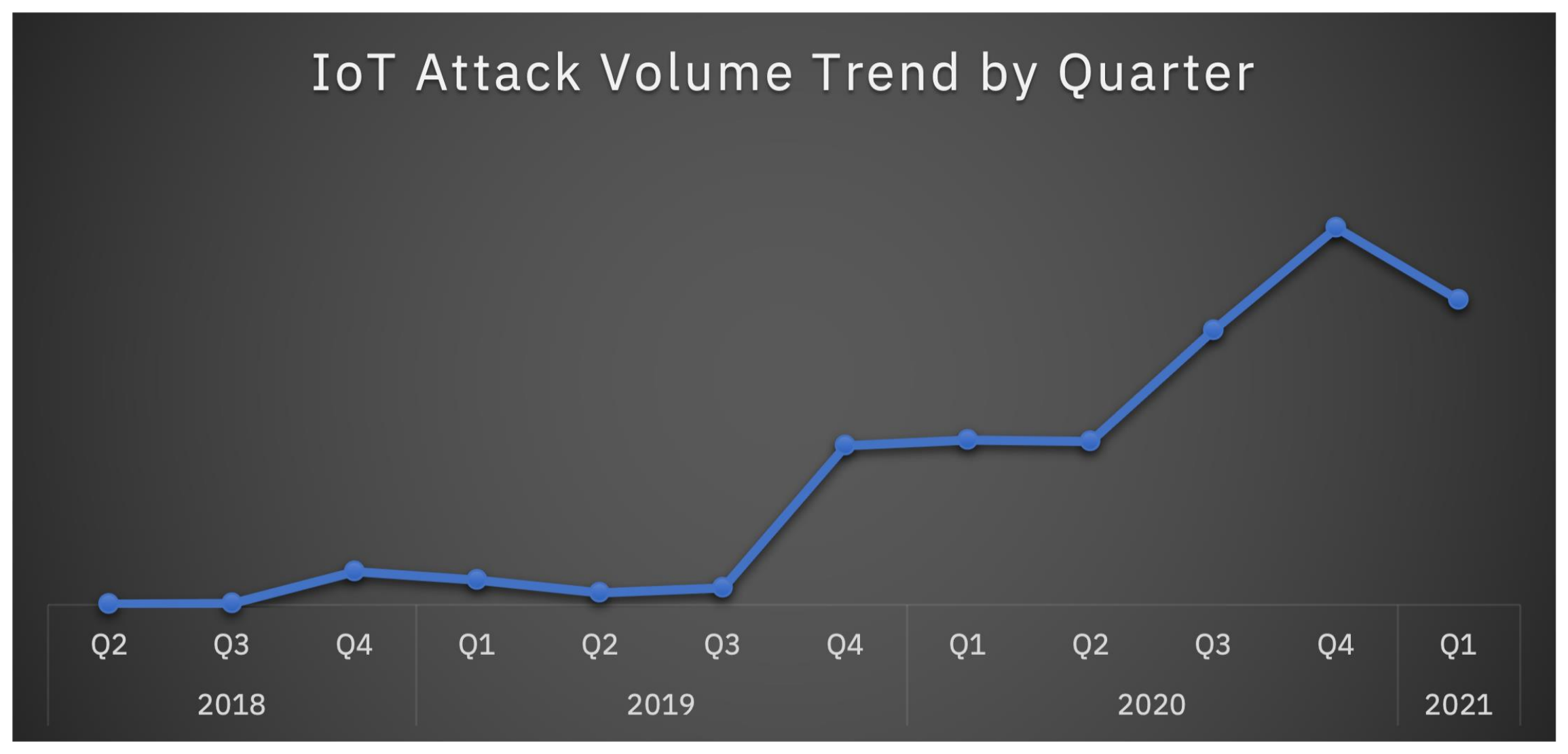
Detecting Anomalies in IoT Device Communication Based on MUD Profiles with Zeek and Python

Rohan Nunugonda[1], Vyas Sekar[2], Matthew McCormack[2], Timothy Corica[1]

The Peddie School[1], Carnegie Mellon University[2]

Background: IoT and MUD

Problem: IoT Attacks On the Rise!



