**Browser History Examiner**

Student Name

Institutional Affiliation

Course

Date

**Browser History Examiner**

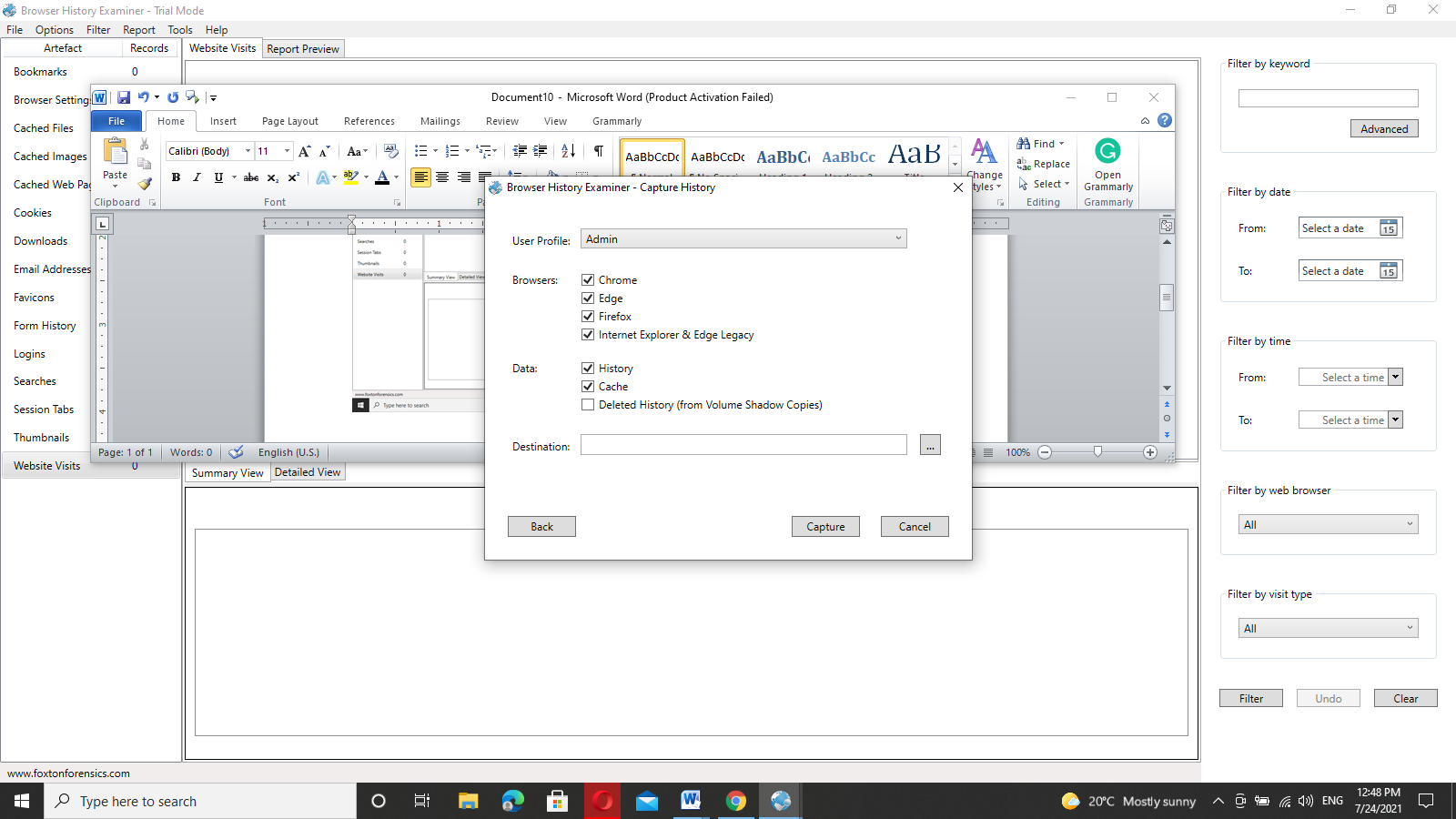
**Introduction**

The Browser History Examiner (BHE) is forensic software that collects, analyzes, and reports on web browsing activity from popular desktop web browsers. BHE can assist with a variety of digital investigations, including civil and criminal digital forensics, security events, human resource inquiries, and reporting on ordinary employee activities.

