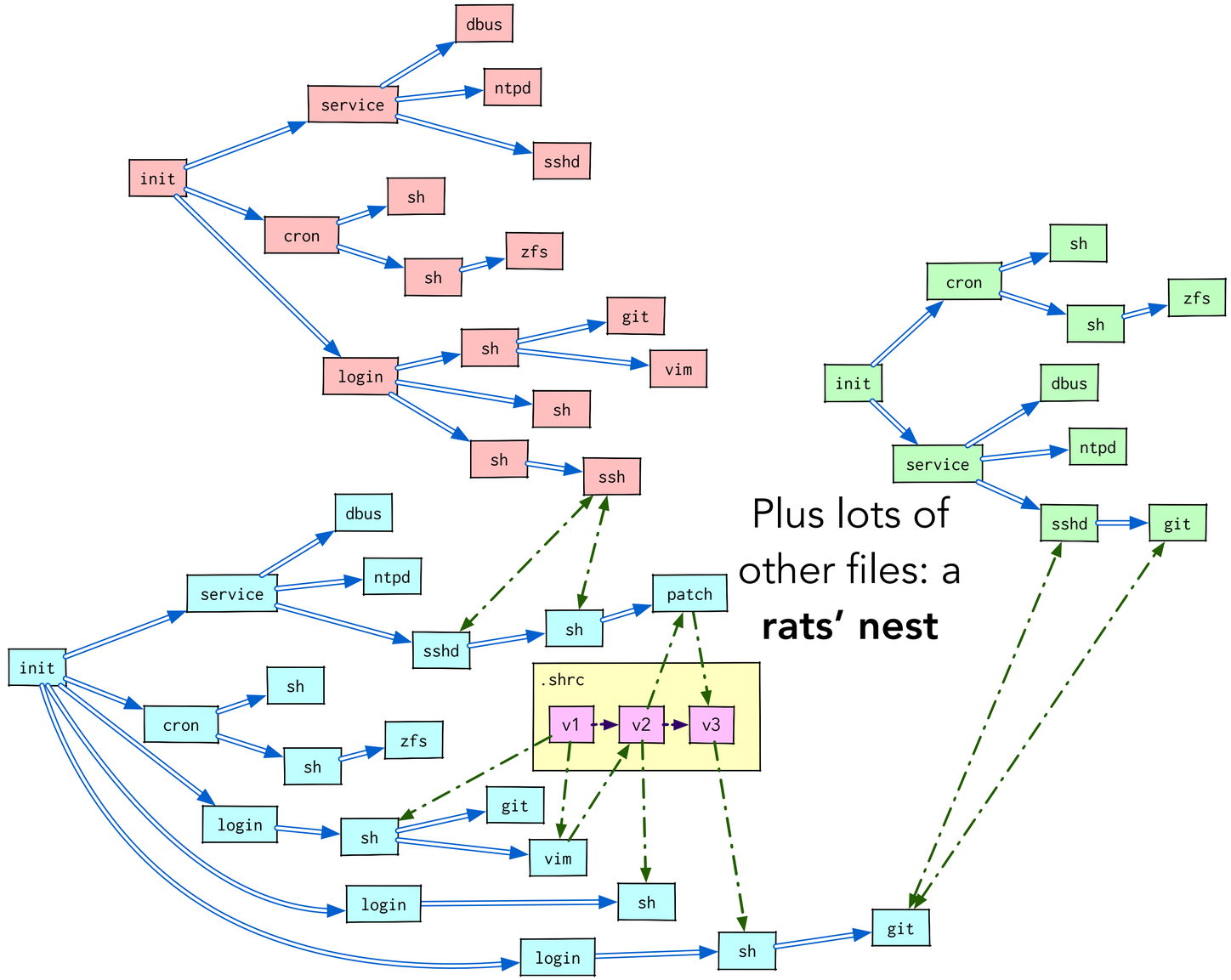
OPUS

Big picture

Worksheets



Plus lots of other files: a **rats' nest**

Just for reference? Something we come back to after our worksheet-based investigations?

runs

data flow

causal relation

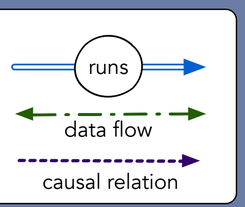
OPUS

Worksheet 1 | New…

Big picture

Worksheets

The analyst's workflow begins with an empty worksheet for exploring hypotheses about host behaviours

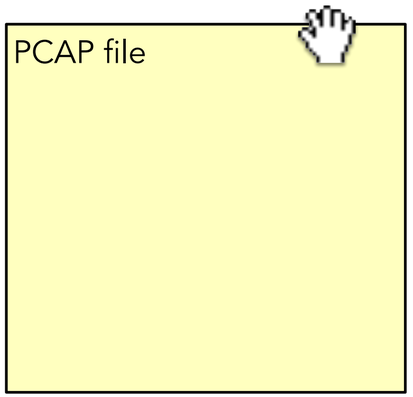


OPUS

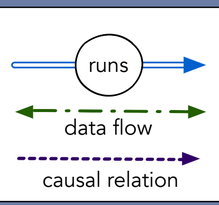
Worksheet 1 | New…

Big picture

Worksheets



An investigation/exploration needs a starting point. In this case, Bro identifies a suspicious connection; the analyst drags a PCAP file into the worksheet. OPUS uses this to find the 4-tuple of the relevant connection in the causality graph.