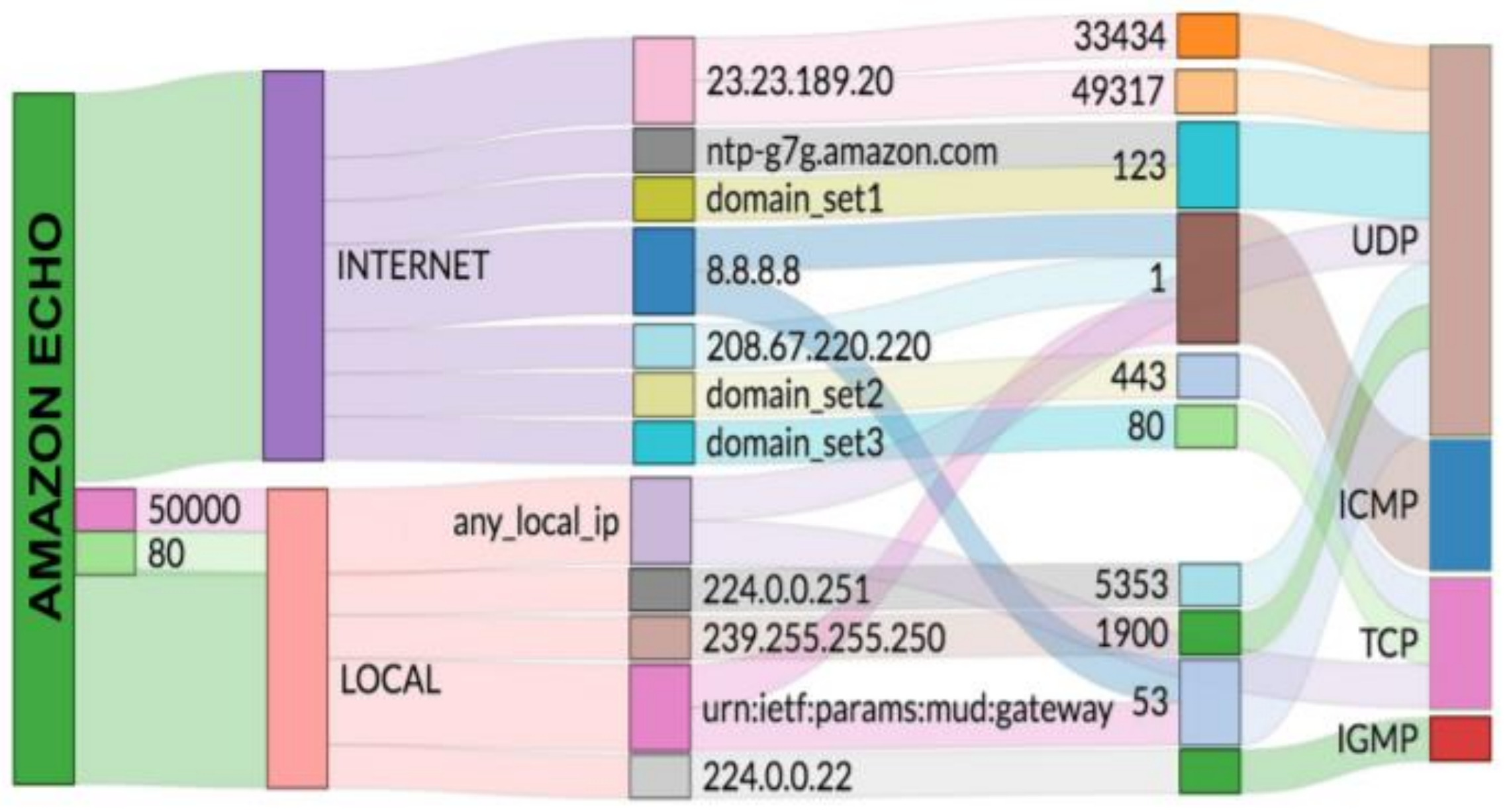
Hackers can "Faxploit" Connected Fax Machines