My choice for this tool is because it is easy to use. It does not require a complicated installation and setup process. The forensic tool is also available with a free trial version. The free trial version includes many features that are good for analyzing a browser. It can also work on Chrome browser, Firefox browser, Edge, and Microsoft Internet Explorer. Foxton Forensics has developed the tool, and to download it, one has to visit the site (<https://www.foxtonforensics.com>).

**Background**

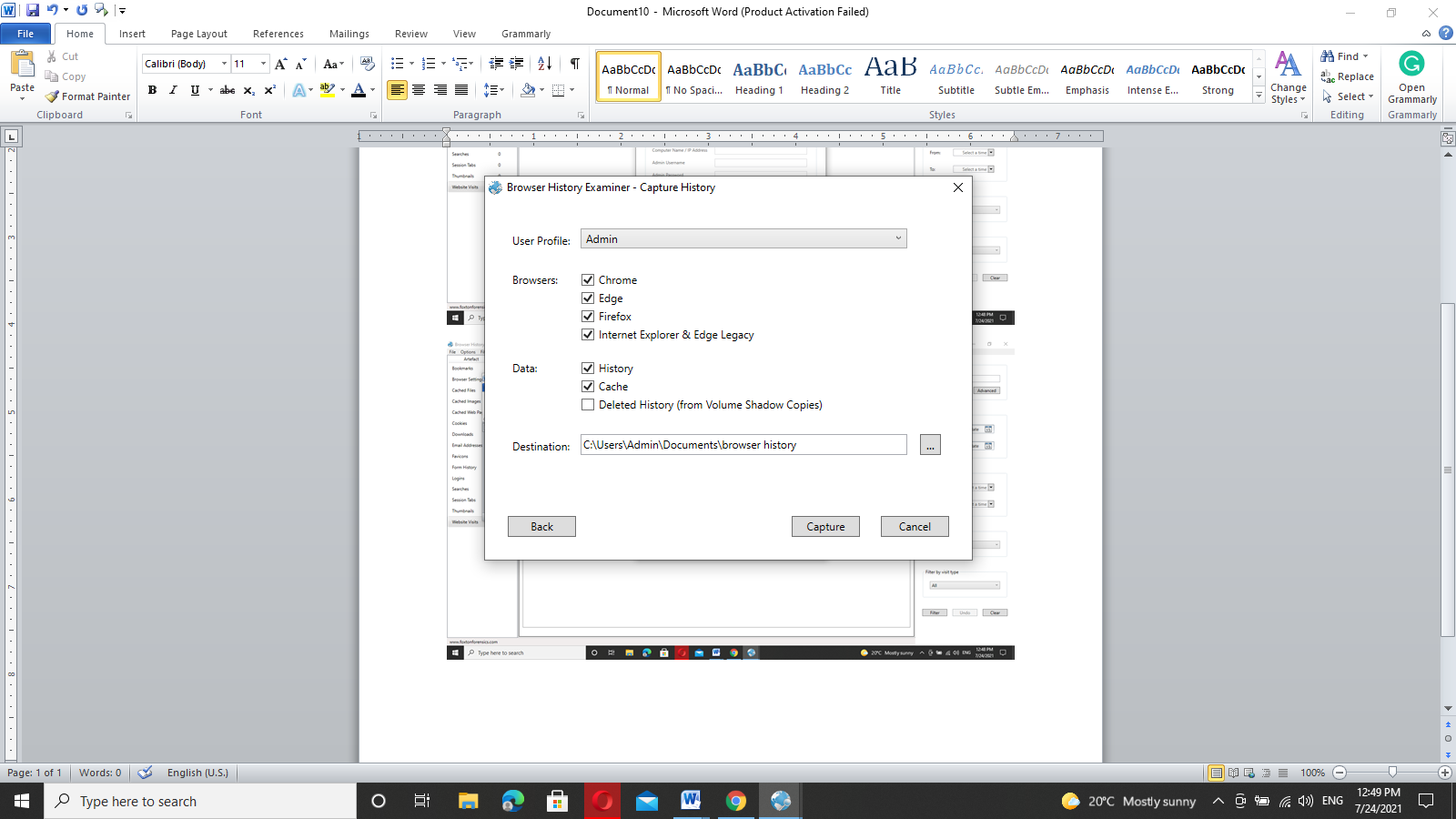
Using Foxton Forensics' Browser History Capturer (the free app!) on a USB means a minor intrusion into a system that records Internet history to investigate using Browser History Examiner or any other tool off live evidence or custodian machine. Additionally, data can be imported from an external hard disk. Additionally, you can record from a distance (Adamu). The tool can be used to analyze Google Chrome, Maxilla Firefox among other browsers as shown below.



