**Detection of Cryptomining application from the originating from browser using network captured data**

**Digital Forensics (Network & RAM)**

**CDAC, Noida**

**CYBER GYAN VIRTUAL INTERNSHIP PROGRAM**

**Submitted By:**

Ujjwal Kumar

Mr. Mahesh Adsure , (May-June) 2024

**BONAFIDE CERTIFICATE**

This is to certify that this project report entitled **Detection of cryptomining application from the originating from browser using network captured data** submitted to CDAC Noida, is a Bonafede record of work done by **Ujjwal Kumar** under my supervision from **6th June 2024** to **25th June 2024.**

(Signature) (Signature)

HEAD OF THE DEPARTMENT SUPERVISOR

**Declaration by Author(s)**

This is to declare that this report has been written by me. No part of the report is plagiarized from other sources. All information included from other sources have been duly acknowledged. I aver that if any part of the report is found to be plagiarized, I shall take full responsibility for it.

Name of Author : Ujjwal Kumar

**TABLE OF CONTENTS**

1. Problem Statement ….............................................. 1

2. Learning Objective …................................................ 1

3. Approach.................................................................. 2

3.1. Tools and Technology Used…........................ 2

3.2 Infrastructure Setup ……………………………………2

4 . Implimentation ...................................................... 3

4.1. Install and Configure Tools ……………………….. 4

4.2. Capture Network Traffic …………………………… 6

4.3. Create Forensic Image …………………………….. 7

4.4. Data Analysis ……………………………………………..8

5. Conclusion and Recommendations …………........... . 9

5.1. Conclusion …………………………………………………9

5.2 Countermeasures ………………………………………11

6. List of References .................................................. 11

**ACKNOWLEDGEMENT**

I would like to offer my heartfelt gratitude to all persons and institutions that contributed to the successful completion of this research, which focused on detecting cryptomining activity from a browser using network-captured data analysis.   
  
First and foremost, I want to express my gratitude to Mr. Mahesh Adsure, my project adviser, for his great guidance, support, and encouragement during the project's duration. His knowledge and views were critical in determining the direction and scope of this study.  
  
I am grateful to the Centre for Development of Advanced Computing (CDAC) Noida, part of the Ministry of Electronics and Information Technology (MeitY), Government of India, for providing the necessary resources and environment for the successful completion of this research. CDAC Noida's facilities and support were critical for undertaking thorough forensic investigation and network traffic examination.  
  
Furthermore, I want to thank the creators and contributors to the important tools used in this project, notably FTK Imager, Wireshark, and Python libraries like pyshark and pyad. The open-source contributions from these tools were critical to the forensic investigation and network traffic assessment carried out throughout this study.

Finally, I'd like to recognize my family and friends' continuous support and understanding during this effort.  
  
Thank you for your important contributions and encouragement.  
  
Sincerely,   
Ujjwal Kumar

**Detection of cryptomining application from the originating from browser using network captured data**

**PROBLEM STATEMENT:**

SOC alerted that there is some traffic related to crypto mining from a PC that was just joined to the network. The incident response team acted immediately, observed that the traffic is originating from browser applications. After collecting all key browser data using forensic imaging application, it is your job to use the ad1 file to investigate the crypto mining activity.

So, create a Cryptomining application and then detect the same using the browser forensic.

**Learning Objective**

• Experience FTK Imager for forensic imaging, including creating and verifying images of digital storage devices.   
• Learn Wireshark to capture and analyze network traffic, including filtering and packet analysis.  
• Develop and install a rudimentary cryptomining application in JavaScript and HTML.   
• Use Python scripting to automate forensic data extraction and analysis, improving efficiency and accuracy in detecting suspicious actions.   
• Understand how to document the forensic investigation process, including data collection, analysis, and findings. Develop the ability to create detailed, clear, and comprehensive reports.

**APPROACH:**

1. **Tools and Technologies Used:**
   * + Browser: To run the crypto-mining application and generate traffic.
     + Web Server: To host the crypto-mining application.
     + Python: Scripting language used for automating data analysis tasks.
     + FTK Imager: Forensic tool used to create and analyze disk images.
     + Wireshark: Network protocol analyzer used to capture and analyze network traffic.
2. **Infrastructure Setup:**

**Test PC:**

* IP Address: 192.168.1.8
* Role: Runs the browser with the crypto mining application.
* Software: Browser (e.g., Chrome ), Wireshark for capturing traffic.

**Web Server:**

* IP Address: 192.168.1.8
* Role: Hosts the crypto-mining application.
* Software: Apache or Nginx.

**Forensic Workstation:**

* IP Address: 192.168.1.8
* Role: Conducts forensic analysis and scripting tasks.
* Software: FTK Imager, Python.

**Firewall:**

* IP Address: 192.168.1.8
* Role: Manages and monitors network traffic.

1. **Steps to Follow:**

* **Simulate Crypto-mining Activity:**
  + Host the crypto-mining HTML file on the web server (192.168.1.8).
  + Access the page from the test PC (192.168.1.8) using a web browser to generate crypto mining traffic.
* **Capture Network Traffic:**
  + Use Wireshark on the test PC (192.168.1.8) to capture network traffic while the crypto mining application is running.
  + Save the captured traffic as a .pcap file.
* **Create Forensic Image:**
  + Use FTK Imager on the forensic workstation (192.168.1.8) to create a forensic image of the test PC's disk.
  + Extract browser artifacts such as history, cache, and cookies from the ad1 file.
* **Analyze Data:**
  + Analyze the captured network traffic using Wireshark to identify cryptomining patterns.
  + Use Python scripts on the forensic workstation to further analyze the browser artifacts and correlate them with network traffic data.
* **Document and Report:**
  + Document each step of the process in a detailed report.
  + Create a PowerPoint presentation summarizing the findings and methodology.

This method can be used to efficiently detect and analyze crypto mining activity coming from a browser, together with the tools and infrastructure that are mentioned.