RCE Vulnerability in Hikvision devices could lead to network compromise

1. *McMillen, Dave. "Internet of Threats: IOT Botnets Drive Surge in Network Attacks." Security Intelligence, IBM, 22 Apr. 2021, https://securityintelligence.com/posts/internet-of-threats-iot-botnets-network-attacks/.*
2. "Can Fax Machines Be Hacked and What Is Faxploit." EFax, 2 June 2020, https://www.efax.co.uk/blog/fax-machine-exploit#:~:text=Yes%2C%20fax%20machines%20can%20be,be%20manipulated%20by%20external%20sources.
3. Haworth, Jessica. "Zero-Click RCE Vulnerability in Hikvision Security Cameras Could Lead to Network Compromise." *The Daily Swig | Cybersecurity News and Views*, The Daily Swig, 20 Sept. 2021, https://portswigger.net/daily-swig/zero-click-rce-vulnerability-in-hikvision-security-cameras-could-lead-to-network-compromise.

Goal: Log suspicious connections using MUD

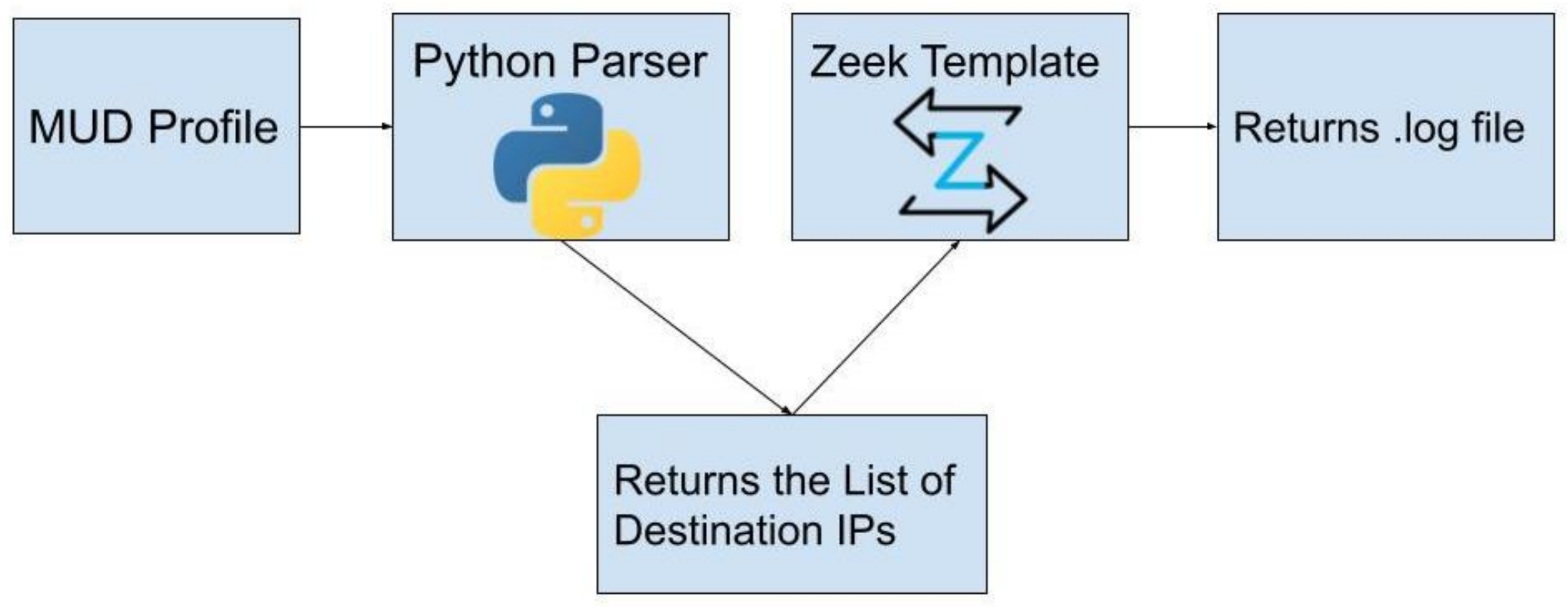
MUD: Manufacturer Usage Description



1. A. Hamza, D. Ranathunga, H. Habibi Gharakheili, M. Roughan and V. Sivaraman, "Clear as MUD: Generating, Validating, and Applying IoT Behavioural Profiles", ACM Sigcomm Workshop on IoT Security and Privacy (IoT S&P), Budapest, Hungary, Aug 2018.