Chrome stores data in the SQLite database format, which may be seen using the SQLite database viewer. Google Chrome keeps its browsing history in the standard file of history. These tables provide detailed information that includes private data, which are required for forensic purposes (Rathod, 2017). Mozilla Firefox is a cross-platform browser that works on Mac OS X, Microsoft Windows, and Linux. Furthermore, it is incredibly adaptable, has a simple layout, and is simple to use, which may explain why it is the first choice of many users. Web browsers save the cache, history, cookies, usernames, and passwords, as well as a list of downloaded files. Similarly, Firefox saves browser records in an SQLite database that investigators can access. The following section goes into detail on the Firefox web browser, including its log data files and formats (Rathod, 2017).

**Methodology**

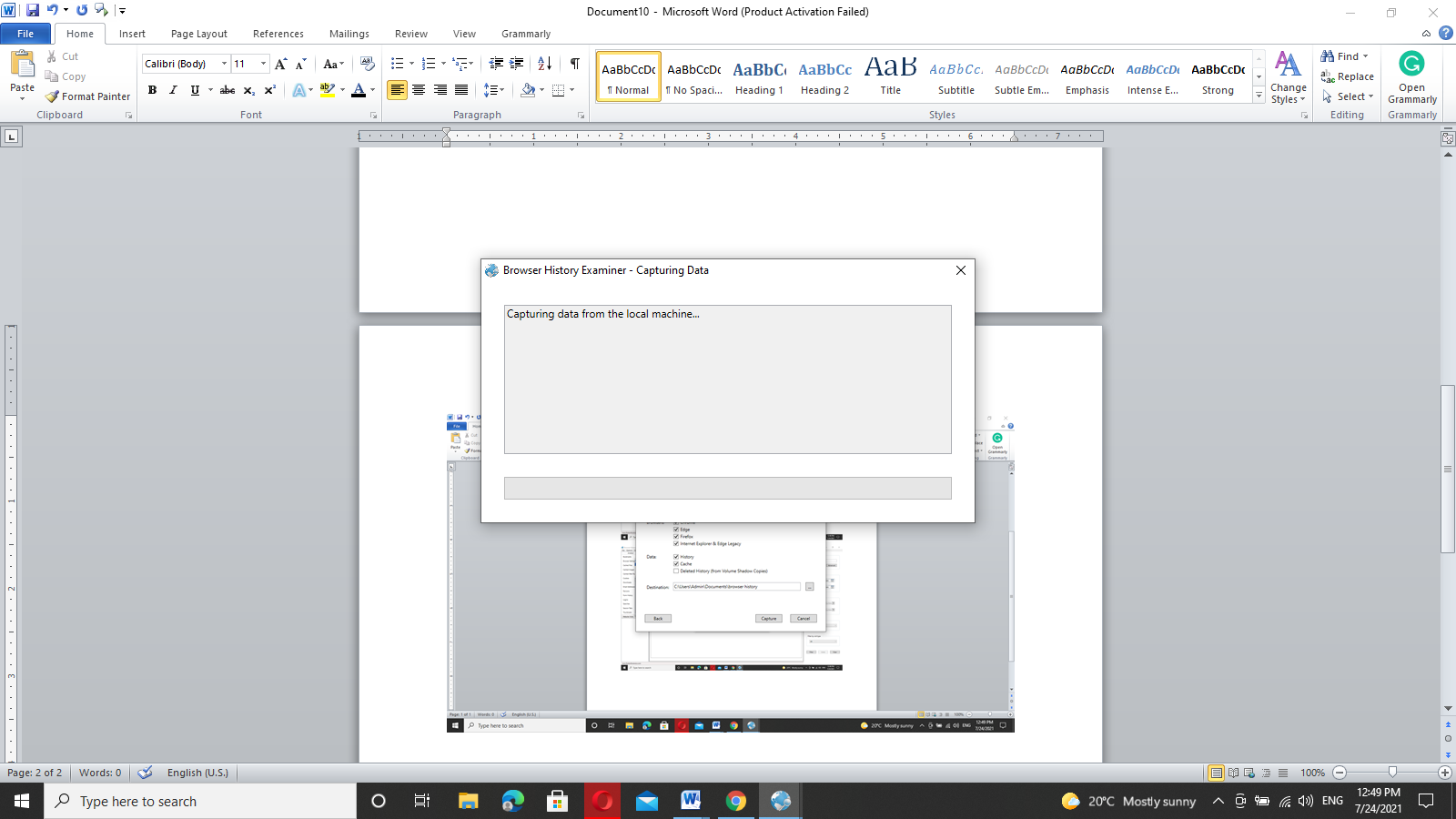
I have included Screenshots of how I used the tool to generate my browsers' history at the end of the discussion. Loading Internet history is straightforward. The app runs reasonably quickly. The data is processed promptly. It's simple to view the output and create reports. I've been in a couple of situations where Internet history was the primary or sole objective (internet abuse policy violations, general "bad" Internet activity, etc.), and this tool would have fit in well had I been aware of it at the time. Finally, Now I understand after learning how to use it. After opening the forensic tool, one can choose which specific areas to analyze on the browser, as shown in the following screenshot.



