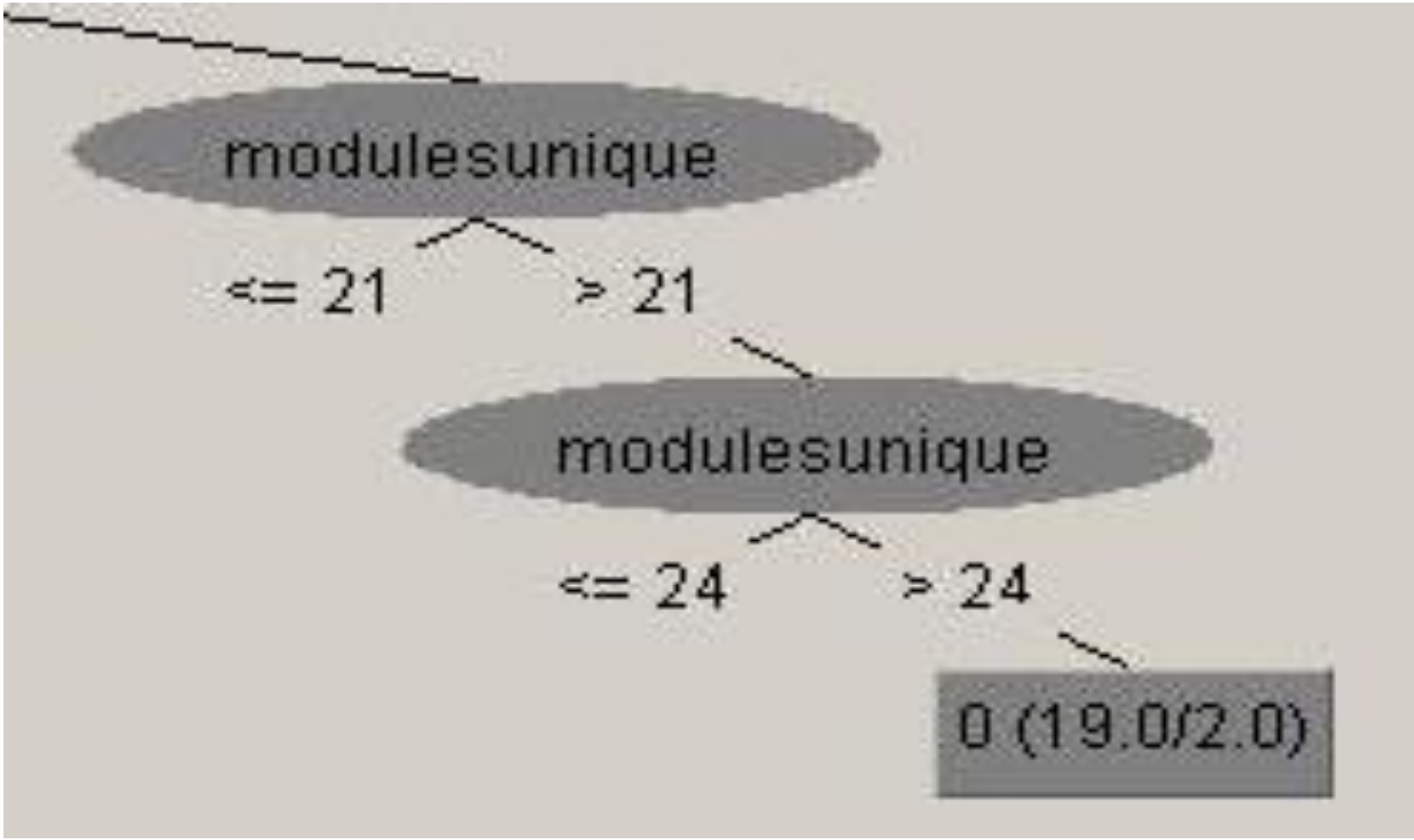
Exercise Details 1

- Physician and Residents



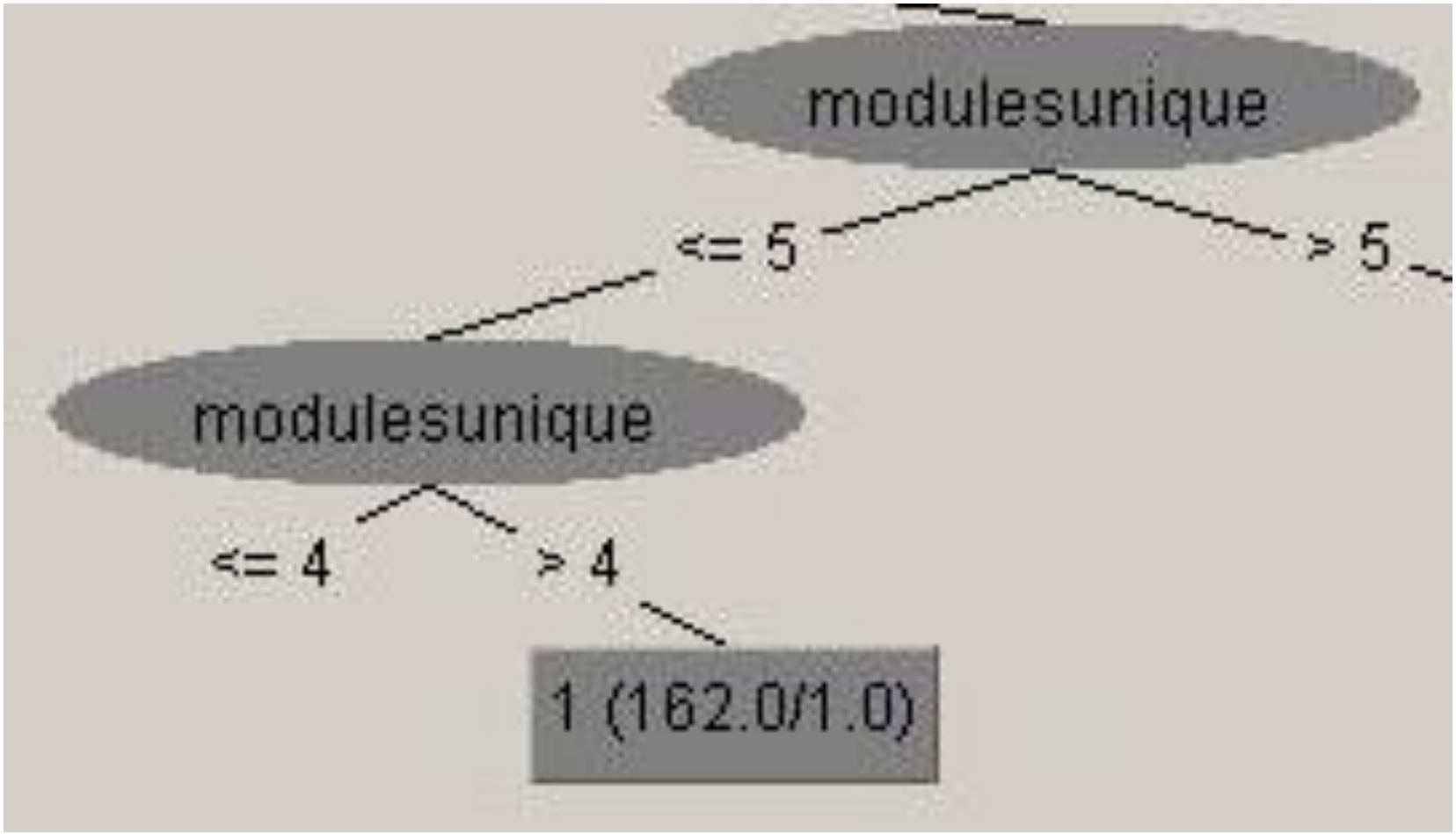
Exercise Details 2

- Physician and Residents