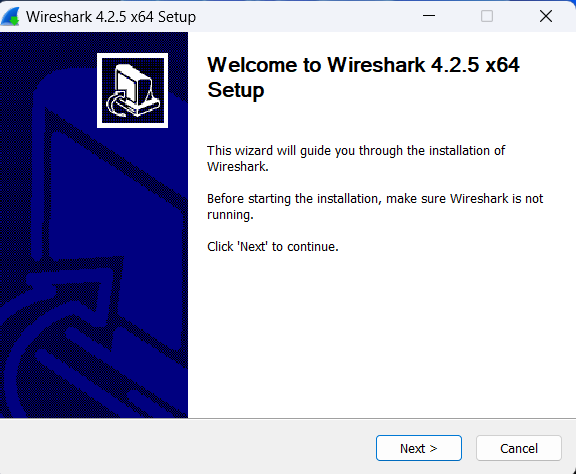
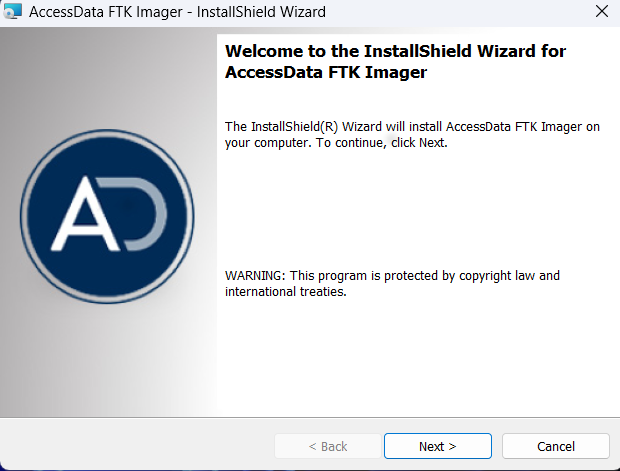
**IMPLEMENTATION:**

Step-by-Step Process to Solve the Problem:

* 1. **Setup and Preparation:**

1. **Install and Configure Tools:**

* Install FTK Imager, Wireshark, and Python on the forensic workstation (IP: 192.168.1.8).

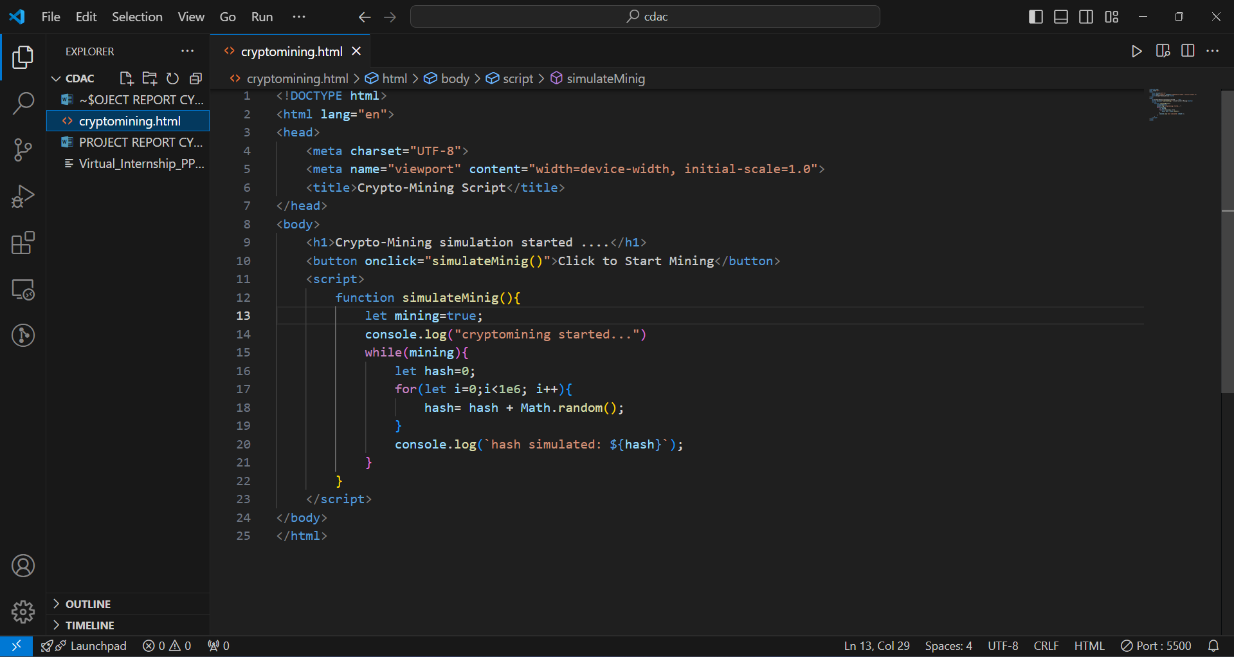


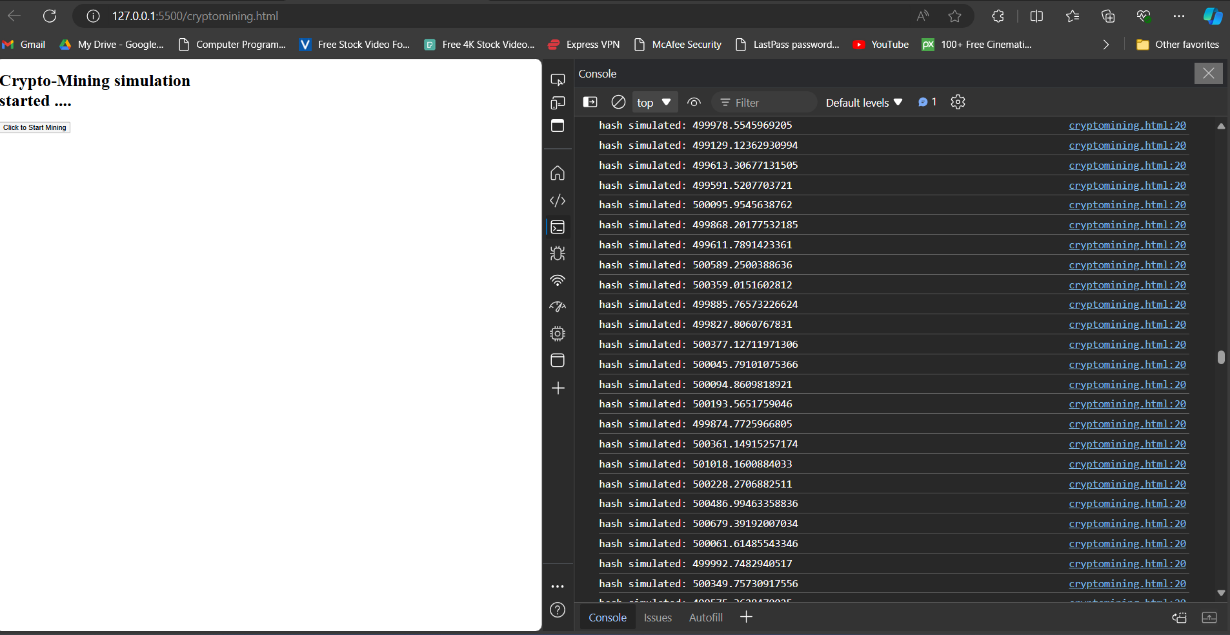
1. **Create Crypto-mining Application:**

o Develop a simple crypto-mining HTML script.