Our Work: Synthesize IDS policies from MUD profiles

Workflow Diagrams



MUD Profile

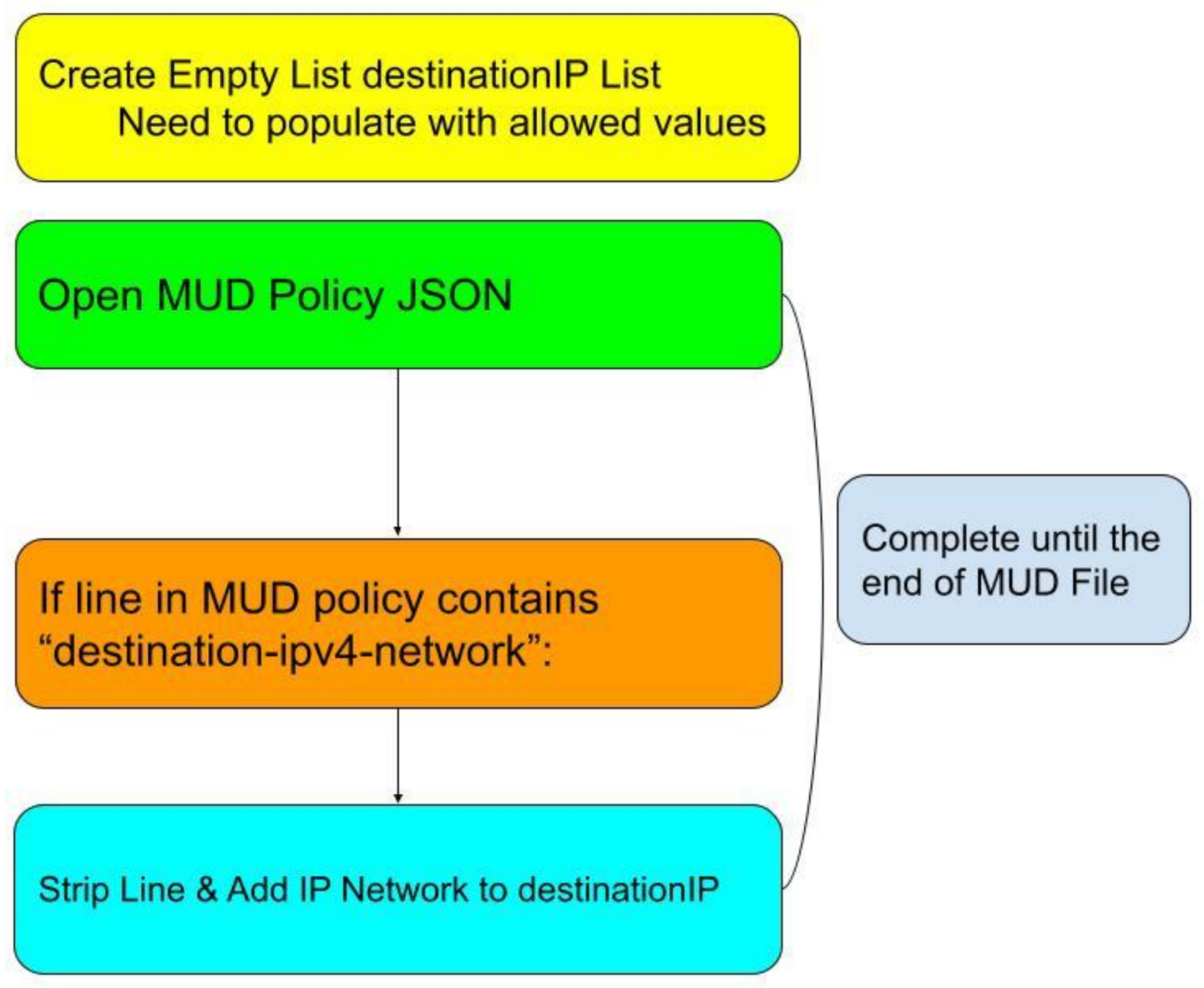
Python Parser

Zeek Template

Returns .log file

Returns the List of Destination IPs

