Software Security Project-2 Assignment

Submitted By: Group-33

Team Members:
Snigdha Sri Nemani
Saideepthi Korupolu
Venkat Ratnam Sabbavarapu

Contributions:

1) Question 1- Snigdha Sri Nemani
2) Question 2– Saideepthi Korupolu
3) Question 3 – Venkat Ratnam Sabbavarapu

The workload has been allocated equally to all the team members of our project.

Running the code:

1) The log file will be created by running the "sudo sysdig" command in the ubuntu terminal.
2) By using the command, the log will be loaded into the input.txt file.
3) This input.txt will be moved to our local machine.
4) Now, we need to open the python file in google collaboratory.
5) After uploading the filename.txt, we need to run the code.
6) After the models run, 3 output files will be generated
   a) part2input.txt
   b) final_graph.gv.pdf
   c) backtrack.gv.pdf

Q-1: Below is the screenshot of the tuple that has been generated. In the below screenshots, each log entry is represented by a subject, object, and operation. The operations included in our tuple are read, write, sendmsg (send message), and recvmsg (receive message).

In the below screenshot, "IndexDB" is the subject which is performing write operation on a file.

```python
f=open("tuples.txt","a")
for tuple in tuples:
    f.write(str(tuple))
    print(tuple)
    f.write("\n")
f.close()
```

```
Streaming output truncated to the last 5000 lines.
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
```

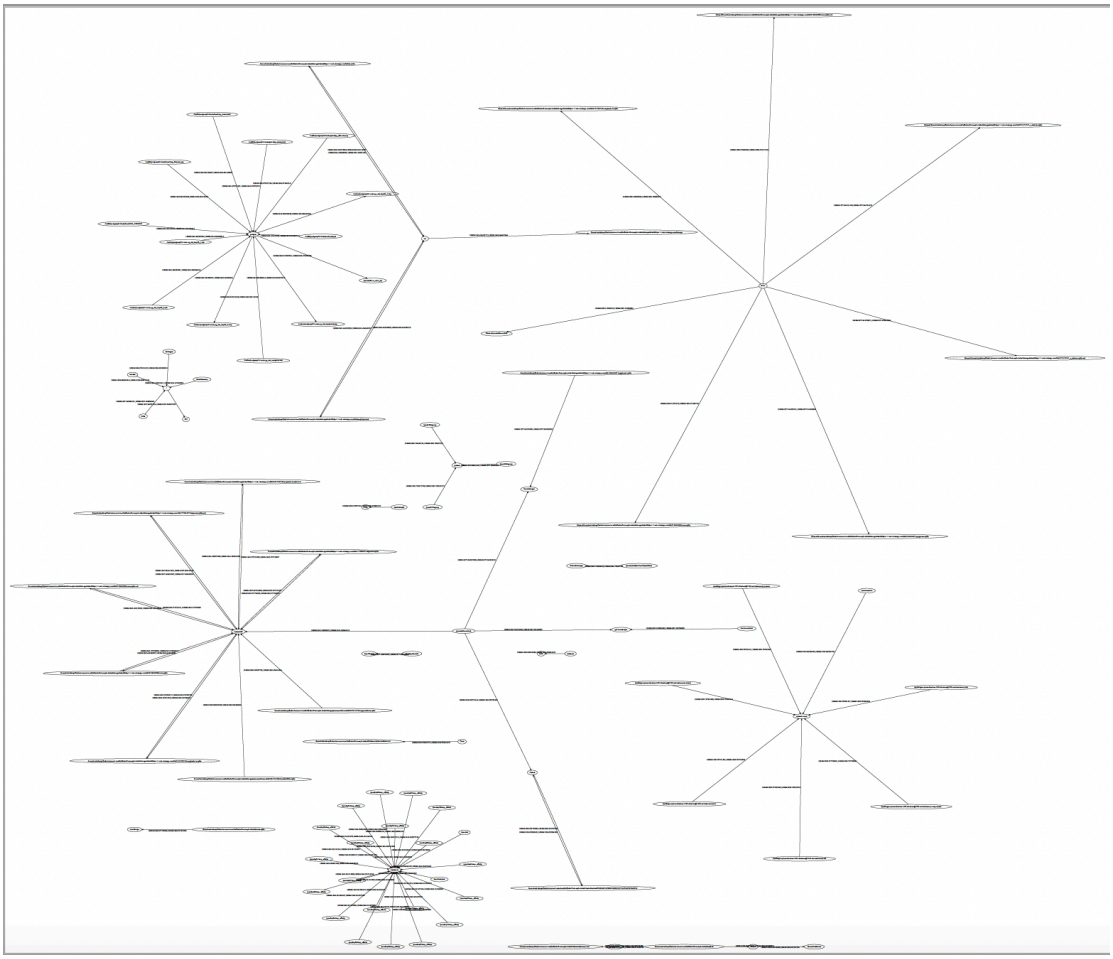
```python
f=open("tuples.txt","a")
for tuple in tuples:
    f.write(str(tuple))
    print(tuple)
    f.write("\n")
f.close()
```

```
('DOM', 'sendmsg', '/')
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
```

