Disk Forensics

As we've previously highlighted, adhering to the sequence of data volatility is crucial. It's imperative that we scrutinize each byte to detect the subtle traces left by cyber adversaries. Having covered memory forensics, let's now shift our attention to the area of `disk forensics` (disk image examination and analysis).

Many disk forensic tools, both commercial and open-source, come packed with features. However, for incident response teams, certain functionalities stand out:

- `File Structure Insight`: Being able to navigate and see the disk's file hierarchy is crucial. Top-tier forensic tools should display this structure, allowing quick access to specific files, especially in known locations on a suspect system.
- `Hex Viewer`: For those moments when you need to get up close and personal with your data, viewing files in hexadecimal is essential. This capability is especially handy when dealing with threats like tailored malware or unique exploits.
- `Web Artifacts Analysis`: With so much user data tied to web activities, a forensic tool must efficiently sift through and present this data. It's a game-changer when you're piecing together events leading up to a user landing on a malicious website.
- `Email Carving`: Sometimes, the trail leads to internal threats. Maybe it's a rogue employee or just someone who slipped up. In such cases, emails often hold the key. A tool that can extract and present this data streamlines the process, making it easier to connect the dots.
- `Image Viewer`: At times, the images stored on systems can tell a story of their own. Whether it's for policy checks or deeper dives, having a built-in viewer is a boon.
- `Metadata Analysis`: Details like file creation timestamps, hashes, and disk location can be invaluable. Consider a scenario where you're trying to match the launch time of an app with a malware alert. Such correlations can be the linchpin in your investigation.

Enter Autopsy: a user-friendly forensic platform built atop the open-source Sleuth Kit toolset. It mirrors many features you'd find in its commercial counterparts: timeline assessments, keyword hunts, web and email artifact retrievals, and the ability to sift results based on known malicious file hashes.

Once you've loaded a forensic image and processed the data, you'll see the forensic artifacts neatly organized on the side panel. From here, you can:

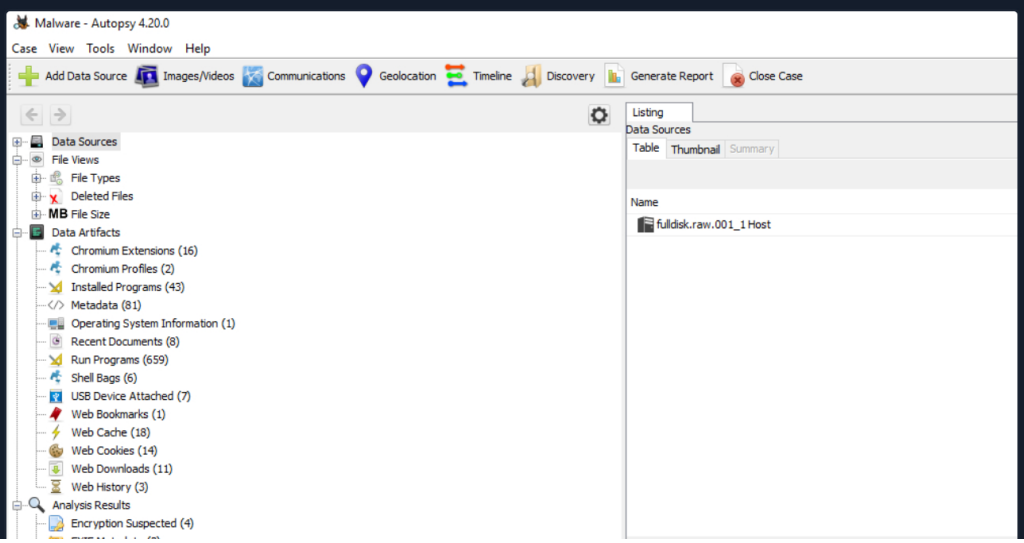


Table of Contents

Introduction to Digital Forensics
Windows Forensics Overview
Evidence Acquisition Techniques & Tools

Evidence Examination & Analysis

Memory Forensics
Disk Forensics
Rapid Triage Examination & Analysis Tools
Practical Digital Forensics Scenario

