Experiment- 4

Live Incident Response

1. Perform live incident response on a system

2. View all browser history in a computer

3. List out all established network connections in a computer Hint: Triage Incident Response

Title: Live Incident Response using Triage Method

1. Aim

To perform **Live Incident Response** on a running computer system and collect volatile evidence such as **running processes, browser history, and active network connections** using **Triage Incident Response techniques**.

2. Objectives

- To understand the concept of **Live Incident Response**
- To collect **volatile data** from a running system
- To view **browser browsing history**
- To identify **established network connections**
- To learn **basic incident response commands**

3. Tools / Software Required

- Windows Operating System
- Command Prompt (Administrator Mode)
- Web Browser (Chrome / Edge / Firefox)

4. Theory

Live Incident Response

Live Incident Response is the process of collecting and analyzing **volatile data** from a system **while it is powered ON**.
This method is used when shutting down the system may result in loss of important evidence such as:

- Running processes
- Network connections
- Logged-in users
- RAM data

Triage Incident Response

Triage Incident Response focuses on:

- **Quick identification of threats**
- **Prioritizing critical evidence**
- **Minimal system disturbance**

5. Procedure

Task1: Perform Live Incident Response on a System

Step-by-Step Process

1. Power ON the system
2. Login with **Administrator account**
3. Open **Command Prompt as Administrator**
4. Record current system **date and time**
5. date
6. time
7. Check logged-in users
8. query user
9. View running processes
10. tasklist
11. View running services
12. net start
13. Observe system startup programs
14. wmic startup get caption,command

Note:

- Do not shut down the system
- Avoid unnecessary file creation or deletion

Task2: View All Browser History in a Computer

Method 1: Using Browser Interface

1. Open the web browser (Chrome / Edge / Firefox)
2. Press **Ctrl + H**
3. The complete browsing history will be displayed
4. Observe:
    - Visited websites
    - Date and time
    - Search keywords

Method 2: Browser History File Location

Google Chrome:

C:\Users\Username\AppData\Local\Google\Chrome\User Data\Default\History

Mozilla Firefox:

places.sqlite

These files can be analyzed using forensic tools if required.

Task3: List All Established Network Connections

(Triage Incident Response)

Step-by-Step Process

1. Open **Command Prompt (Administrator mode)**
2. Run the following command:
3. netstat -an | find "ESTABLISHED"
4. Observe the output:
    - Local IP Address
    - Remote IP Address
    - Port Numbers
    - Connection State

Advanced Analysis

1. To view process ID (PID):
2. netstat -ano
3. Match PID with running process:
4. tasklist | find "PID"

6. Observations

- System date and time were recorded successfully
- Active users and running processes were identified
- Browser browsing history was accessed
- Established network connections were listed

7. Result

Thus, **Live Incident Response** was successfully performed on a running system using **Triage Incident Response techniques**, and volatile evidence such as **processes, browser history, and network connections** was collected.

8. Precautions

- Do not shut down the system during investigation
- Avoid installing new software
- Use administrator privileges carefully
- Maintain evidence integrity

9. Viva Voce Questions

1. What is Live Incident Response?
2. What is volatile data?
3. Why is netstat command used?
4. What is Triage Incident Response?
5. What happens if the system is shut down?

----------Lab Manual End----------

What is Triage in Triage Incident Response?

Meaning of the word "Triage"

Triage ane word **medical field** nundi vachindi.

Hospital lo emergency situation lo:

- Doctors **andarini okesari treatment cheyyaleru**
- So they **prioritize patients** based on seriousness

Same concept Digital Forensics lo apply chestharu.

Triage – Simple Definition

"Triage means **quickly identifying, sorting, and prioritizing important evidence** during an incident so that the most critical data is handled first."

Triage in Incident Response – Explanation

When a cyber incident occurs:

- Time is very less
- Data chala ekkuva untundi
- System ON state lo untundi

So investigator:

- **Everything analyze cheyyadu**
- **Important & dangerous evidence first** collect chesthadu

Idi Triage Incident Response

Why Triage is Important?

