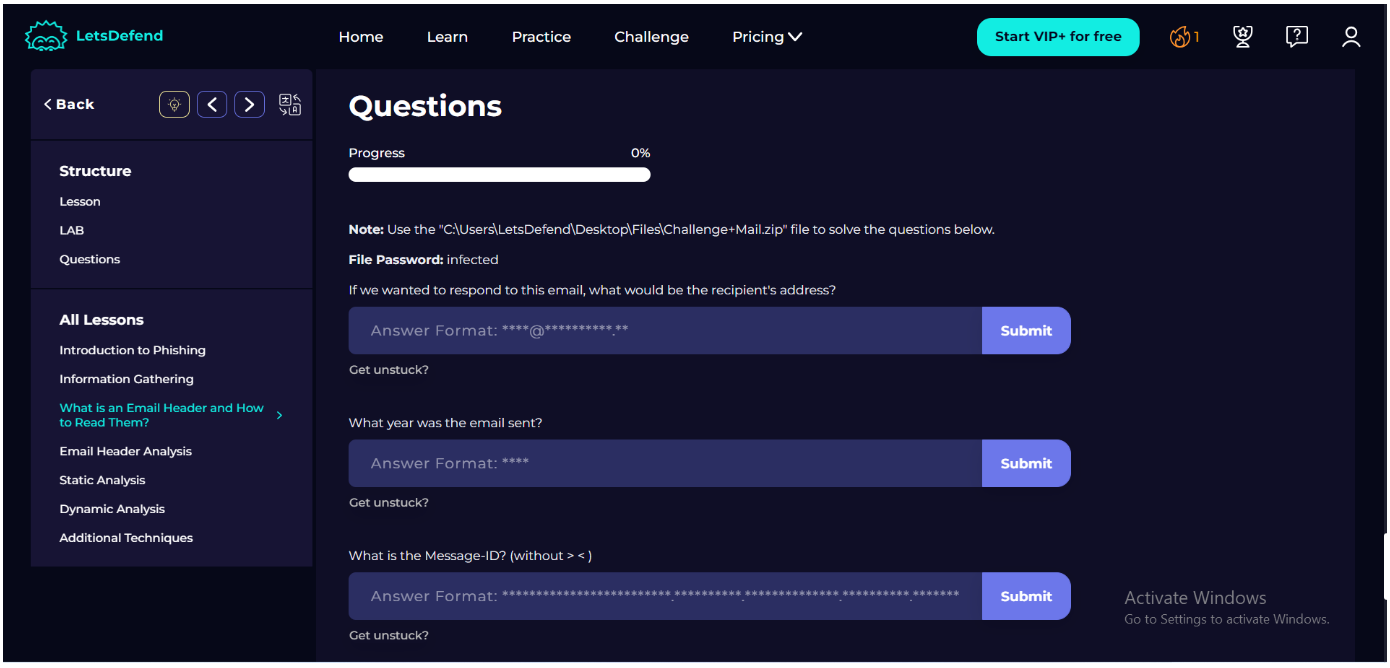
Check Point Active Defense 3.0

https://app.letsdefend.io/training/lessons/phishing-email-analysis
https://app.letsdefend.io/training/lessons/malware-analysis-fundamentals
https://app.letsdefend.io/training/lessons/how-to-investigate-a-siem-alert

QUESTION 1- PHISHING EMAIL ANALYSIS



Questions

Progress 0%

Note: Use the "C:\Users\LetsDefend\Desktop\Files\Challenge+Mail.zip" file to solve the questions below.

File Password: infected

If we wanted to respond to this email, what would be the recipient's address?

Answer Format: ****@**********.** Submit

Get unstuck?

What year was the email sent?

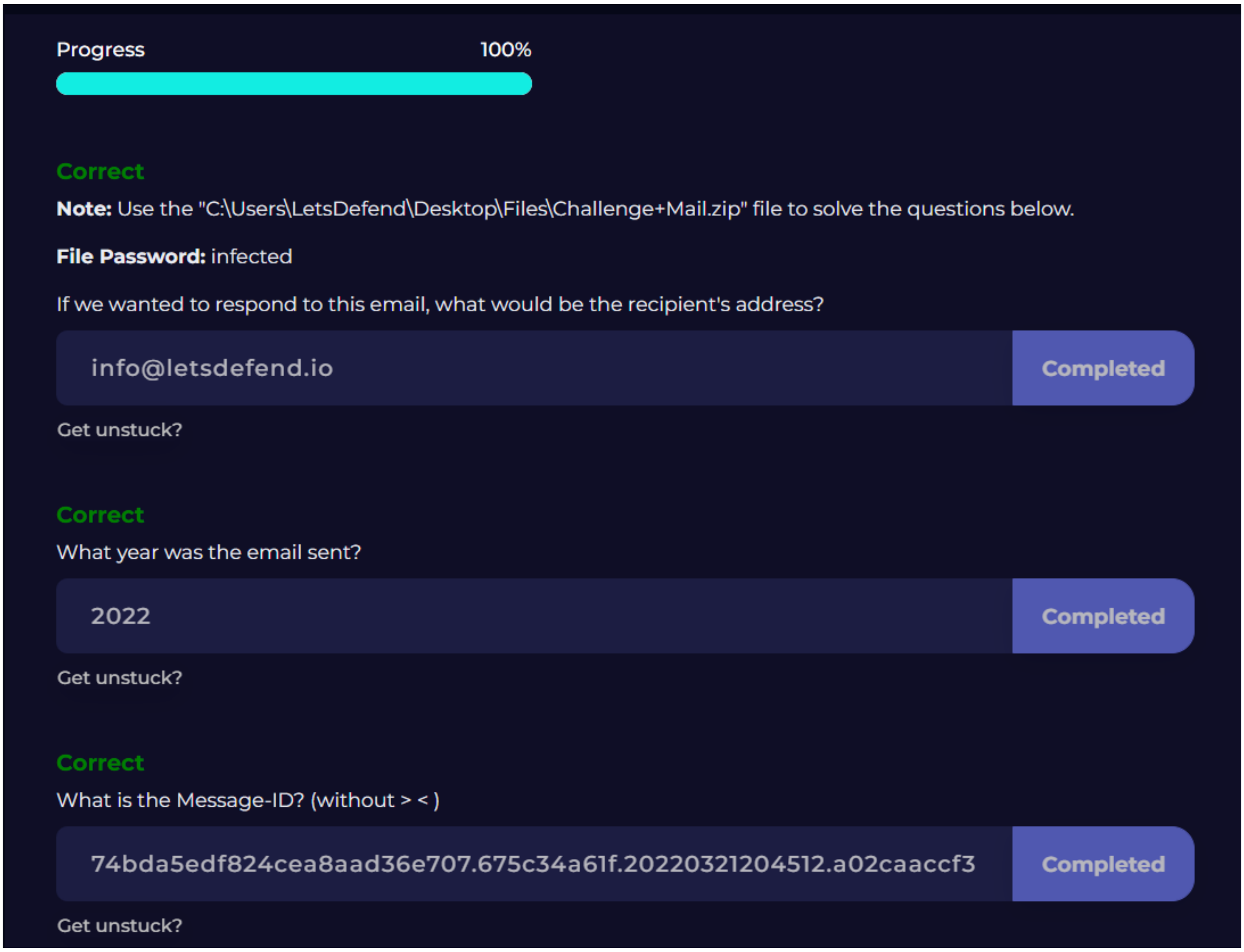
Answer Format: **** Submit

Get unstuck?

What is the Message-ID? (without > <)

Answer Format: ***********************.**********.*************.**********.******* Submit

Get unstuck?



Progress 100%

Correct

Note: Use the "C:\Users\LetsDefend\Desktop\Files\Challenge+Mail.zip" file to solve the questions below.

File Password: infected

If we wanted to respond to this email, what would be the recipient's address?

info@letsdefend.io — Completed

Get unstuck?

Correct

What year was the email sent?