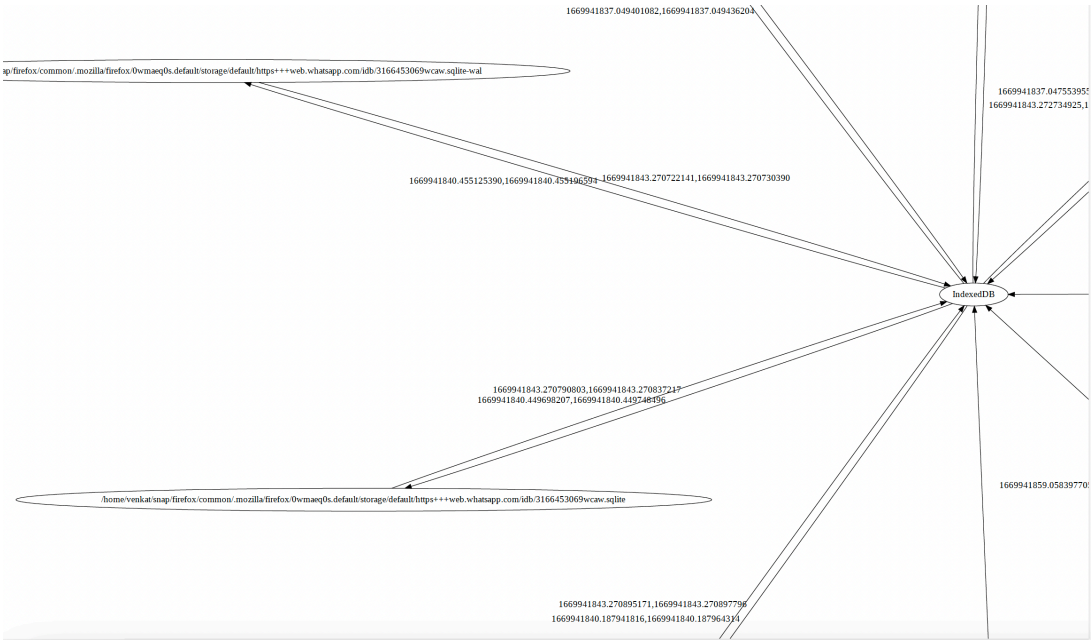
```
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IPC', 'recvmsg', '/')
('IPC', 'recvmsg', '/')
('DOM', 'sendmsg', '/')
('DOM', 'sendmsg', '/')
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IndexedDB', 'read', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot.
('IPC', 'recvmsg', '/')
('IPC', 'recvmsg', '/')
('DOM', 'sendmsg', '/')
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
('IndexedDB', 'write', '/home/venkat/snap/firefox/common/.mozilla/firefox/0wmaeq0s.default/storage/default/https+++web.whatsapp.com/idb/1773850371fetgsa-rsot
```

Q-2: Below are the screenshots of the output graph that has been generated using the tuple generated in the first question. In this graph, the nodes represent the system entities which are files and the edges are represented by the time stamps, and direction of edges represent which operation is being performed i.e read, write, sendmsg, or recvmsg.

Drive link for output graph:
https://drive.google.com/file/d/1uU_Jq9g7FzKtzDHE4Co8665ifLIBU1Bx/view?usp=share_link

