Network Security Monitoring

INFO-6081 – Monitoring & Incident Response

FANSHAWE

Learning Outcomes

- Security Onion Components
- Analyst Tools
- Security Onion Deployment Types
- Security Onion Node Types
- Installing Security Onion
- QuickStart – Configuring Security Onion

Security Onion Core Components

Logstash

- A server-side data processing pipeline that processes data, transforms it, then sends it to a “stash”

Elasticsearch

- A distributed, RESTful search and analytics engine that can search many types of data (structured, unstructured, geo, metric)

Kibana

- Visualize Elasticsearch data and navigate the Elastic Stack

Security Onion Auxiliary Components

Curator

- Management for Elasticsearch indices and snapshots

ElastAlert

- Framework for alerting on anomalies, spikes, or other patterns of interest

FreqServer

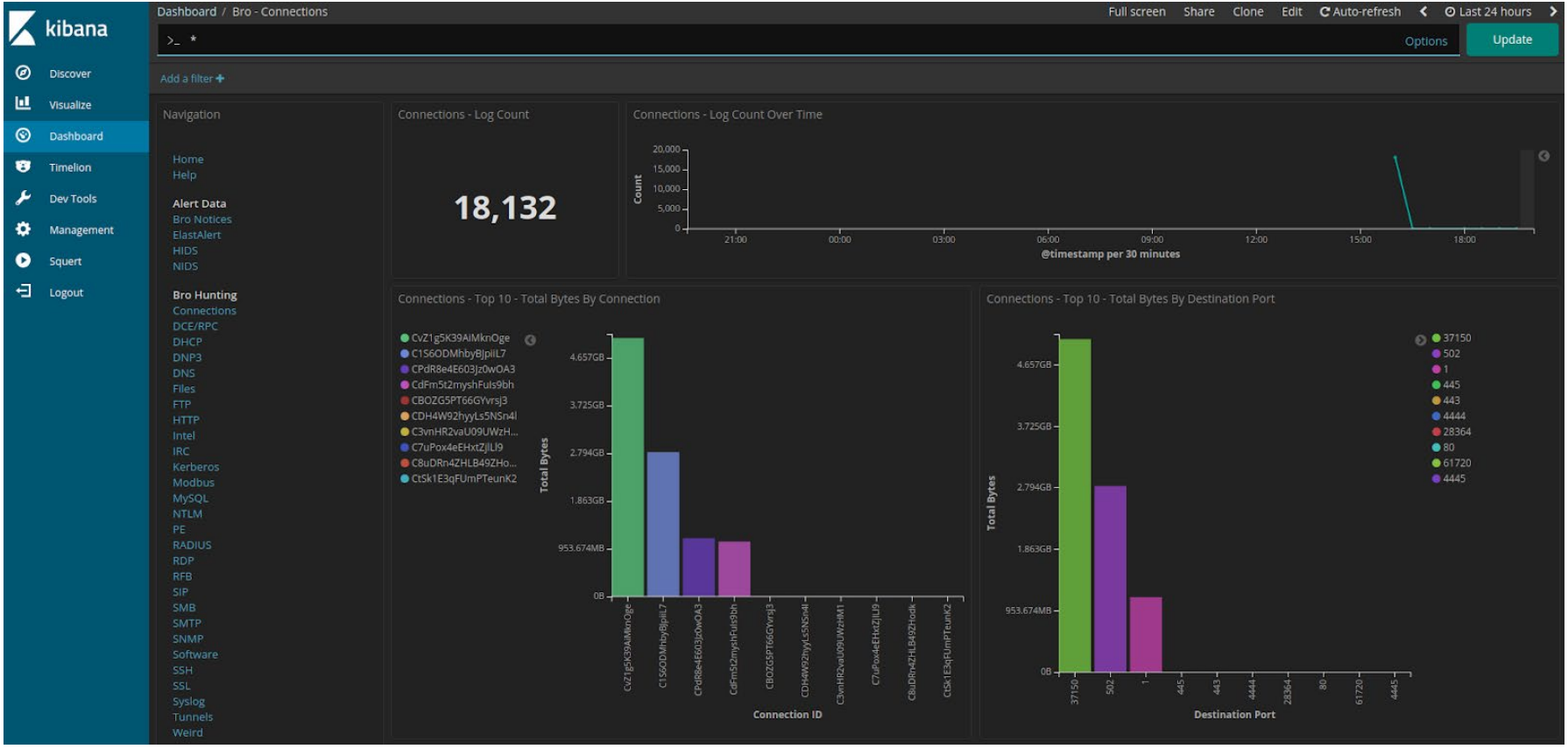
- Detect randomness using character pair frequency analysis