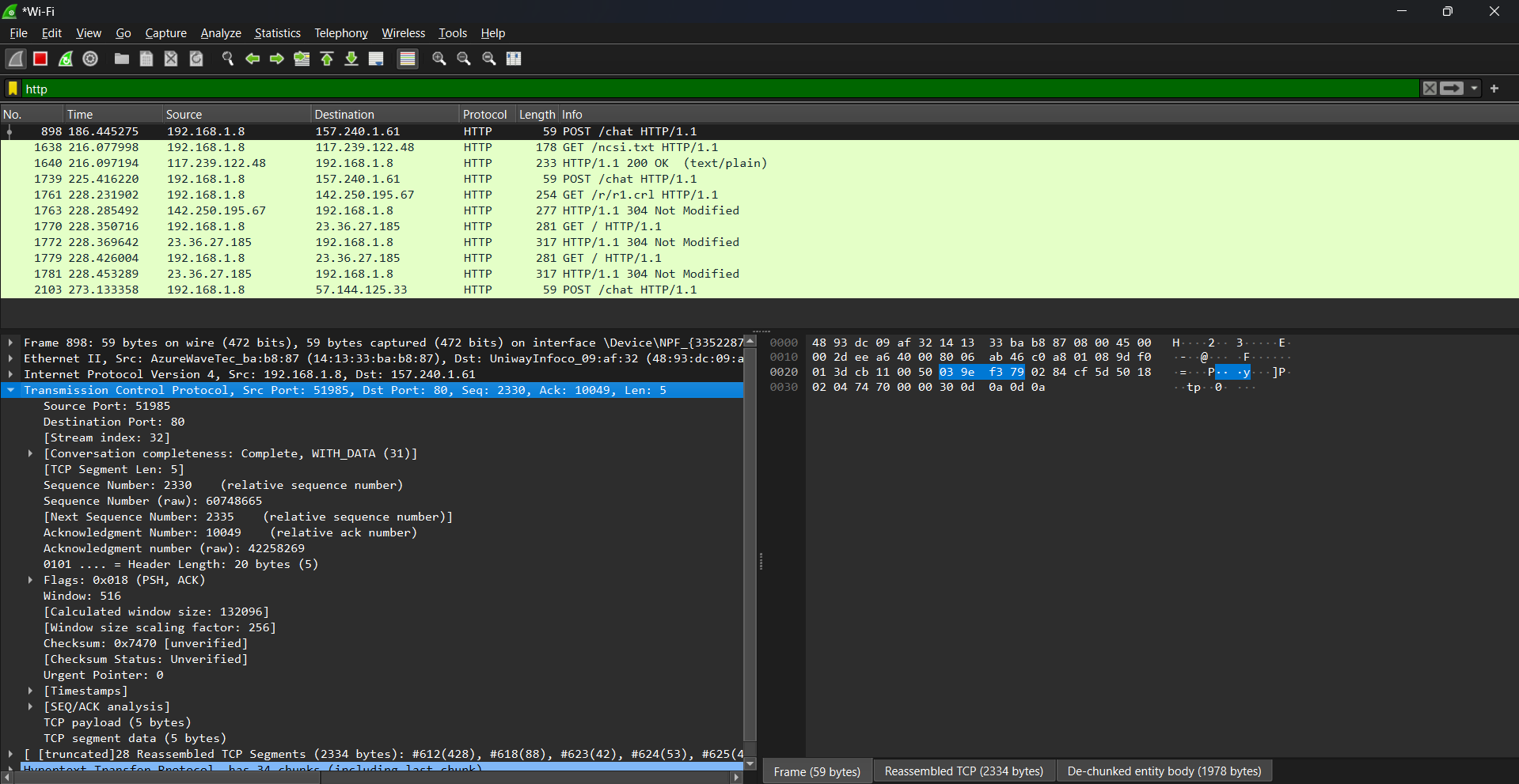
o Host the script on the web server at

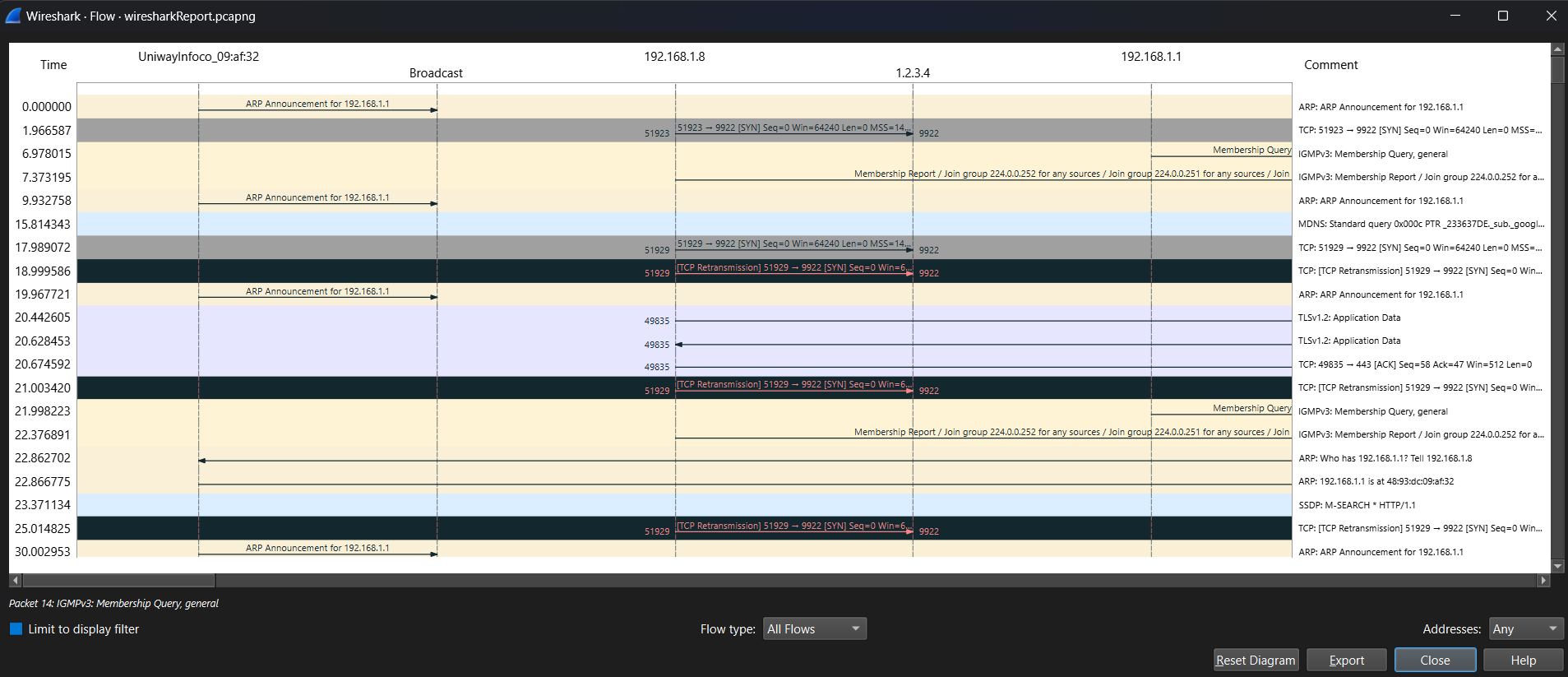
**http://127.0.0.1:5500/cryptomining.html** .

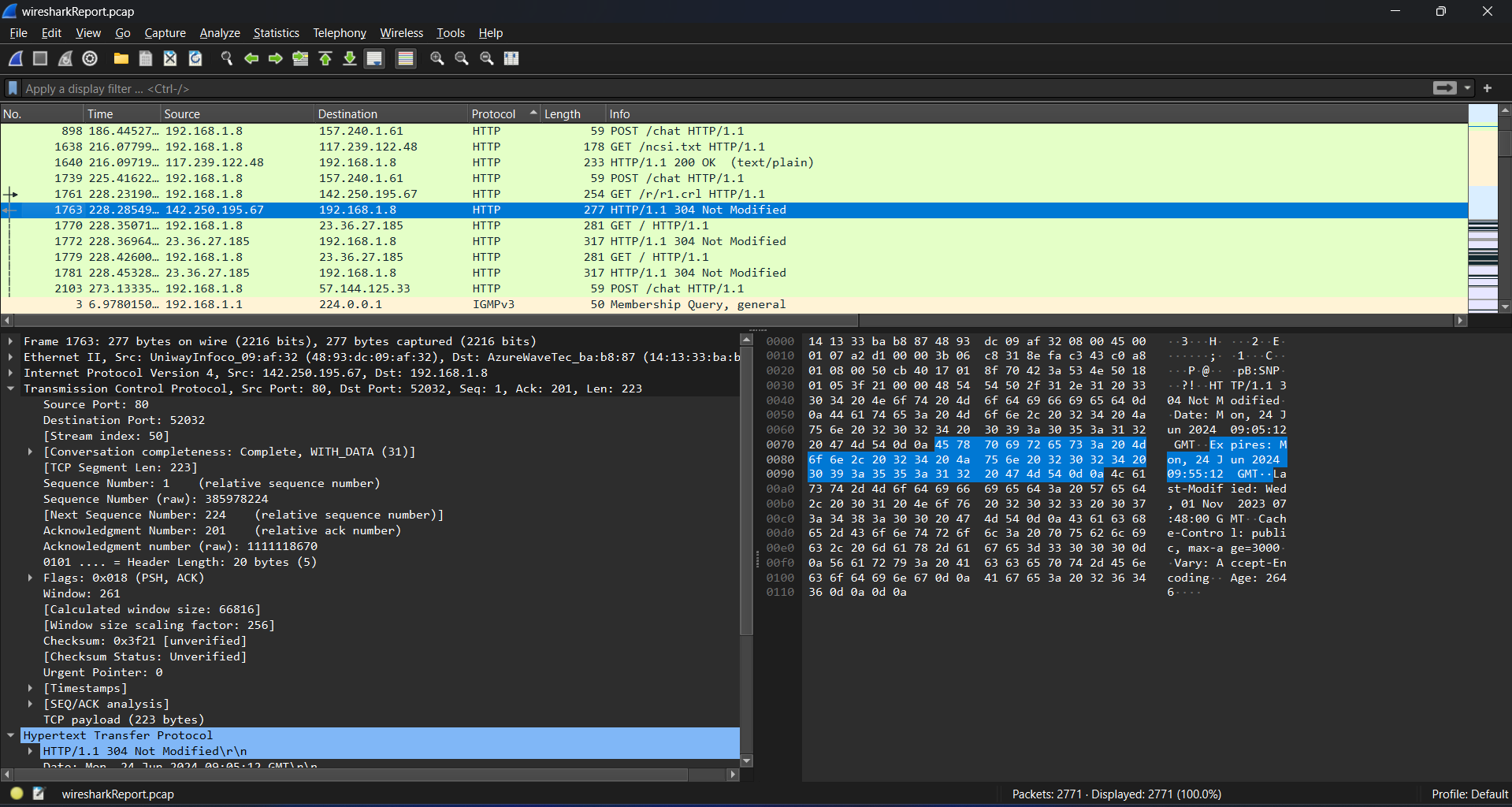
****



* 1. **Capture Network Traffic :**
     + 1. **Start Wireshark on Test PC (IP: 192.168.1.8):**
* Open Wireshark and start a capture session.
  + - 1. **Run Crypto-mining Application:**
    - Open a web browser on the test PC and navigate to the crypto-mining URL.
    - Let the crypto-mining script run for a few minutes to generate traffic.
      1. **Stop and Save Wireshark Capture:**
    - Stop the Wireshark capture and save the .pcap file.

