**Digital Forensics report**

**Q1: As a forensic examiner, you are required to analyze the given capture file using Wireshark and answer the following questions in your report: https://drive.google.com/file/d/16GR5hpLa-Jlo7HcJiN2BFAIMLO0I3IG5/view?usp=sharing**

**1) Is this an Attack? Justify your answer.**

Denial of service (DOS) attack , because I see multiple IP Addresses sending requests to this IP 10.0.64.129 in order to to overwhelm the server

**2) Discover the source geo IP country? (do your own research)**

source geo IP countries are

1-Argentina in city of Buenos Aires

2-Belgium in city of Brussels

3-Canada

4-China in both cities Wenzhou Tianjin and others

5- Colombia

6- Croatia in city of Split and others

7- Germany in cities of Dusseldorf ,Bonn ,Frechen ,Noerten-Hardenberg ,Nassenfels,Berlin,Cologne,Wesseling,Remagen,Stuttgart,Berlin,Bad Freienwalde

,Golzow,Bad Oeynhausen,Bergisch Gladbach,Rhede,Karlsruhe,Düsseldorf,

Dortmund,Werl,Frankfurt am Main,Erlangen,Ludwigshafen am Rhein,Gaggenau and others

8-India

9-Israel in cites of Tel Aviv,Ramat Gan , Ness Ziona and others

10- Jaban in city Tokyo and others

11- Mexico in cites Campeche and Solidaridad

12- Russia

13- Slovenia

14-Sweden in city of Degerfors

15- Switzerland in city of Adliswil

16- The Netherlands

17-Turkey in cities of Guzelbahce , Ankara and others

18-United Kingdom in cities of London ,Acton ,Willenhall ,Barnet and others

19-United States in cities of Chandler,Baton Rouge,San Antonio,Ashburn,Baton Rouge,Charlottesville,Vinita,Omaha,Muncie,Oakland,Indianapolis,Southborough, Tappahannock,Walla Walla,Benton City,Austin,Dallas

**3) How many countries are involved?**

19 countries involved in this attack

**4) Choose any of the identified locations in Question 2, how many packets come from the location you choose? Mention the location and the number of packets.**

Israel came from it 23 packets and from each city

Ness Ziona came from it 2 packets

Ramat Gan came from it 14 packets

Tel Aviv came from it 7 packets

**5) Are these packets made by a bot or normal devices?**

bot , because we observed a large number of requests coming from a limited set of IP addresses. This indicates a coordinated attack from a botnet.

**6) Extract the TTL of the packets and show how it can be used in discovering attacks?**

all packet have TTL value 254

Normal TTL Behavior: Every packet has a TTL value, which represents the maximum number of hops it can traverse. As the packet moves through routers, the TTL decreases by one at each hop.

Baseline Establishment:Create a baseline or normal range of TTL values for your network under regular conditions. This baseline reflects the typical number of hops between different parts of your network.

Anomaly Detection: Monitor TTL values in real-time. Sudden deviations from the established baseline could indicate a problem.

TTL Exhaustion: In a DoS attack, attackers may flood the network with packets, deliberately setting TTL values to very low numbers. This causes routers to quickly discard the packets, generating a large number of ICMP Time Exceeded messages.

Detection of Unusual Patterns: Look for unusual patterns, such as a flood of packets with TTL values outside the normal range. This could suggest an attack.

Thresholds and Rate Limiting: Implement thresholds for acceptable TTL values and consider rate limiting. If incoming packets exceed expected limits or if TTL values fall outside predefined thresholds, it may indicate a DoS attack.

**Q2: As a forensic examiner, you received a storage image file with its SHA256 hash code.**

**1) Forensically speaking, what should be done before attempting to the storage image file?**

Calculate hash values of the acquired storage image file. Compare these hash values with the hash values of the original device to ensure the integrity of the forensic image. This verification process helps establish that the acquired image is an identical copy of the original.

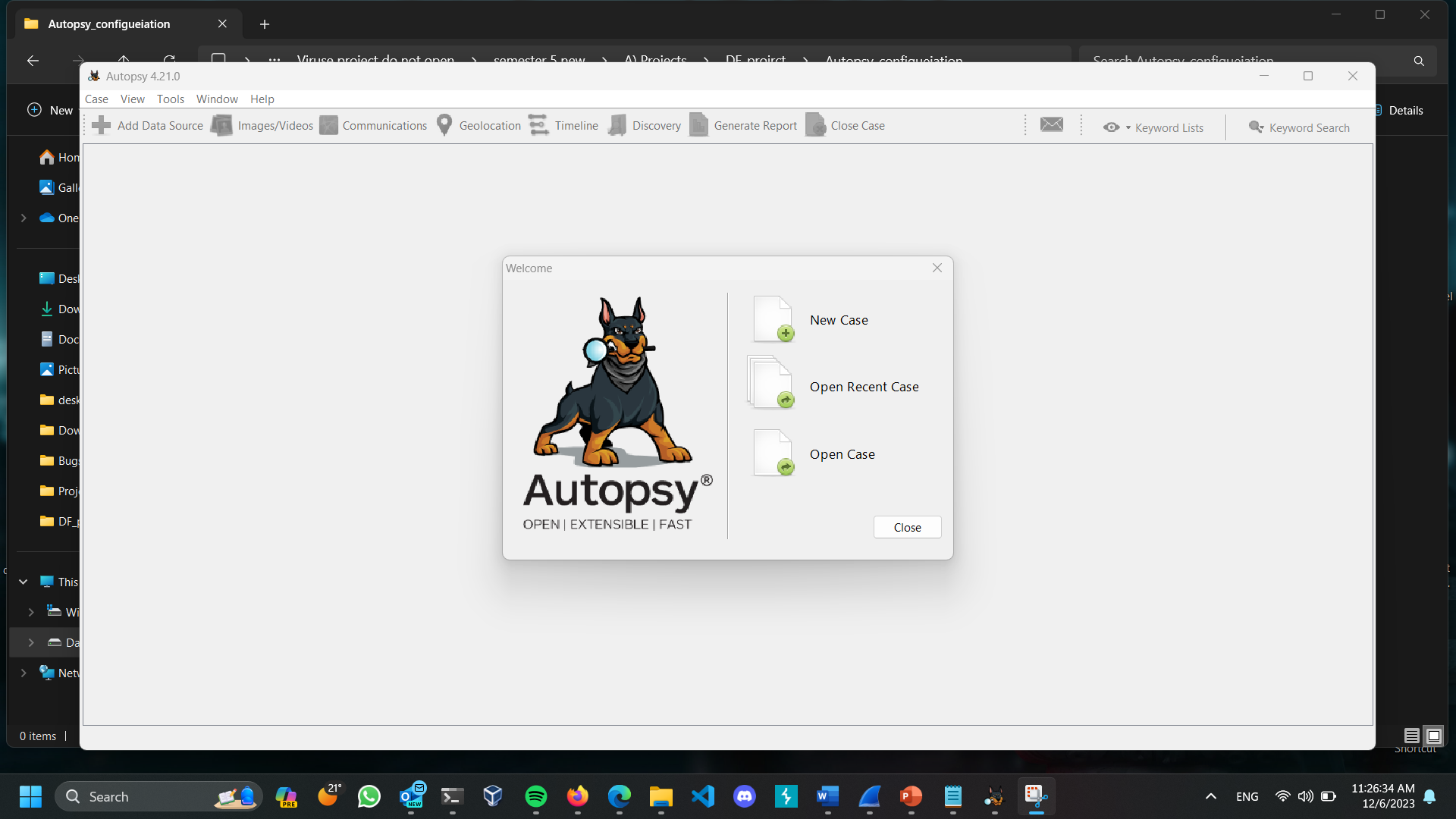
**2) Is this file considered intact? Justify your answer.**