DomainStats

- Performs mass domain analysis

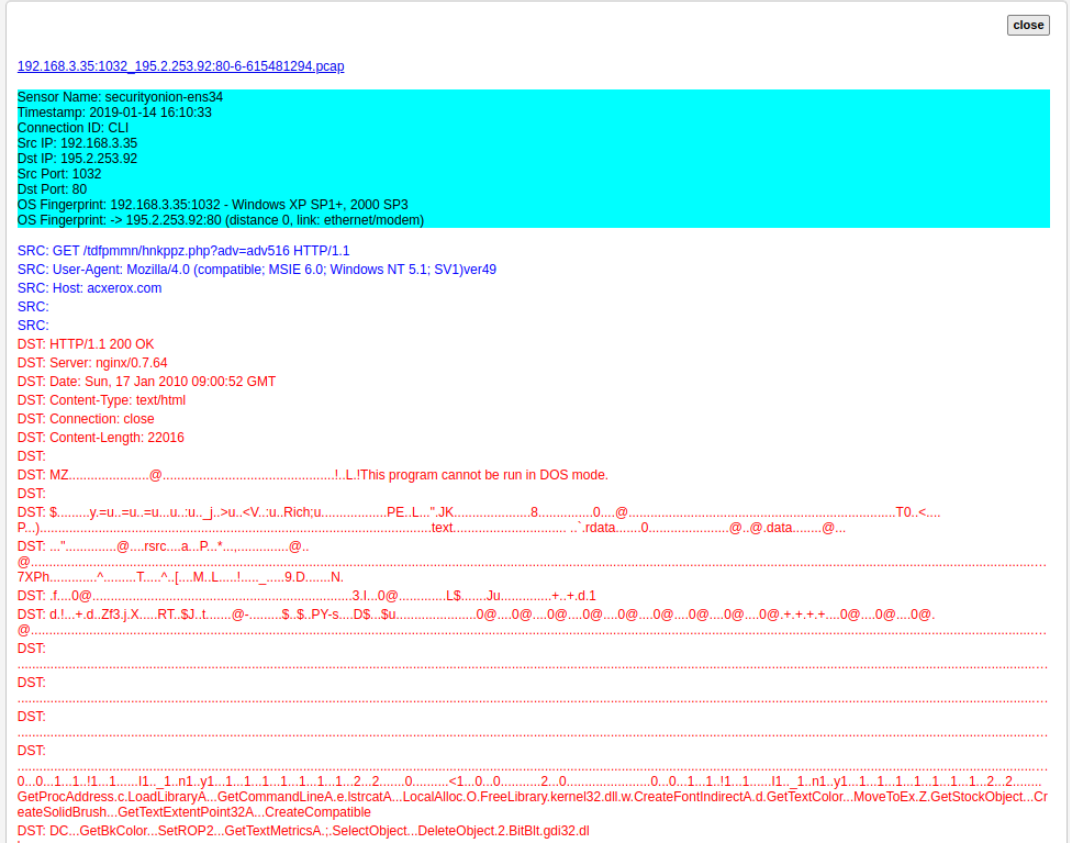
Security Onion Analyst Tools – Kibana

Visualize Elasticsearch data and navigate the Elastic Stack



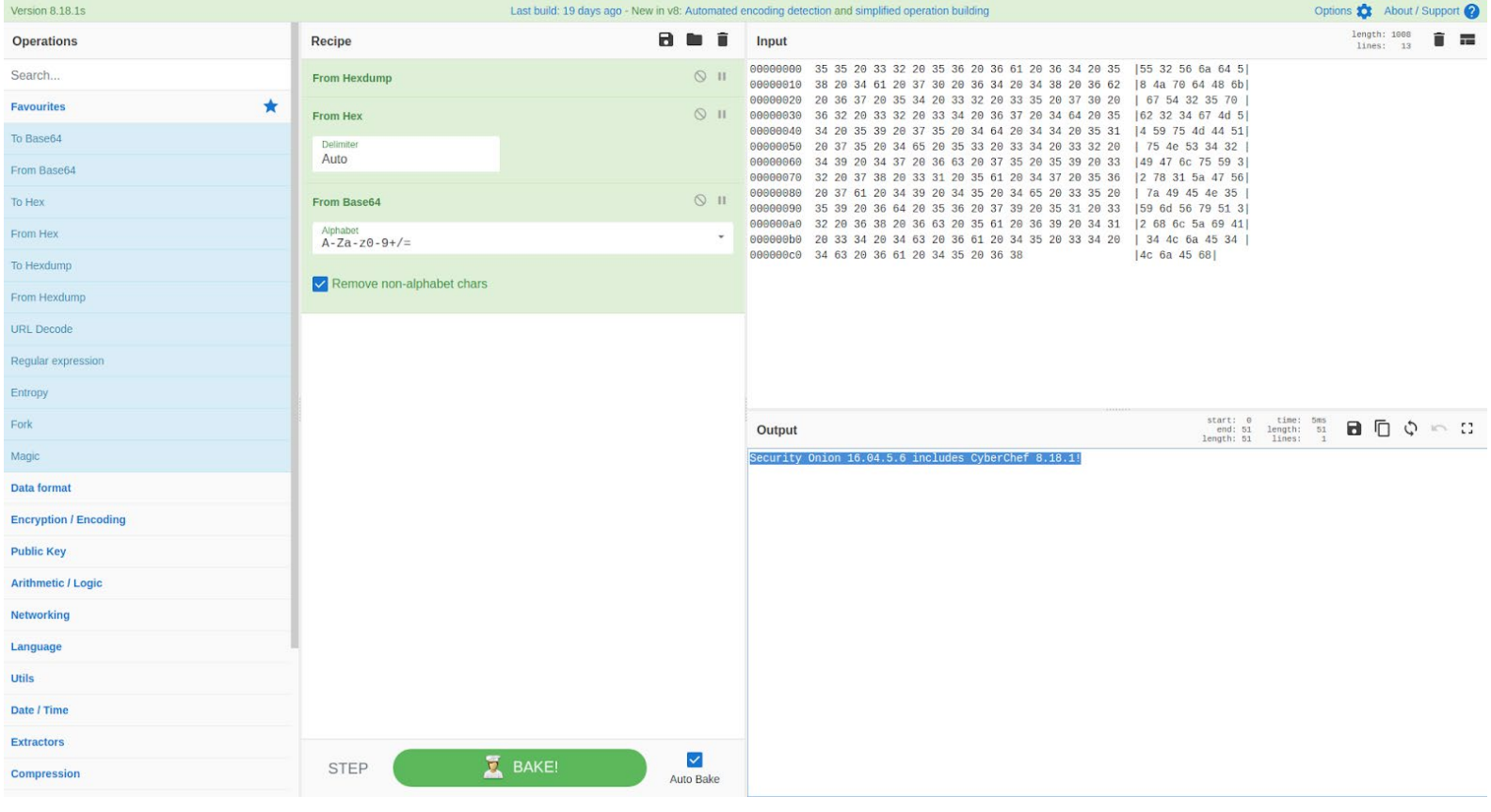
Security Onion Analyst Tools – CapME

View pcap transcripts



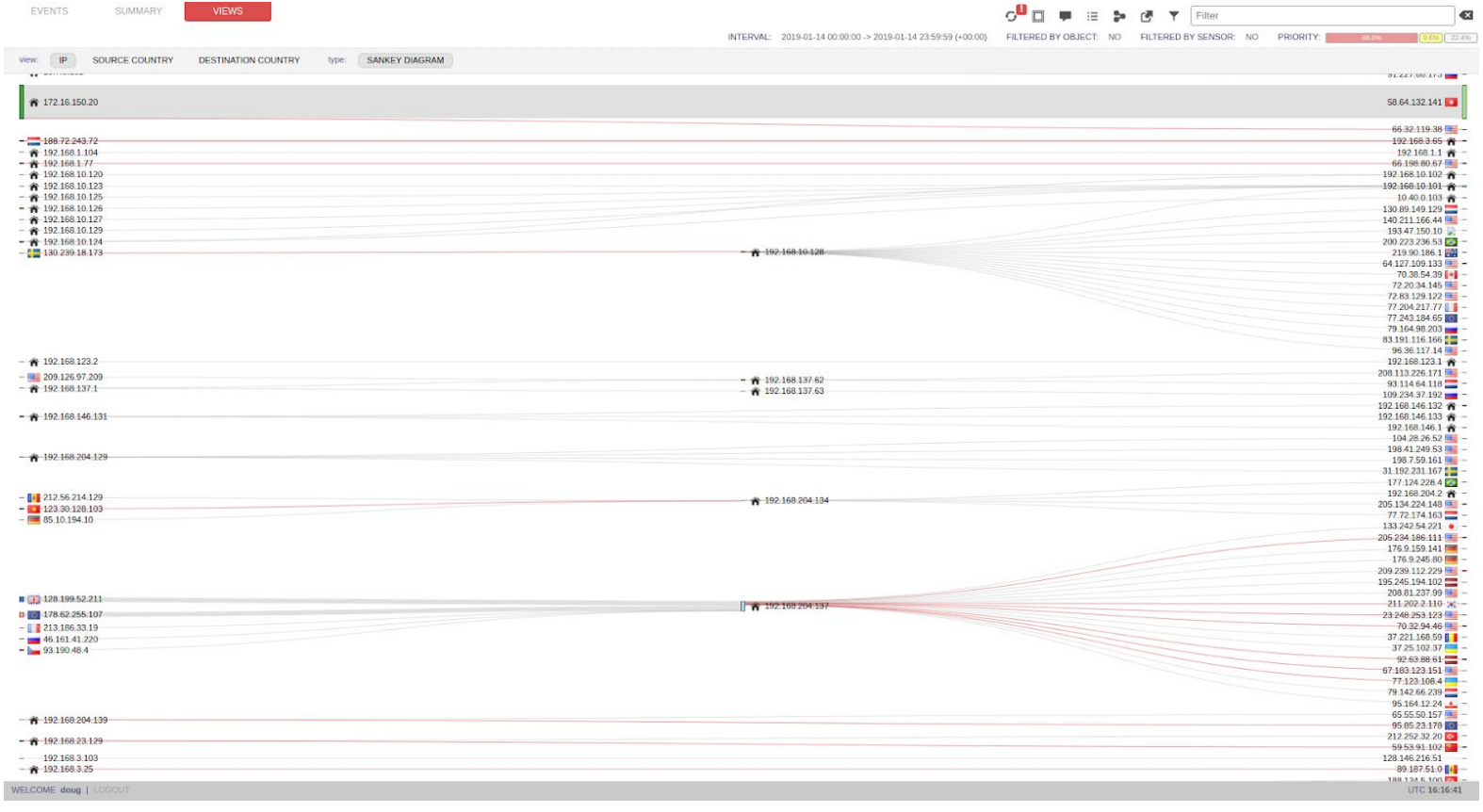
Security Onion Analyst Tools – CyberChef

Manipulate data such with encoding like XOR, Base64, AES, etc…



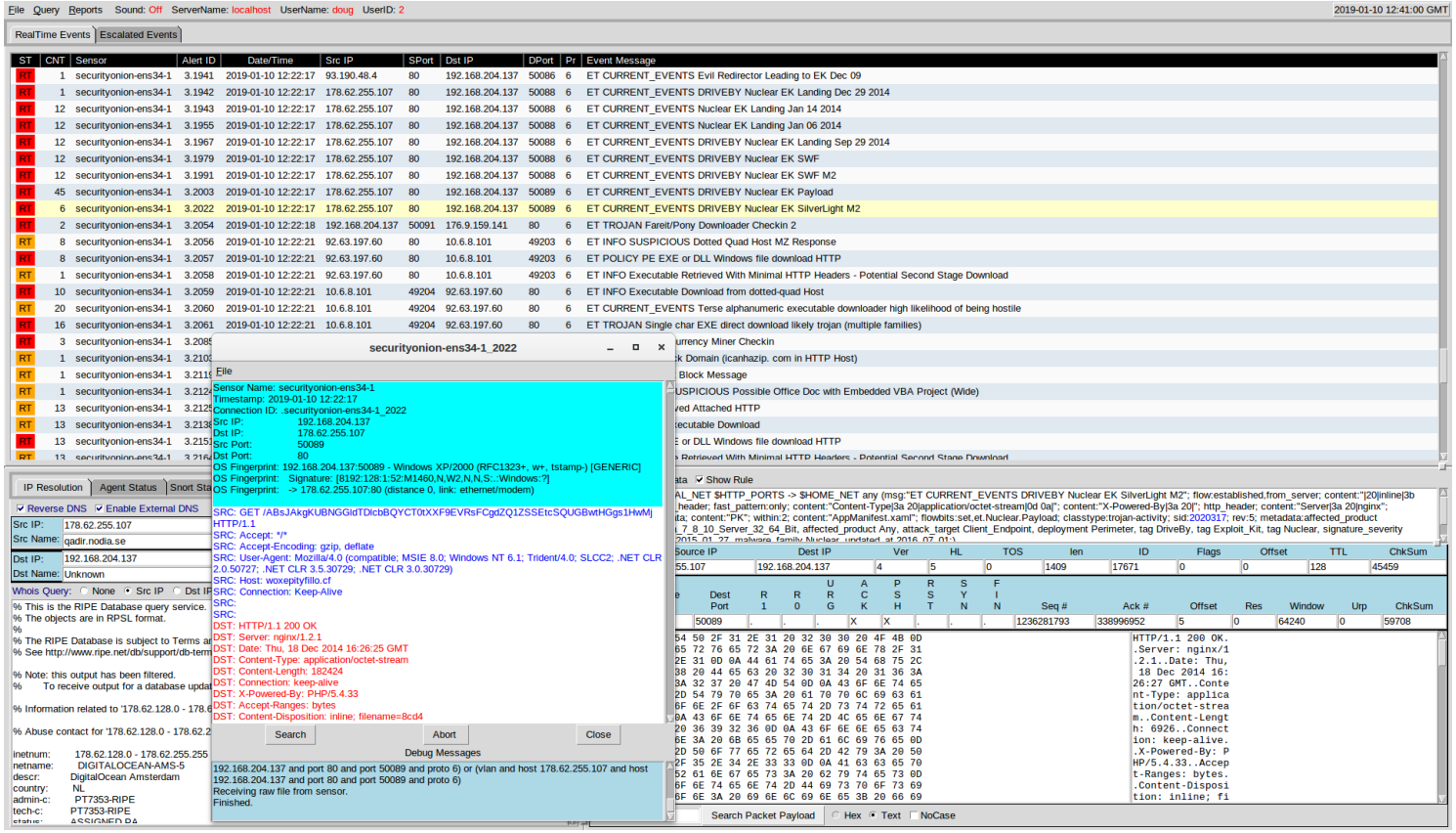
Security Onion Analyst Tools – Squert

View event data from Sguil database (IDS alerts)