Skills Assessment

Skills Assessment

My Workstation

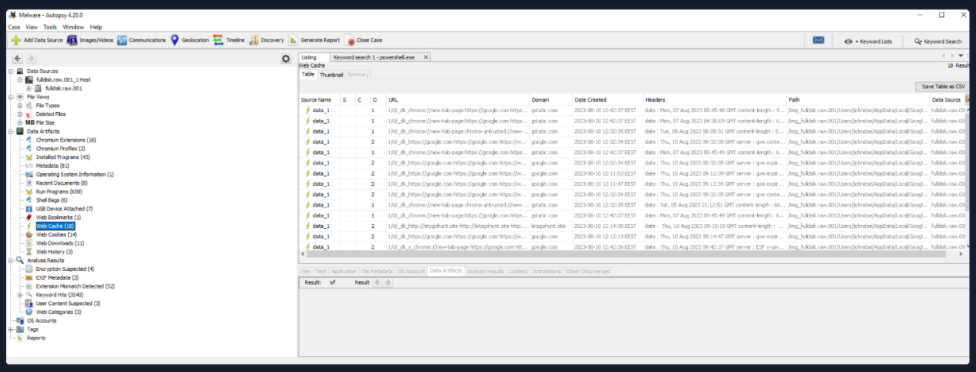
OFFLINE

Start Instance

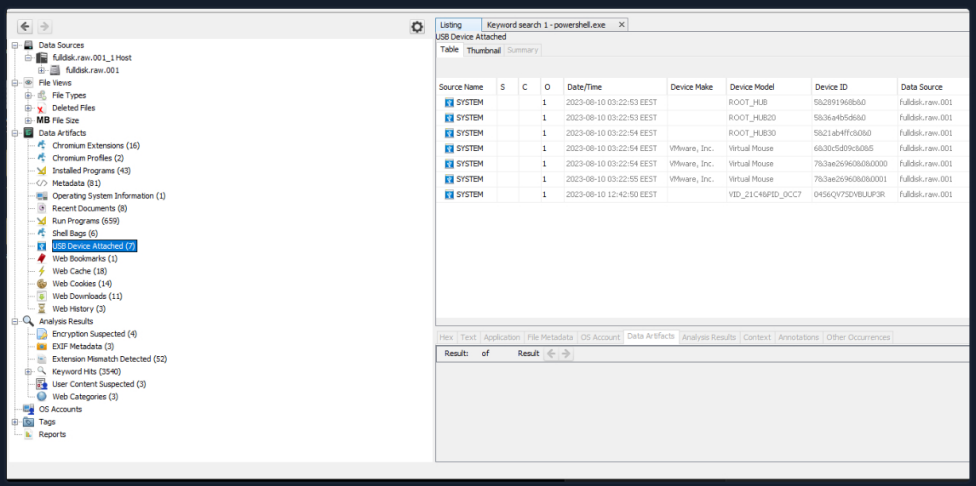
∞ / 1 spawns left

- Dive into `Data Sources` to explore files and directories.

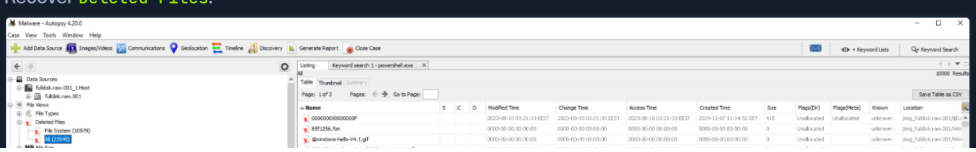
- Examine `Web Artifacts`.

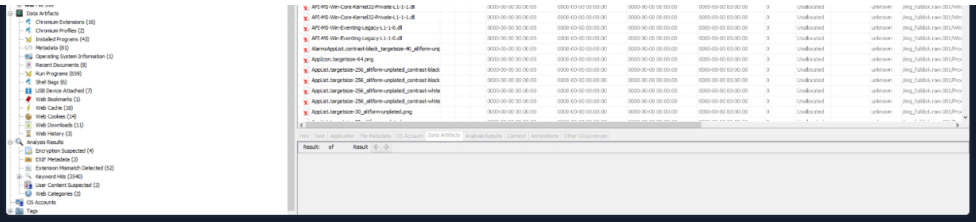


- Check `Attached Devices`.