Full Project Workflow



Create Empty List destinationIP List
Need to populate with allowed values

Open MUD Policy JSON

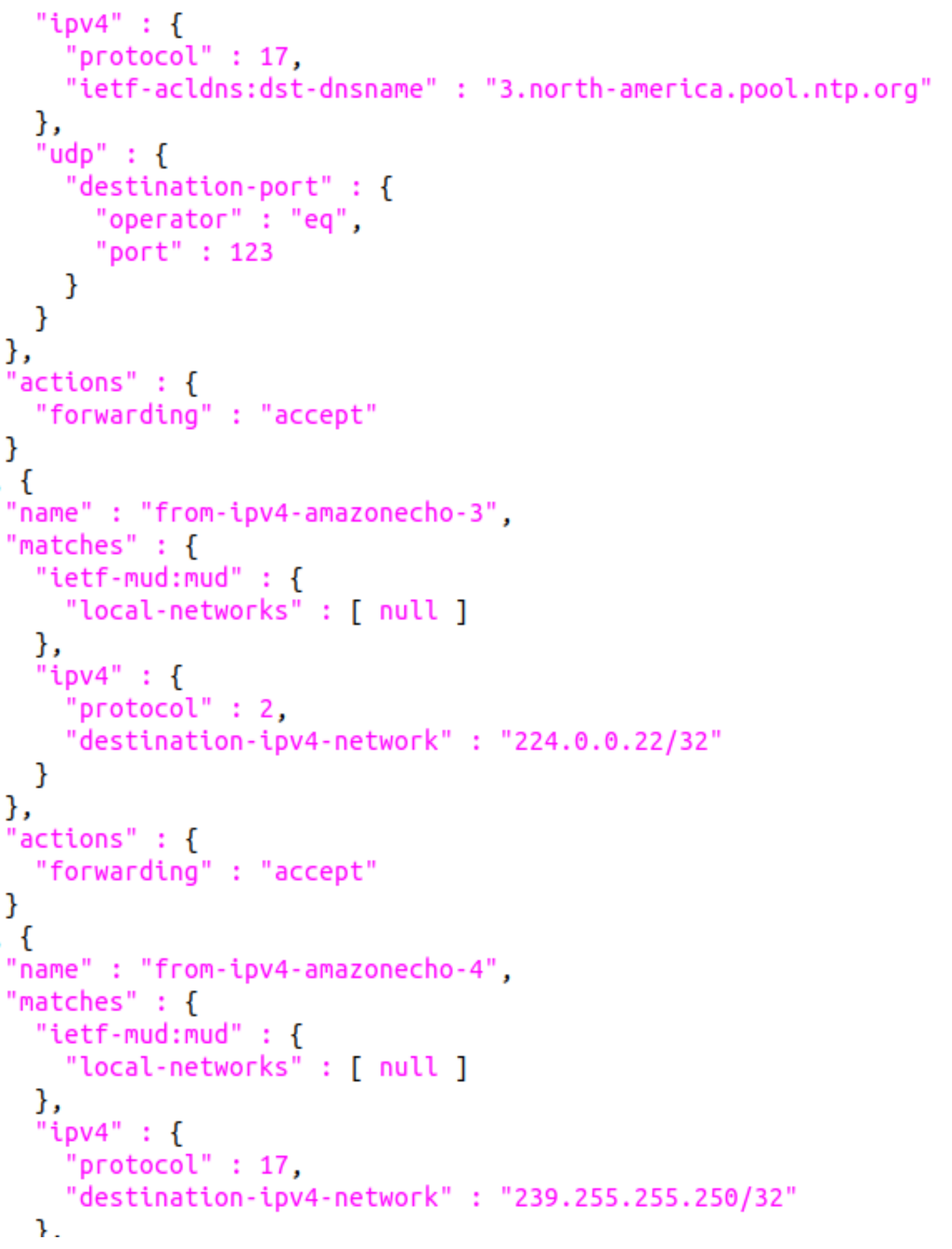
If line in MUD policy contains "destination-ipv4-network":

