# Objective: Recover the Tolkien Ring—Questions Only

After talking to Santa on the North Pole to get your objectives, find the entrance to the underground caverns the elves and sporcs (!) have carved. Then find your way to the Tolkien Ring.

A picture containing text

Description automatically generated A picture containing text, paper

Description automatically generated

## Wireshark Practice

Click the Wireshark Phishing terminal next to Sparkle Redberry to get started with this challenge. Basic networking skills and knowledge of what can be found in packet captures are essential for cyber security

A picture containing text

Description automatically generatedText

Description automatically generated

The suspicious pcap you will analyze is available in the link in the objective, or in the PCAP link that Sparkle talks about. Here is the link: <https://storage.googleapis.com/hhc22_player_assets/suspicious.pcap>

Remember to type hint in the top panel of the terminal if you need help. When you complete the terminal, it will automatically exit and give you credit for the objective on your badge.

Graphical user interface, website

Description automatically generated Text

Description automatically generated

## Windows Event Logs

If you work in digital forensics, incident response, threat hunting, or even a SOC, you need to be able to extract information from Windows event logs.

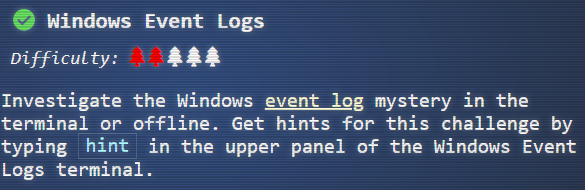
A picture containing graphical user interface

Description automatically generated

Text

Description automatically generated<https://storage.googleapis.com/hhc22_player_assets/powershell.evtx>

Be sure to watch this talk. It gives you valuable information you will need for the challenge.  
Text

Description automatically generated  
<http://www.youtube.com/watch?v=5NZeHYPMXAE>  
  
<https://storage.googleapis.com/hhc22_player_assets/powershell.evtx>

Both Dusty’s discussion and the objective give you a link to the event log you will need.

Pay careful attention to the Event ID that Eric uses in the talk. It will save time for you.

**Your goal is to extract all the commands that were executed. Then you will have what you need to answer the questions**.

If you like Linux, the logs are in the terminal in text format, and you can do everything with grep. One thing to note: one of your searches may need the line following the match to give you the information you need.   
grep -A 1  
to the rescue!

If you like PowerShell, note that at 7:00 in Eric’s talk he starts working on powershelllogs. txt. The download is in evtx format. To get to text so you can follow along with Eric’s PowerShell, open powershell.evtx in Event Viewer. At the far right, select Save All Events As… Then save the file in Tab delimited (\*.txt) format.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

## Suricata Regatta

The Snort, and now Suricata, rule language has become the default for Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Dusty Giftwrap has a hint for you since you solved the Wireshark phish terminal, and Fitzy has something to say as well. This challenge is an extension of the Wireshark phish. You use the same pcap and write Suricata rules to detect that attack.

Text

Description automatically generatedA green screen with white text

Description automatically generated with medium confidence<https://suricata.readthedocs.io/en/suricata-6.0.0/rules/intro.html>

Graphical user interface

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

### Question 1

Fitzy wants you to add rules to his existing suricata.rules file. He wants you to create a rule that alerts on a DNS lookup (i.e., query) for adv.epostoday.uk. To help you get started, he has a rule in suricata.rules that is similar to what you need.  
alert dns $HOME\_NET any -> any any (msg:"ET WEB\_CLIENT Malicious Chrome Extension Domain Request (stickies .pro in DNS Lookup)"; dns.query; content:"stickies.pro"; nocase; sid:2025218; rev:4;)

The first page in [the suricata document](https://suricata.readthedocs.io/en/suricata-6.0.0/rules/intro.html) is very helpful if you have never done Snort/Suricata rules before; please read it.

Also note that every rule requires a sid with a unique number. That is how suricata keeps track of rules. User rules are traditionally numbered 1,000,000 and up. You do not need the rev unless you want it.

What is the first rule?

### Question 2

Now Fitzy wants you to alert if there is any traffic to the evil IP address.

*“STINC thanks you for your work with that DNS record! In this PCAP, it points to 192.185.57.242.*

*Develop a Suricata rule that alerts whenever the infected IP address 192.185.57.242 communicates with internal systems over HTTP.*

*When there's a match, the message (msg) should read Investigate suspicious connections, possible Dridex infection”*

Some hints:

1. You need to check traffic in both directions instead of one. There’s a symbol for that.
2. You do not need to check for content, the IP address is enough. You do need a sid, though.
3. Fitzy said to check for HTTP.

Question 3

Fitzy has another request. *“We heard that some naughty actors are using TLS certificates with a specific CN. Develop a Suricata rule to match and alert on an SSL certificate for heardbellith.Icanwepeh.nagoya.  
When your rule matches, the message (msg) should read Investigate bad certificates, possible Dridex infection.”*

You will need to use a [TLS keyword](https://suricata.readthedocs.io/en/suricata-6.0.0/rules/tls-keywords.html) to solve this one. In TLS-speak, a CN is a Common Name, often used as the subject. Remember to use the TLS protocol.

### Question 4

Fitzy has one last request for us.

*“OK, one more to rule them all and in the darkness find them. Let's watch for one line from the JavaScript: let byteCharacters = atob. Oh, and that string might be Gzip compressed - I hope that's OK!*

*Just in case they try this again, please alert on that HTTP data with message Suspicious JavaScript function, possible Dridex infection.”*

Do not let the comment about Gzip bother you. If you use the correct keyword, the parser will automatically unzip as needed. Remember that you are looking in the body of the response from the web server.