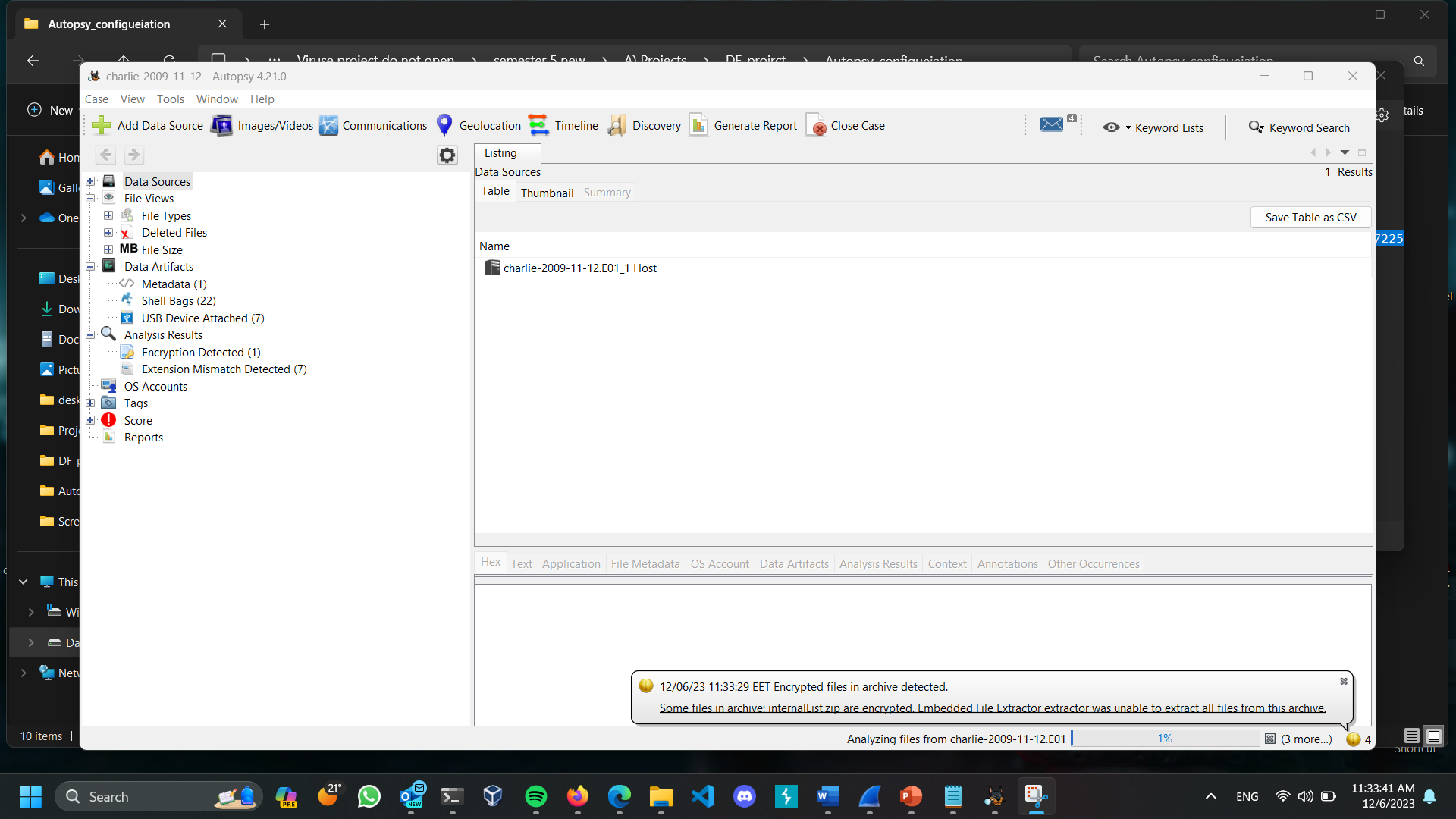
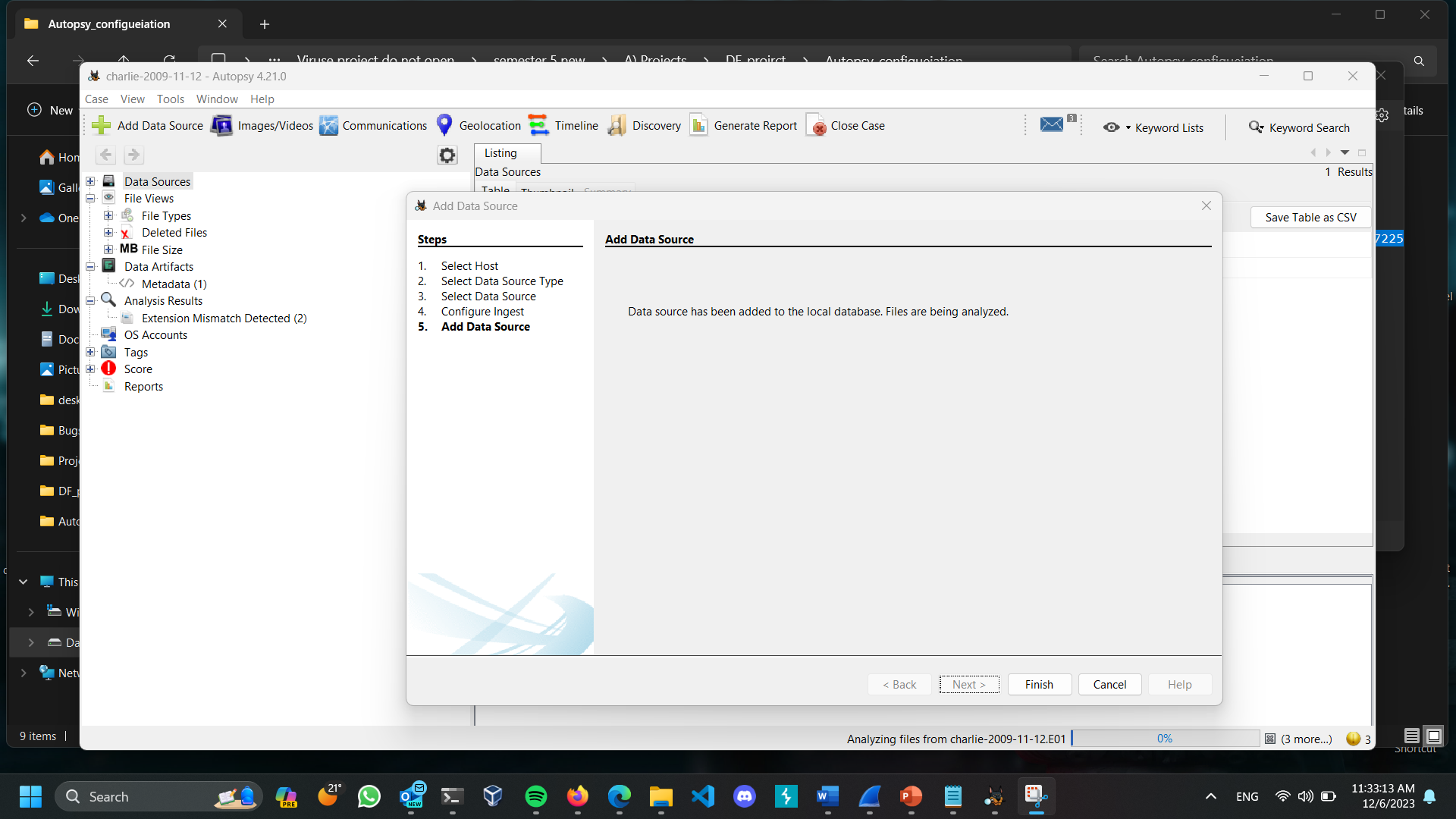
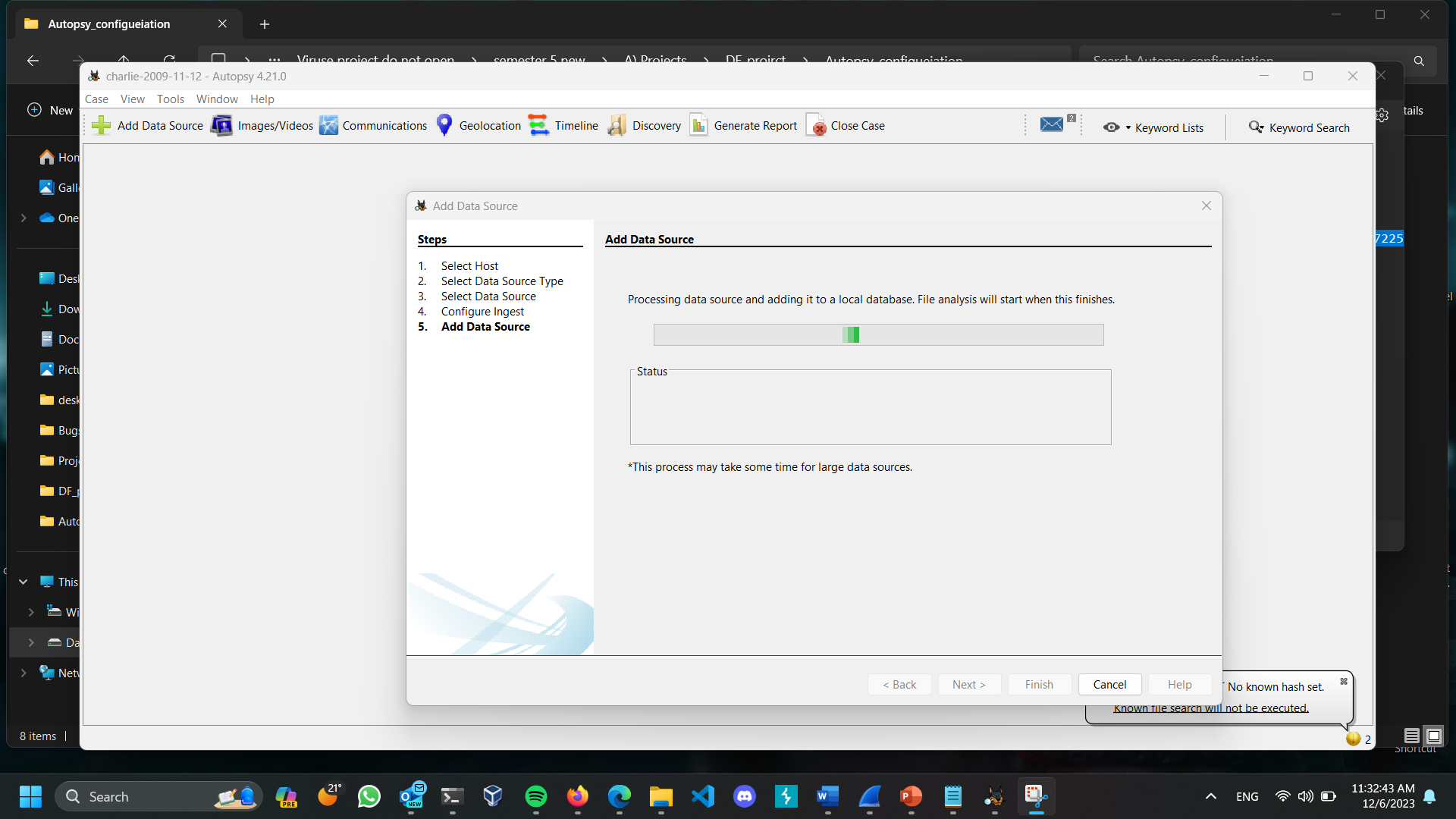
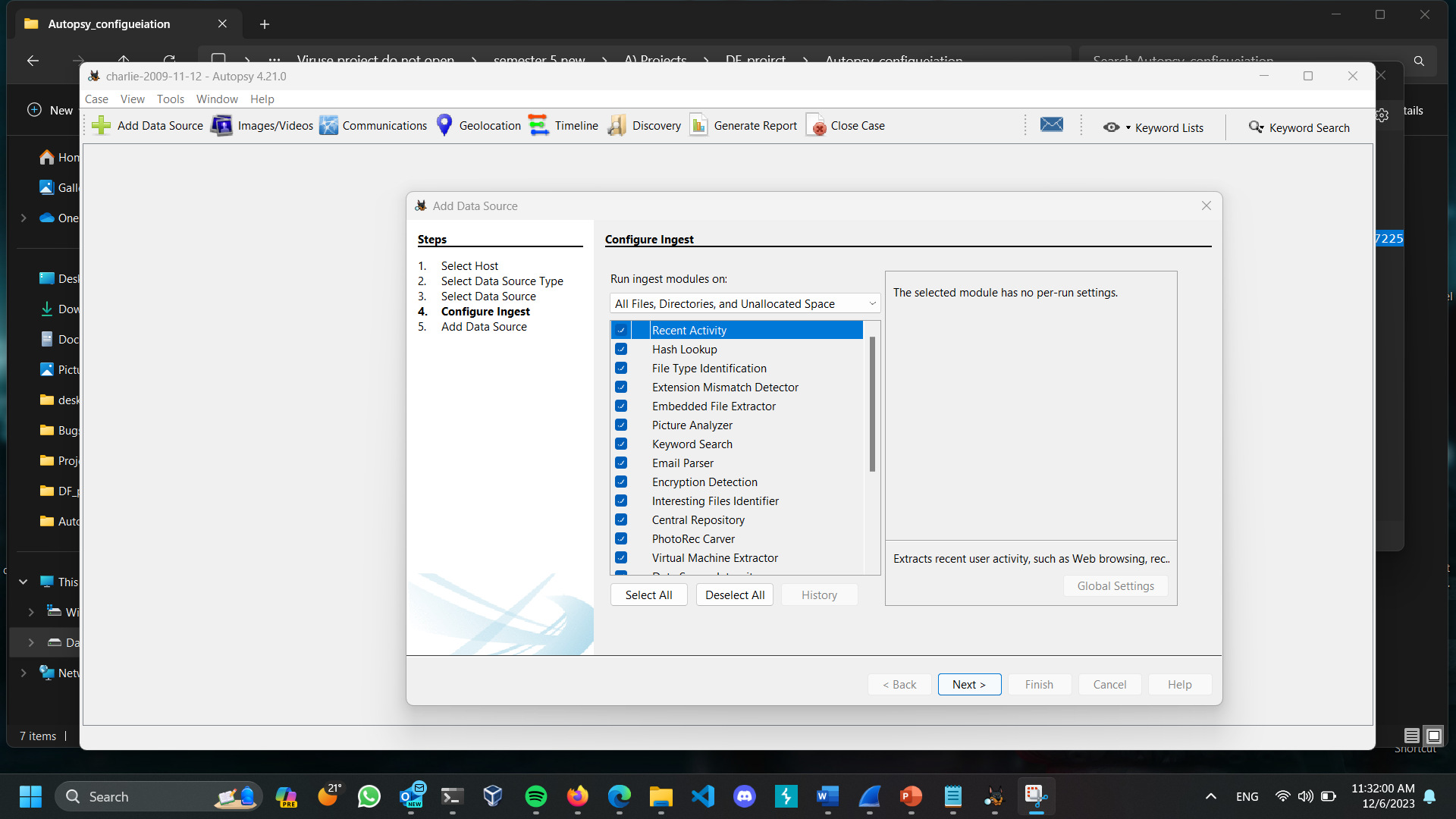