Because:

- Volatile data (RAM, network connections) **system OFF ayithe pothundi**
- Malware **hide or escape** avachu
- Attack **spread avvachu**

So **quick decisions** must be taken.

What is Collected First in Triage?

Priority order:

1. **Running Processes**
2. **Network Connections**
3. **Logged-in Users**
4. **RAM-related data**
5. **System Time**

One-Line Exam Answer

Triage Incident Response is the process of **quickly identifying and prioritizing critical evidence from a live system to prevent loss of volatile data.**

Real-Time Example

System hack ayindi anukondi:

- You will NOT first copy all files
- First you check:
  - netstat → suspicious connections
  - tasklist → unknown processes

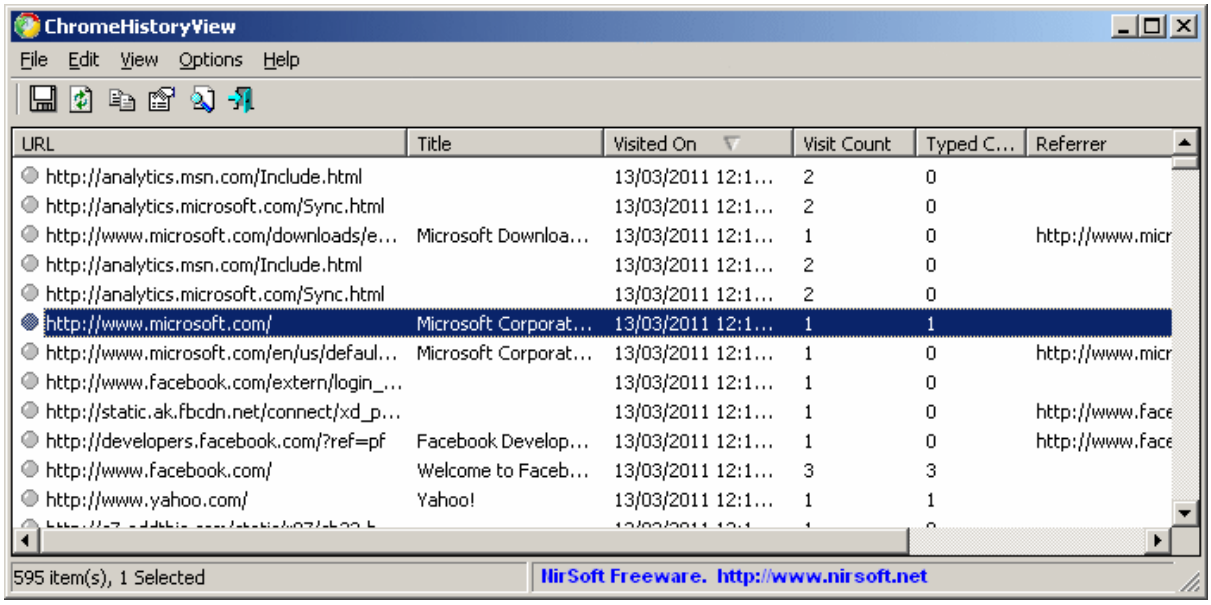
This quick checking = TRIAGE

Difference: Normal IR vs Triage IR

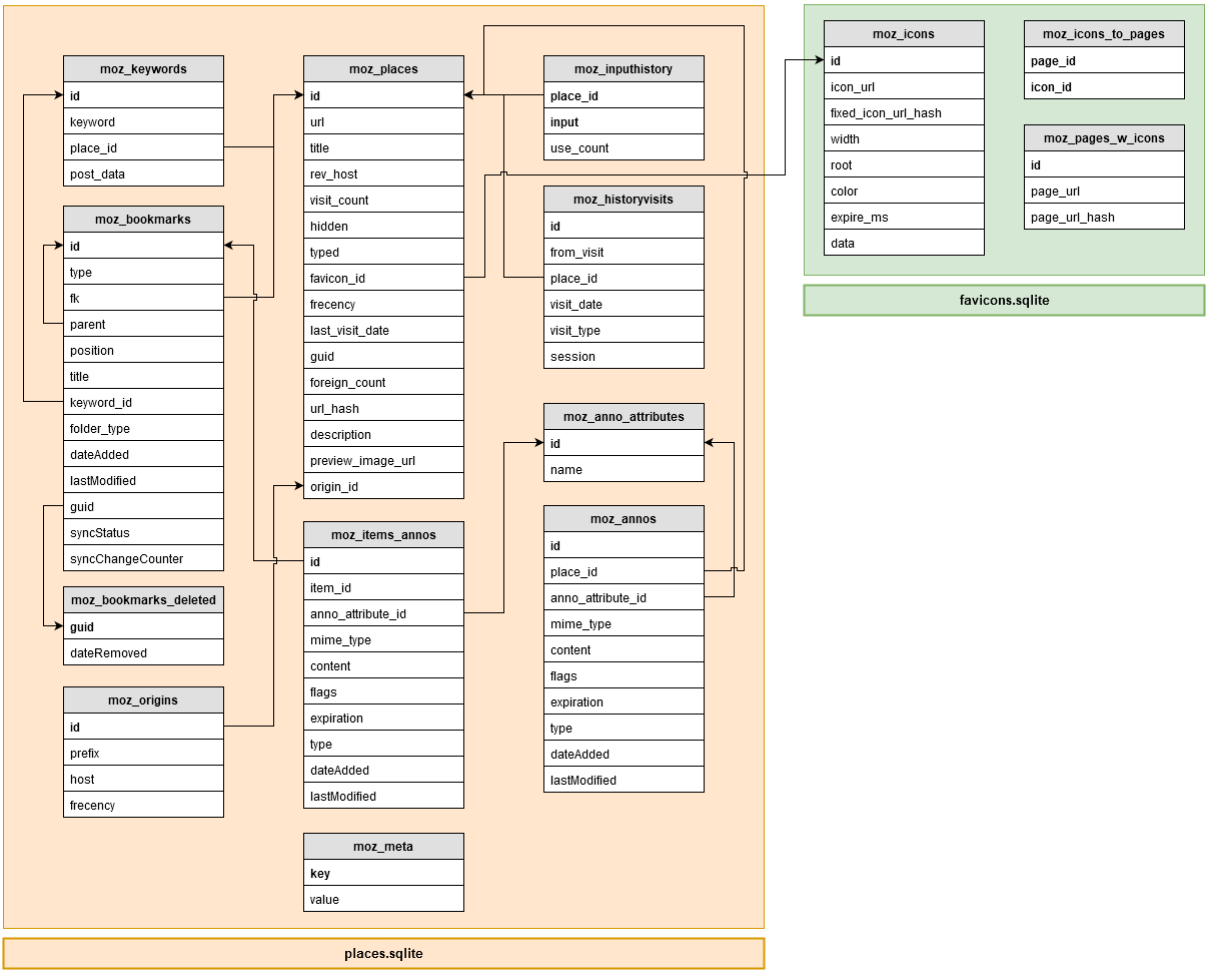
Normal Incident Response	Triage Incident Response
Detailed analysis	Quick analysis
Time consuming	Time critical
Full disk analysis	Live volatile data