2022 — Completed

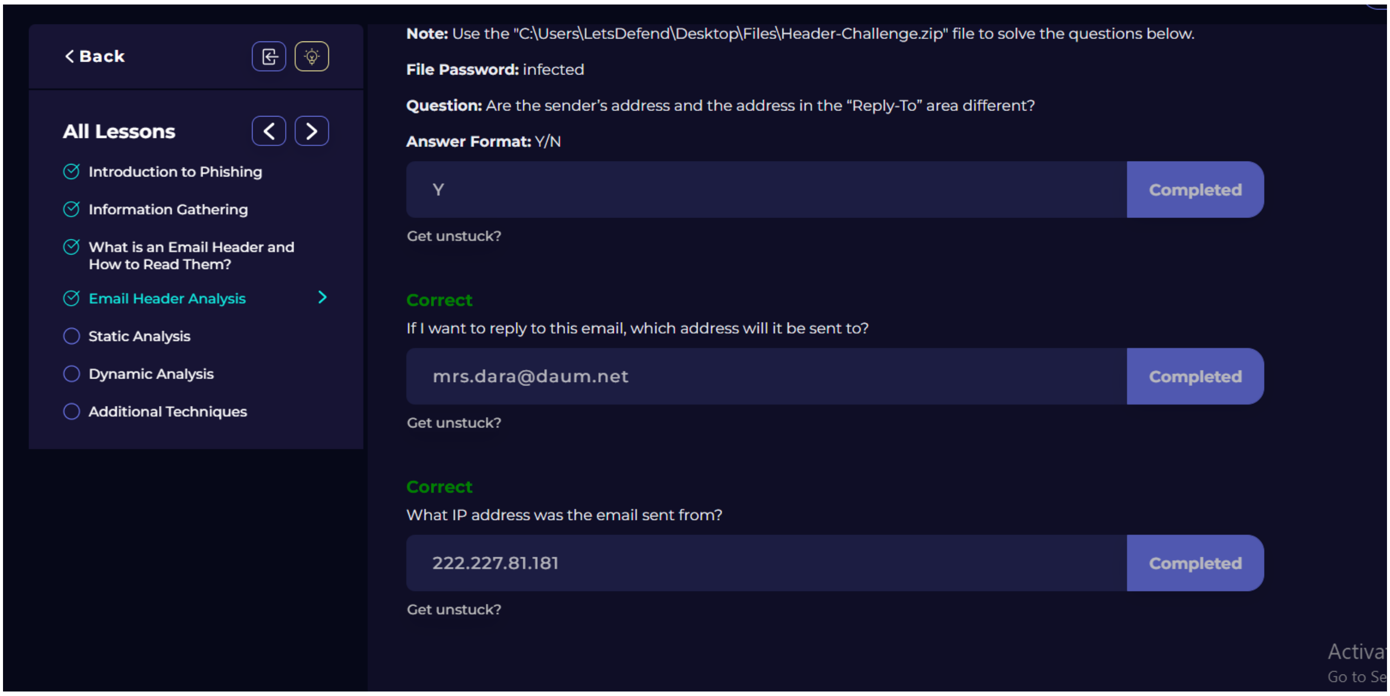
Get unstuck?

Correct

What is the Message-ID? (without > <)

74bda5edf824cea8aad36e707.675c34a61f.20220321204512.a02caaccf3 — Completed

Get unstuck?



All Lessons

- ✓ Introduction to Phishing
- ✓ Information Gathering
- ✓ What is an Email Header and How to Read Them?
- ✓ Email Header Analysis >
- ○ Static Analysis
- ○ Dynamic Analysis
- ○ Additional Techniques

Note: Use the "C:\Users\LetsDefend\Desktop\Files\Header-Challenge.zip" file to solve the questions below.

File Password: infected

Question: Are the sender's address and the address in the "Reply-To" area different?

Answer Format: Y/N

Y — Completed

Get unstuck?

Correct

If I want to reply to this email, which address will it be sent to?

mrs.dara@daum.net — Completed

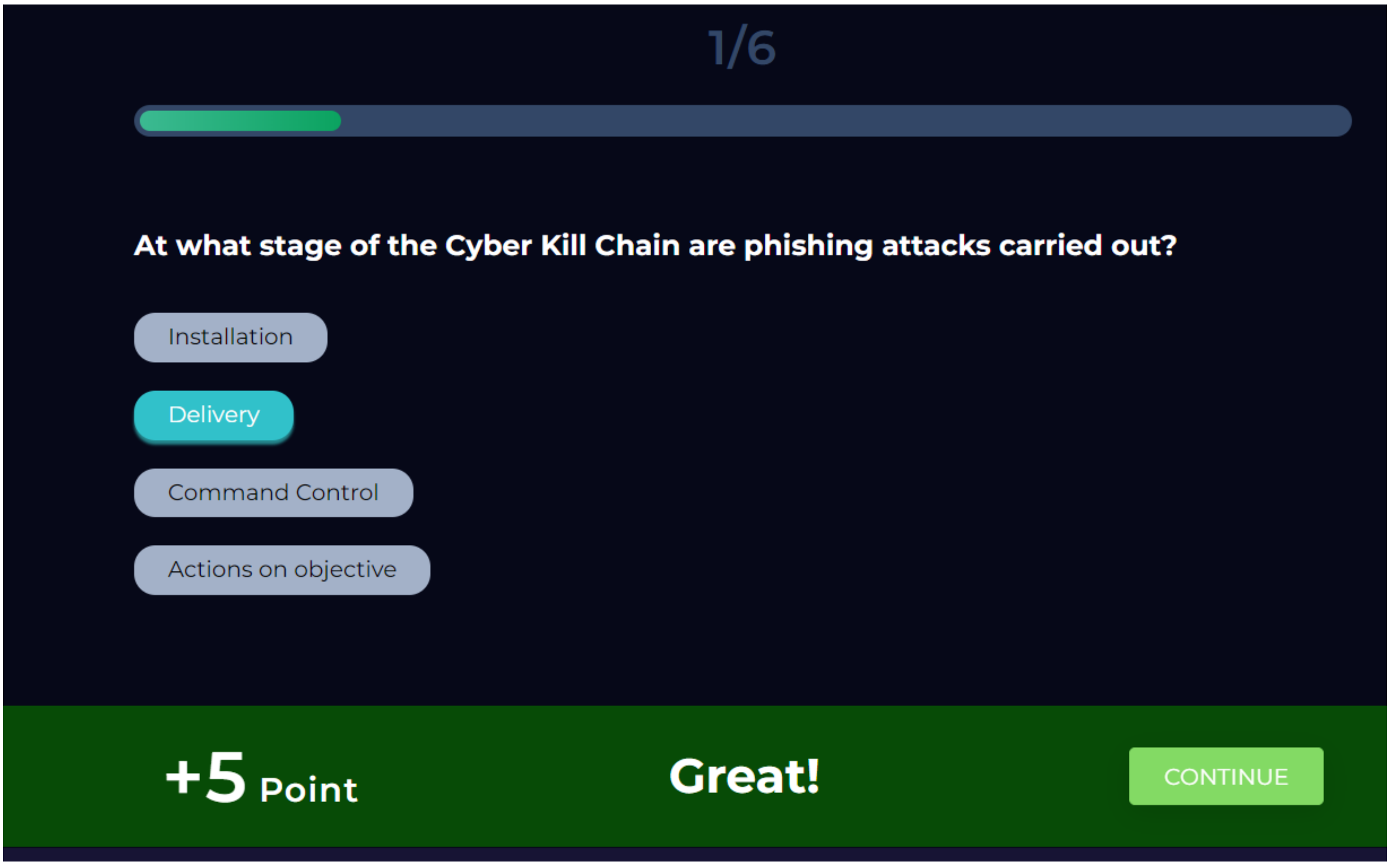
Get unstuck?

Correct

What IP address was the email sent from?