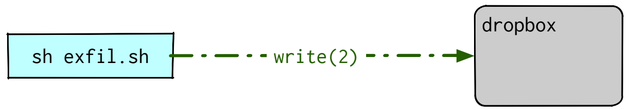


OPUS

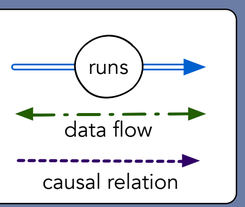
Worksheet 1 | New…

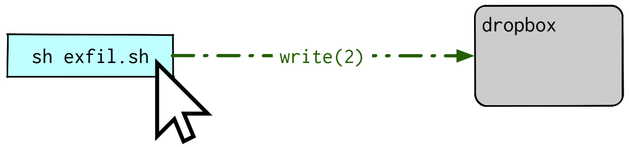
Big picture

Worksheets

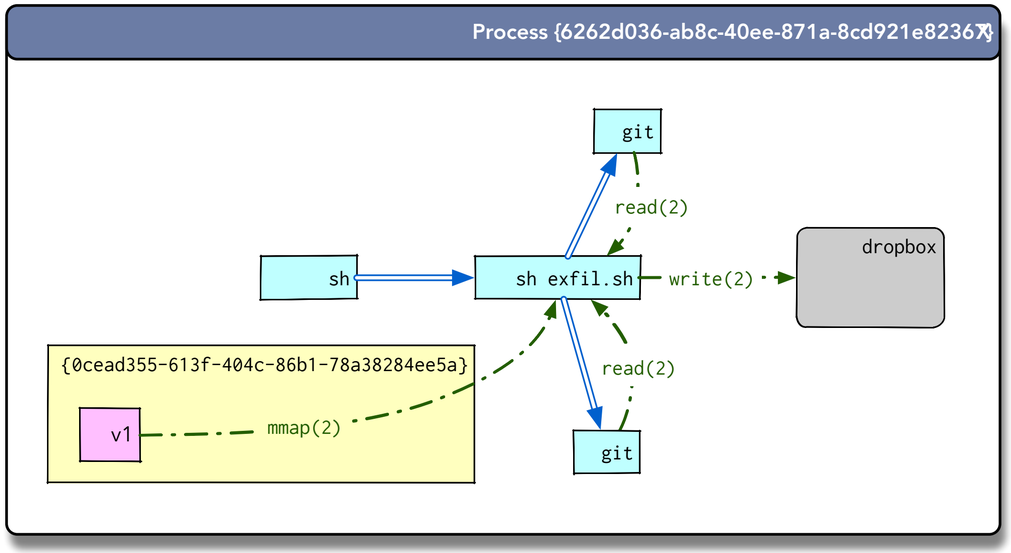


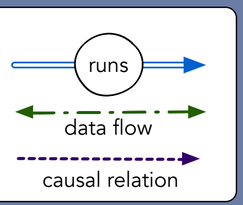
OPUS displays the connection identified by Bro in the worksheet.





The analyst clicks on the process that sent the suspicious data, opening a window with that process' immediate control- and data-flow relationships.