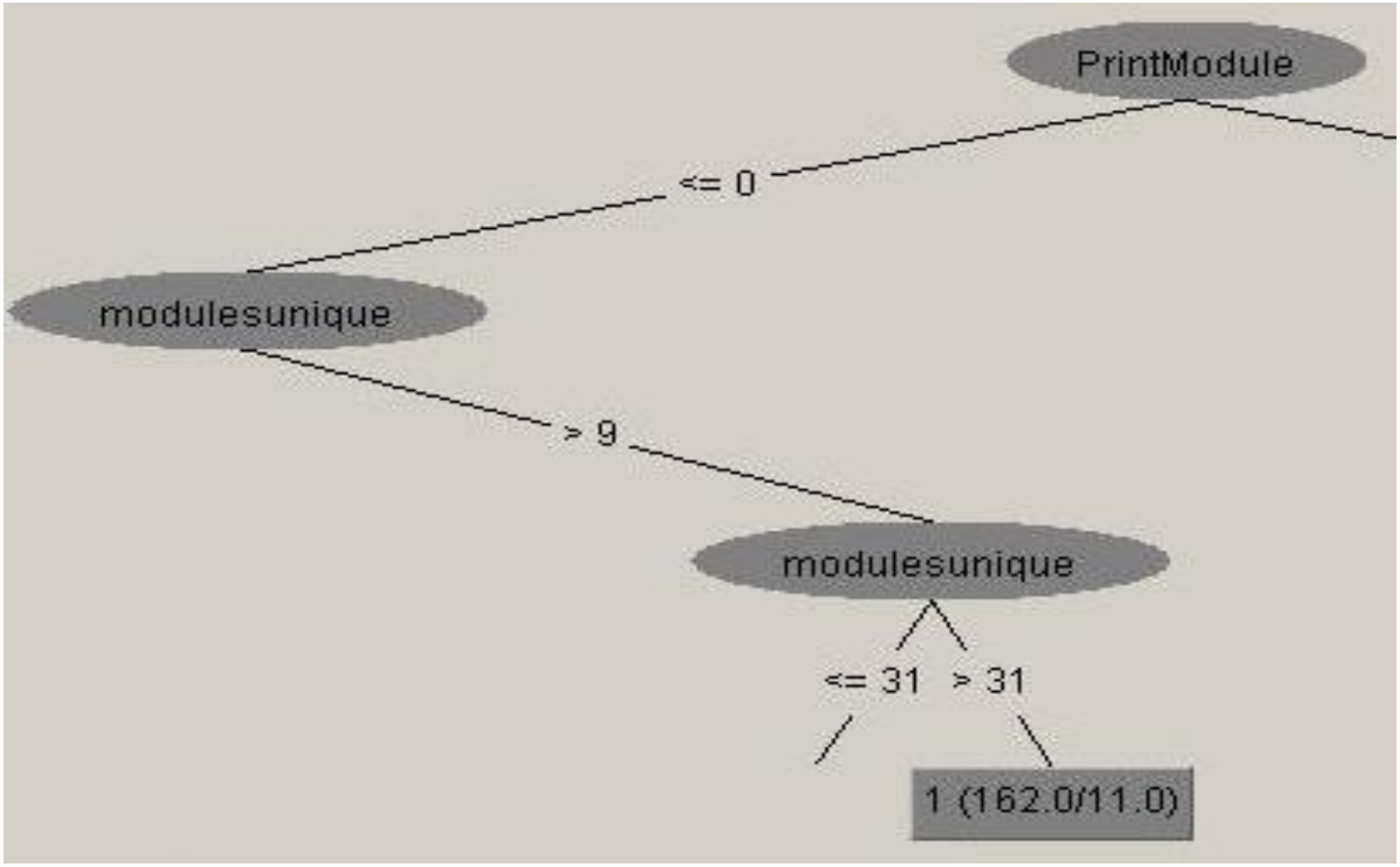
Exercise Details 3

- Physician and Residents



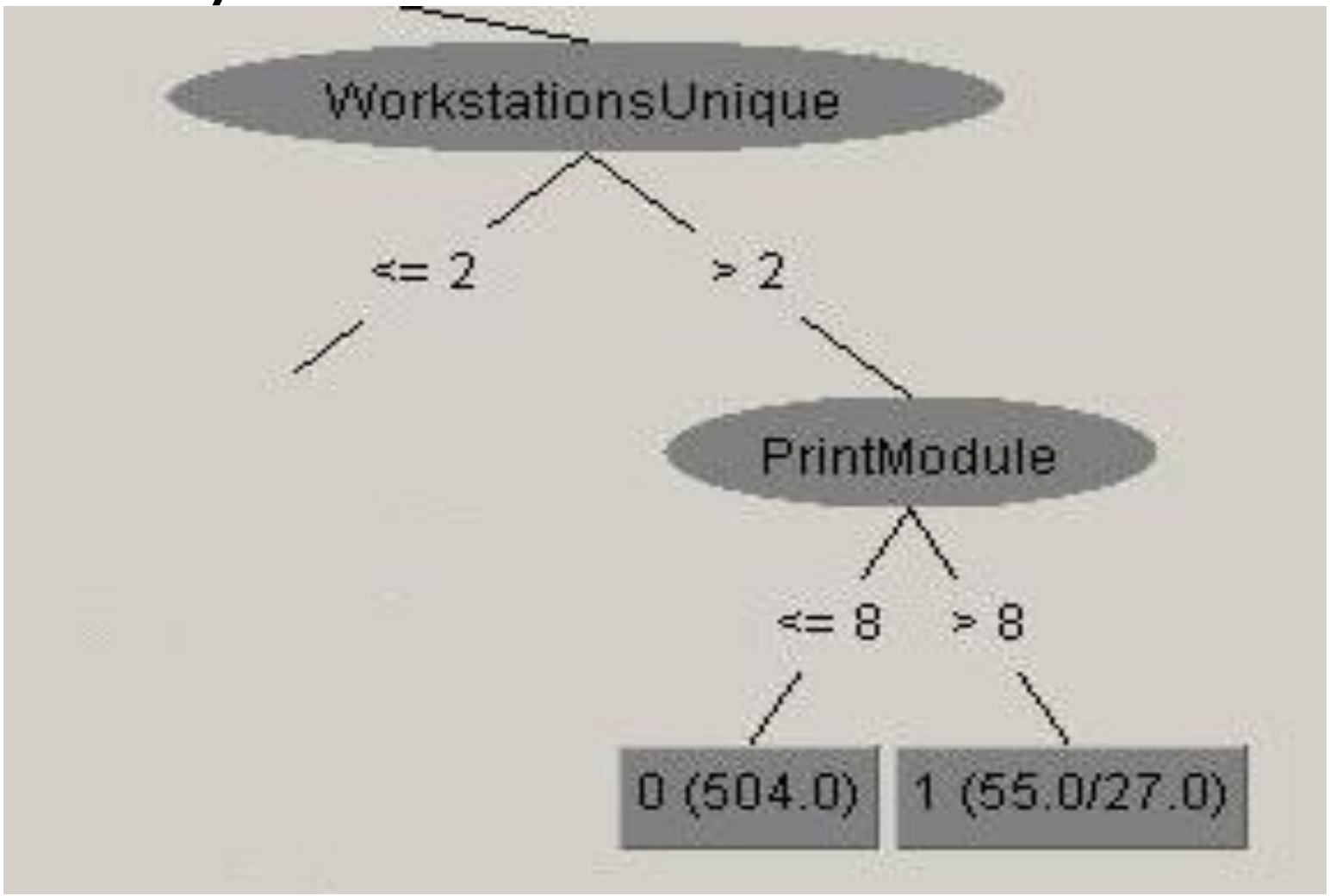
Exercise Details 4

- Physician Assistants



Exercise Details 5

- Physician Assistants



Findings

- Unusual billing
- System testing
- Training
- Multiple Roles
- Shared credentials

Going Forward

- Improvements
  - Tuning
  - Combined exercise methods
  - Accurate user information
- Other Uses

Summary

- 16 Screens
- Process to detect suspicious activity
- Significant reduction in effort
- Compliance