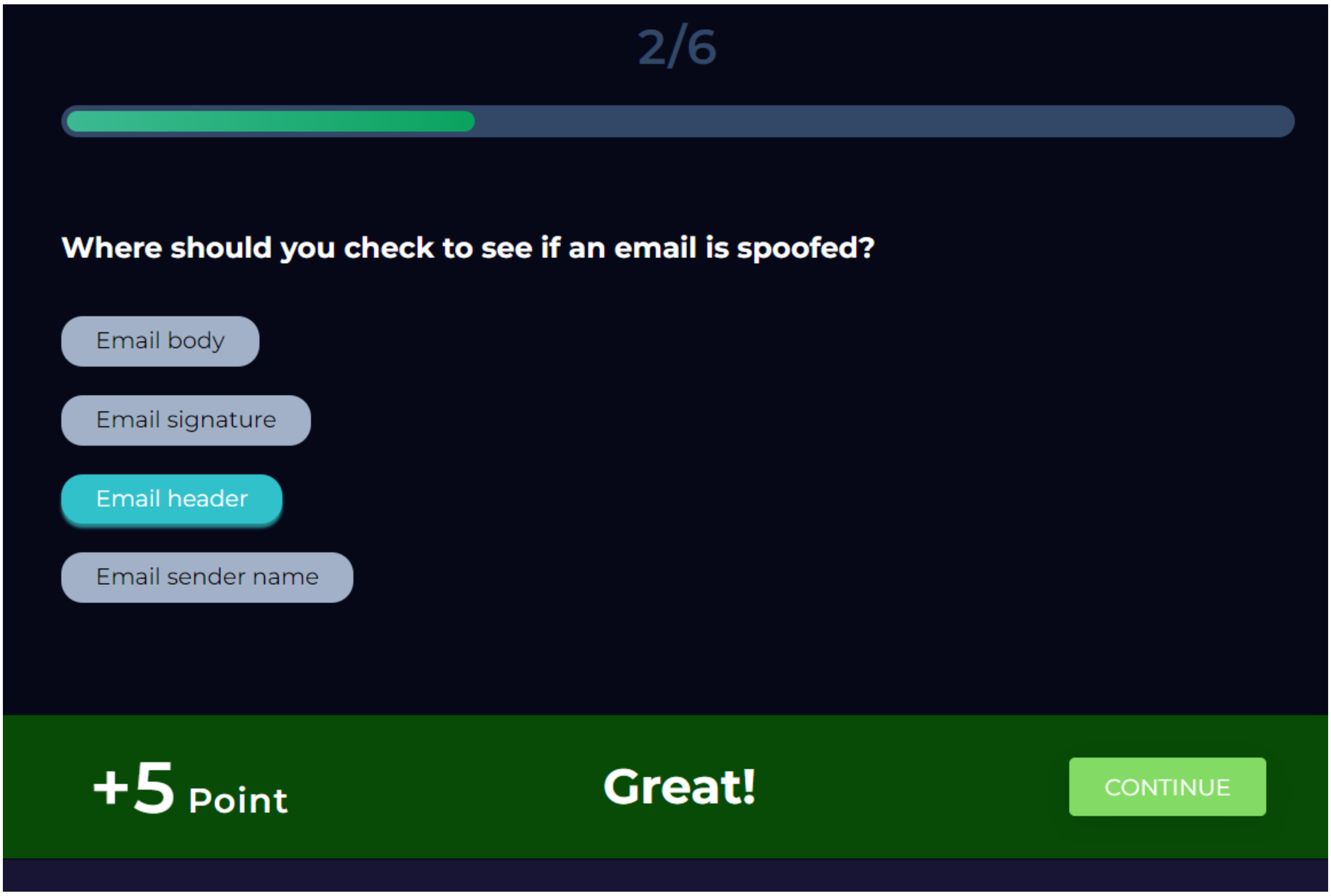
222.227.81.181 — Completed

Get unstuck?



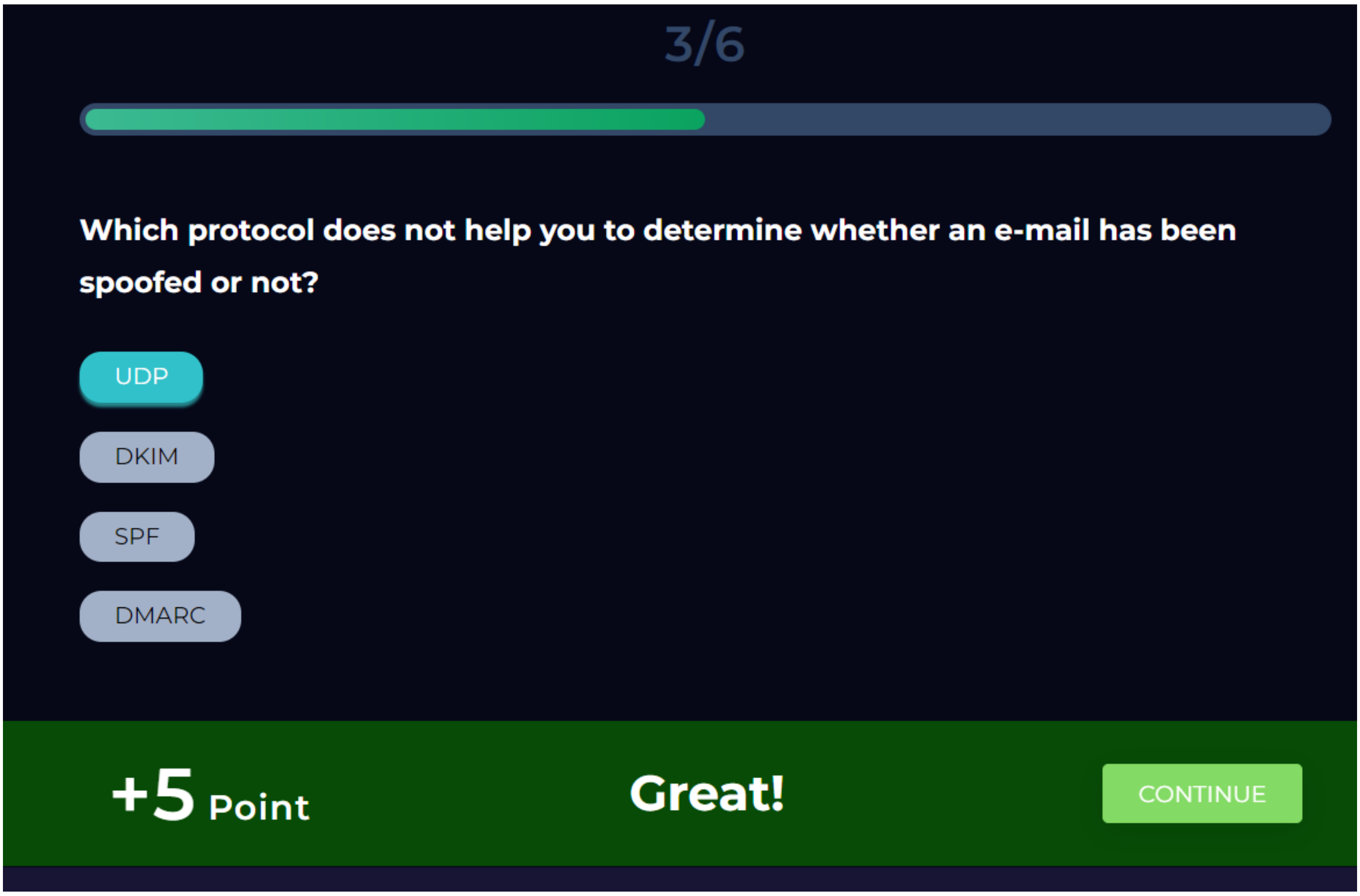
At what stage of the Cyber Kill Chain are phishing attacks carried out?

