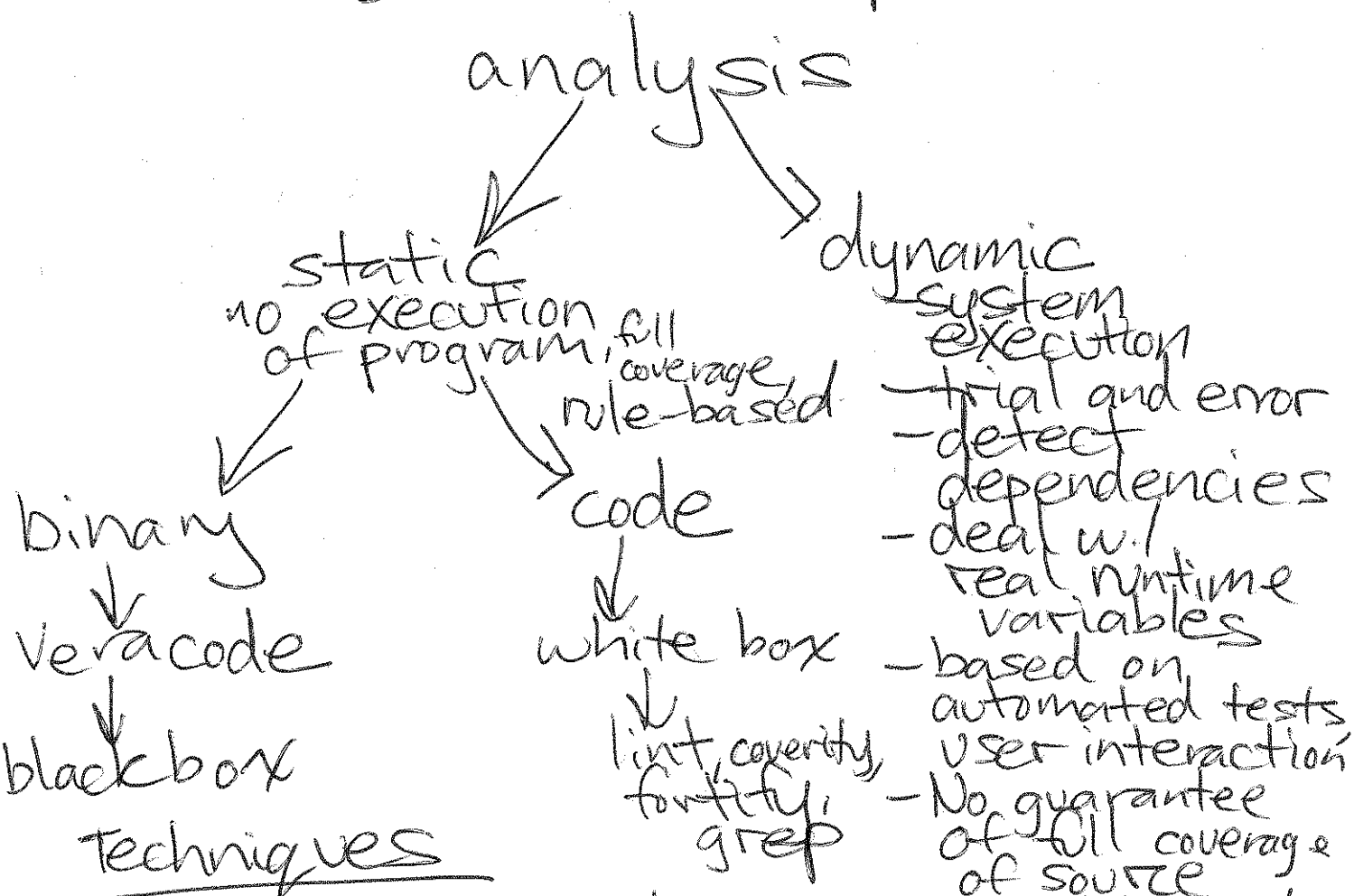
COMP 116: Analysis

⓪ Assignment 5

① Assignment 4 postmortum



Techniques

① Data flow analysis
- Collect runtime info about data while in a static state
  - ↳ Basic block (the code)
  - ↳ Control flow
  - ↳ Control path

② Control graph
- ↳ Node ⇒ block
- ↳ Edges ⇒ jumps/paths

③ Taint analysis (also DFA)
Identify variables that have been tainted; uses vuln fns known as sink

④ Lexical analysis
Code ⇒ tokens

```
gets(&buf);
/* ... gets */
```

Strengths, weaknesses
- (+) find vulns w/ high confidence
- (-) false positives, false negatives
- (-) can't find config issues
- (-) can you prove they are vulns?

More on tainting (Perl/Ruby)

- Anything derived from tainted data is tainted

```
i = getinput()
two = 2
if (i % 2 == 0) {
    j = i + two
    l = j; //#wtf
} else {
    k = two * two;
    l = k;
}
jump l; //sink
```