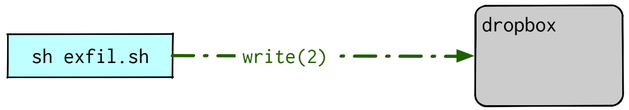


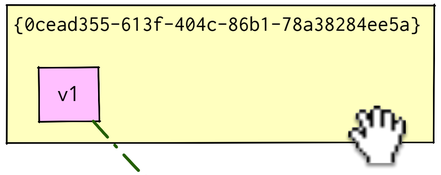
OPUS

Worksheet 1 | New…

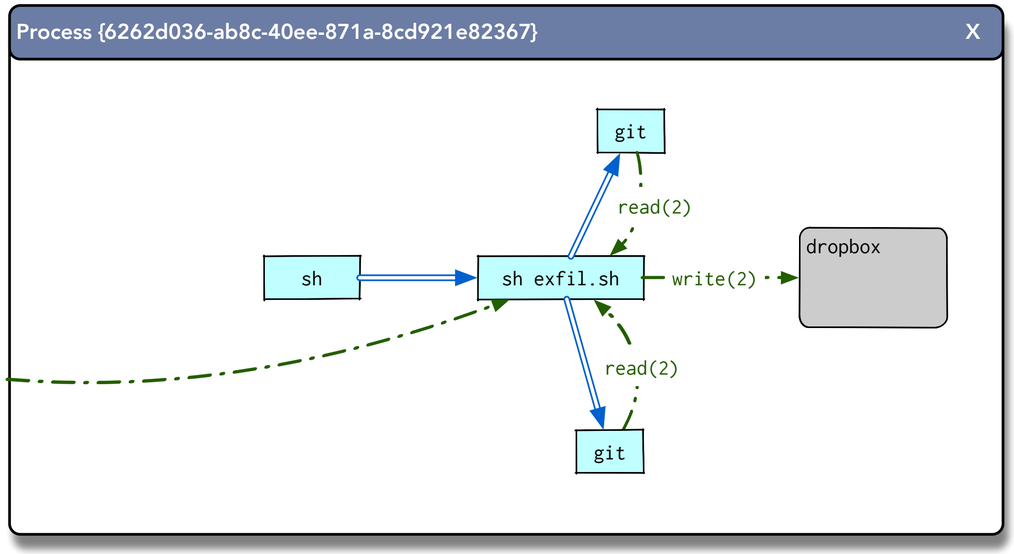
Big picture

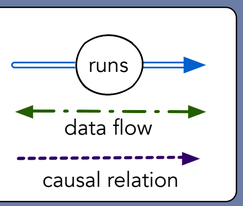
Worksheets





The analyst drags one of the immediately-connected nodes into the worksheet to incorporate it in the investigation and test the hypothesis that it is involved in a larger attack.





06 Drag additional node into worksheet

Fri Jun 16 22:22:51 NDT 2017

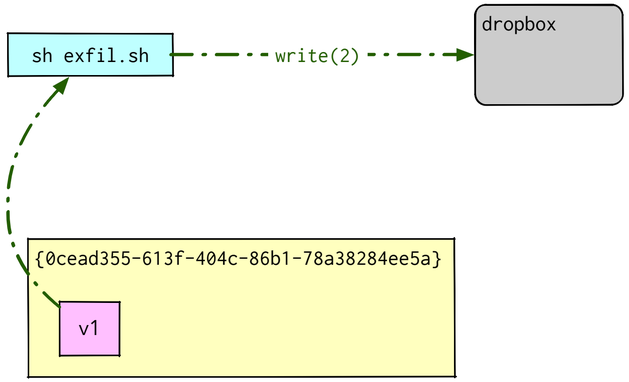
mocks.graffle

OPUS

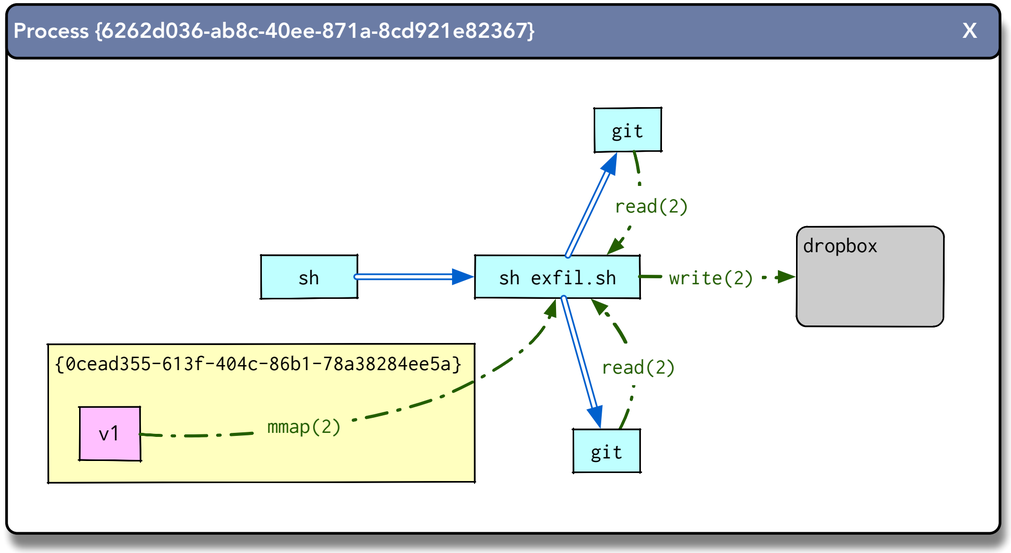
Worksheet 1 | New…

Big picture

Worksheets



After dragging a new node to the worksheet, all of its connections to existing workspace nodes are added.