****

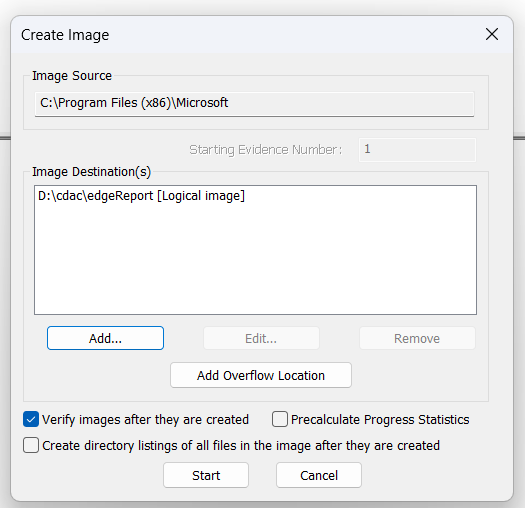
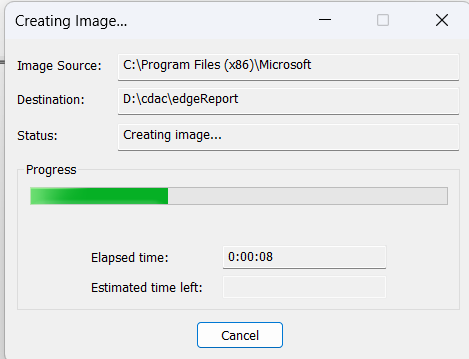
****