Strip Line & Add IP Network to destinationIP

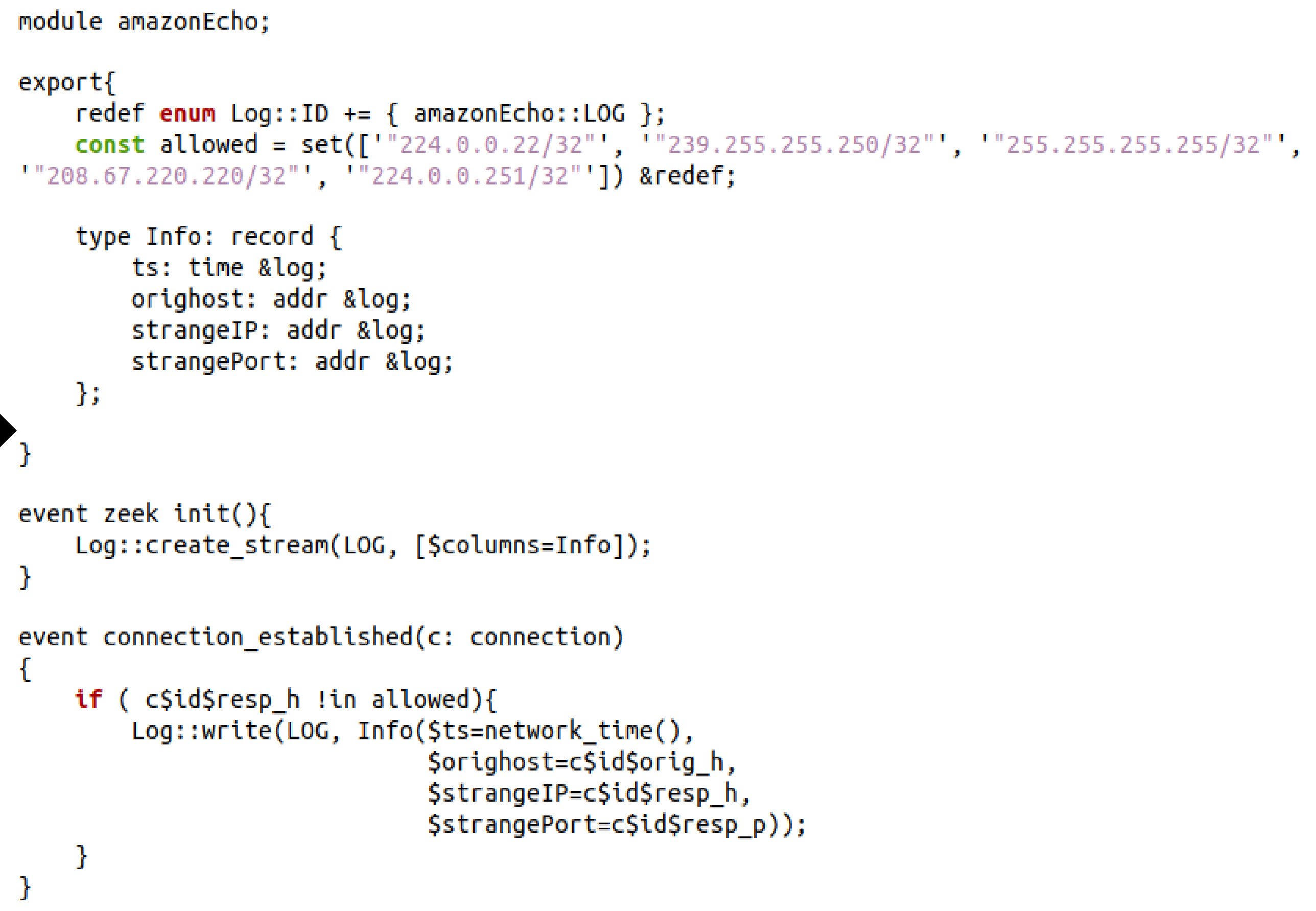
Complete until the end of MUD File

Python Script Workflow

MUD → Zeek



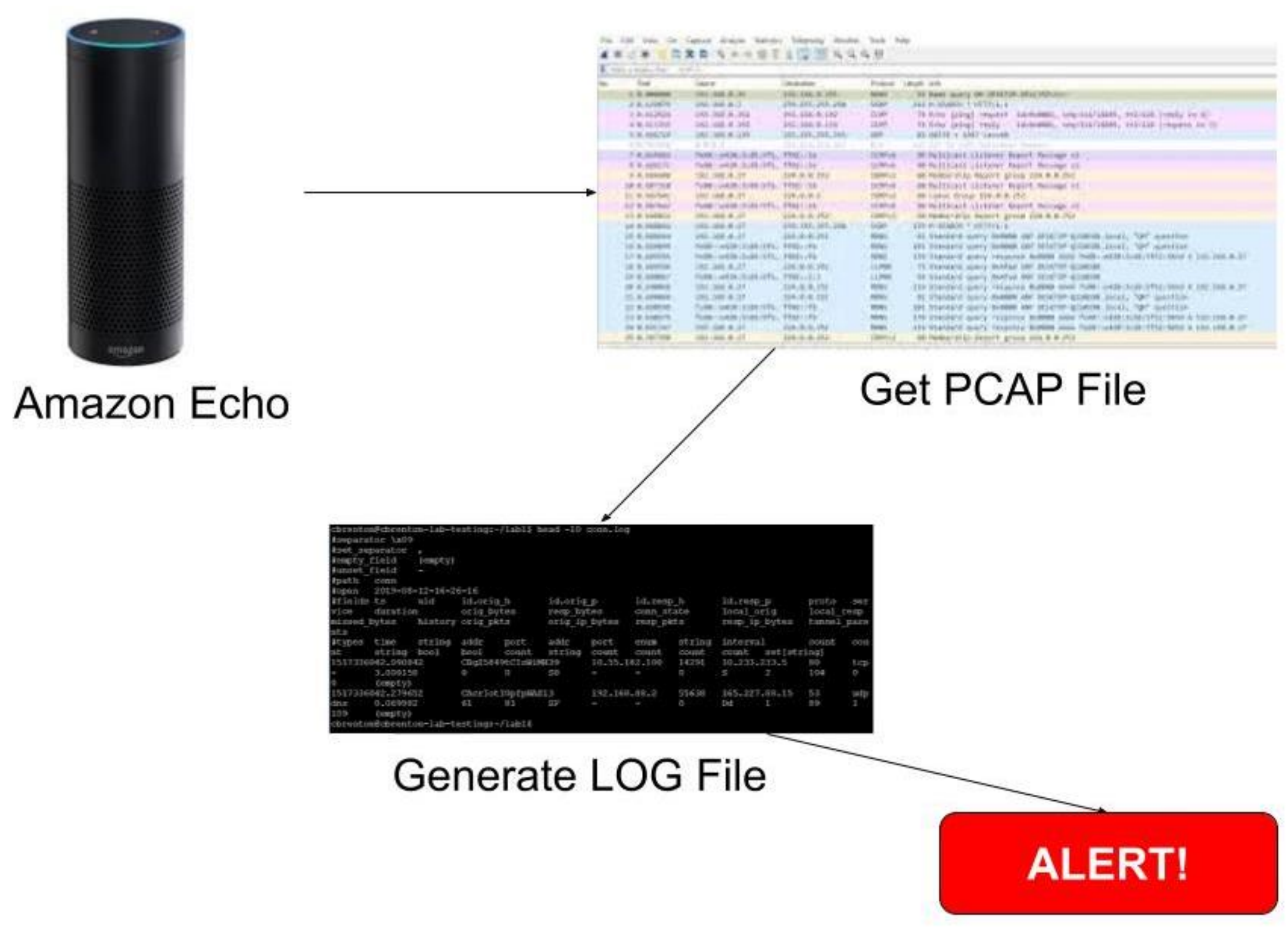
```
    "ipv4" : {
      "protocol" : 17,
      "ietf-acldns:dst-dnsname" : "3.north-america.pool.ntp.org"
    },
    "udp" : {
      "destination-port" : {
        "operator" : "eq",
        "port" : 123
      }
    }
  },
  "actions" : {
    "forwarding" : "accept"
  }
}, {
  "name" : "from-ipv4-amazonecho-3",
  "matches" : {
    "ietf-mud:mud" : {
      "local-networks" : [ null ]
    },
    "ipv4" : {
      "protocol" : 2,
      "destination-ipv4-network" : "224.0.0.22/32"
    }
  },
  "actions" : {
    "forwarding" : "accept"
  }
}, {
  "name" : "from-ipv4-amazonecho-4",