runs

data flow

causal relation

07 Links of new node

Fri Jun 16 22:22:51 NDT 2017

mocks.graffle

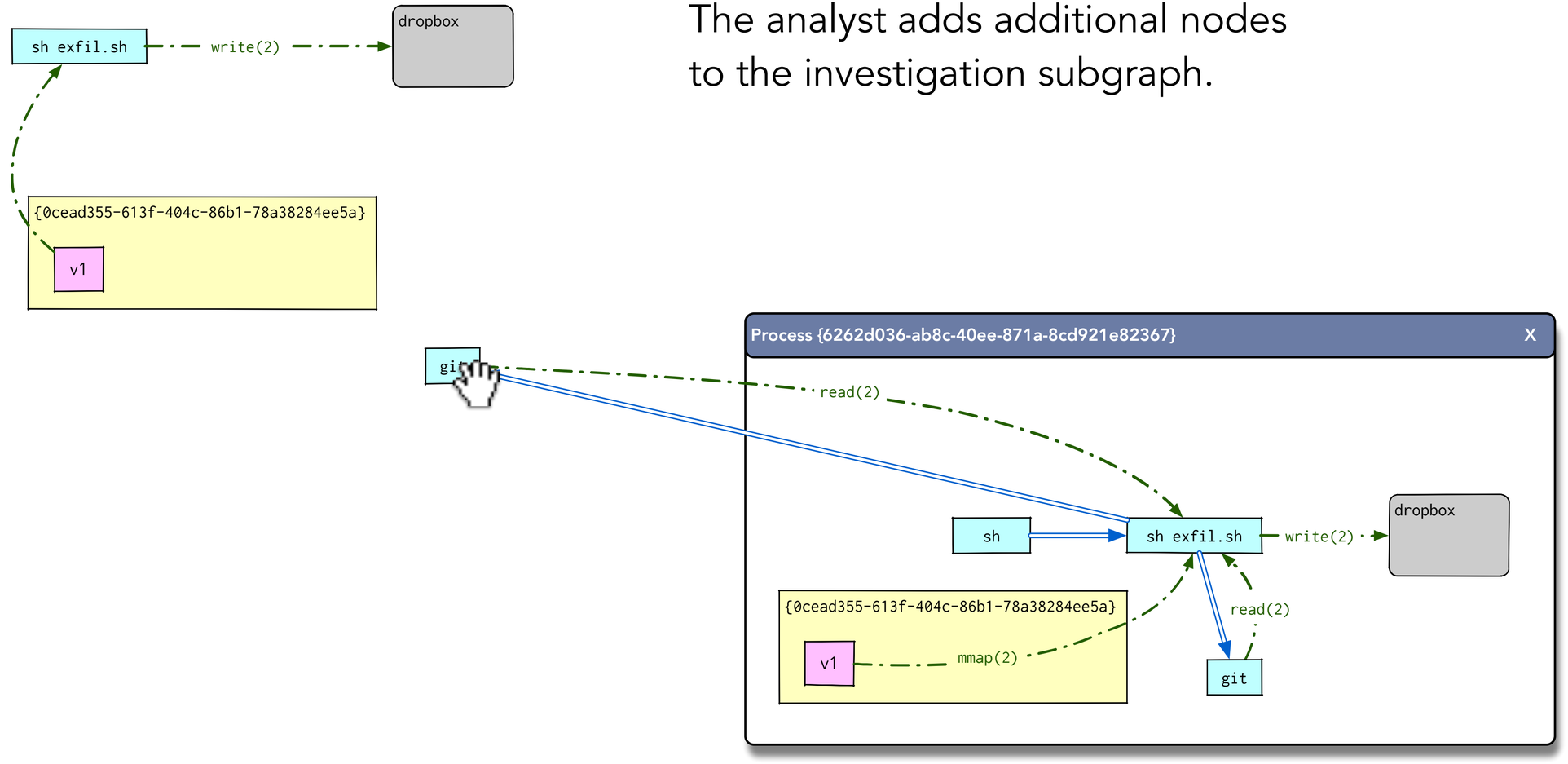
OPUS

Worksheet 1 | New…

Big picture

Worksheets

The analyst adds additional nodes to the investigation subgraph.