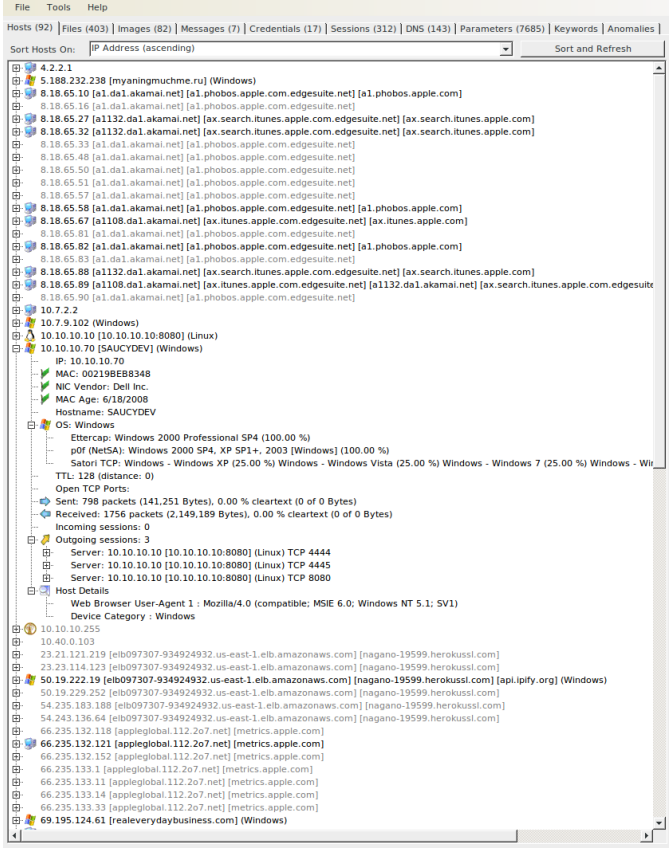
Security Onion Analyst Tools – Sguil

Access to realtime events, session data, and raw packet captures



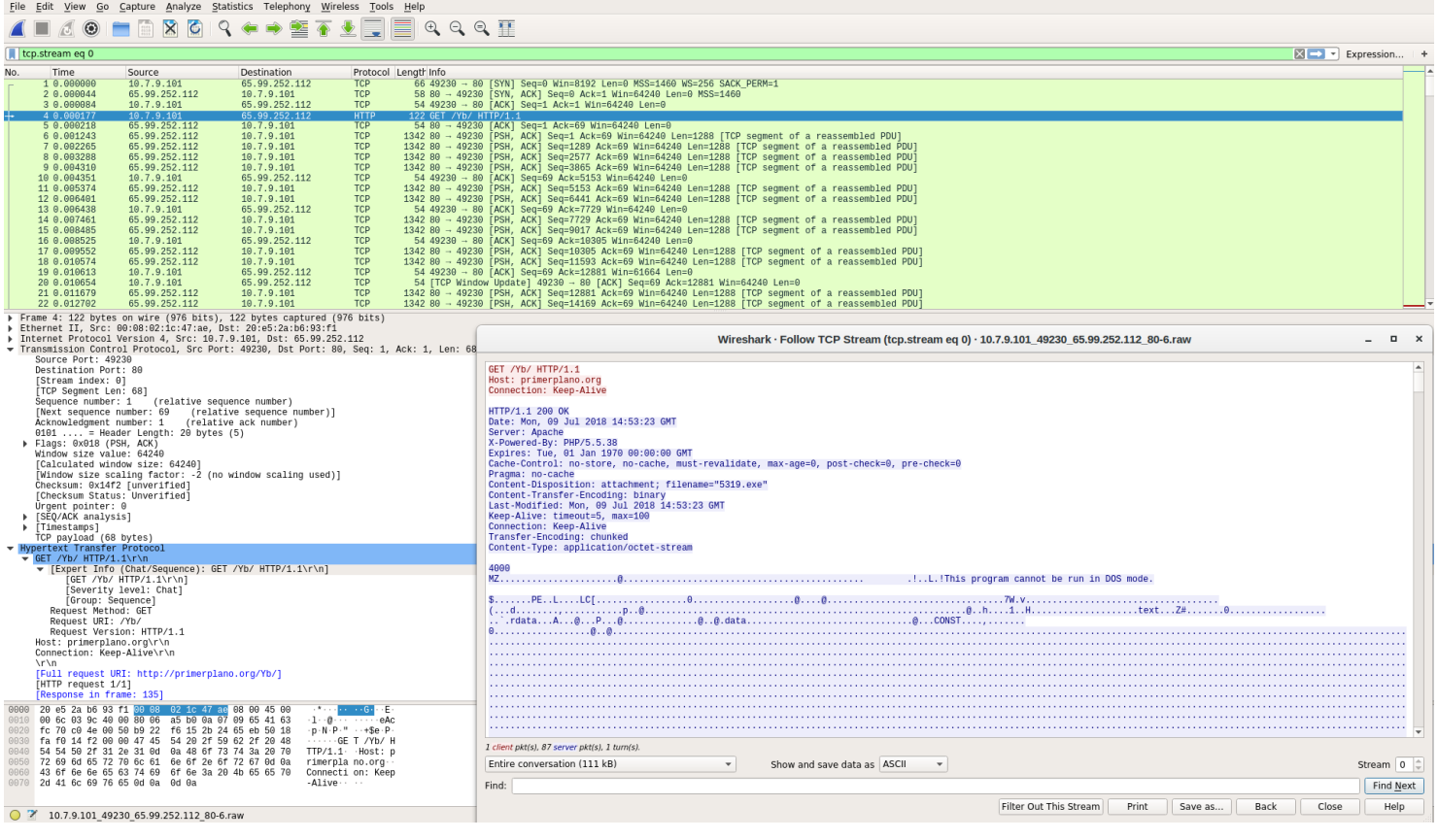
Security Onion Analyst Tools – NetworkMiner

off-line analysis and reassembly of transmitted files from pcap



Security Onion Analyst Tools – Wireshark

Analyze network traffic in a network protocol analyzer



Security Onion Deployment Types

Stand Alone

- A self-contained, appliance style solution to collect and present data
- Often used in smaller deployments

Heavy Distributed

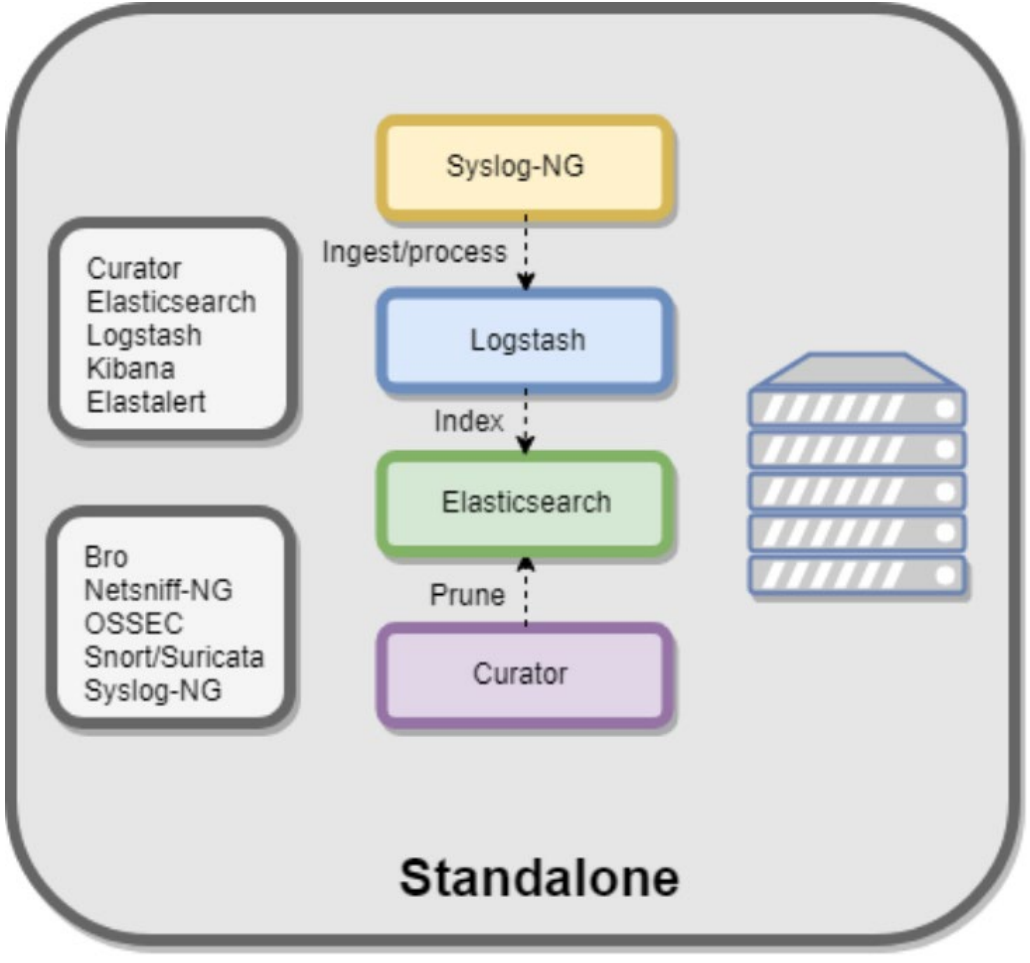
- A distributed platform, with multiple heavy nodes reporting to a master server
- Recommended only when a standard deployment is not possible