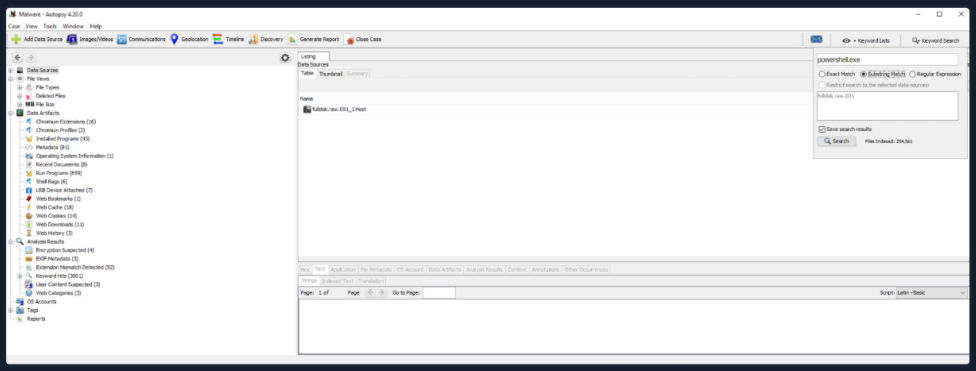


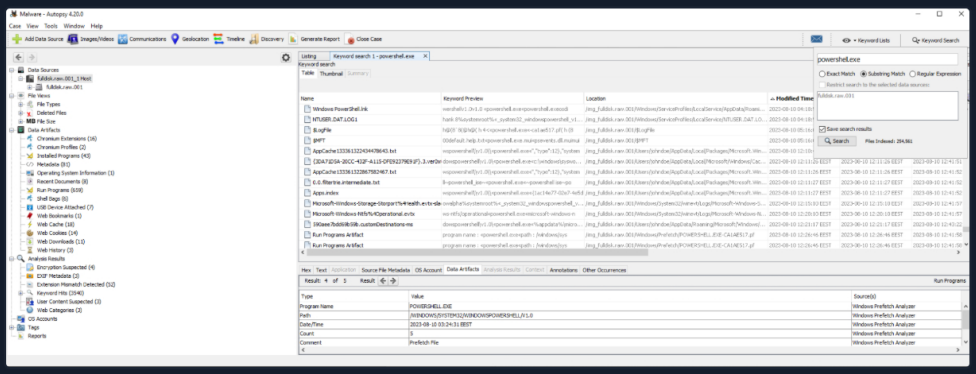
- Recover `Deleted Files`.