- Installation
- [✓ Delivery]
- Command Control
- Actions on objective



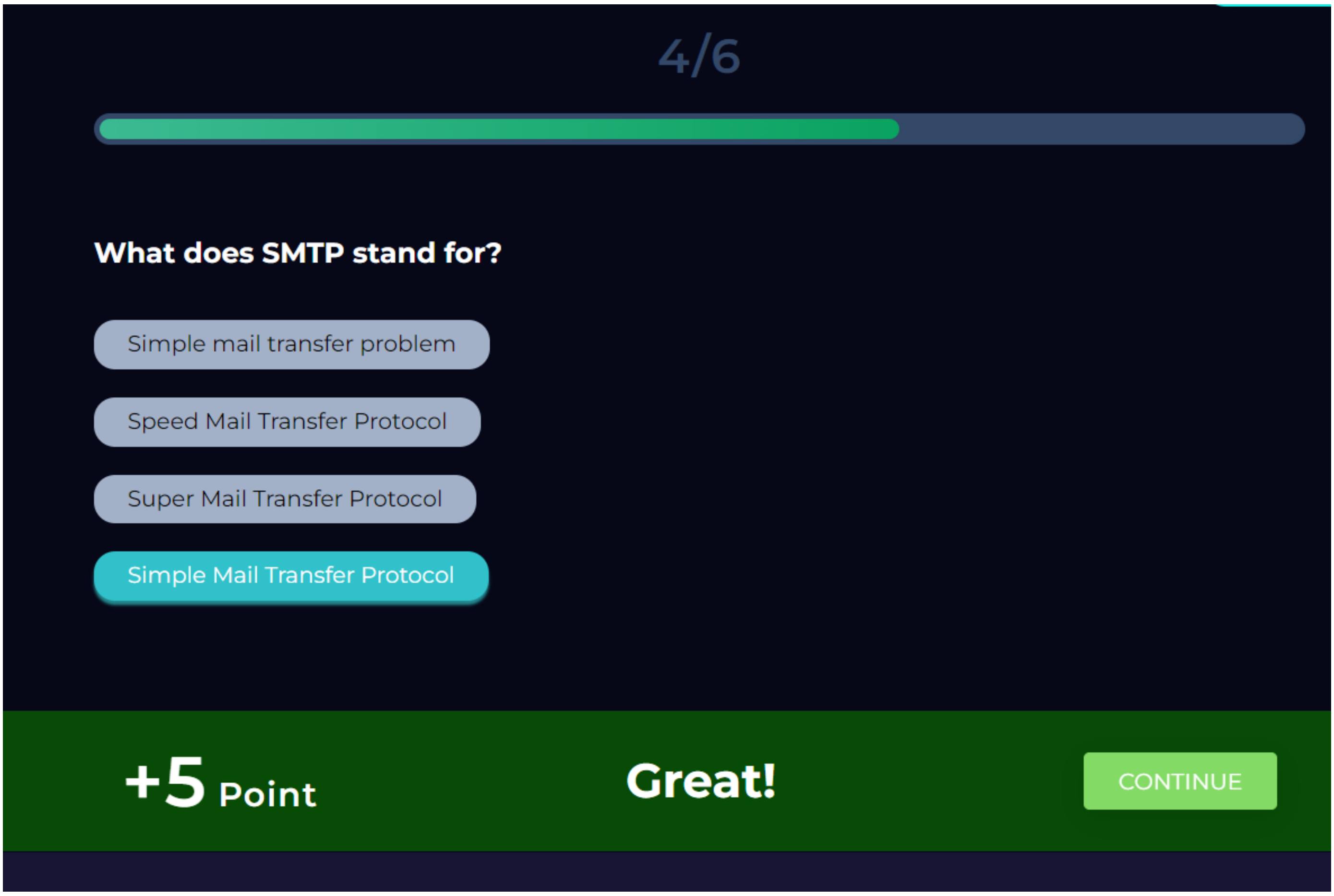
Where should you check to see if an email is spoofed?

- Email body
- Email signature
- [✓ Email header]
- Email sender name



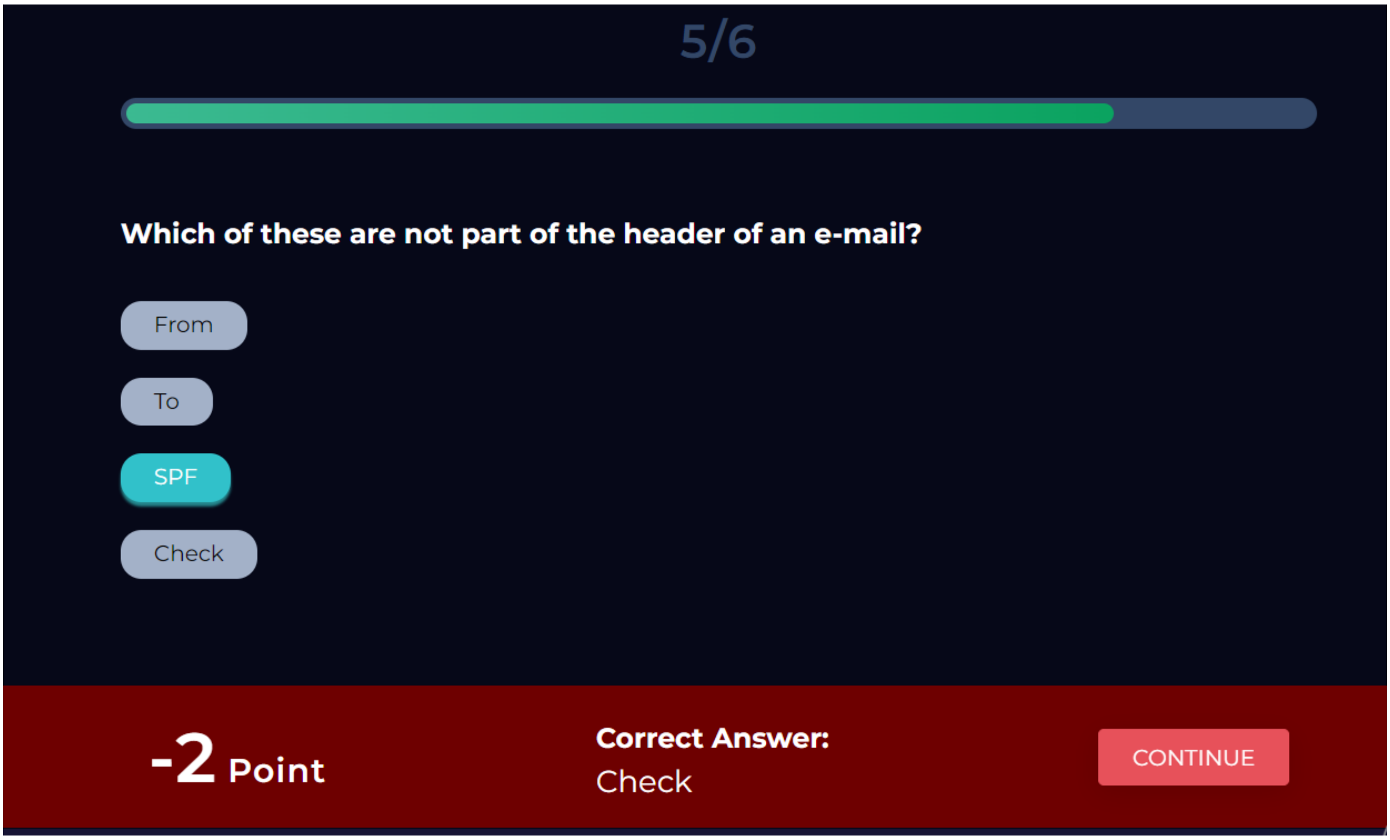
Which protocol does not help you to determine whether an e-mail has been spoofed or not?

- [✓ UDP]
- DKIM
- SPF
- DMARC



What does SMTP stand for?

- Simple mail transfer problem
- Speed Mail Transfer Protocol
- Super Mail Transfer Protocol
- [✓ Simple Mail Transfer Protocol]