  "matches" : {
    "ietf-mud:mud" : {
      "local-networks" : [ null ]
    },
    "ipv4" : {
      "protocol" : 17,
      "destination-ipv4-network" : "239.255.255.250/32"
    },
```



```
module amazonEcho;

export{
    redef enum Log::ID += { amazonEcho::LOG };
    const allowed = set(['"224.0.0.22/32"', '"239.255.255.250/32"', '"255.255.255.255/32"',
'"208.67.220.220/32"', '"224.0.0.251/32"']) &redef;

    type Info: record {
        ts: time &log;
        orighost: addr &log;
        strangeIP: addr &log;
        strangePort: addr &log;
    };

}

event zeek init(){
    Log::create_stream(LOG, [$columns=Info]);
}

event connection_established(c: connection)
{
    if ( c$id$resp_h !in allowed){
        Log::write(LOG, Info($ts=network_time(),
                             $orighost=c$id$orig_h,
                             $strangeIP=c$id$resp_h,
                             $strangePort=c$id$resp_p));
    }
}
```

1. A. Hamza, D. Ranathunga, H. Habibi Gharakheili, M. Roughan and V. Sivaraman, "Clear as MUD: Generating, Validating, and Applying IoT Behavioural Profiles", ACM Sigcomm Workshop on IoT Security and Privacy (IoT S&P), Budapest, Hungary, Aug 2018.

Proof of Concept



Amazon Echo

Get PCAP File

Generate LOG File

ALERT!

Future Work

- Run Zeek Scripts with PCAP test data
- Automate scripts for real-time checks
- Use connection ports and protocol

Acknowledgements

- Dr. Vyas Sekar & Matthew – CMU mentors for research
- Dr. Peretz and Ms. Cozine – Peddie EXP mentors
- Mr. Corica and Ms. Wolfe – Peddie project mentors