Security Onion Deployment Types

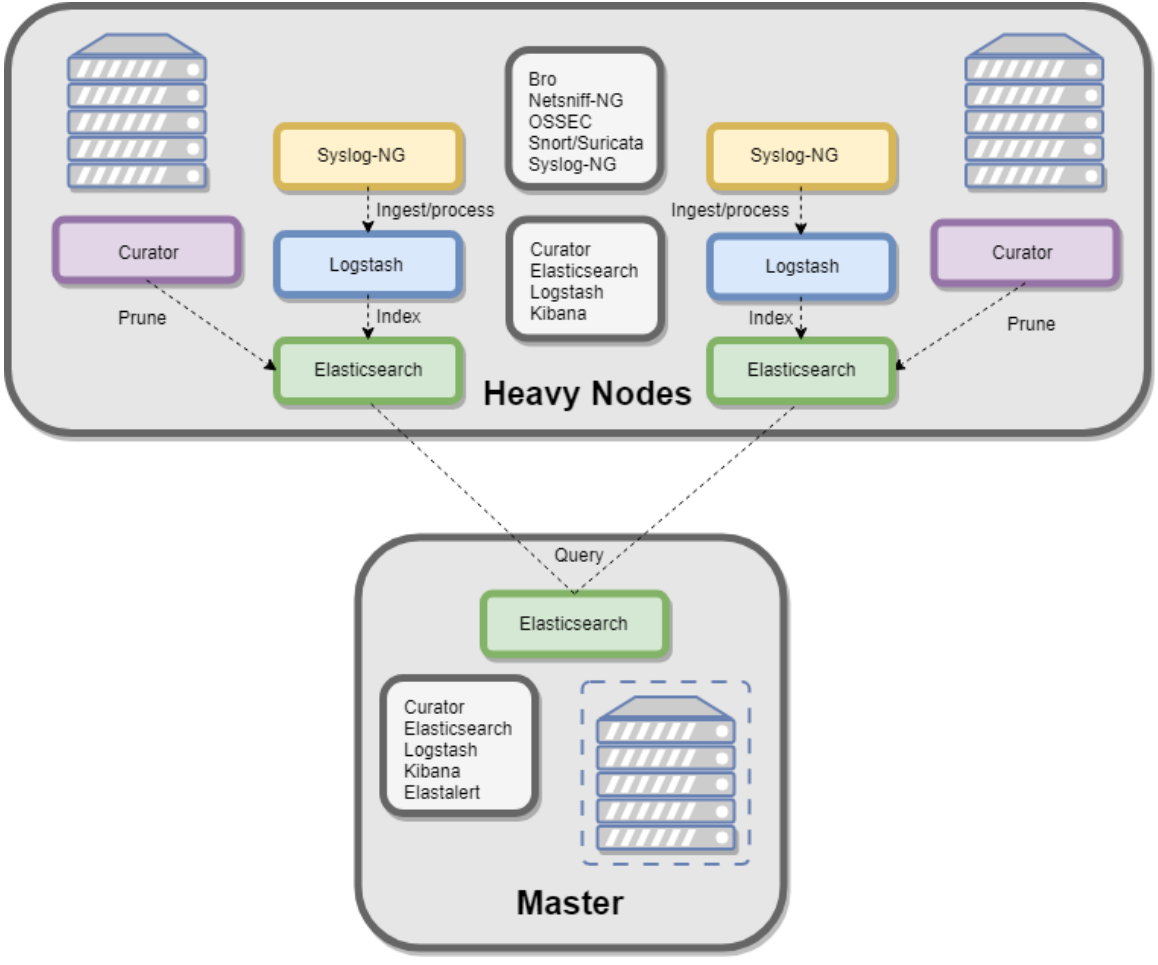
Distributed

- A distributed platform, with forward nodes collecting data, a master server aggregating and presenting the data to analysists, and storage nodes
- Preferred in environments where multiple sensors are required
- Sensors can be deployed globally, as long as they can connect to the central server

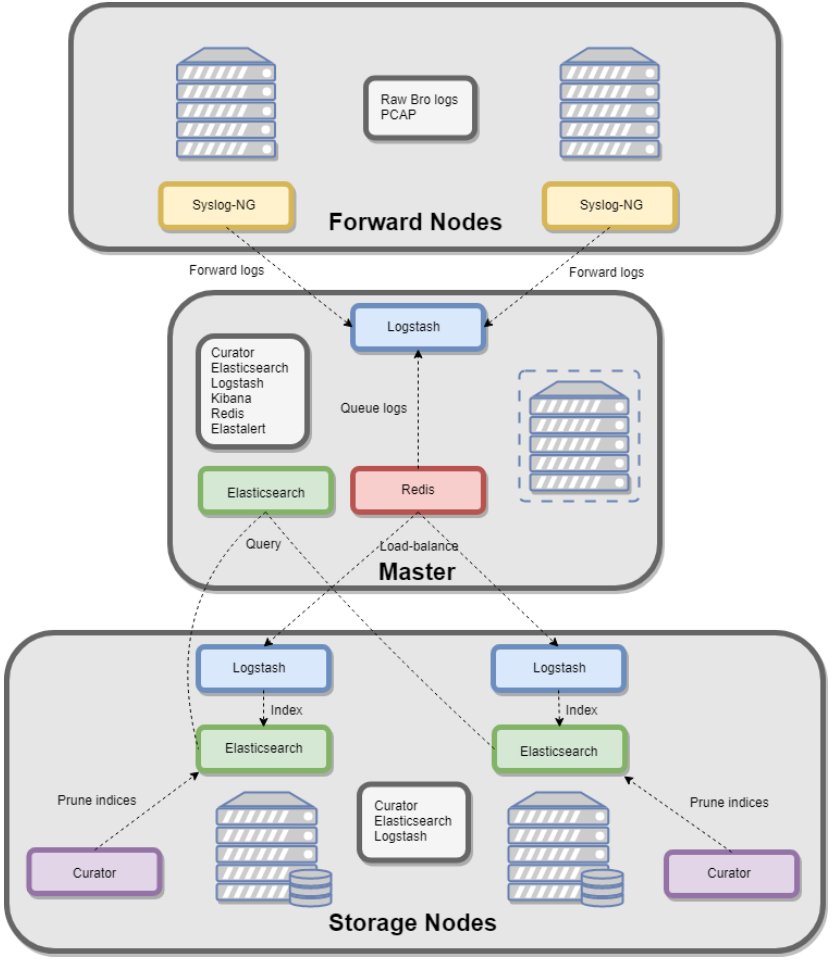
Stand Alone Example



Heavy Distributed Example



Distributed Example



Node Types – Master

- The master runs Elasticsearch, and manages cross-cluster search
- Analysists connect to perform queries and retrieve data
- The Master Node is comprised of:
  - Elasticsearch
  - Logstash
  - Kibana
  - Curator
  - Elastalert
  - Redis (Only if configured to output to a storage node)
  - OSSEC
  - Sguild

Node Types – Forward Node

- Forward nodes capture and forward all logs to the master via an autossh tunnel
- The master stores the forwarded data in Elasticsearch, or forwards the data to the storage nodes (if configured)
- The Forward Node is comprised of:
  - Zeek
  - Snort/Suricata
  - Netsniff-NG
  - OSSEC
  - Syslog-NG

Node Types – Heavy Node

- Heavy Nodes provide distributed deployments with Elasticsearch's cross-cluster search
- The Heavy Node is comprised of:
  - Elasticsearch
  - Logstash
  - Curator
  - Zeek
  - Snort/Suricata
  - Netsniff-NG
  - OSSEC
  - Syslog-NG (forwards logs locally to Logstash)

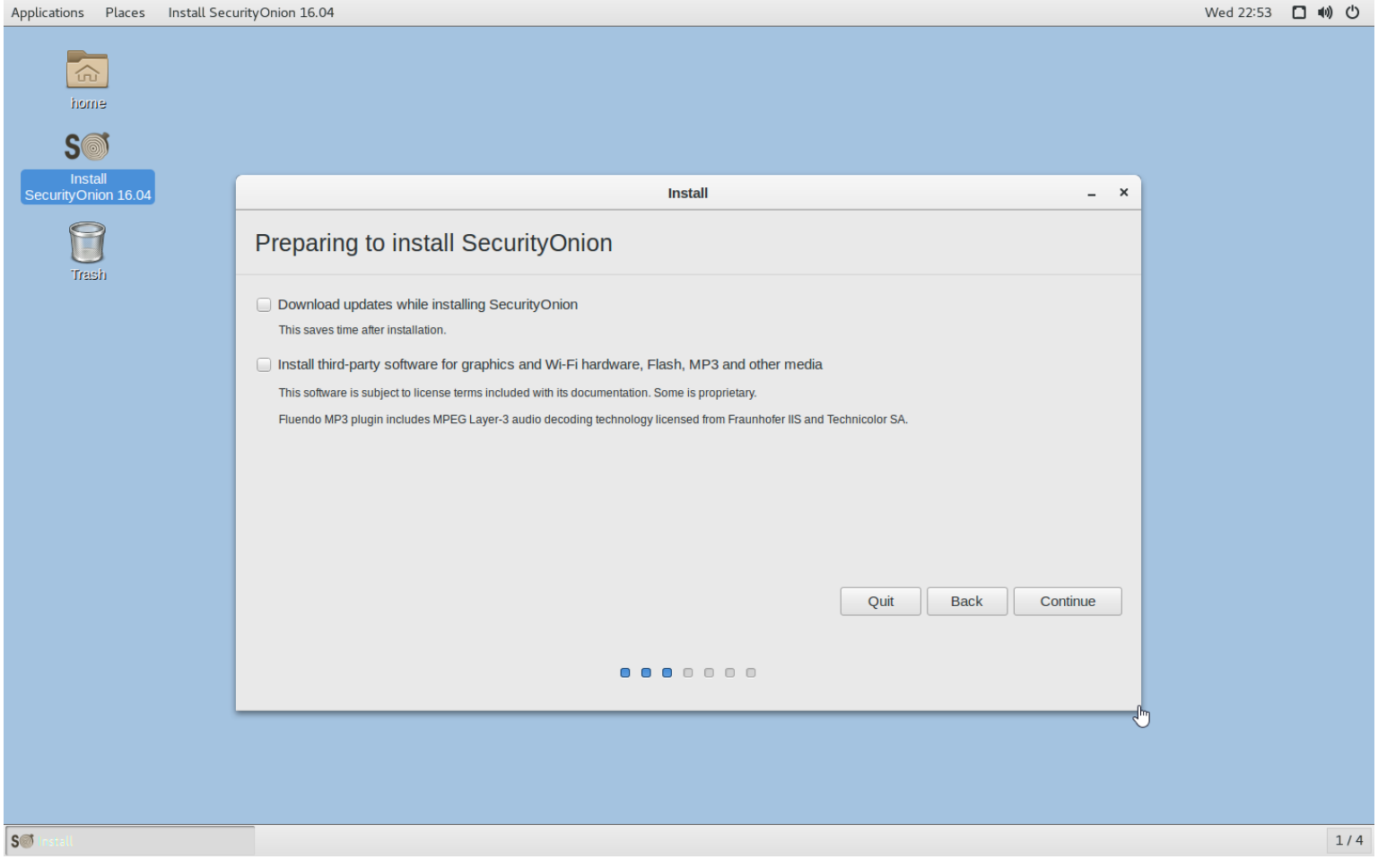
Node Types – Storage Node

- Storage nodes extend the processing and storage capabilities of the master node
- Any data residing on the storage node can be queried by the master via Elasticsearch
- The Heavy Node is comprised of:
  - Elasticsearch
  - Logstash
  - Curator
  - OSSEC