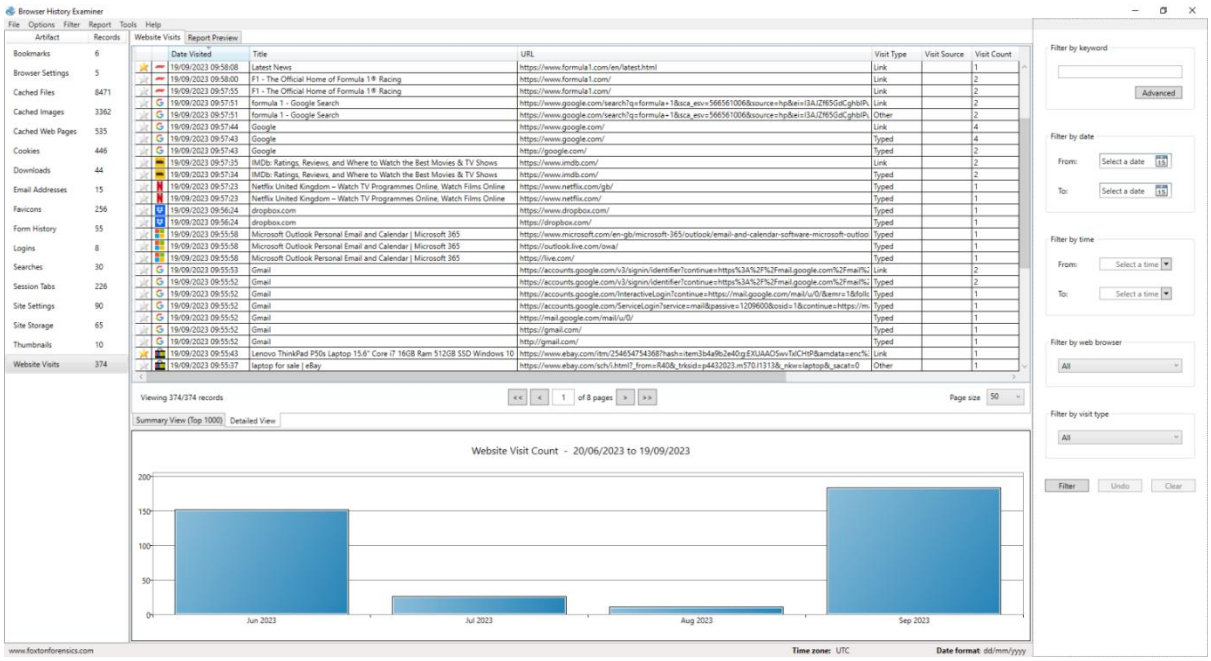
Easy Memory Trick
Triage = Emergency Room Thinking

- Emergency → Priority → Quick action



2019/07/09 - Firefox 68 - v52 - https://github.com/crazy-max/firefox-history-merger





What does "Browser History File Location" mean?

Simple ga cheppali ante
Browser (Chrome / Firefox) **mee visited websites list ni okka file lo store chesthundi**
Aa file ni **forensic tools tho open chesi history chudachu**

First Important Point (Beginner Note)

Ee file **normal double-click cheste open avvadu**
Idi **forensic / database file**

Google Chrome – History File Explained

File Path:

C:\Users\Username\AppData\Local\Google\Chrome\User Data\Default\History

Step-by-Step Meaning:

- C:\Users\Username\ → Mee computer user name
- AppData → Hidden folder
- Google\Chrome\User Data\Default\ → Chrome user profile
- History → **Browser history database file**

Ee file lo:

- Visited websites
- Date & time
- Search keywords

How Forensic Tools Use This?

1. **FTK Imager open cheyyandi**
2. Browser **History file ni add cheyyandi**
3. Tool **automatically history readable format lo chupistundi**

Human readable format (URLs, time, titles)

Mozilla Firefox – places.sqlite Explained

File Name:

places.sqlite

Where is it located?

C:\Users\Username\AppData\Roaming\Mozilla\Firefox\Profiles\

Meaning:

- places.sqlite is a **SQLite database**
- Firefox history + bookmarks store chesthundi

Firefox History Forensic Analysis

1. **Do NOT open with Notepad**
2. Open using:
    - FTK Imager
    - Autopsy
    - DB Browser for SQLite

Appudu history clear ga kanipistundi

Why Not Use Ctrl + H Always?

Ctrl + H	History File
User can delete history	File data may still exist
Shows only current user	Shows forensic artifacts
Not reliable for evidence	Court-usable evidence

Simple Exam Explanation (You Can Write This)

Browser history is stored in internal database files such as **History** in Google Chrome and **places.sqlite** in Mozilla Firefox. These files cannot be opened normally and are analyzed using forensic tools to recover browsing activity.

One-Line Easy Memory

Ctrl + H = Normal User
History file = Forensic Investigator