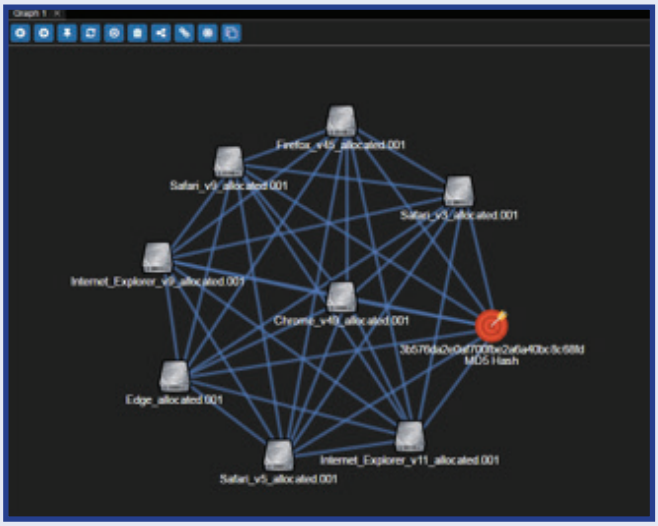
DOD CYBER CRIME CENTER

Technical Solutions Development



MISSING LINKS

Missing Links is a forensic analysis tool suite comprised of two software components: the **Missing Links Explorer** and the **Missing Links Extractor**. The concept originated with a need to support forensic examiners, in both field and lab settings, in quickly identifying "missing" pieces of evidence associated with a case. **Missing Links** leverages the processing power of commercial tools to scale correlation capabilities across thousands of data sources and over a billion forensic artifacts.

MISSING LINKS EXTRACTOR

The Missing Links Extractor is a stand-alone capability, which can be executed in a bootable environment or command-line interface, to extract forensic artifacts from a live machine or forensic copy.

Quickly triage identify cloud storage accounts (e.g., Amazon Drive, DropBox, Apple iCloud), network storage mounts, and physical devices connected to the target machine

Generate an HTML report that can be quickly reviewed by examiners, as well as a SQLite database to allow for machine analysis or ingest into other tools like Missing Links Explorer

MISSING LINKS EXPLORER

The Missing Links Explorer leverages COTS and GOTS tools to ingest data and visualize correlations across small and large collections.

Ingest existing data into a central repository, eliminating the need to reprocess years of collection data

Utilizing a documented API, easily customize and define pertinent data to be ingested into a REDIS or SQLite data repository

Correlate and pivot across multiple devices on a wide variety of forensic artifacts from file hashes to MAC addresses to social media account names

Quickly scale Explorer to increase performance based on the amount of data that your organization ingests

Technologies utilized/supported:

Autopsy® MAGNET FORENSICS Cellebrite Quincy redislabs HOME OF REDIS PostgreSQL