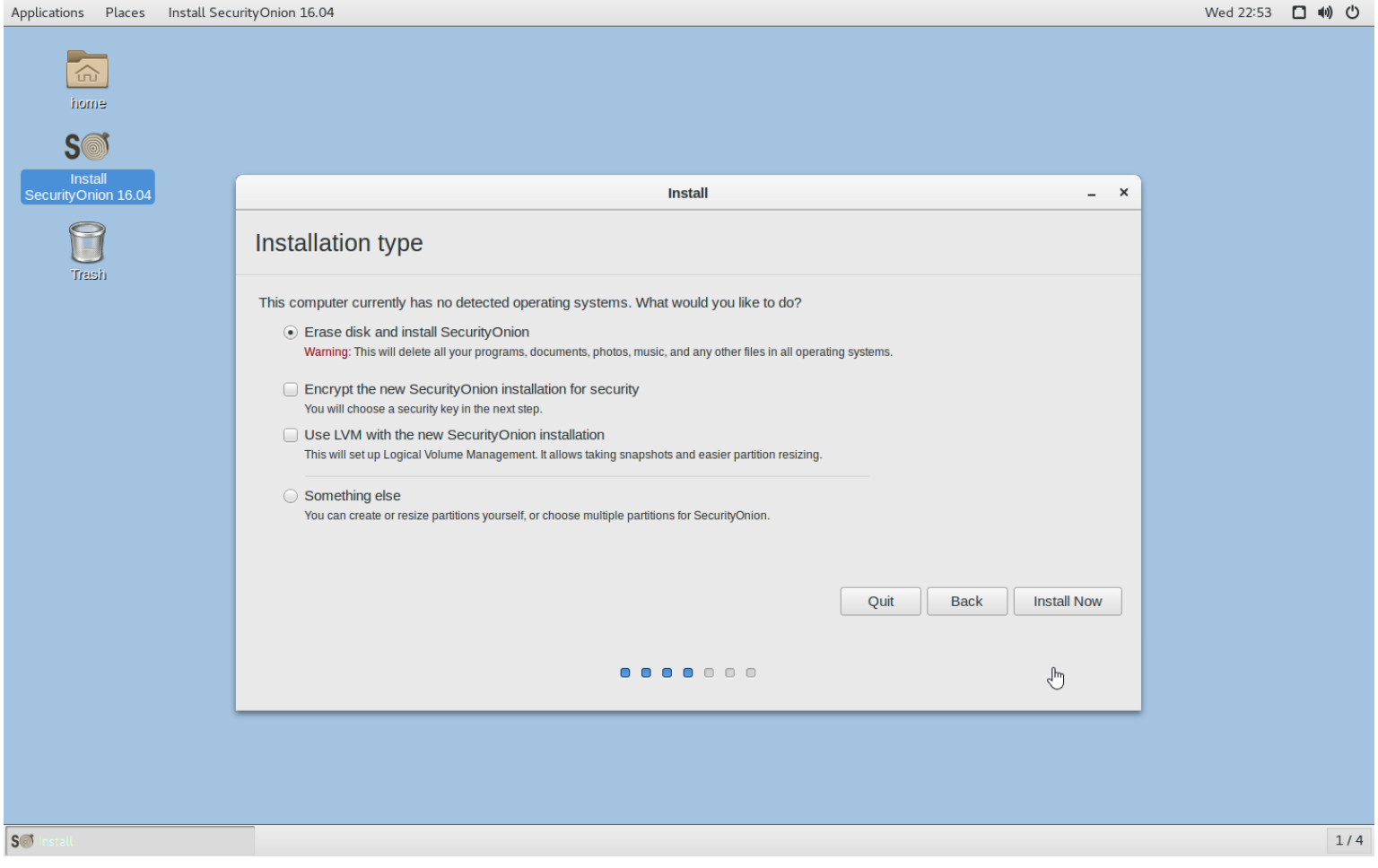
Installing Security Onion

- Security Onion is available as an iso from https://securityonion.net/
- Alternatively, SO can be added to an existing Ubuntu 16.04 machine by adding the SO PPA and packages
- The install iso can be used as a live system for troubleshooting installation issues, or installing SO to your hard drive (required for enterprise use)