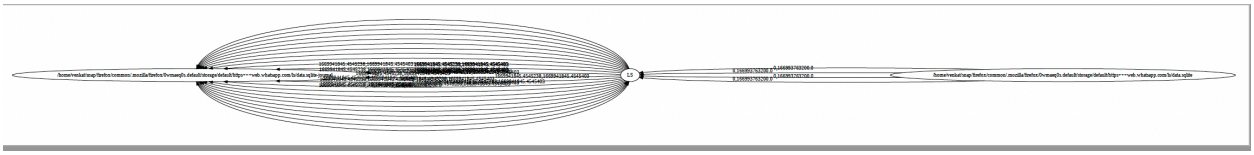


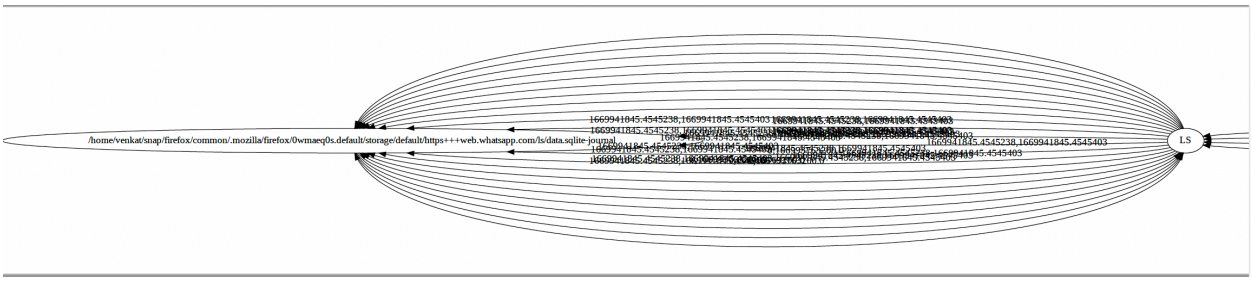
If we observe in the below graph, IndexDB is the subject and /home/Venkat/snap… is the object which is a file. The edges are represented by the respective time stamp. In the below screenshot, there are 2 types of operations being performed between the subject and object, they are read operation and write operation.

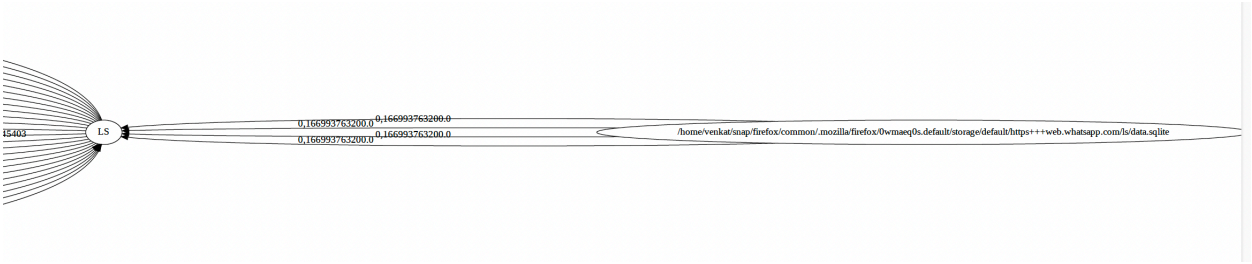


Q-3: Below are the screenshots is the output of the backtracking algorithm that is performed on the graph generated as part of Question-2. The graph is generated in such a way that if the start time of the incoming edge is less than the end time of the current edge, then it is considered, if the condition is not satisfied, then the edge is deleted. This process will be continuously done until there are no more edges left. Also, we have taken a random edge of POI event and started the search from that point. The backtracking has been performed by taking the timestamp into consideration.

Drive Link for backtrack graph:
https://drive.google.com/file/d/1EiQz0OT7VYMdk1MwtDPQJEgdZ5XY-hDg/view?usp=sharing