runs

data flow

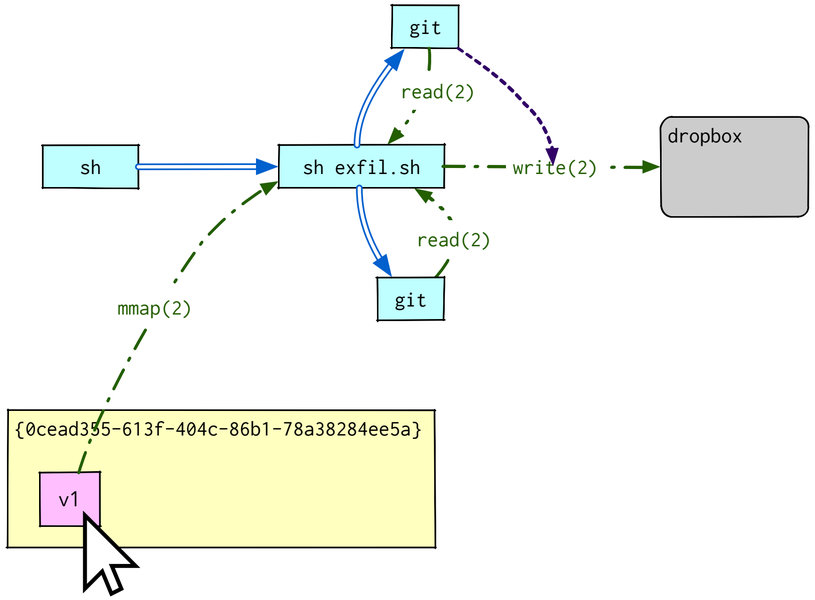
causal relation

OPUS

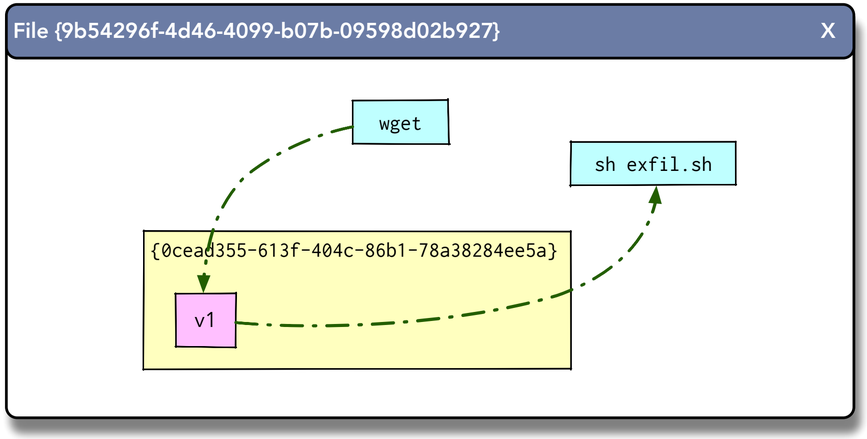
Worksheet 1 | New…

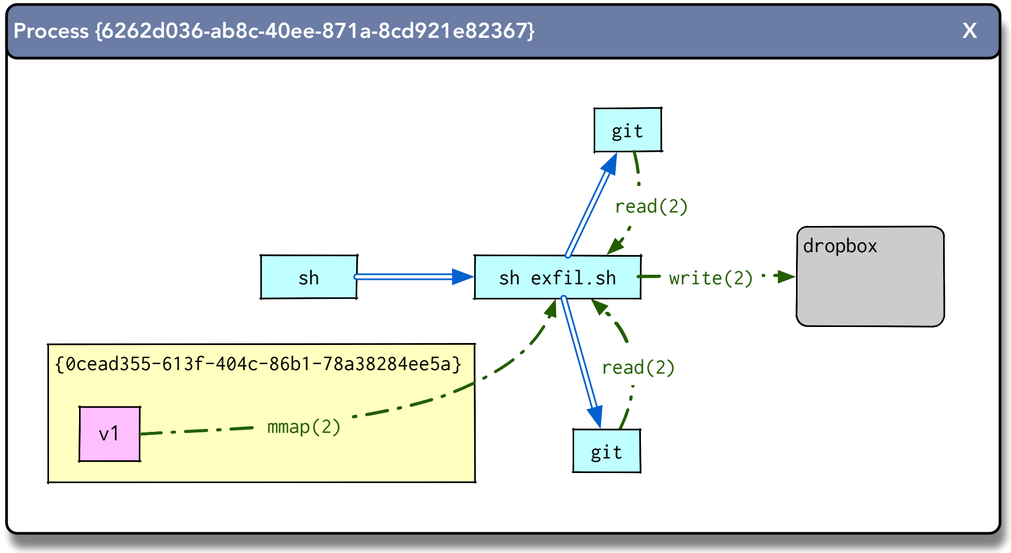
Big picture

Worksheets



The analyst expands the investigation by iteratively exploring more nodes and their connections.