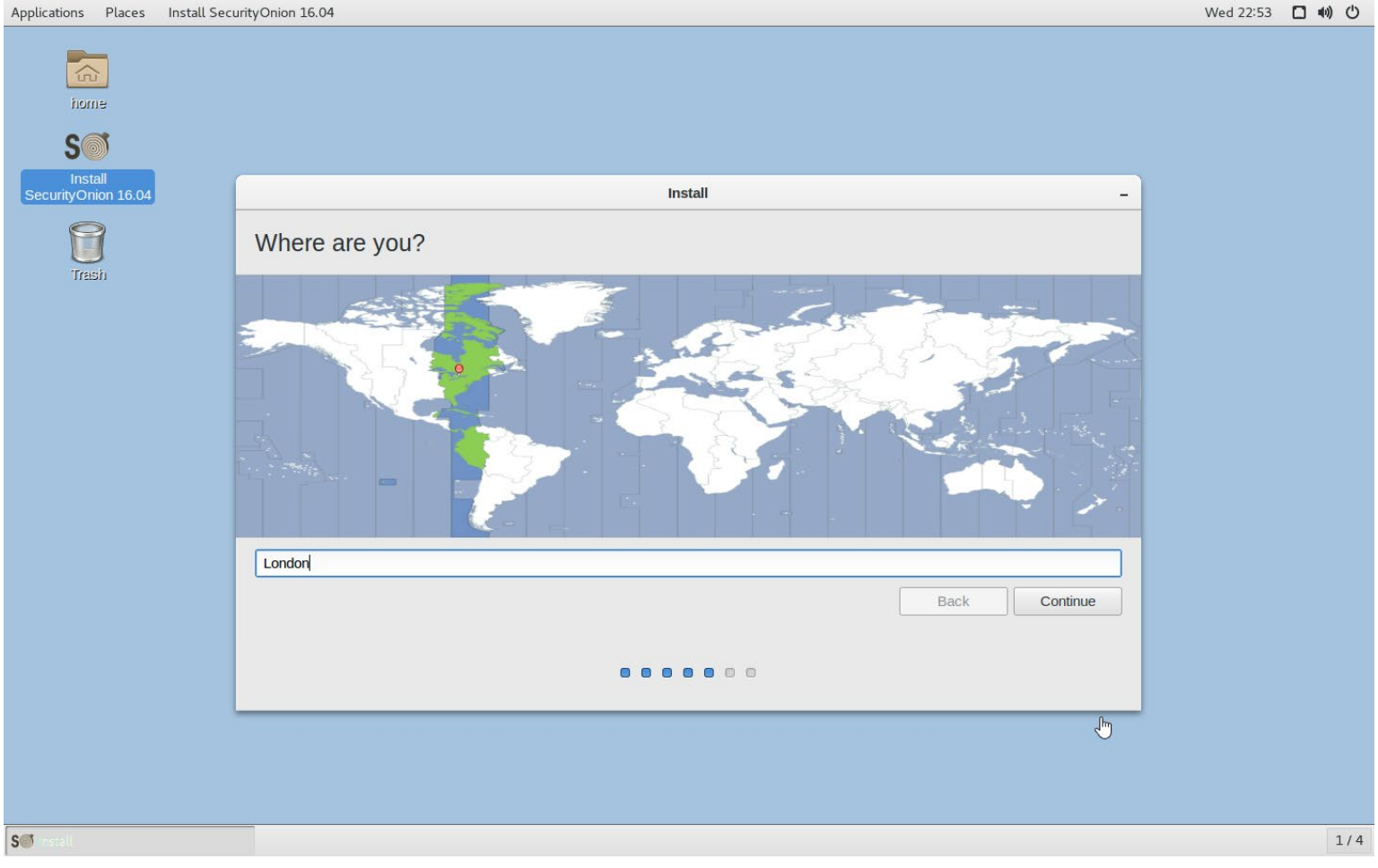
QuickStart – Configuring Security Onion



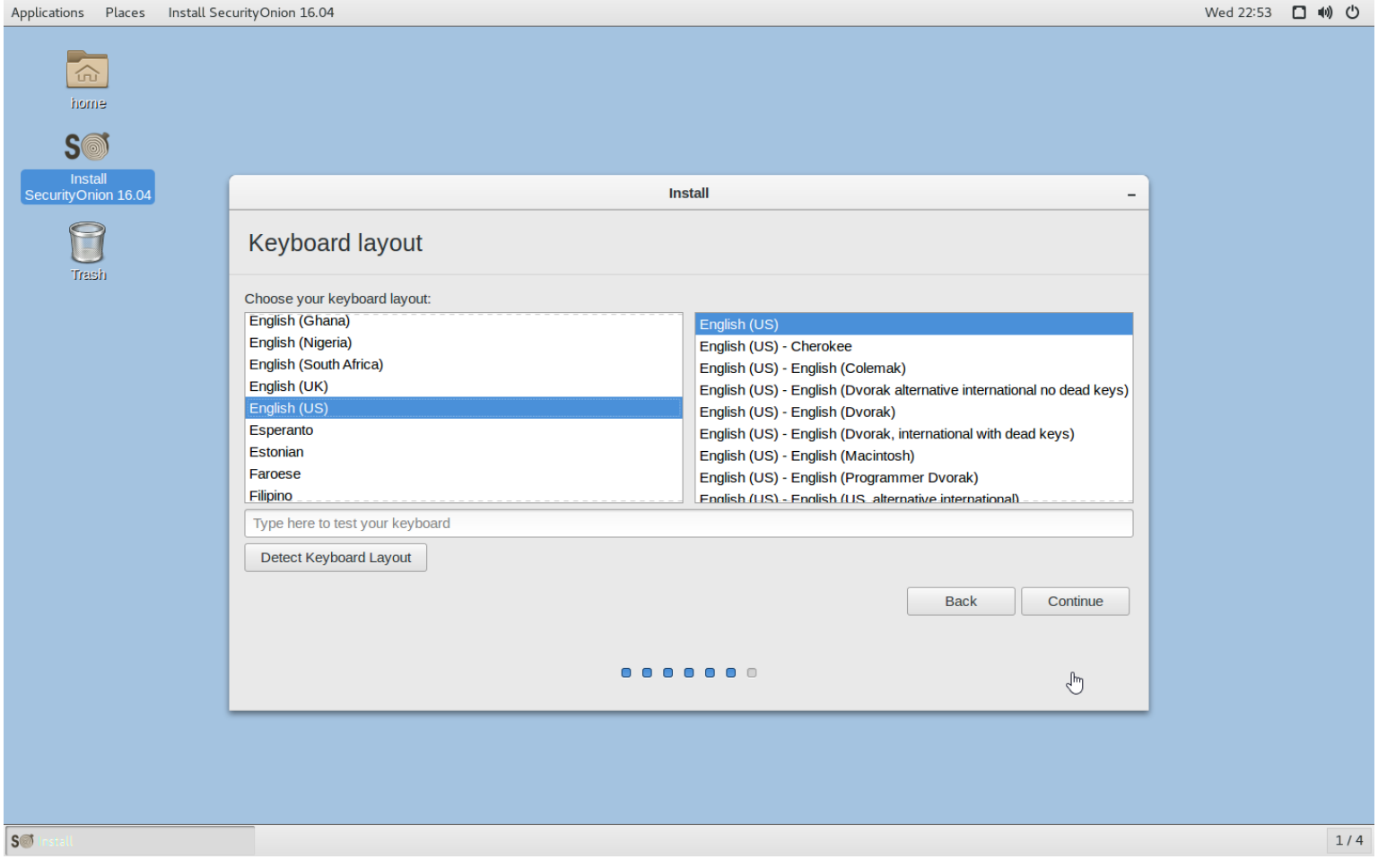
QuickStart – Configuring Security Onion



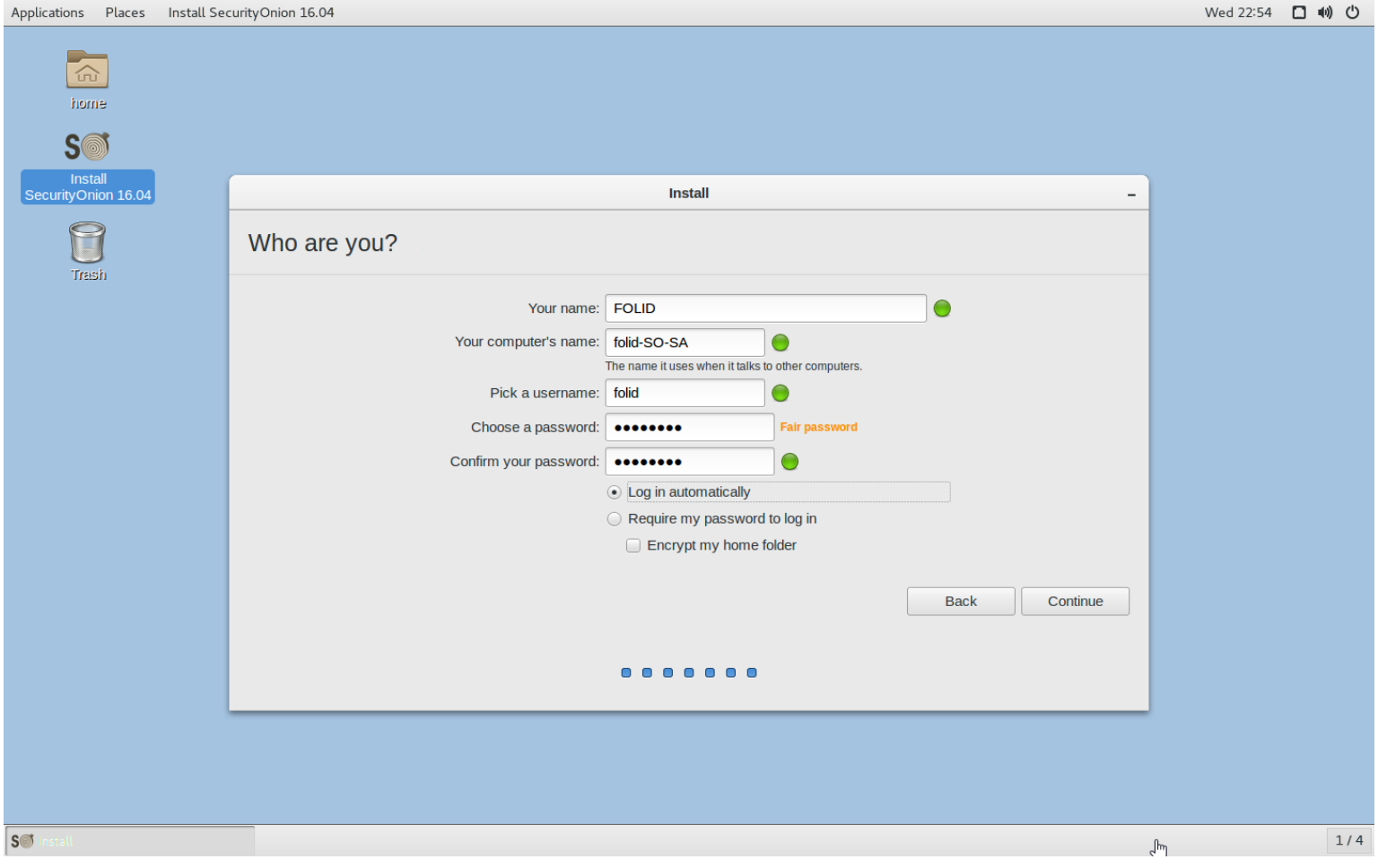
QuickStart – Configuring Security Onion



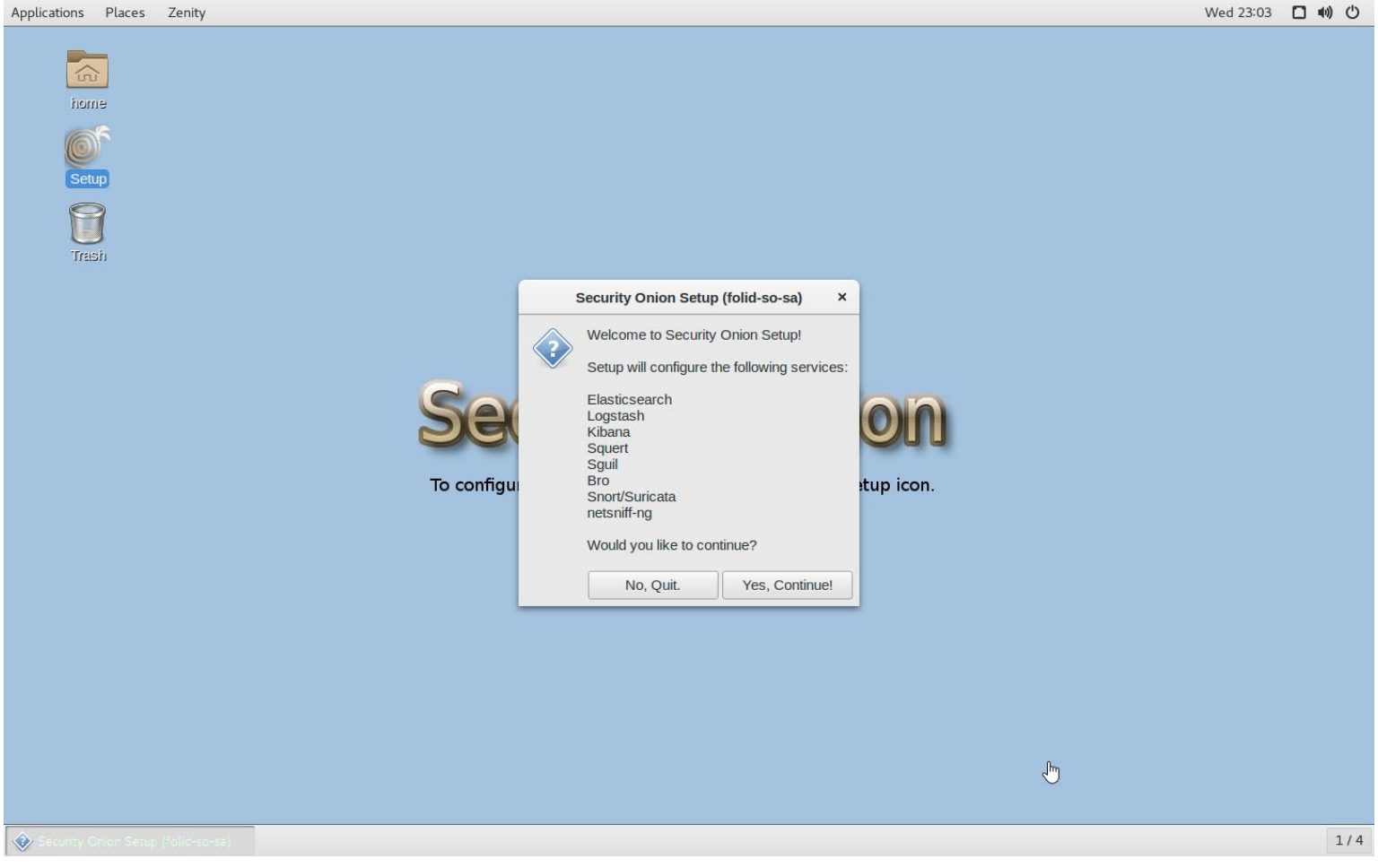
QuickStart – Configuring Security Onion



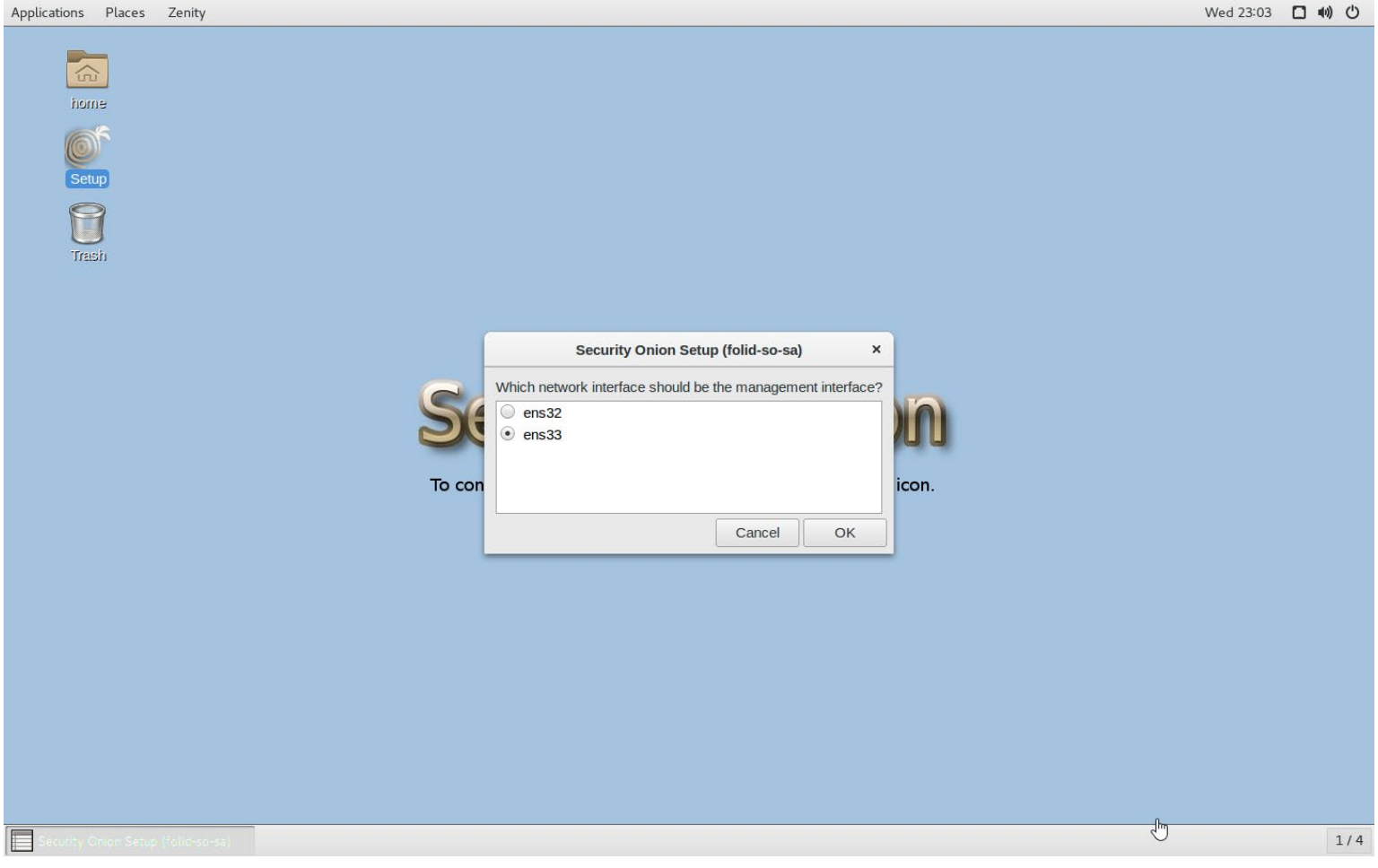
QuickStart – Configuring Security Onion



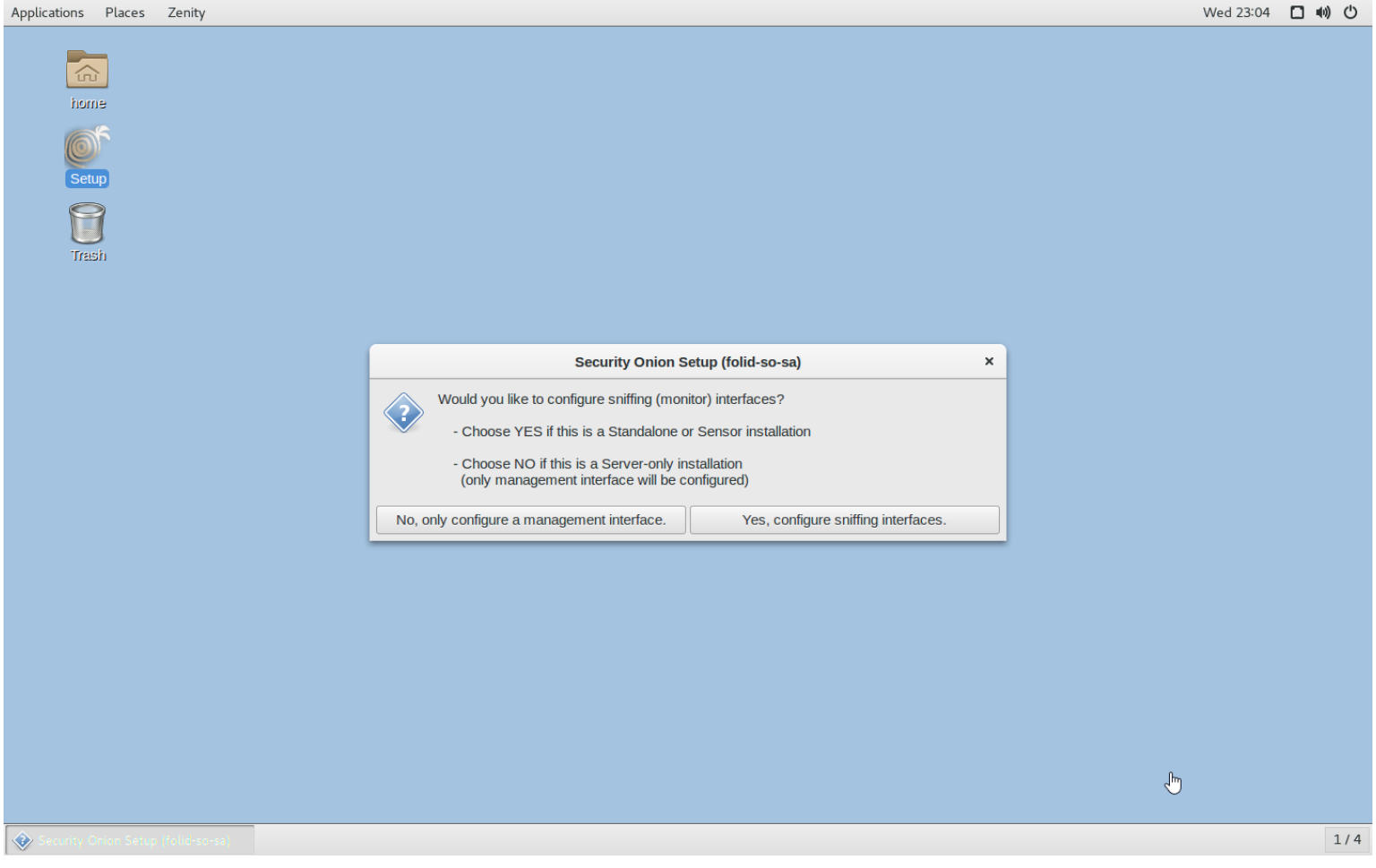
QuickStart – Configuring Security Onion



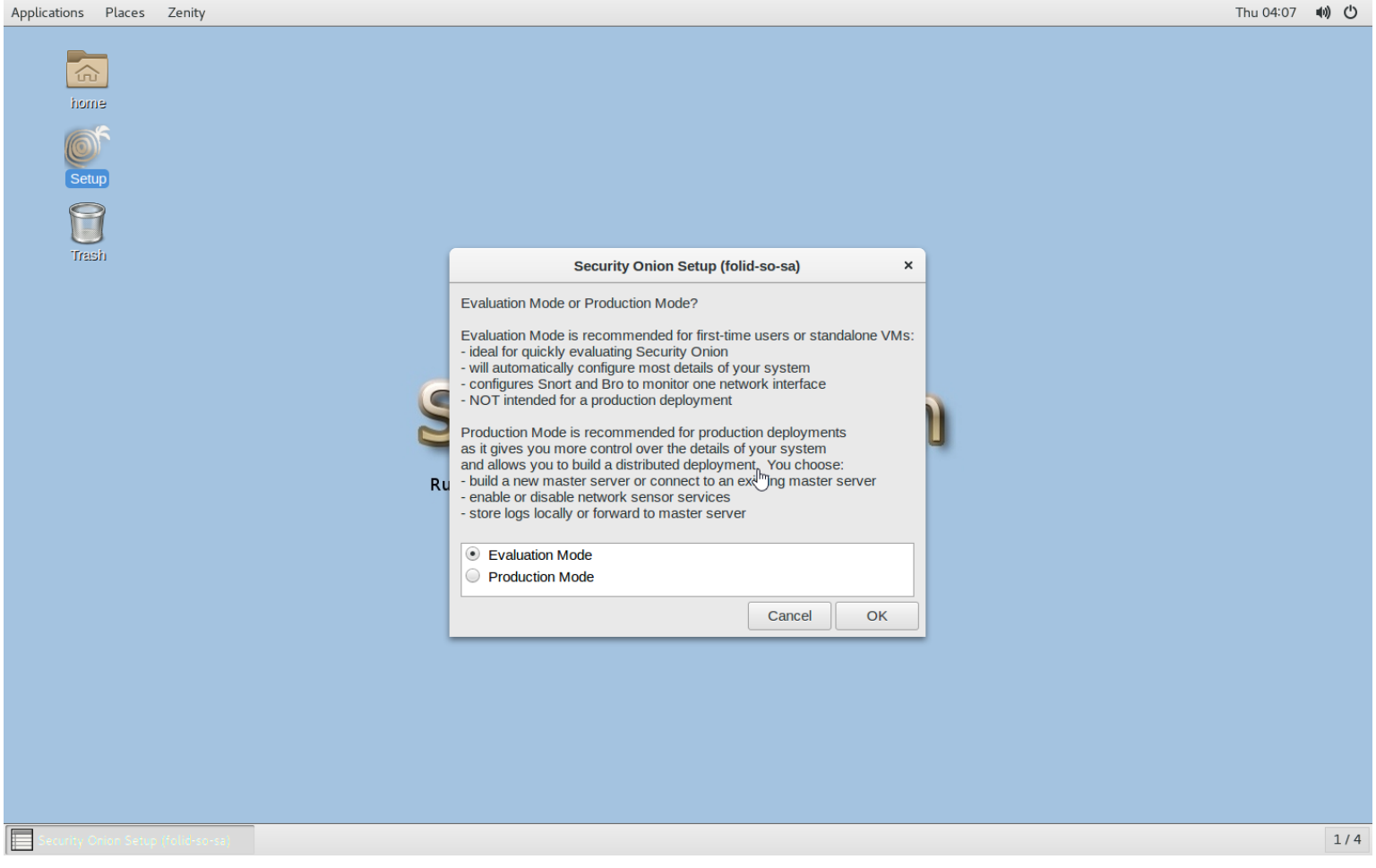