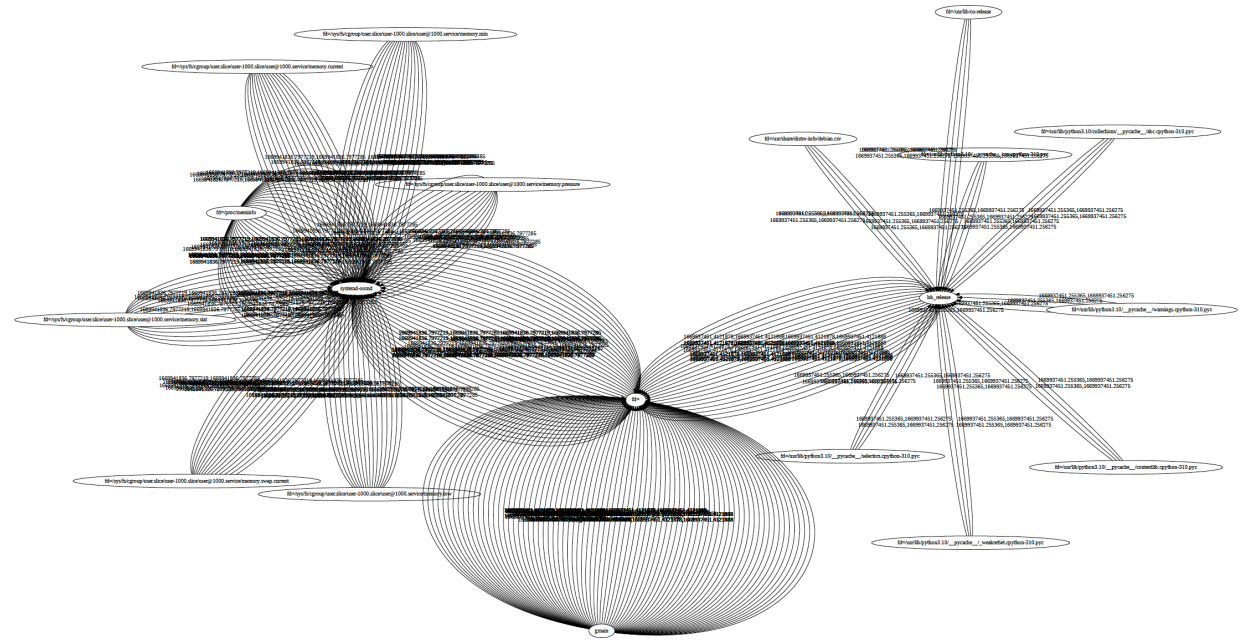


Example: We are considering the following tuple from the log file:

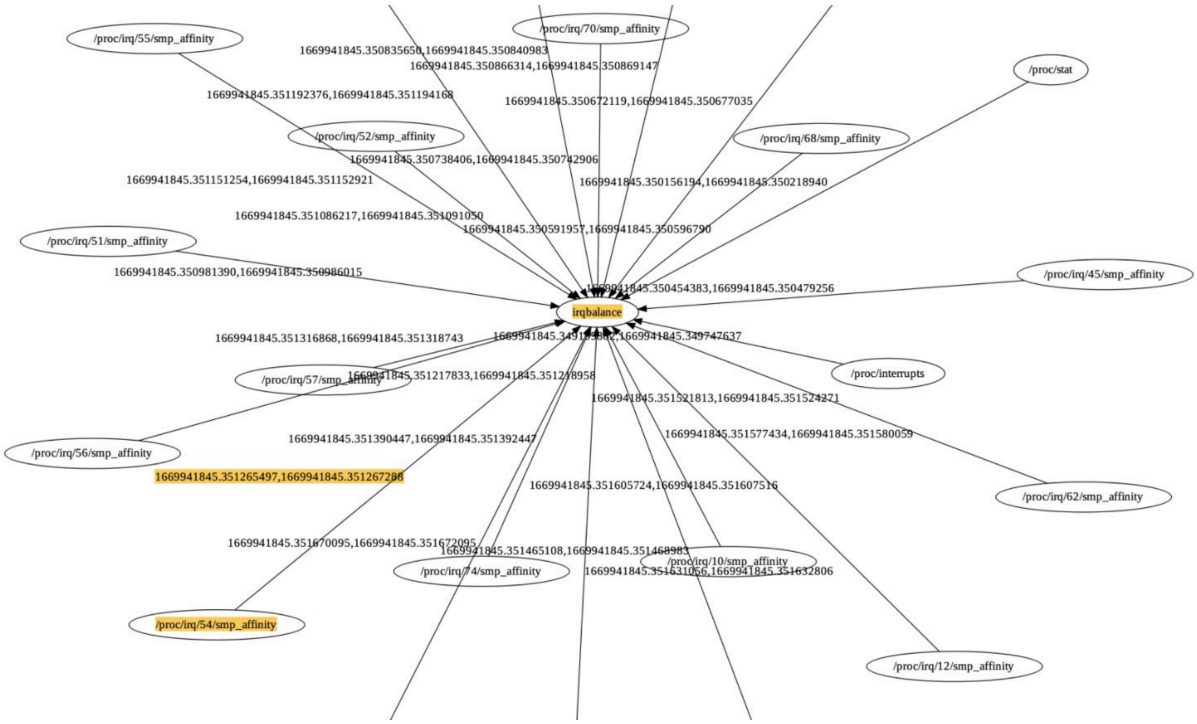
/sys/fs/cgroup/user.slice/user-1000.slice/user@1000.service/memory.low","systemd-oomd",1669941836.797721981,1669941836.797728480)

Now, below is the output obtained from backtracking this. Below is the screenshot of the output.