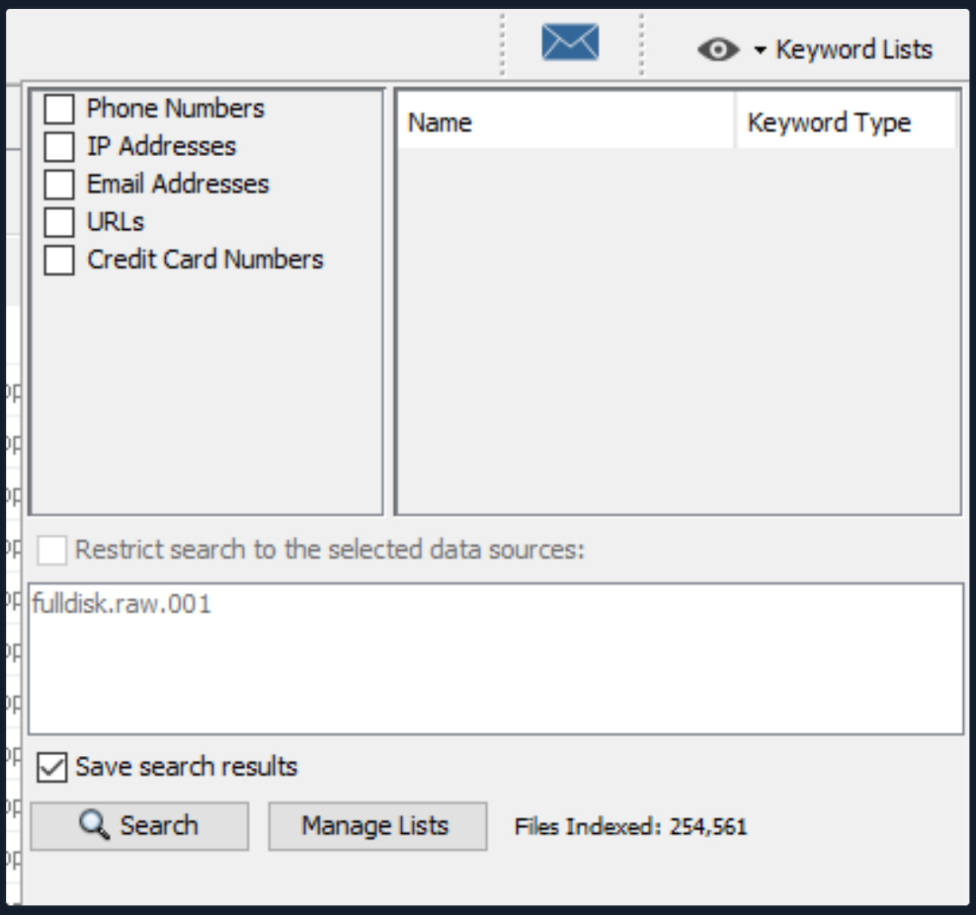


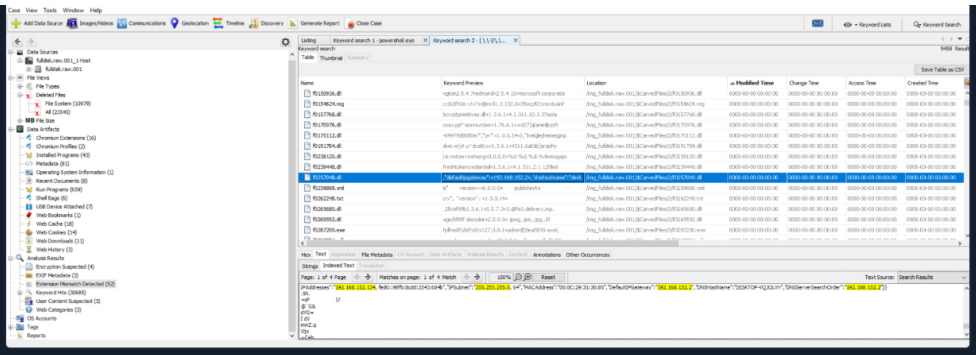
- Conduct `Keyword Searches`.



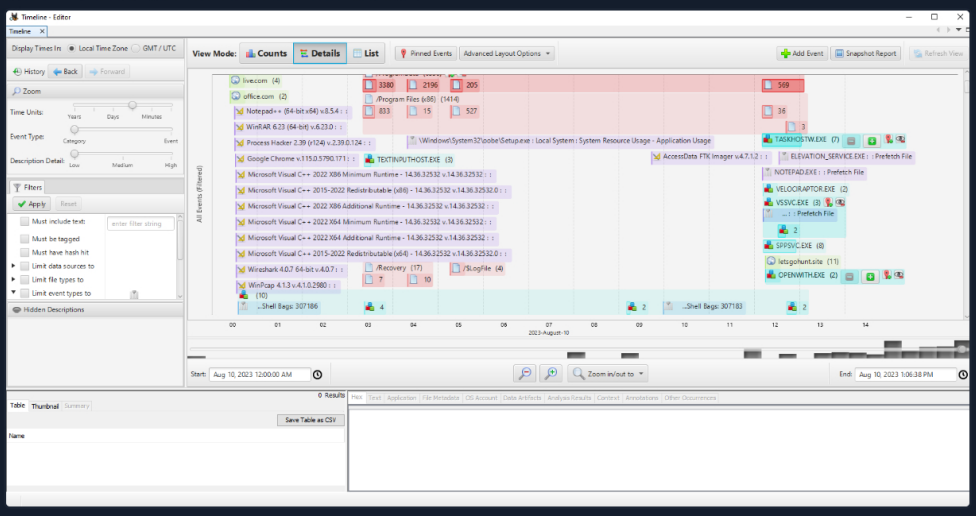


- Use `Keyword Lists` for targeted searches.





- Undertake `Timeline Analysis` to map out events.



We'll be heavily utilizing Autopsy in the forthcoming "Practical Digital Forensics Scenario" section.