QuickStart – Configuring Security Onion



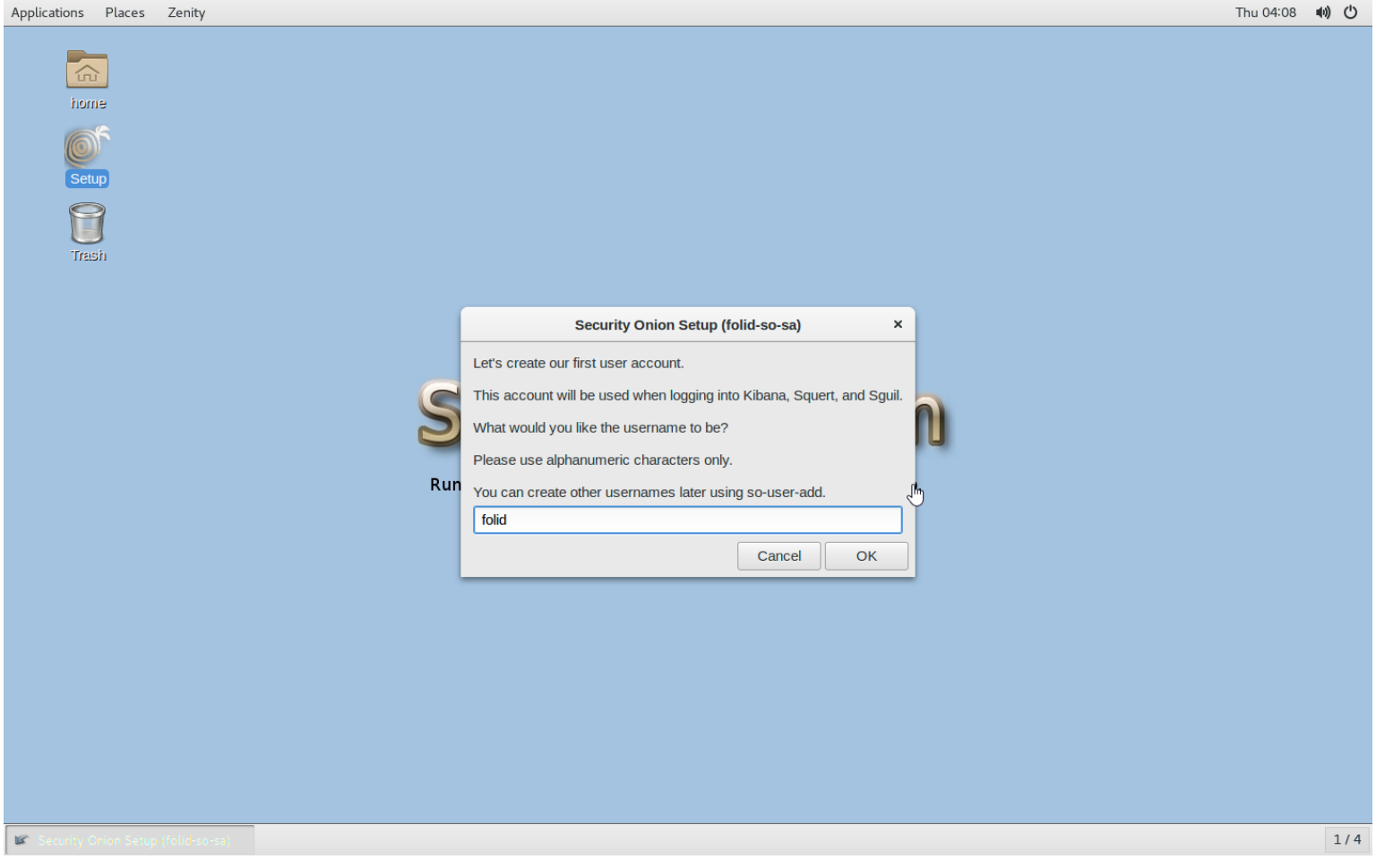
QuickStart – Configuring Security Onion



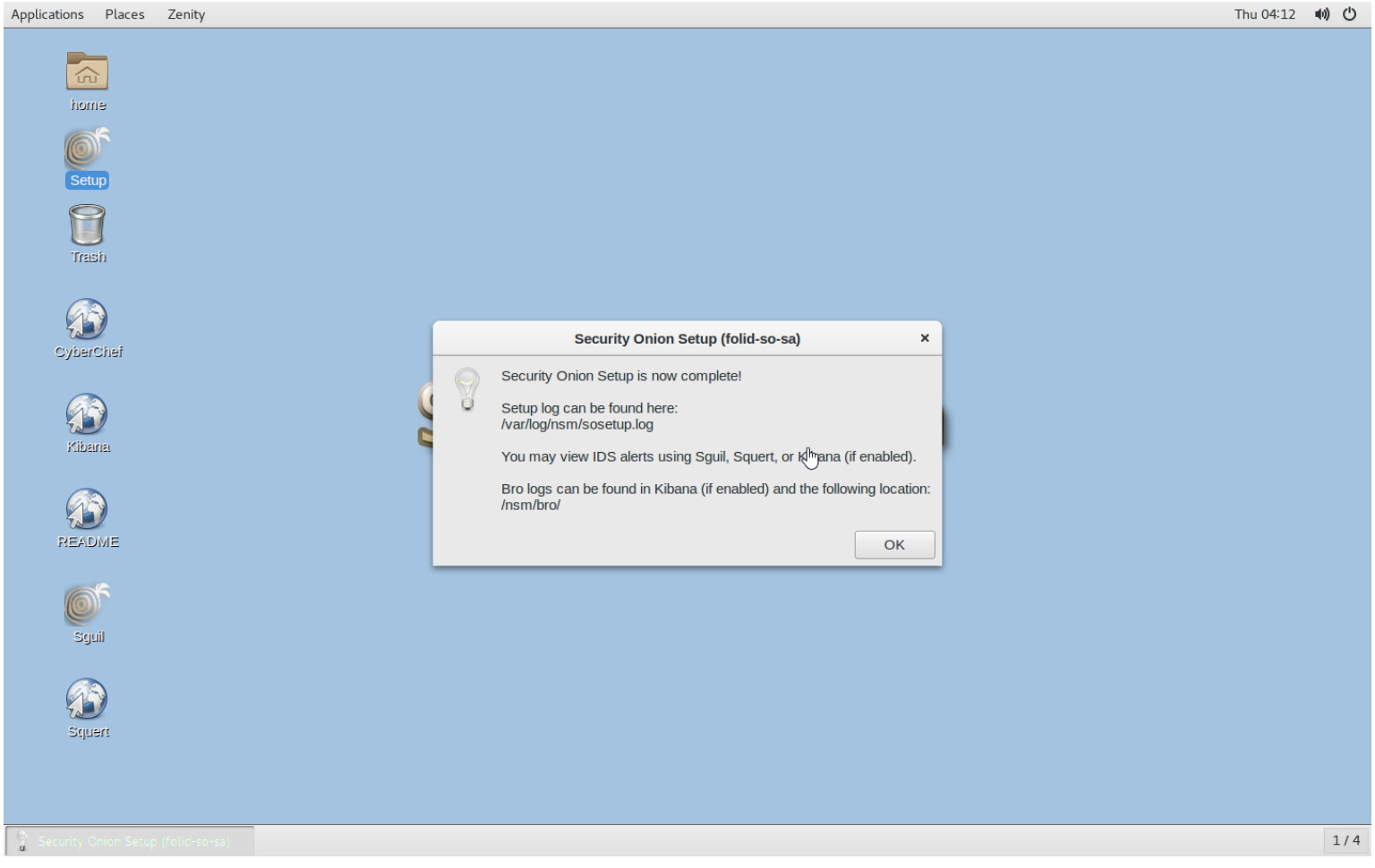
QuickStart – Configuring Security Onion



QuickStart – Configuring Security Onion



QuickStart – Configuring Security Onion



Summary

- Security Onion Core Components include Logstash, Elasticsearch and Kibana
- Analysts connect to tools such as Kibana, CapME, and Squert to analyze network traffic
- SO can be deployed in a number of different configurations, with distributed being the preferred configuration for enterprise environments
- SO node types include, master, forward, storage, heavy and stand-alone
- SO installs similarly to other Linux distributions, with a two-step configuration process required before use

References

- Bejtlich, R. (2013). Chapter 3: Stand-alone NSM Deployment and Installation. In The practice of network security monitoring understanding incident detection and response. San Francisco: No Starch Press.
- Security Onion Solutions. (2020). Security Onion: Security Onion Documentation. Evans, GA: Author.