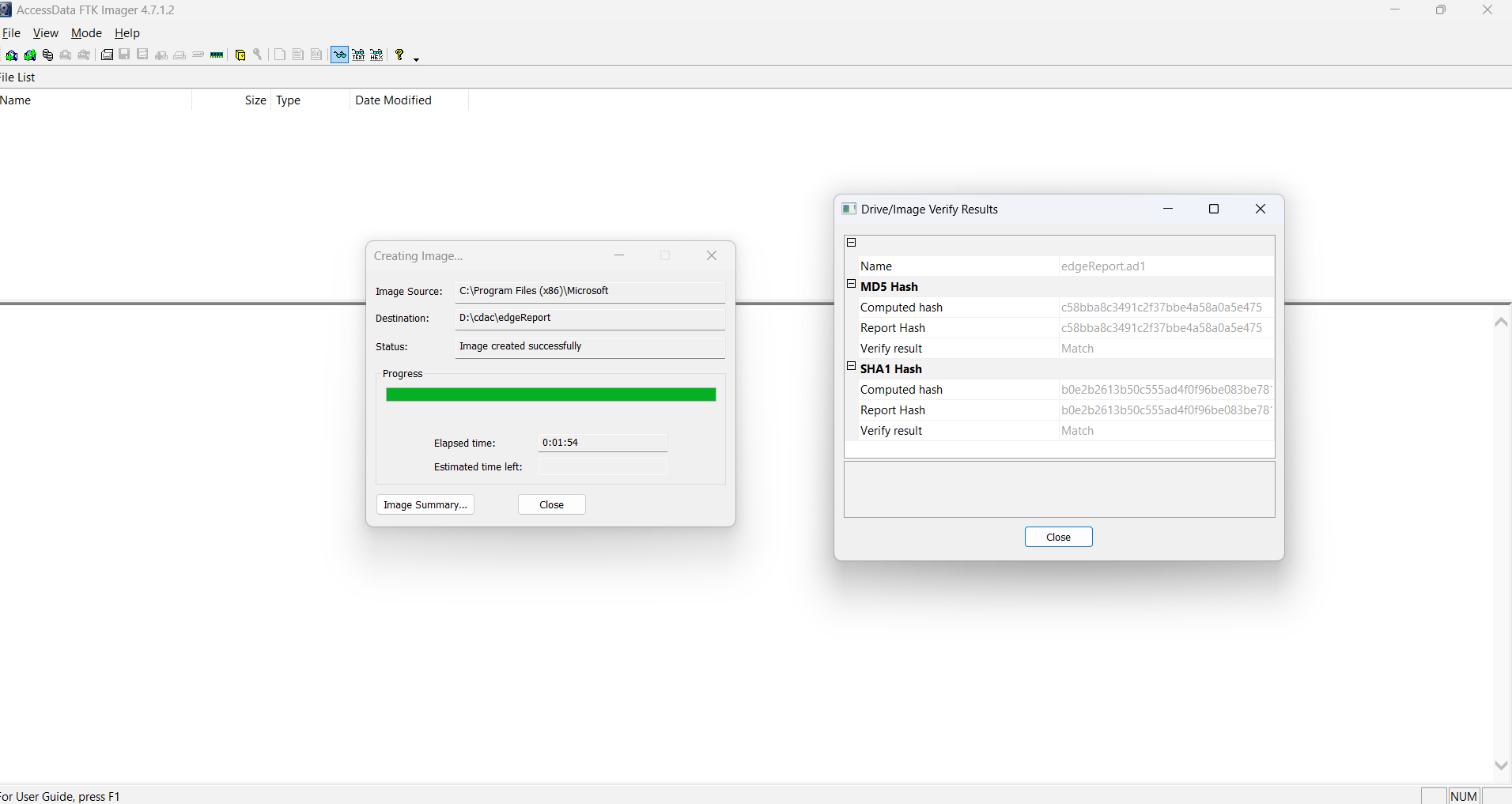
****

**3. Create Forensic Image:**

1. **Use FTK Imager:**

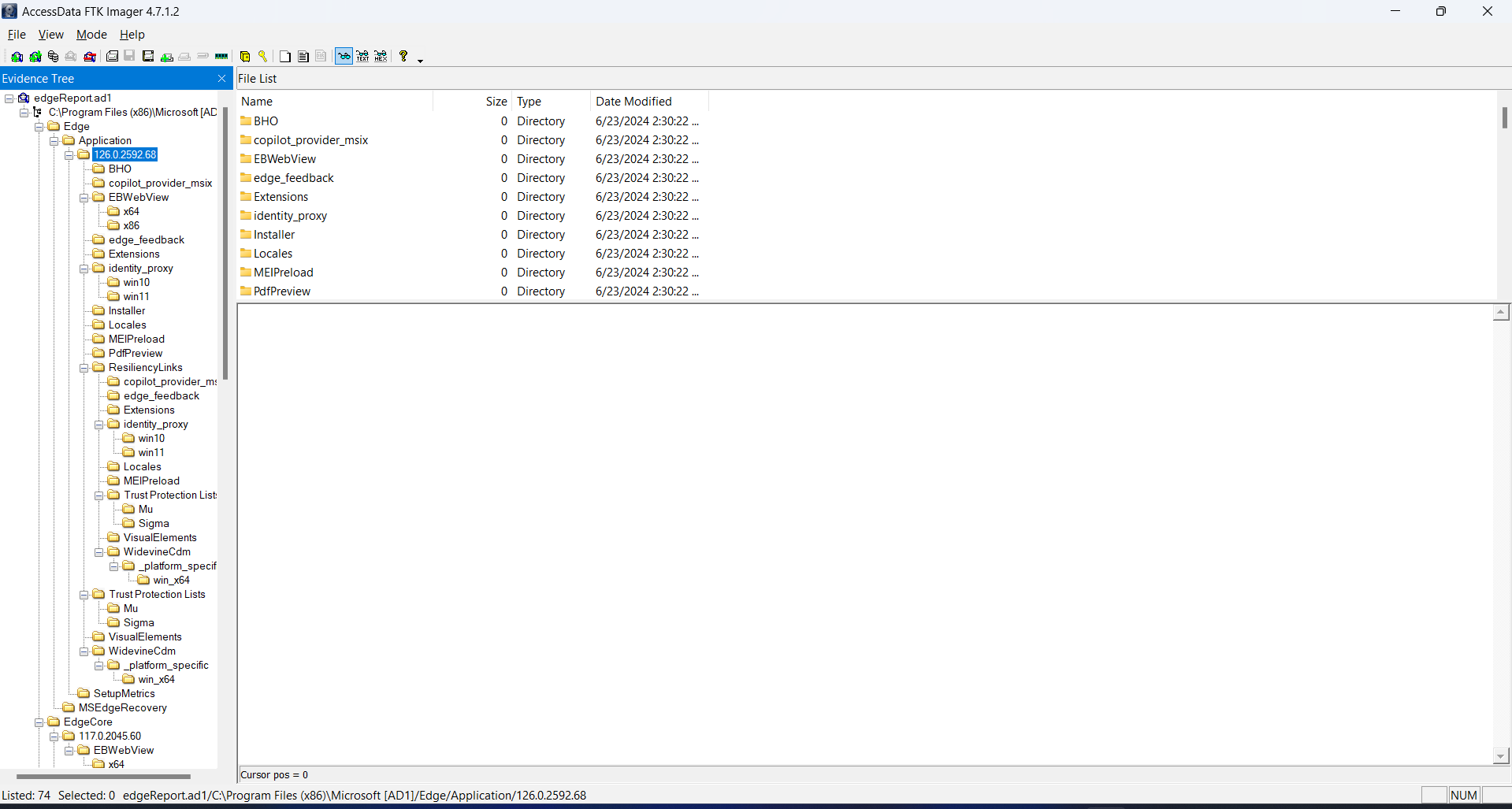
* Open FTK Imager on the forensic workstation.
* Select "File" -> "Create Disk Image" and choose the test PC's disk.
* Save the image as an ad1 file.