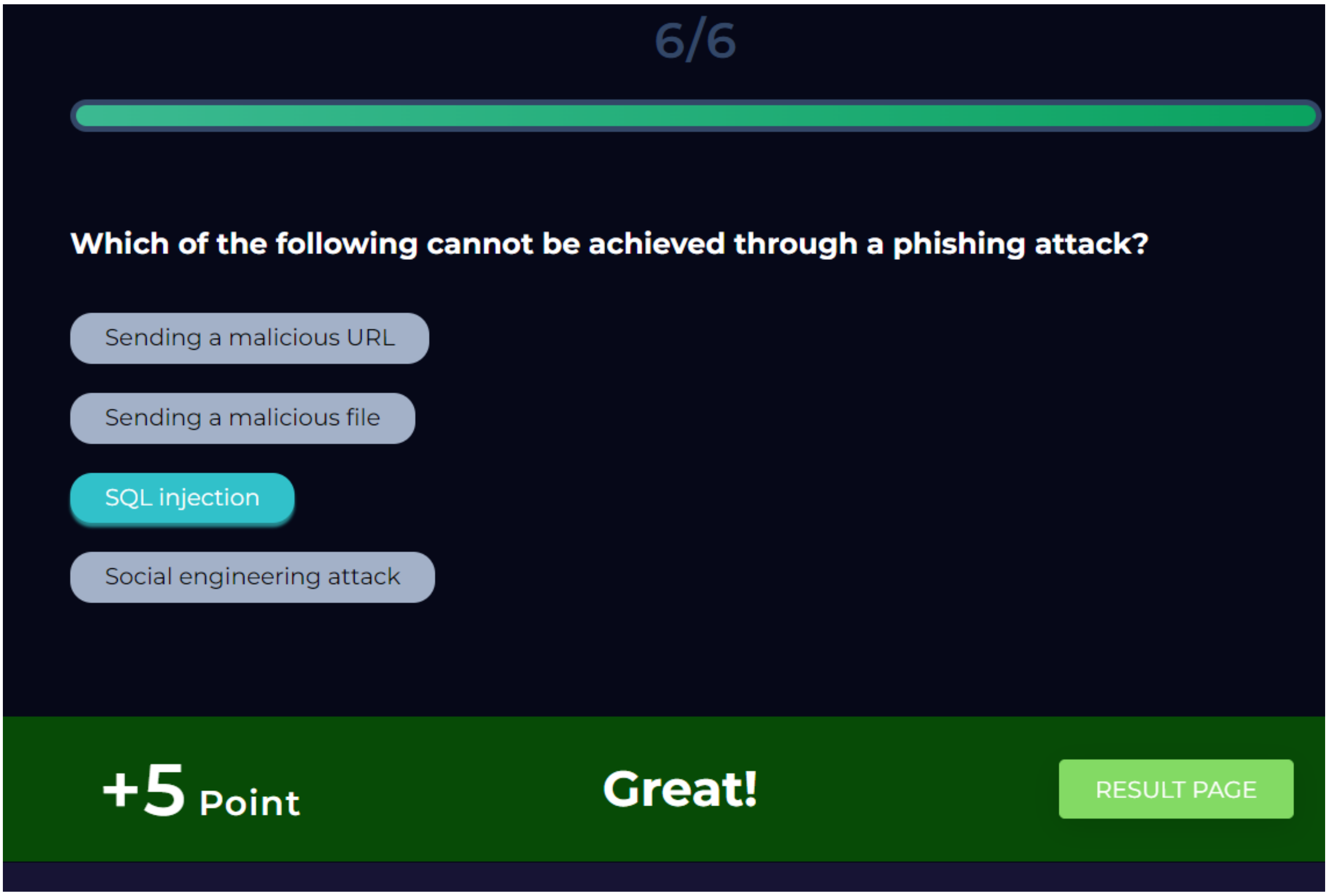


5/6

Which of these are not part of the header of an e-mail?

-2 Point

Correct Answer: Check

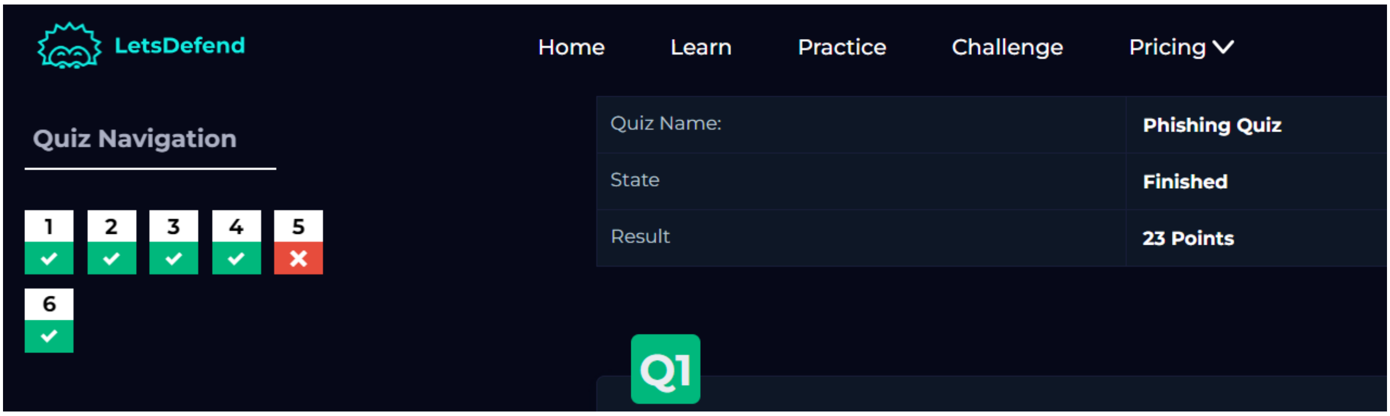


6/6

Which of the following cannot be achieved through a phishing attack?

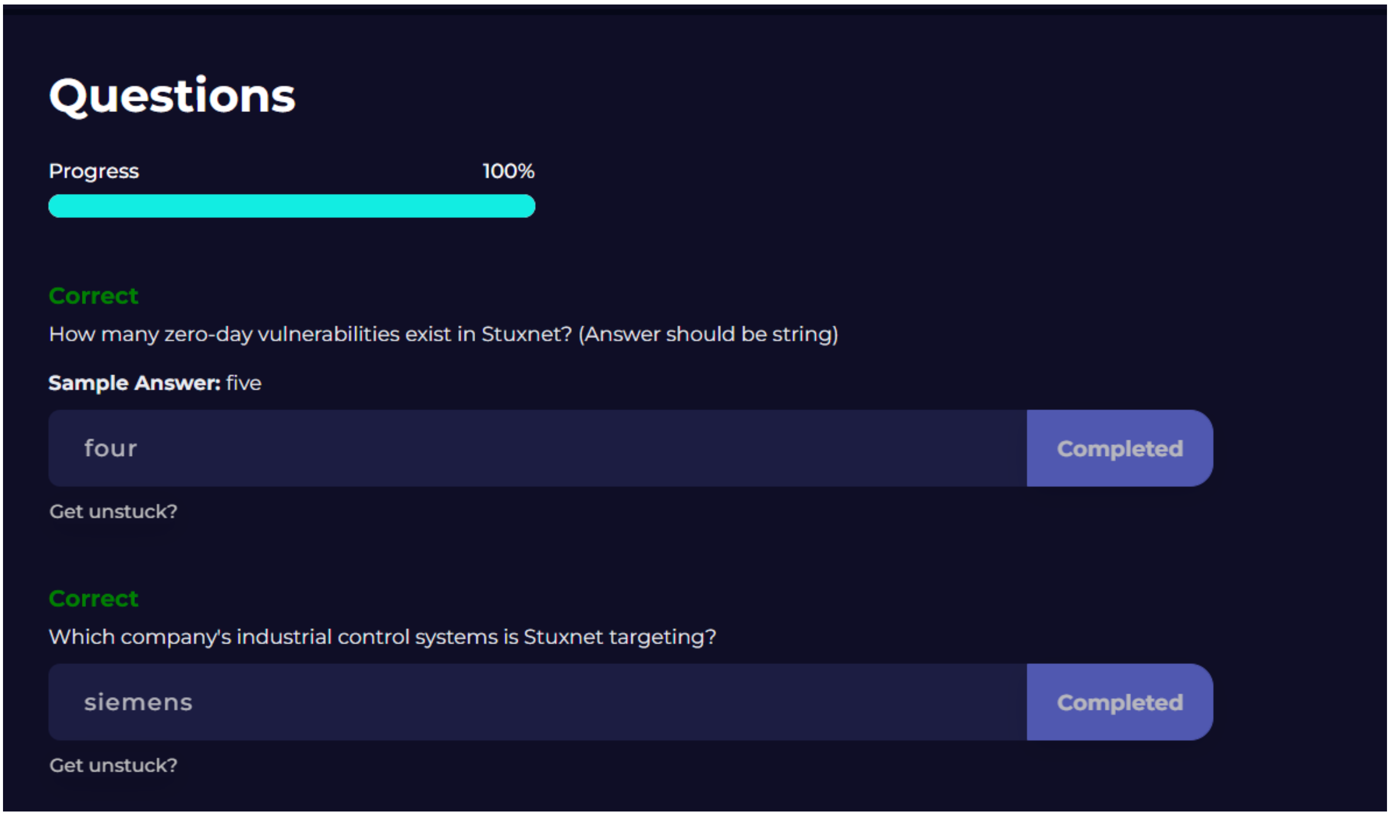
+5 Point

Great!