runs

data flow

causal relation

09 A more interesting subgraph

Fri Jun 16 22:22:51 NDT 2017

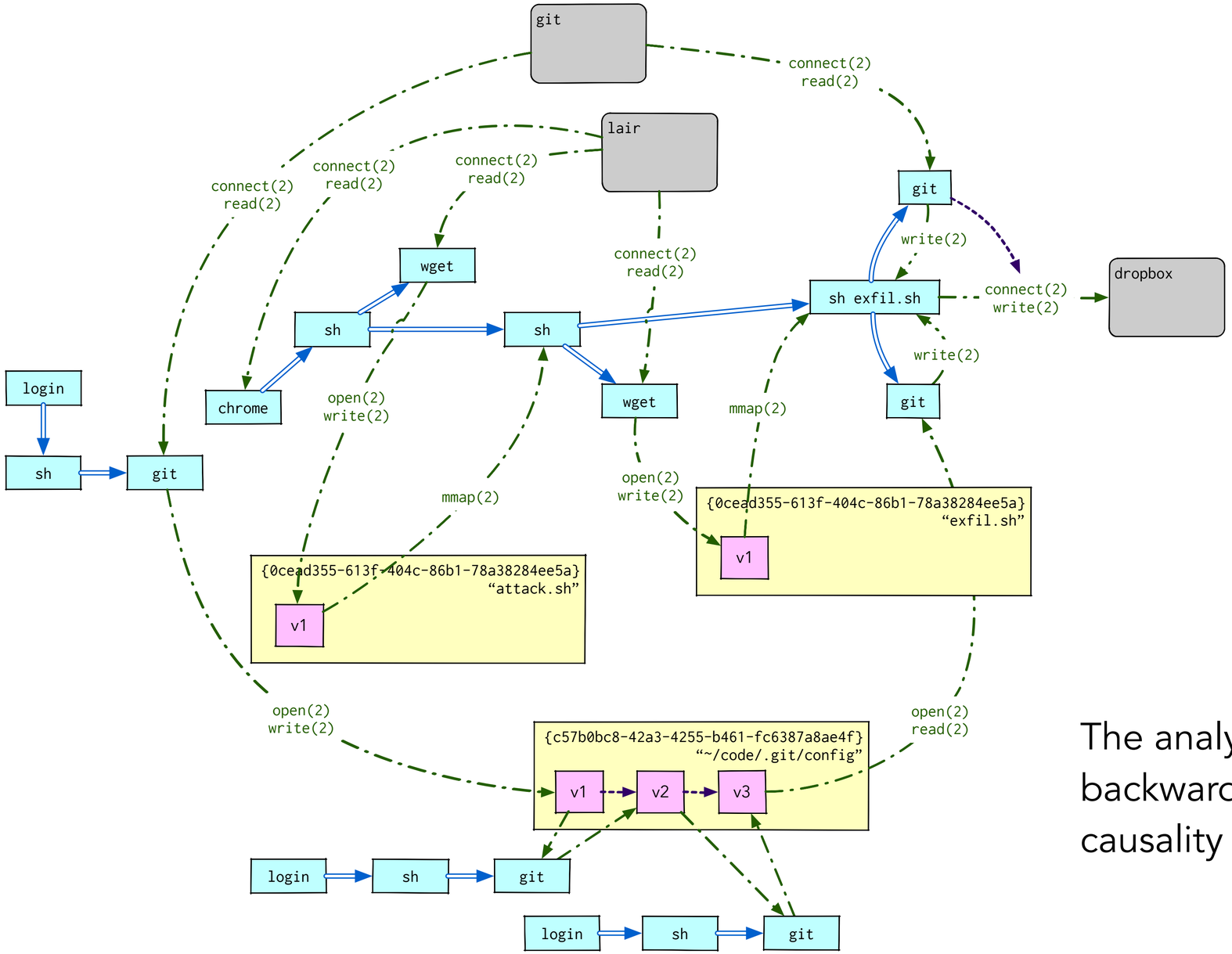
mocks.graffle

OPUS

Worksheet 1 | New…

Big picture

Worksheets



The analyst continues to work backwards until root causes of causality are identified.

