Payatu

Getting Started with DFIR

Digital Forensics & Incident Response

Kumar **Ashwin**

About Me

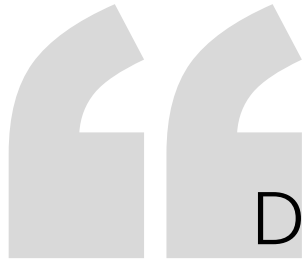
Kumar **Ashwin** (Security Consultant @ Payatu)

Connect with me on 0xCardinal on all socials.

Agenda

- What is Digital Forensics?
- Different Data Sources (Where to find evidence?)
- Chain of Custody
- Need For Digital Forensics
- Browser Forensics
- Challenges & Concerns
- What Next?

What is **Digital Forensics?**



Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.

Source: eccouncil.org

Different Data Sources

- Logs
- Metadata
- Social Media Activity
- Prefetch Files
- LNK Files
- RAM
- Etc.

any device that can store/retrieve data from…

Steps of Digital Forensics

Identification

Preservation

Analysis

Documentation & Presentation

~~Steps of Digital Forensics~~

Chain of Custody

Identification	**Preservation**	**Analysis**	**Documentation & Presentation**

Need for Digital Forensics

- Determining the cause and potential intent of a cyberattack.
- Protecting digital evidence from the attack before it becomes obsolete.
- Increasing security hygiene, tracing hacker paths, and locating hacker tools.
- Looking for data access/extraction.
- Determining the duration of unauthorized network access.
- Etc.

Segregation in Digital Forensics

Disk Forensics

Network Forensics

Wireless Forensics

Database Forensics

Malware Forensics

Email Forensics

Memory Forensics

Browser Forensics

Mobile Forensics

•••

Browser Forensics

- Browsers are considered a goldmine because of the amount of information they contain.

Browser Artifacts

- Artifacts are the files stored in the operating system in some specific directories.
- Each browser stores its files in a different place than other browsers and they all have different names
- Navigation History, Autocomplete Data, Cache, Logins, Browser Sessions, Downloads, etc.

Browser Artifacts

- Each Browser has different paths to store data.
- Mozilla Firefox

  ```
  C:\Users\XXX\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default-release\
  ~/.mozilla/firefox/
  ```

- Chrome

  ```
  C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default
  ~/.config/google-chrome/
  ```

- The artifacts in these locations are different files – txt, json, database files, etc. which store all the information about the browser and all the activities performed on it.

Chain of Custody (Browsers Forensics)

- **Identification**
  - Now we have identified the artifacts that we need to analyze.
  - In our case, it's the data from the browser.

- **Preservation**
  - We can use tools like FTK imager or something similar to get a copy of original data that is to be analyzed.
  - This stage is very much crucial, as we need to perform tasks without much tampering the evidence.
  - And if we perform the analysis in the evidence, we are tampering it, hence we need to preserve the state of the evidence.

Chain of Custody (Browsers Forensics)

- **Analysis**
  - Now that we have the image (E01 extension[1]), we can use it to open it in different tools like Autopsy to analyze.
  - This is the most creative part of the process, as here we figure out different activities performed, to support our case.

- **Document & Presentation**
  - The most important aspect of the process is the documentation of the complete process and what all things you have done as an investigator.
  - And presenting the relevant information that is easy to understand by a non-technical person is a skill must have to be in this field.

Challenges & Concerns

- Anti-forensics
- Evolving Technologies
- Increase in volume of evidence
- The single approach does not work anymore
- Legal Challenges
- Strong encryption techniques

What Next?

- Resources
  - SANS DFIR Cheat Sheets
  - HackTricks Browser Artifacts Notes
  - Private Browser Forensics Research Paper
- Labs
  - CyberDefenders
- Google Everything and Explore

QnA?

Introduction to DFIR | Payatu Webinar

Kumar **Ashwin** | Connect at **0xCardinal**