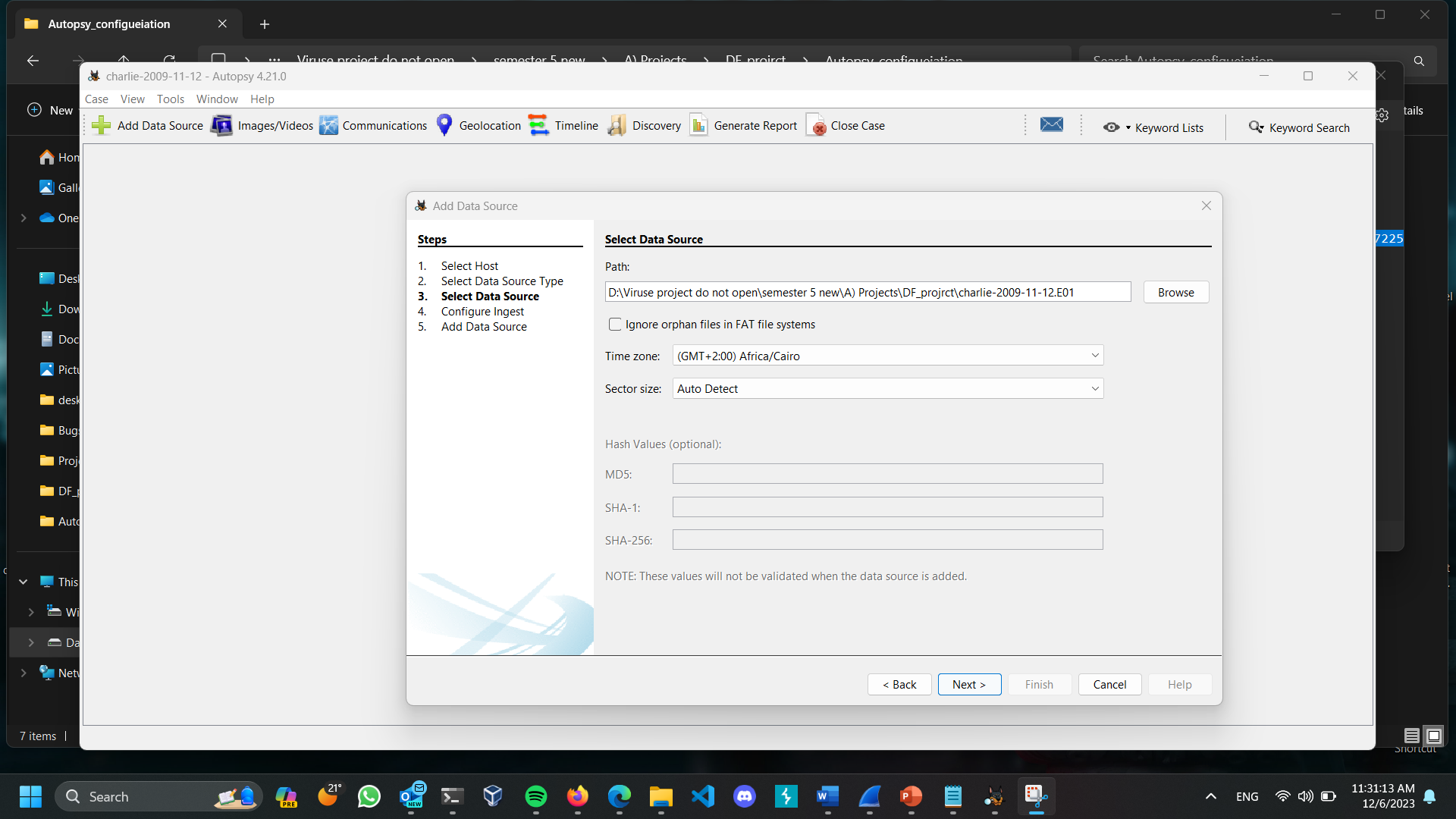
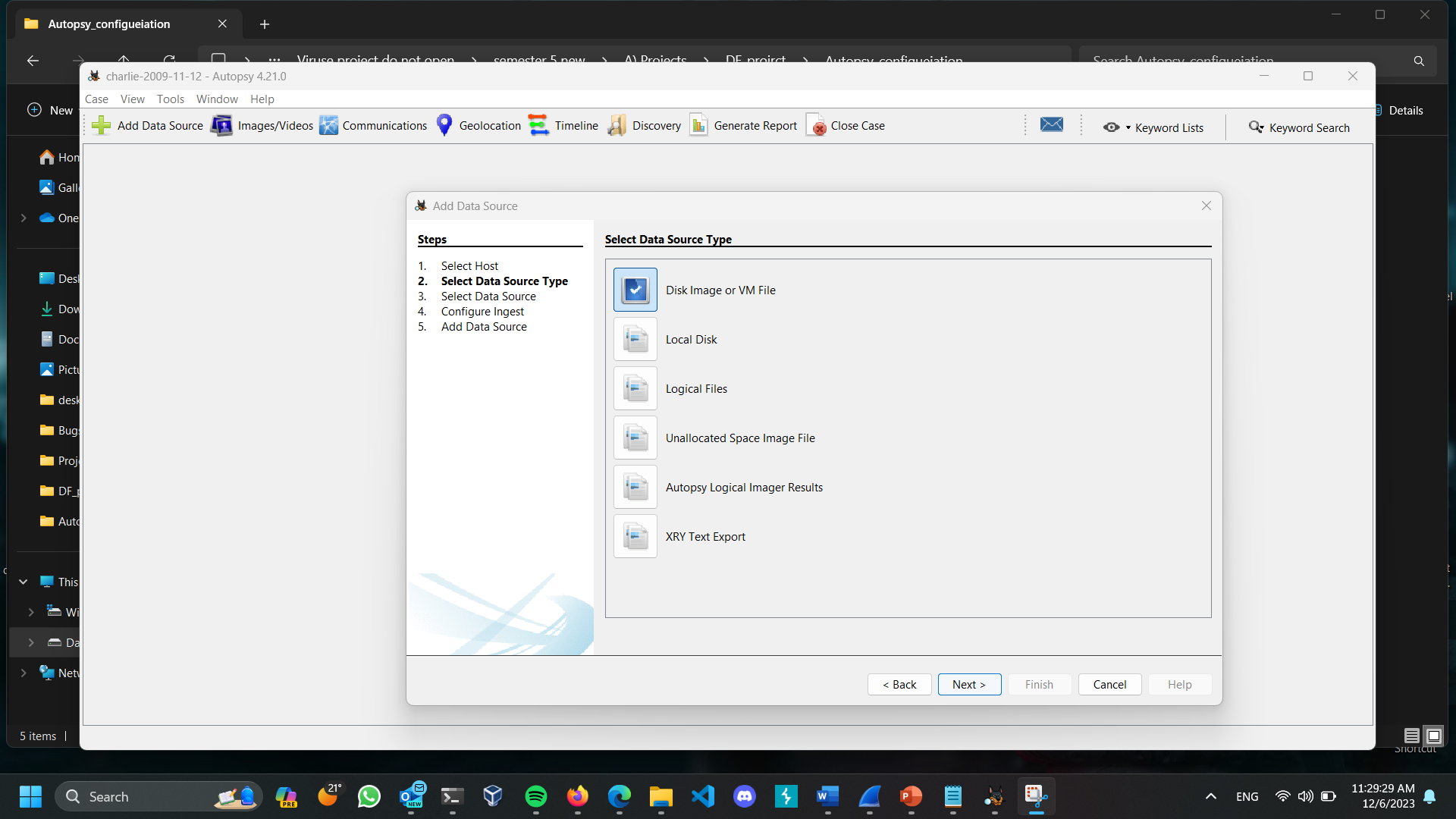
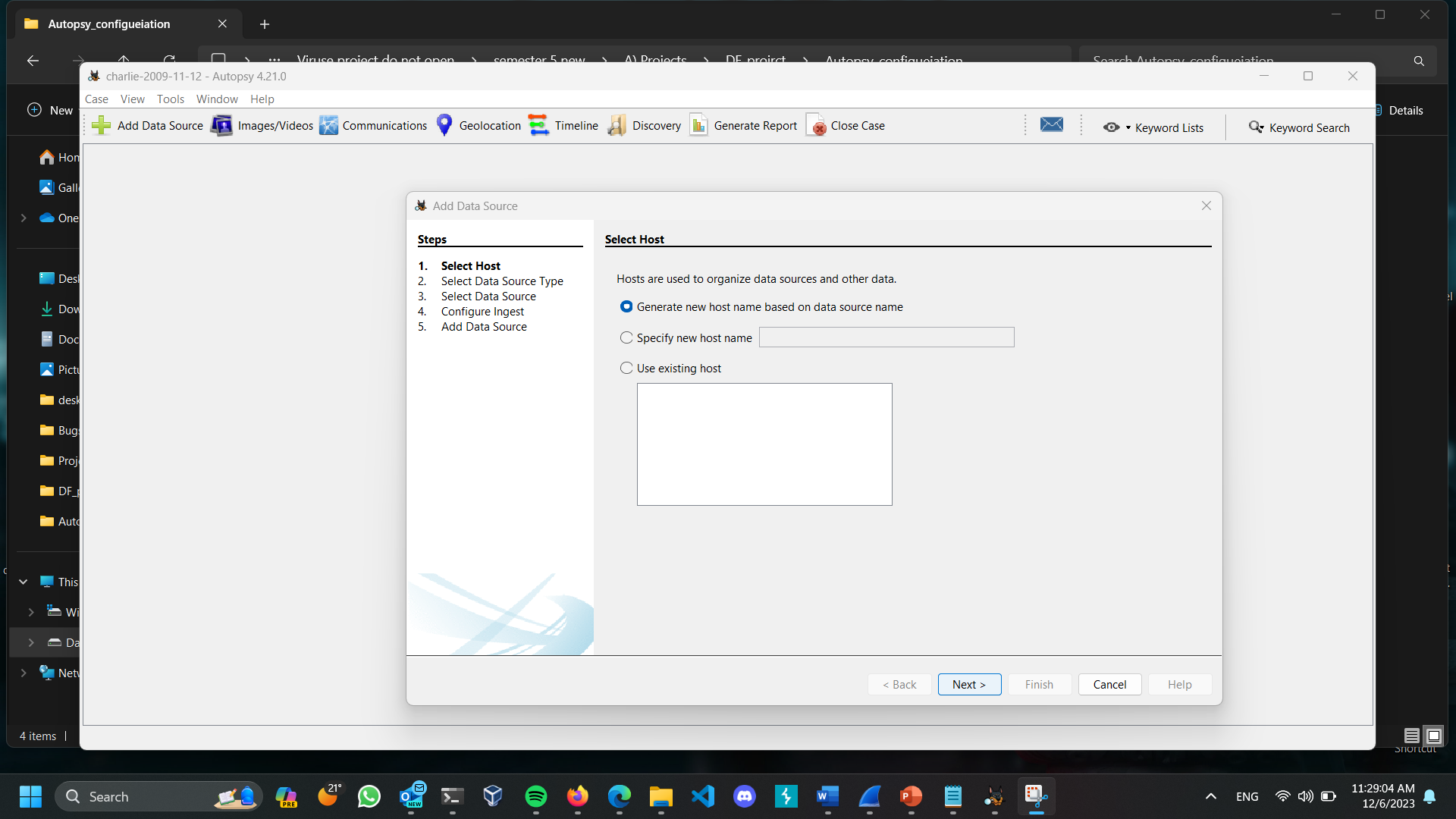
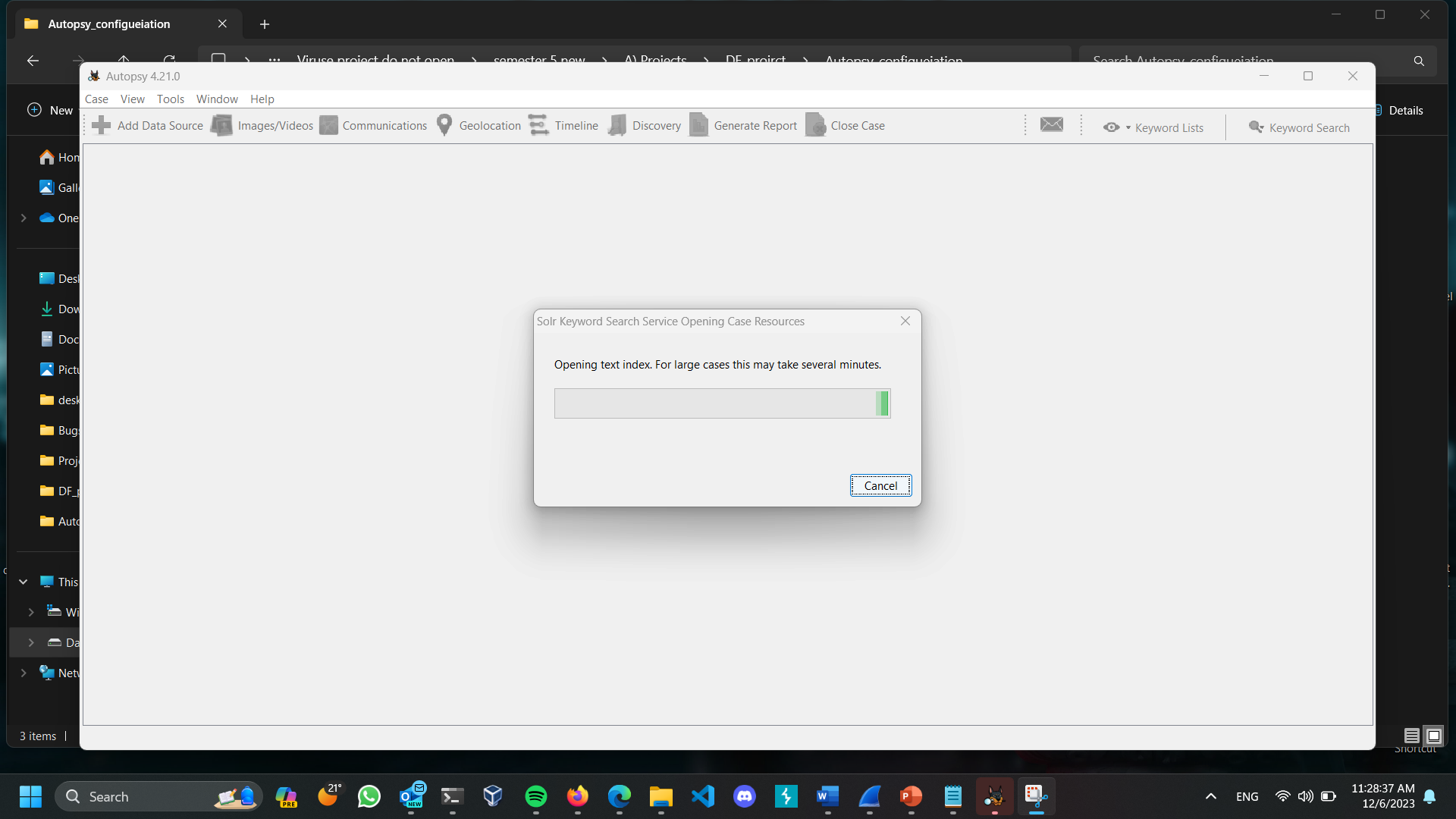
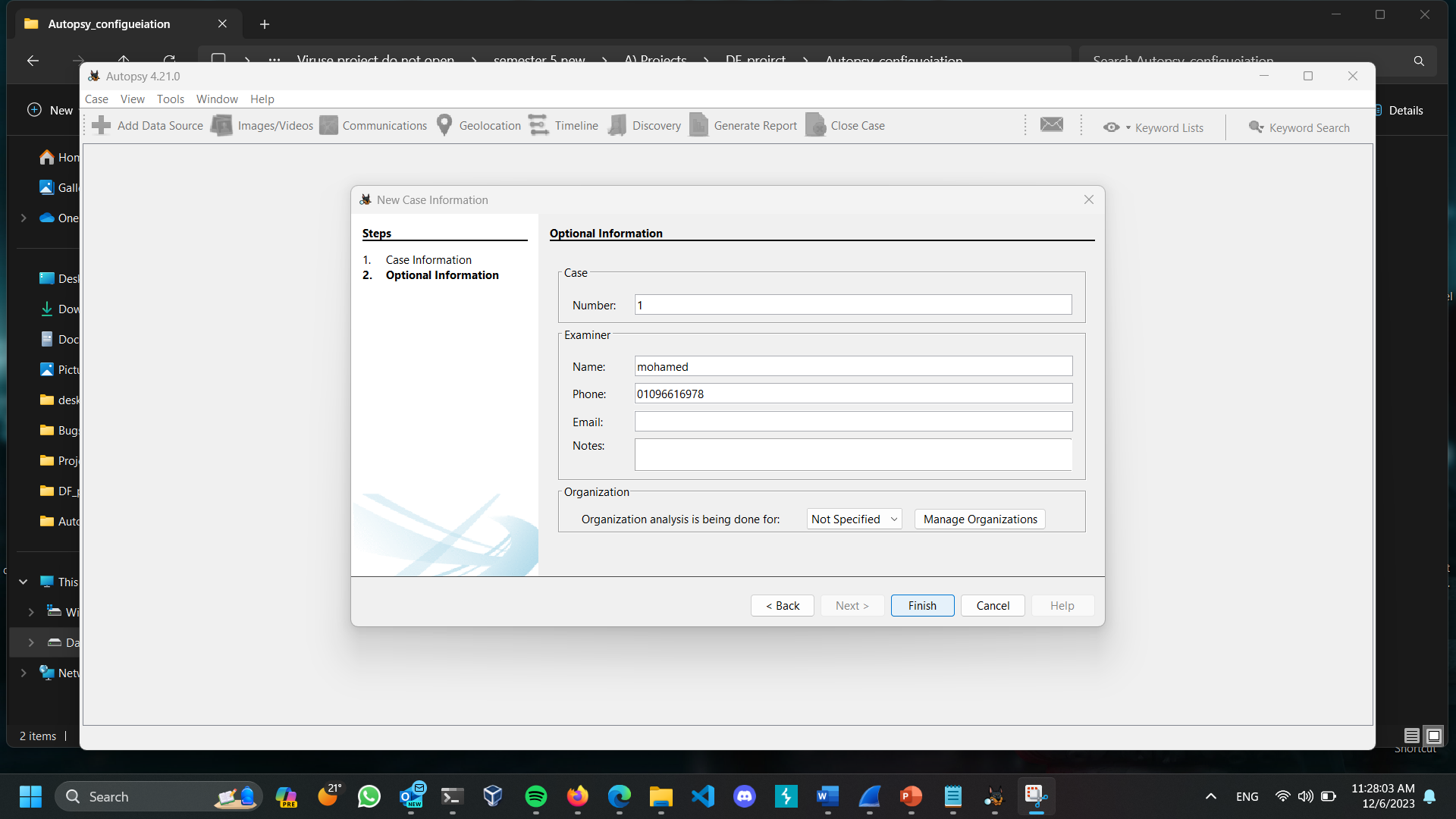