Quiz Name:	**Phishing Quiz**
State	**Finished**
Result	**23 Points**

QUESTION 2- Malware Analysis



Questions

Progress 100%

Correct

How many zero-day vulnerabilities exist in Stuxnet? (Answer should be string)

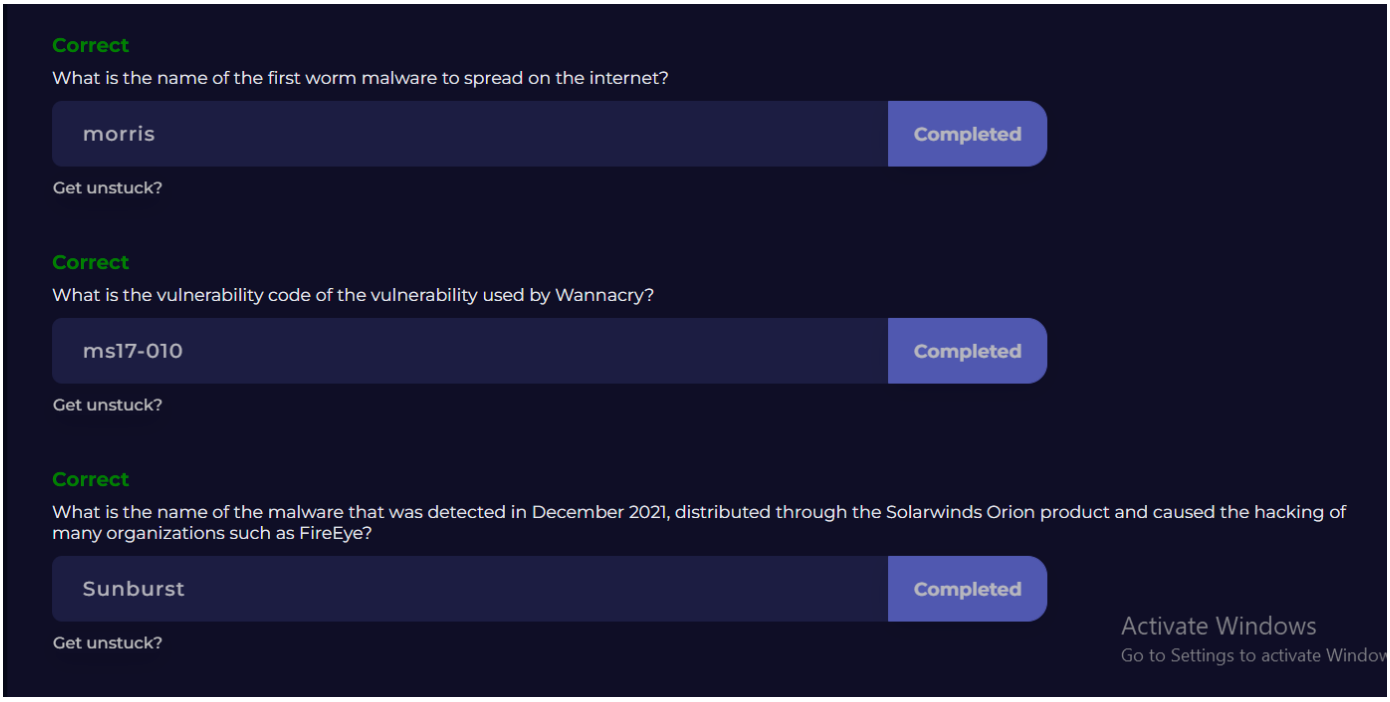
Sample Answer: five

four

Correct

Which company's industrial control systems is Stuxnet targeting?

siemens



Correct

What is the name of the first worm malware to spread on the internet?

morris

Correct

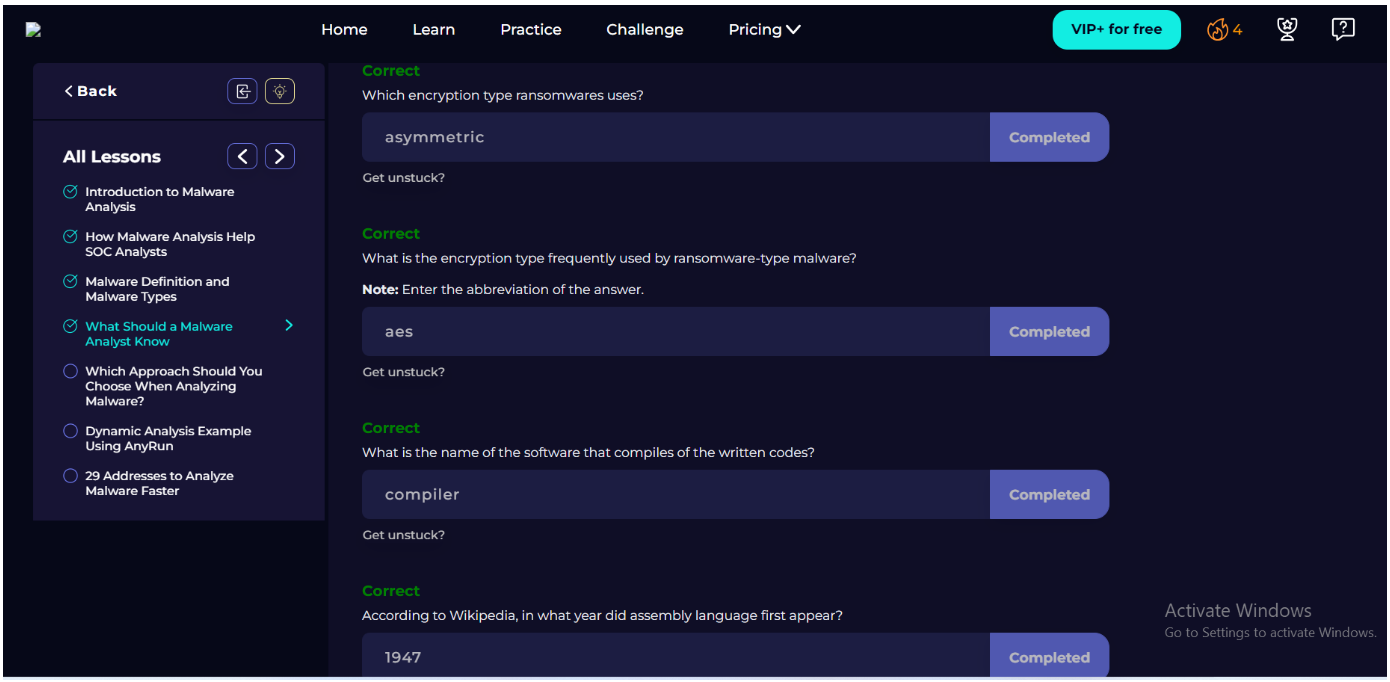
What is the vulnerability code of the vulnerability used by Wannacry?

ms17-010

Correct

What is the name of the malware that was detected in December 2021, distributed through the Solarwinds Orion product and caused the hacking of many organizations such as FireEye?

Sunburst



- Introduction to Malware Analysis
- How Malware Analysis Help SOC Analysts
- Malware Definition and Malware Types
- What Should a Malware Analyst Know
- Which Approach Should You Choose When Analyzing Malware?
- Dynamic Analysis Example Using AnyRun
- 29 Addresses to Analyze Malware Faster

Correct

Which encryption type ransomwares uses?

asymmetric

Correct

What is the encryption type frequently used by ransomware-type malware?

Note: Enter the abbreviation of the answer.