runs

data flow

causal relation

10 Root causes

Fri Jun 16 22:22:51 NDT 2017

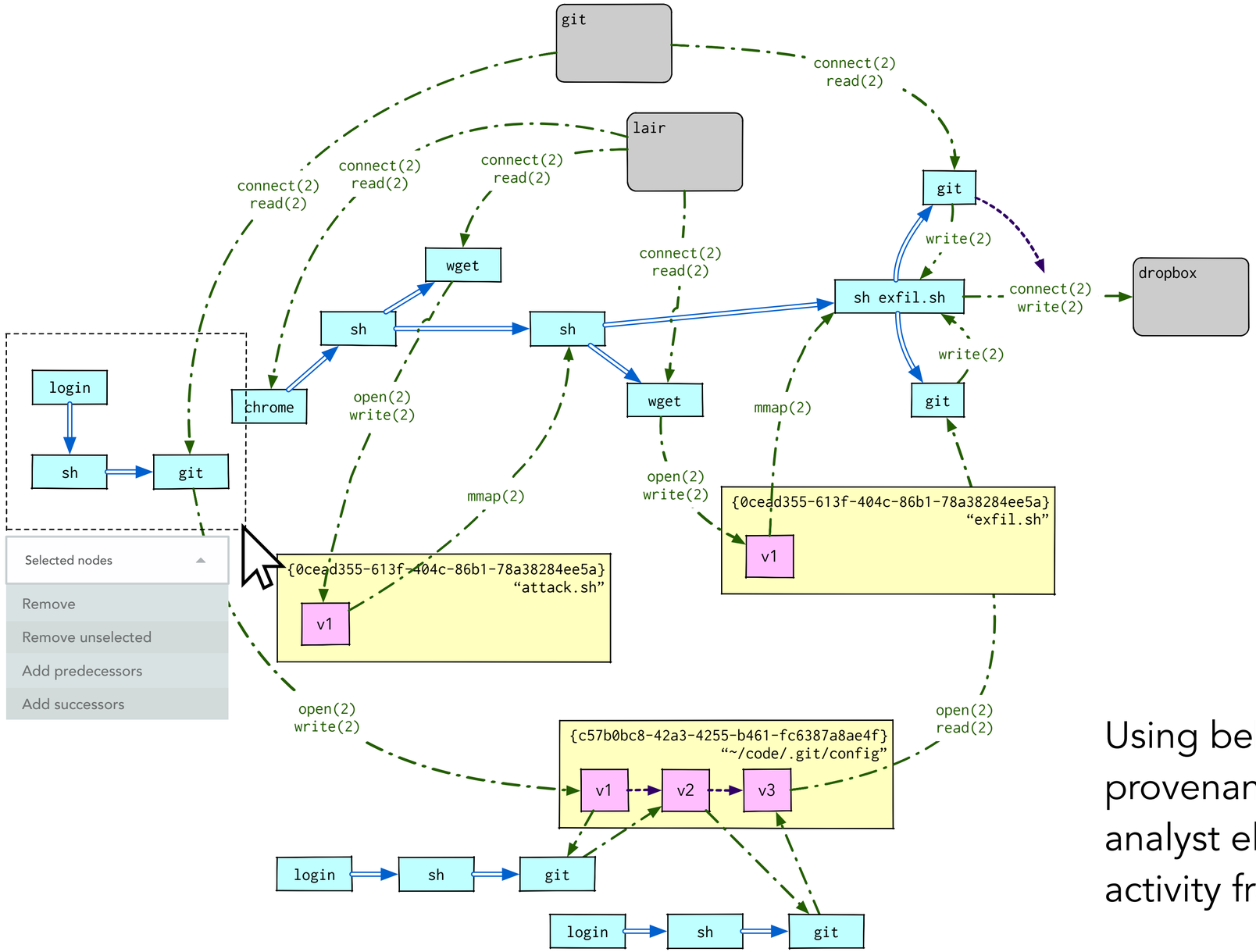
mocks.graffle

OPUS

Worksheet 1 | New…

Big picture

Worksheets



Using behavioural patterns, code provenance and experience, the analyst eliminates legitimate activity from the investigation.