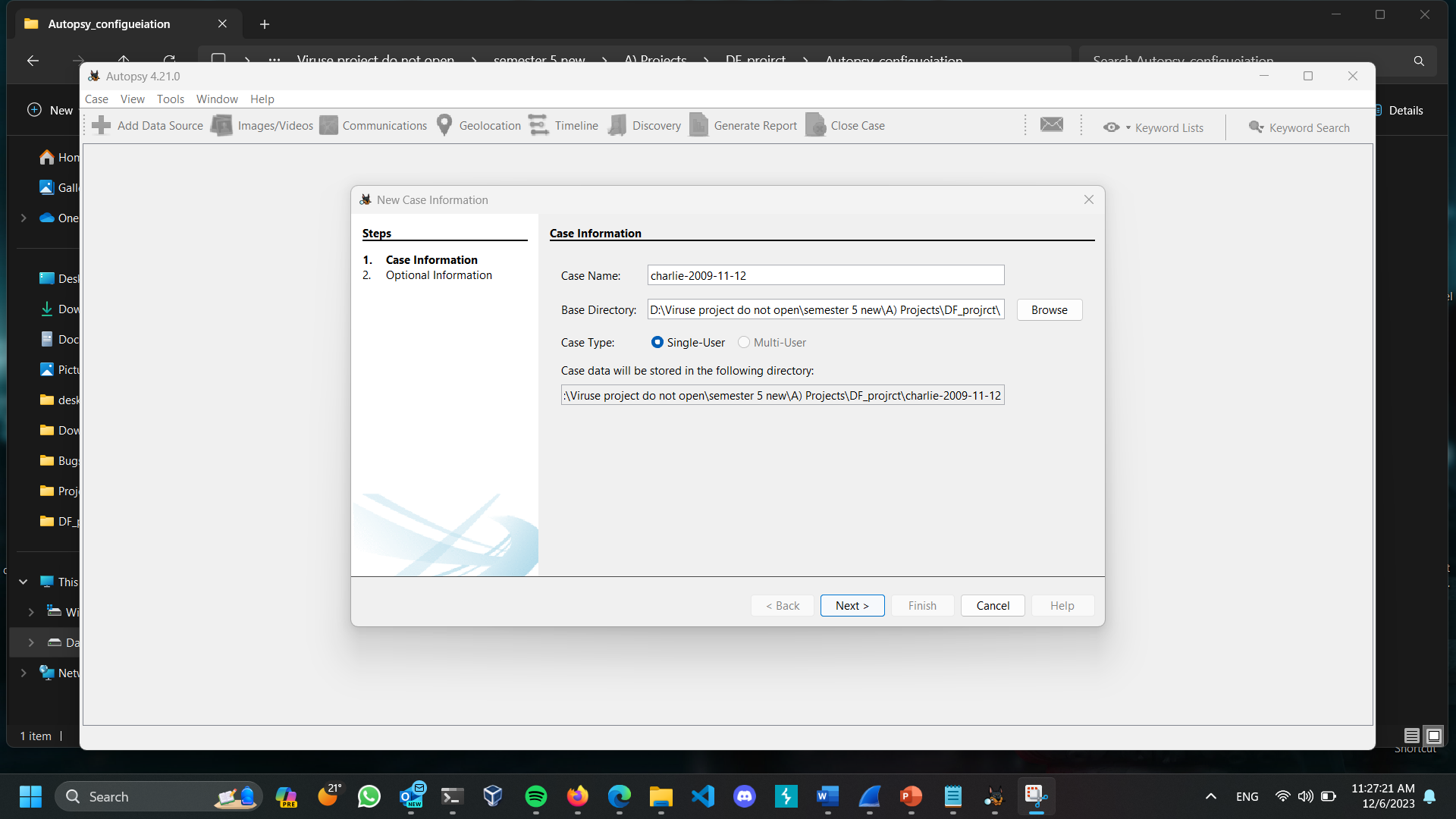
file is intact because ,I used Get-FileHash command to get the value of image file is

AD2F61D34627D5687583A22A410721F2B2B5B52A753905D474F08E1747225598

and it is algorithm is **SHA256** , which they are the same values and algorithm of original data.

**3) Load the image file with Autopsy and analyze the output of the extraction. (show screenshots of the configuration)**



****

**4) You are asked to write a report about the disk image describing all the details of the extracted data.**

**For group 8: Charlie 2009-11-12 Disk** https://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/drives-redacted/

**the SHA256 hash is:** AD2F61D34627D5687583A22A410721F2B2B5B52A753905D474F08E1747225598

**Team member name 1: Mohamed Ehab Osman**

**Team member ID 1 : 7036005**

**Team member name 2: Marco**

**Team member ID 2 :**