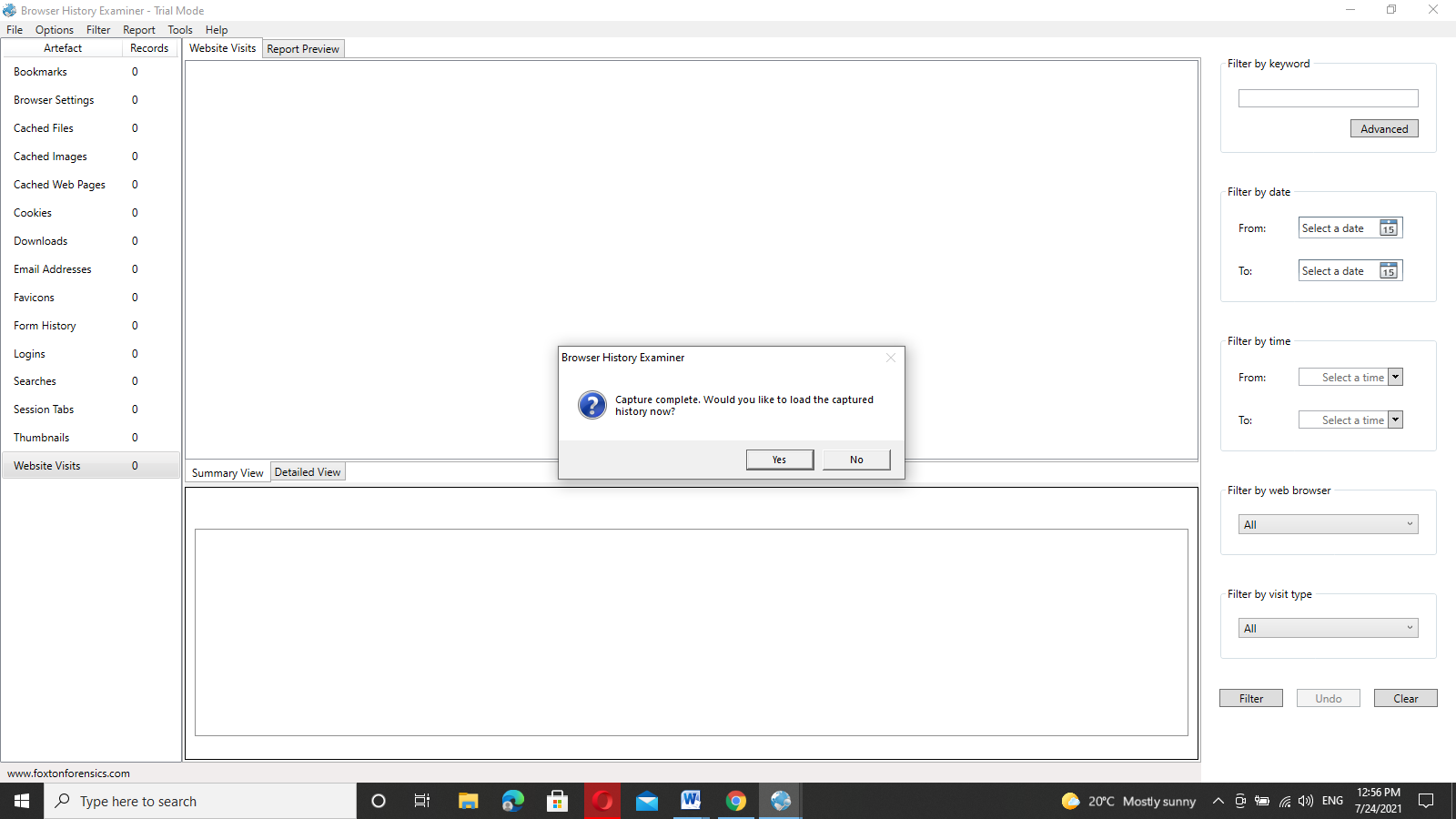
Each of the common characteristics is present. There are filters for keywords, dates, and times. Additionally, you can filter results by web browser type and download status. The viewing glass is fantastic, and the things are exhibited beautifully. The viewing pane displays reconstructed webpages, cached images, a cloud of "search history," and virtually anything else linked to Internet analysis.