aes

Correct

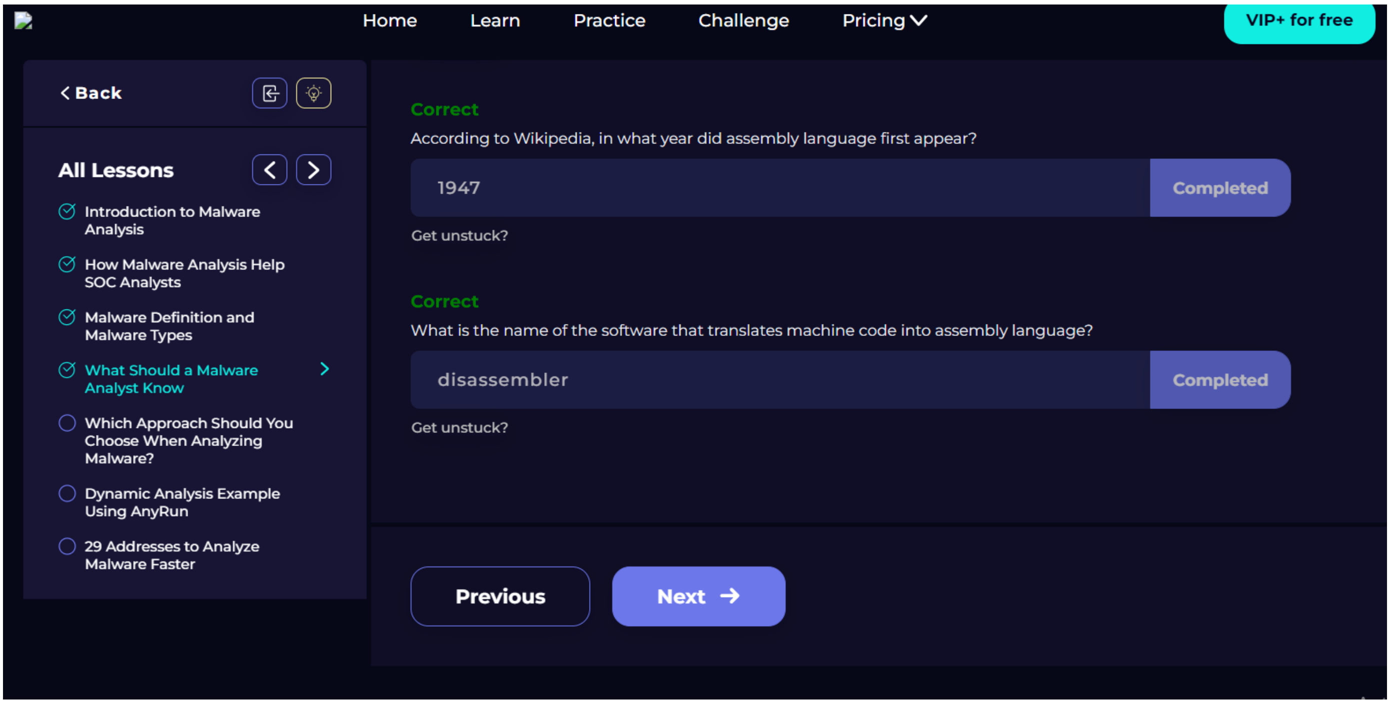
What is the name of the software that compiles of the written codes?

compiler

Correct

According to Wikipedia, in what year did assembly language first appear?

1947


Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Back
All Lessons
✓ Introduction to Malware Analysis
✓ How Malware Analysis Help SOC Analysts
✓ Malware Definition and Malware Types
✓ What Should a Malware Analyst Know
○ Which Approach Should You Choose When Analyzing Malware?
○ Dynamic Analysis Example Using AnyRun
○ 29 Addresses to Analyze Malware Faster

Correct

According to Wikipedia, in what year did assembly language first appear?

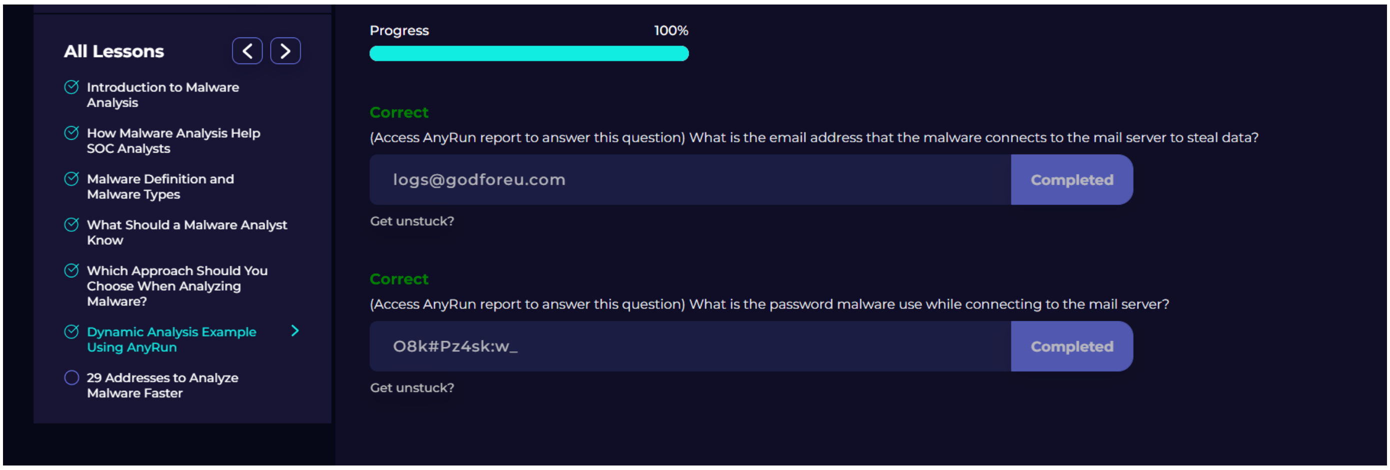
1947

Correct

What is the name of the software that translates machine code into assembly language?

disassembler

Completed
Get unstuck?
Previous
Next


All Lessons
✓ Introduction to Malware Analysis
✓ How Malware Analysis Help SOC Analysts
✓ Malware Definition and Malware Types
✓ What Should a Malware Analyst Know
✓ Which Approach Should You Choose When Analyzing Malware?
✓ Dynamic Analysis Example Using AnyRun
○ 29 Addresses to Analyze Malware Faster
Progress
100%

Correct

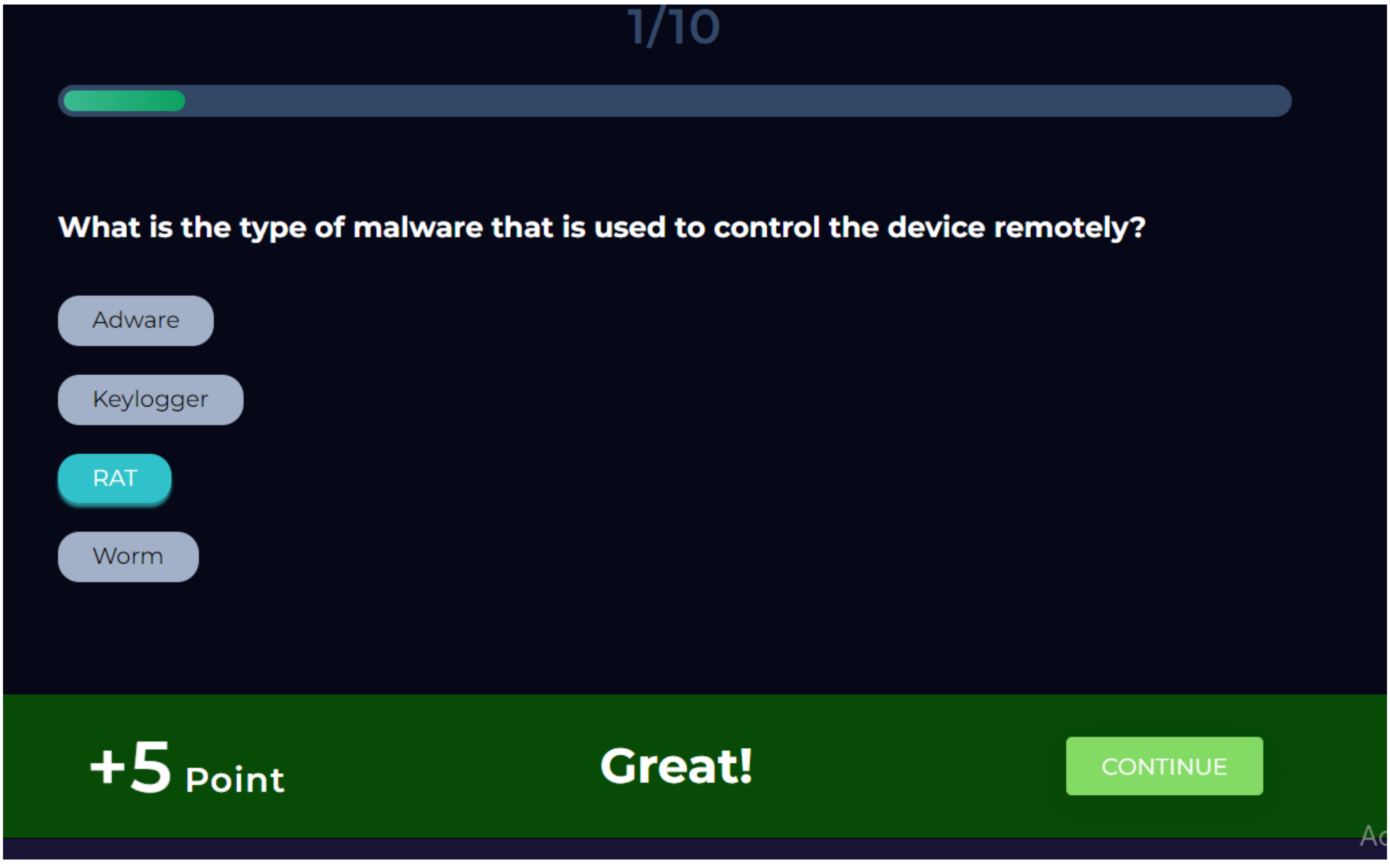
(Access AnyRun report to answer this question) What is the email address that the malware connects to the mail server to steal data?