runs

data flow

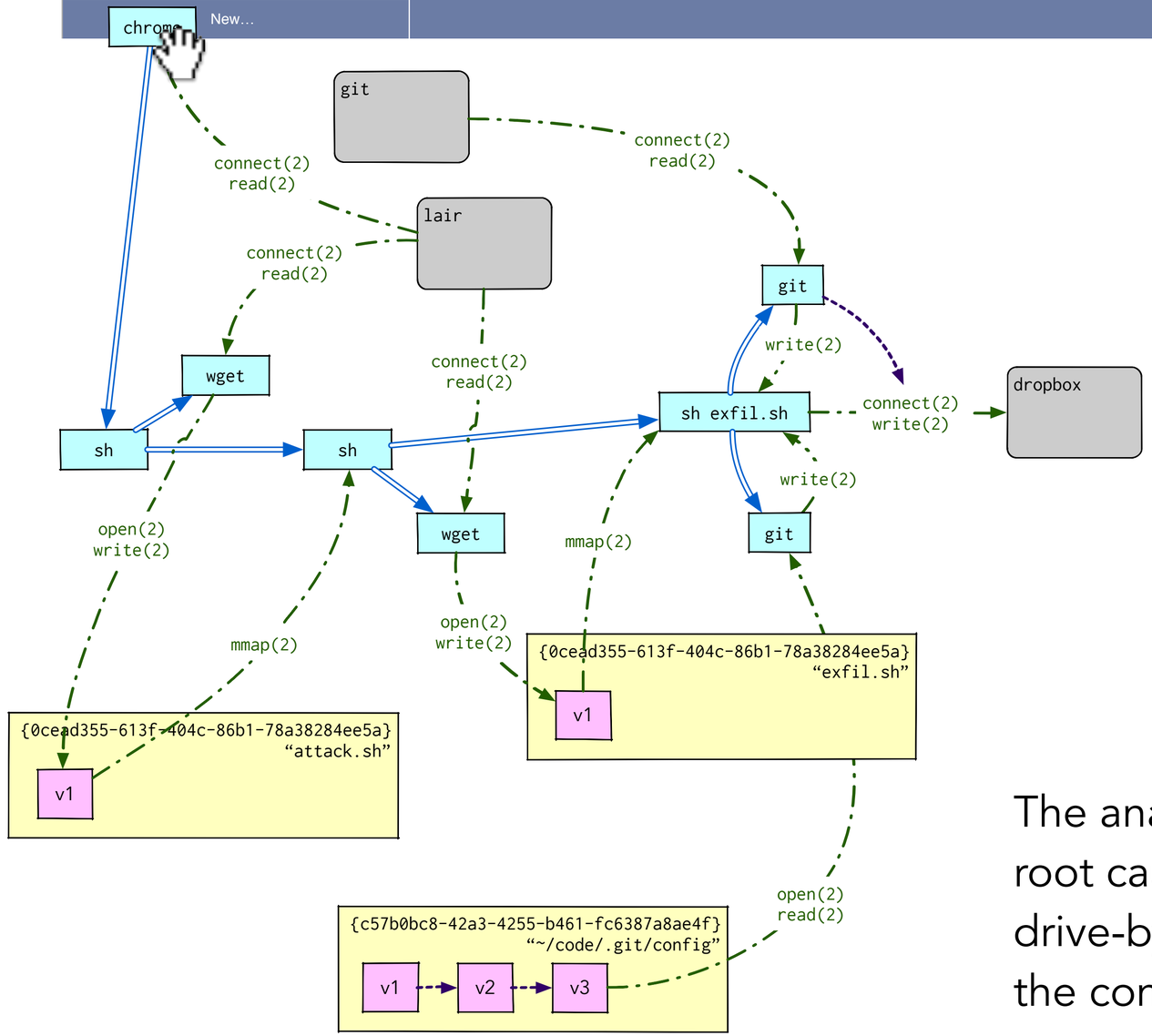
causal relation

OPUS

Worksheet 1 | New…

Big picture

Worksheets



runs

data flow

causal relation

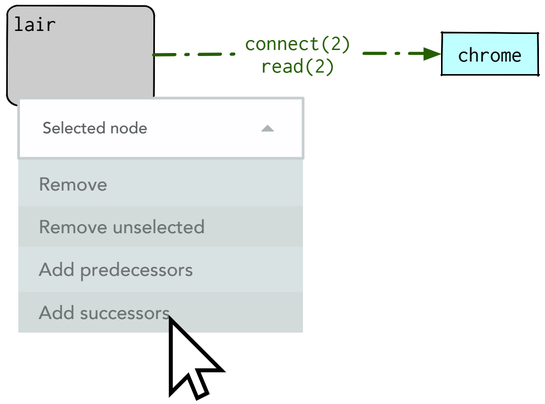
The analyst has identified the root cause of the attack: a drive-by download. They drag the connection in question to a new workspace to perform a damage assessment.

OPUS

Worksheet 1 | **Worksheet 2** | New…

Big picture

Worksheets



The analyst directs OPUS to add all causal successors to the new investigation workspace.

runs

data flow

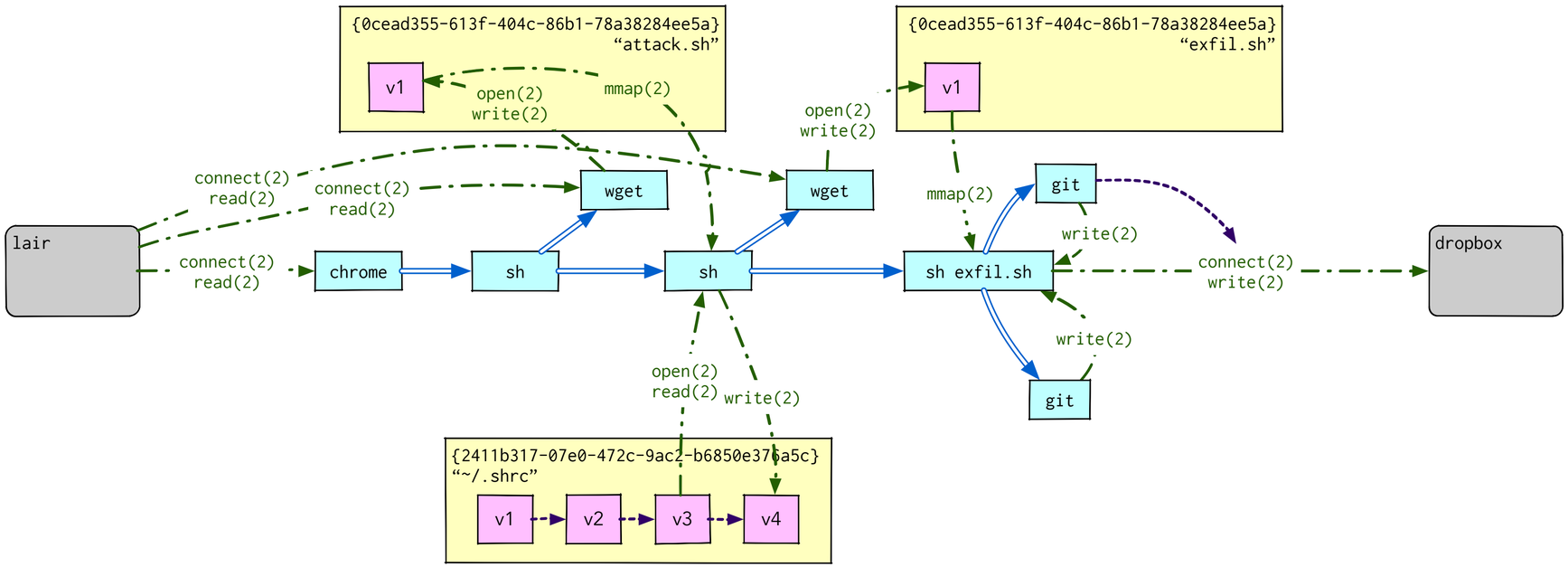
causal relation

OPUS

Worksheet 1 | Worksheet 2 | New…

Big picture

Worksheets



The analyst discovers that, in addition to the known exfiltration, the attacker has left behind a toehold by modifying the user’s .shrc file.

runs

data flow

causal relation

14 Toehold discovered

Fri Jun 16 22:22:51 NDT 2017

mocks.graffle