Drive link for below graph:
https://drive.google.com/file/d/1TQf3Oh1NTIWY665fjGQiln60REBakfxc/view?usp=share_link

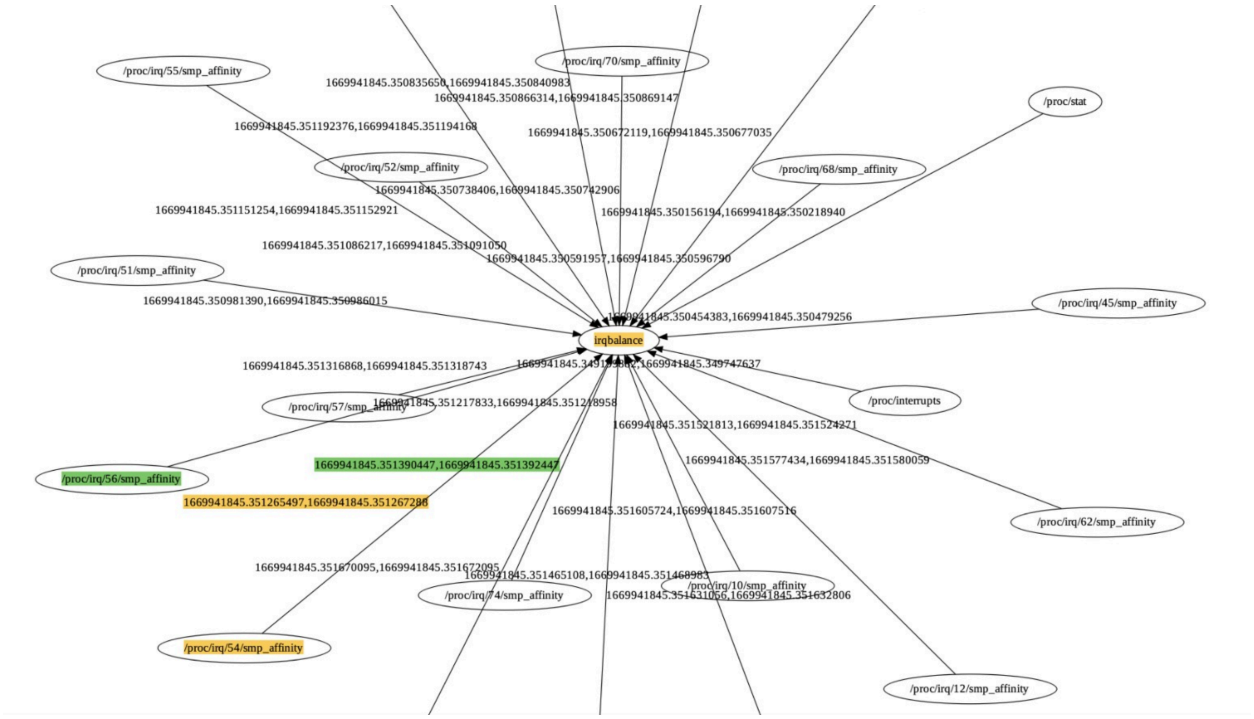


Example-2: We are considering the below node and time stamps in the output graph:



After backtracking, below is the output:

As we can see in the below screenshot, the nodes like this with start time greater than the end time of given input is deleted.


/proc/irq/55/smp_affinity
/proc/irq/70/smp_affinity
1669941845.350835650,1669941845.350840983
1669941845.350866314,1669941845.350869147
/proc/stat
1669941845.351192376,1669941845.351194168
1669941845.350672119,1669941845.350677035
/proc/irq/52/smp_affinity
/proc/irq/68/smp_affinity
1669941845.350738406,1669941845.350742906
1669941845.351151254,1669941845.351152921
1669941845.350156194,1669941845.350218940
1669941845.351086217,1669941845.351091050
1669941845.350591957,1669941845.350596790
/proc/irq/51/smp_affinity
1669941845.350981390,1669941845.350986015
/proc/irq/45/smp_affinity
1669941845.350454383,1669941845.350479256
irqbalance
1669941845.351316868,1669941845.351318743
/proc/irq/57/smp_affinity
1669941845.351217833,1669941845.351218958
/proc/interrupts
1669941845.351521813,1669941845.351524271
1669941845.351577434,1669941845.351580059
/proc/irq/56/smp_affinity
1669941845.351390447,1669941845.351392447
1669941845.351265497,1669941845.351267286
1669941845.351605724,1669941845.351607516
/proc/irq/62/smp_affinity
1669941845.351670095,1669941845.351672095
1669941845.351465108,1669941845.351468983
/proc/irq/74/smp_affinity
/proc/irq/10/smp_affinity
1669941845.351631056,1669941845.351632806
/proc/irq/54/smp_affinity
/proc/irq/12/smp_affinity