****

****

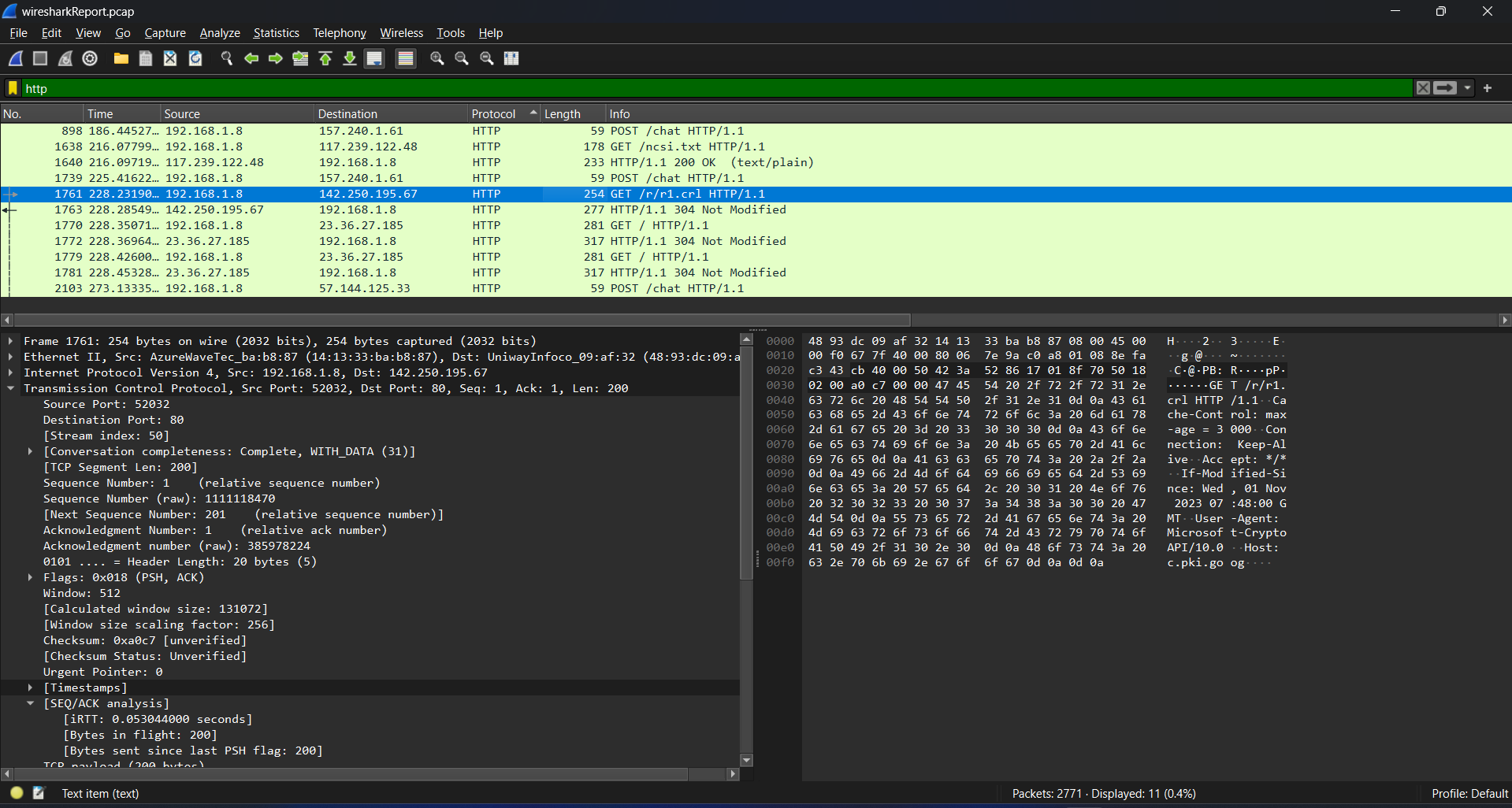
1. **Extract Browser Artifacts:**

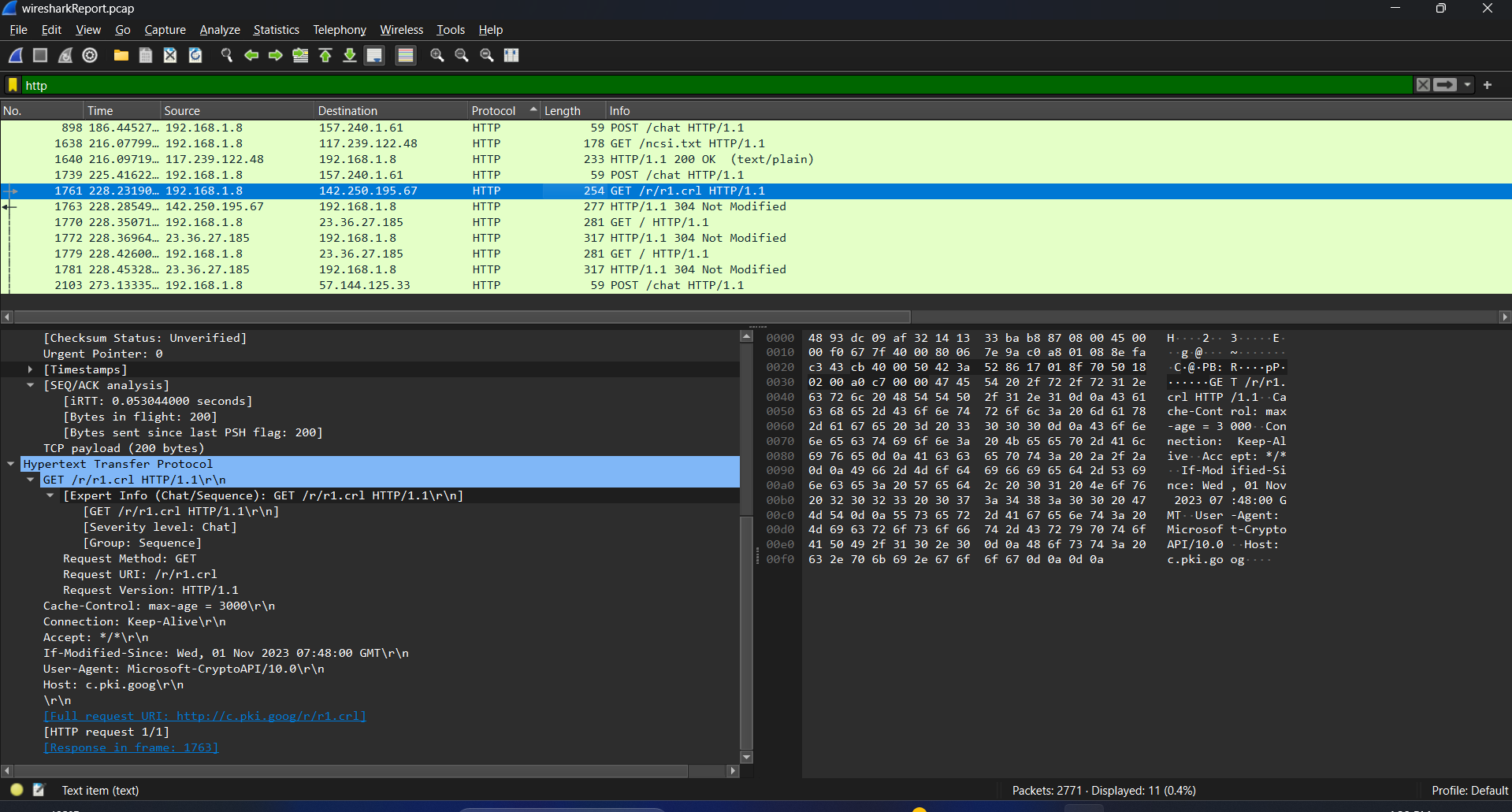
* Open the ad1 file in FTK Imager.
* Extract browser history, cache, and cookies for analysis.