**Analysis**

I can see how remotely getting records and having all of the material I require for an Internet case in minutes may be advantageous (for me). It is relatively quick in providing the user interface to the Internet history to begin looking through it. The following screenshot shows the window of analyzing the web browser.



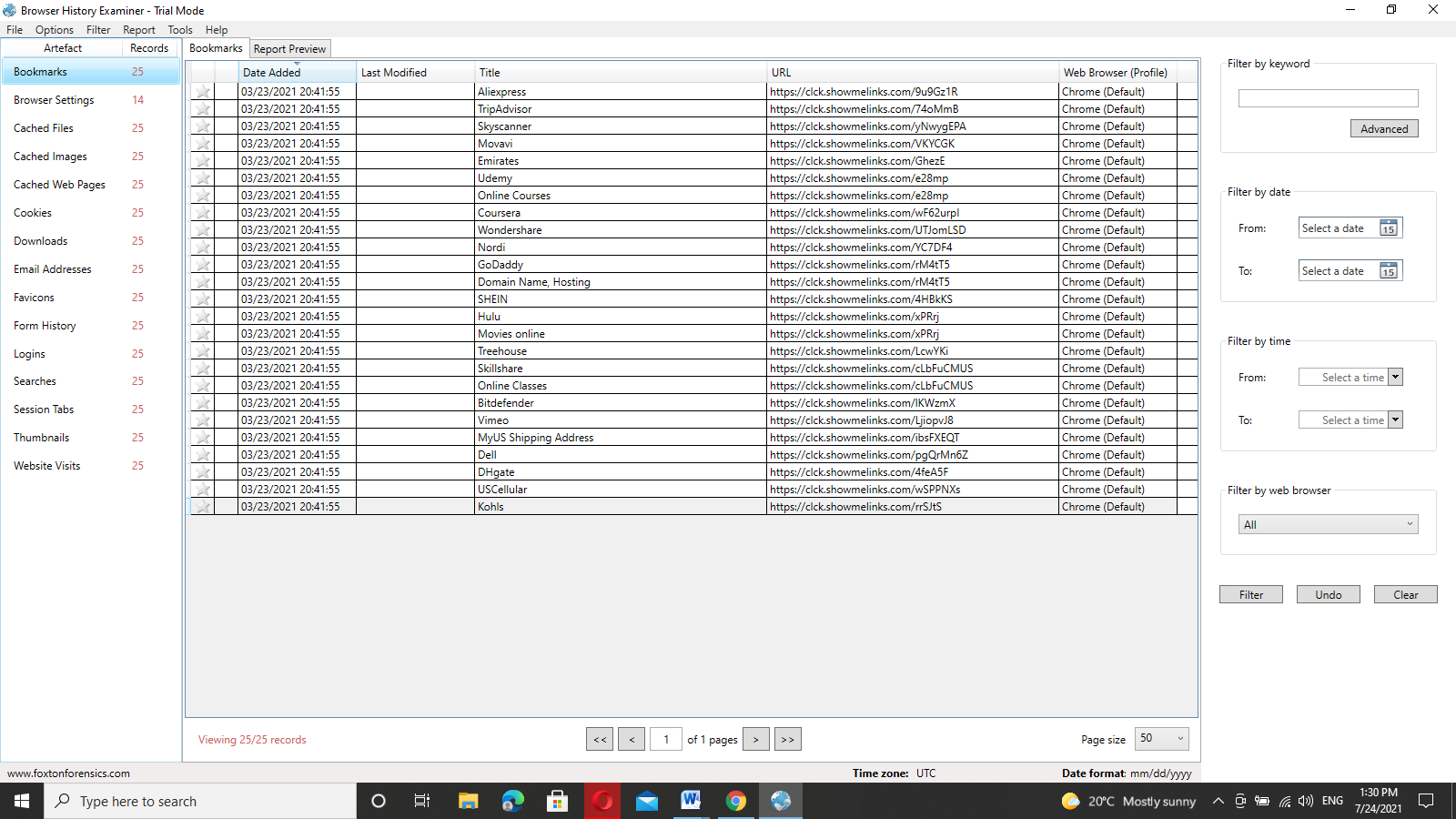
A notification on completion of the analysis process is shown in the following screenshot.



**Findings**

A visually appealing graph representing the number of pages accessed during a specified period displays site visitors. This is necessary to track the growth of internet consumption. A web browser's history can be retrieved from either a local computer or a networked Windows PC. Utilize the thumbnail gallery or the built-in photo viewer to examine images saved in the user archive at their original size. A few suites do an inadequate job of converting history to something only slightly better than hex. Smaller forensic gadgets can help fill in the gaps left by larger equipment (Mahaju, & Atkison, 2017). BHE can aid with civil and criminal digital forensics investigations, security events, human resource inquiries, and simple employee activity reporting, among other things.

The following is a screenshot of the detailed results or report produced by the BHE on my web browser Google Chrome.



**Conclusion**

Because, as previously said, the best tool is the one that is optimized for the task at hand; both large and small forensic suites are equally valuable. This might be a feature-rich suite, a straightforward command-line utility, or something in between. While the majority of suites allow the examiner to check his or her Internet history, some are superior. A sophisticated tool for checking the web browser's history, site History Examiner (BHE) is a piece of software that records, analyzes, and documents your computer's internet history across many web browsers. BHE may be employed in a variety of technological applications, including civil and criminal digital forensics, cyber accidents, human resource assessments, and monitoring general workplace behavior.

**References**

Adamu, H., Ahmad, A. A., & Adamu Hassan, S. A. B. G. Web Browser Forensic Tools: Autopsy, BHE and NetAnalysis.

Mahaju, S., & Atkison, T. (2017, April). Evaluation of firefox browser forensics tools. In *Proceedings of the SouthEast Conference* (pp. 5-12).

Rathod, D. (2017). Web browser forensics: google chrome. *International Journal of Advanced Research in Computer Science*, *8*(7), 896-899.