1. **Analyse Data :**
2. **Network Traffic Analysis in Wireshark:**

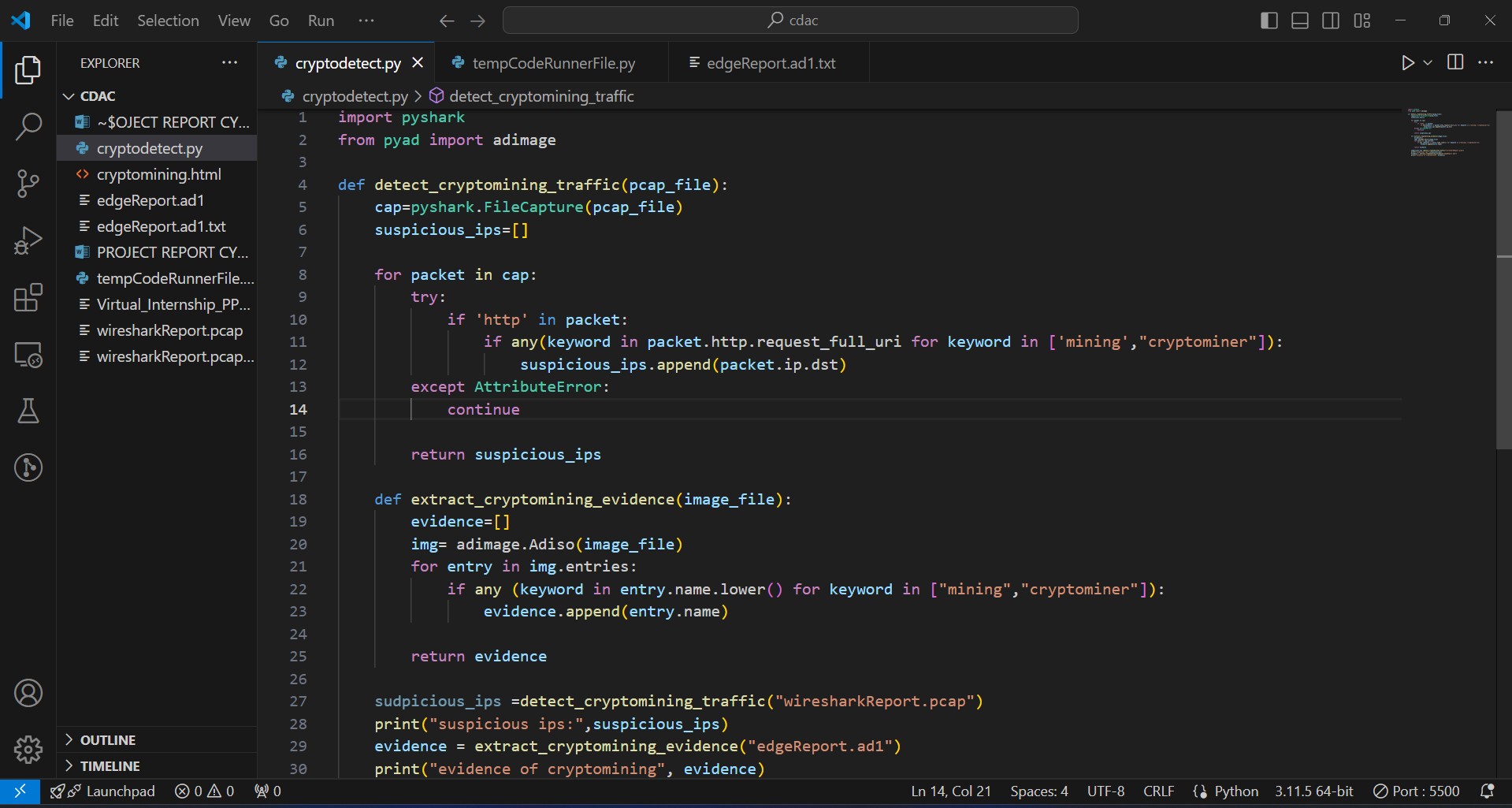
* Open the .pcap file in Wireshark.
* Filter and identify suspicious traffic patterns related to crypto-mining.



****

1. **Browser Artifacts Analysis:**

* Use Python scripts to analyze the extracted browser artifacts.
* Look for URLs, cached scripts, and cookies associated with crypto-mining.

****

**Indicators of Compromise:**

* **System Slowdowns and Lag:**
* Slow application response times, noticeable lag times, and system freezes can all be signs of mining activity.
* **Overheating:**
* The heavy strain that mining places on hardware can lead to overheating. To keep an eye on temps, use programs like HWMonitor (Windows).
* **Unusual Network Traffic:**
* High-frequency HTTP requests to known crypto-mining domains.
* **Increased Bandwidth Usage**:
* Mining software communicates with a mining pool, which can result in increased network activity.
* Monitor network traffic for unusual spikes.

**CONCLUSION & RECOMMENDATIONS:**

The goal of this initiative was to locate and stop PC cryptomining activity. Particularly when done without authorization, cryptomining can severely impair system performance, require more energy, and possibly even destroy hardware by using too many resources.

**Conclusion :**

* **Detection of Cryptomining Activity**:
* **System Performance**: High CPU/GPU usage, system lag, and overheating are strong indicators of cryptomining.
* **Network Traffic**: Increased and unusual outbound network traffic to specific IP addresses and ports associated with mining pools.
* **Processes and Tasks**: Unfamiliar processes and scheduled tasks running in the background, often disguised as legitimate system processes.
* **Tools and Techniques for Detection**:
* **Task Manager, Activity Monitor, top/htop**: Essential for identifying high resource usage.
* **Wireshark**: Effective for capturing and analyzing network traffic to detect connections to mining pools.
* **Antivirus and Antimalware Software**: Critical for detecting and removing cryptomining malware.

 **Common Indicators of Compromise**:

* Persistent high resource usage.
* Unusual system and network behavior.
* Presence of unauthorized software or extensions.

**Countermeasures for Cryptomining Cyber Attack :**

* **Regular Updates**:
* Keep the operating system, software, and security tools up-to-date to protect against vulnerabilities.
* **Strong Security Practices**:
* Use strong passwords, enable firewalls, and implement endpoint protection.
* Use security extensions to block crypto-mining scripts.
* **Uninstall Malicious Software**:
* Remove any unfamiliar or malicious software through system settings.
* **Scheduled Scans**:
* Perform regular antivirus and antimalware scans to detect and remove potential threats.
* **Safe Mode**:
* Boot into Safe Mode to prevent malicious software from running and perform deep scans with tools like Malwarebytes.
* **User Awareness:**
* Educate users about crypto-mining risks and safe browsing practices.
* **Network Monitoring:**
* Continuously monitor network traffic for unusual patterns.
* Set up alerts for high-frequency HTTP requests to crypto mining sites.

**LIST OF REFERENCES:**

1. [**Wireshark User’s Guide**](https://www.wireshark.org/docs/wsug_html_chunked/)**:** for a better understanding of Wireshark.
2. [**FTKImager\_UG**](https://d1kpmuwb7gvu1i.cloudfront.net/Imager/4_7_1/FTKImager_UserGuide.pdf) **:** to learn how to use FTK imager .
3. [**pyshark**](https://pypi.org/project/pyshark/) **:** To learn the use of this library for processing Wireshark capture files.
4. [**pyad**](https://pypi.org/project/pyad/) **:** To learn the use of this library for processing AD1 files.
5. I also referred to the pdf’s provided in the Advanced course section.