logs@godforeu.com

Correct

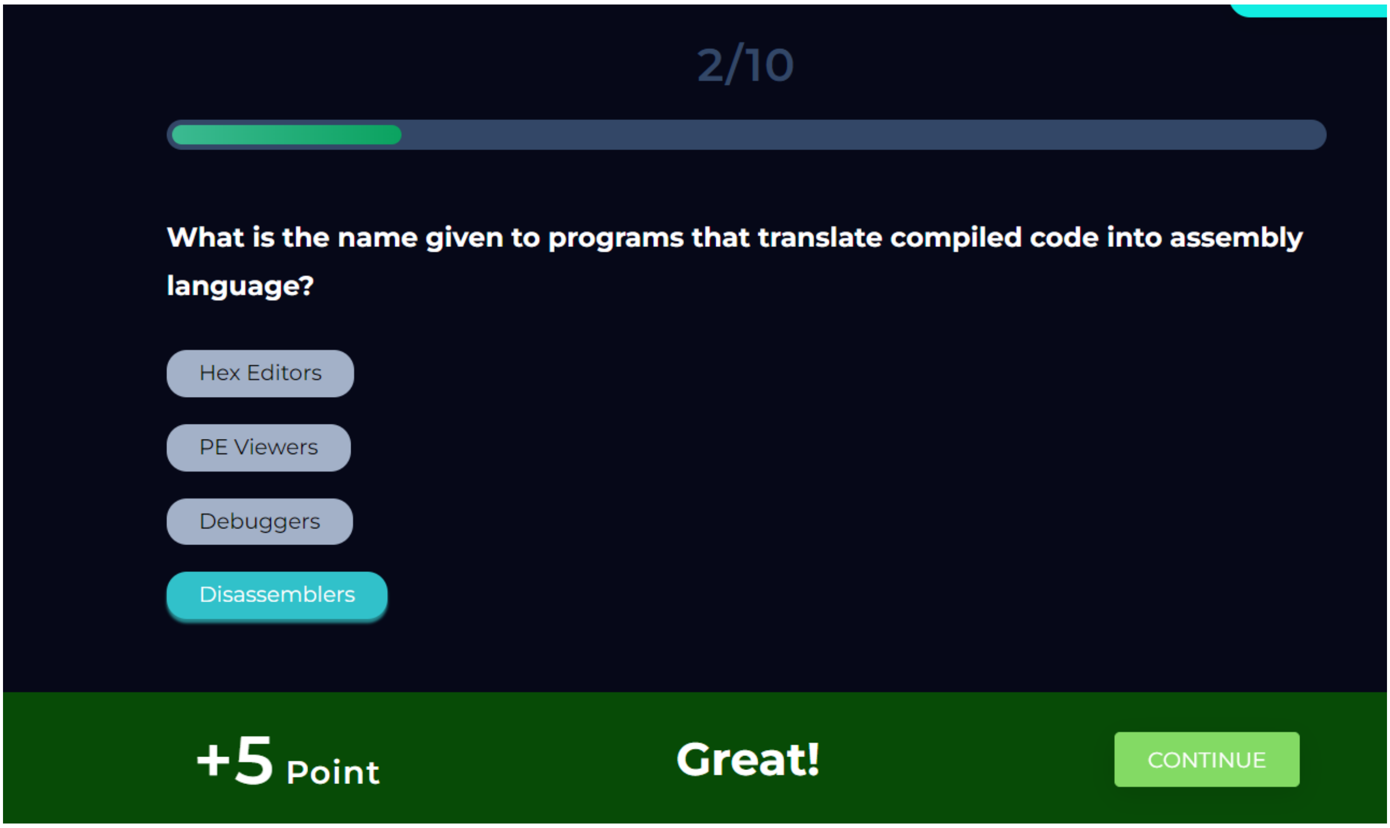
(Access AnyRun report to answer this question) What is the password malware use while connecting to the mail server?

O8k#Pz4sk:w_



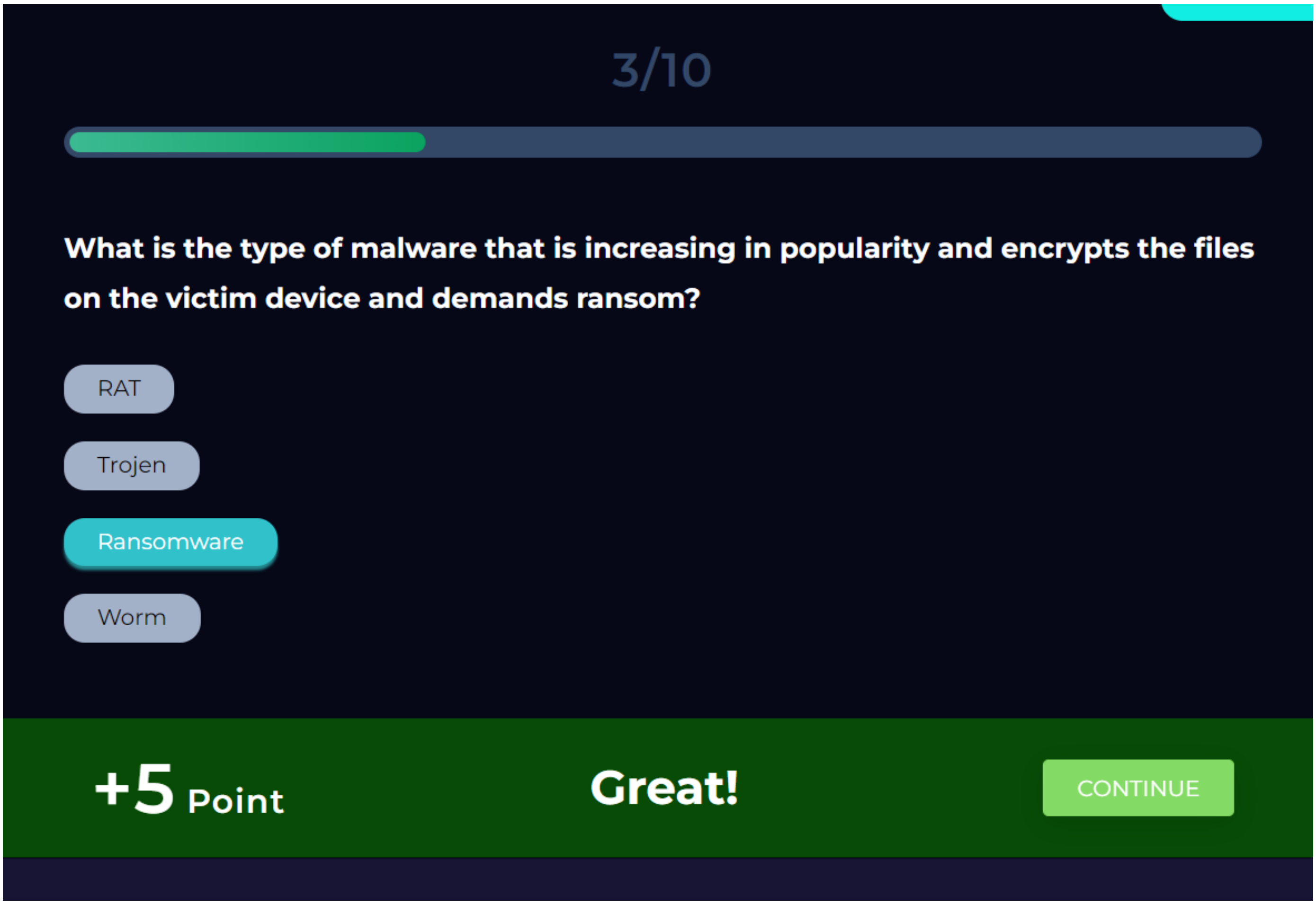
What is the type of malware that is used to control the device remotely?

- Adware
- Keylogger
- [✓ RAT]
- Worm



What is the name given to programs that translate compiled code into assembly language?

- Hex Editors
- PE Viewers
- Debuggers
- [✓ Disassemblers]



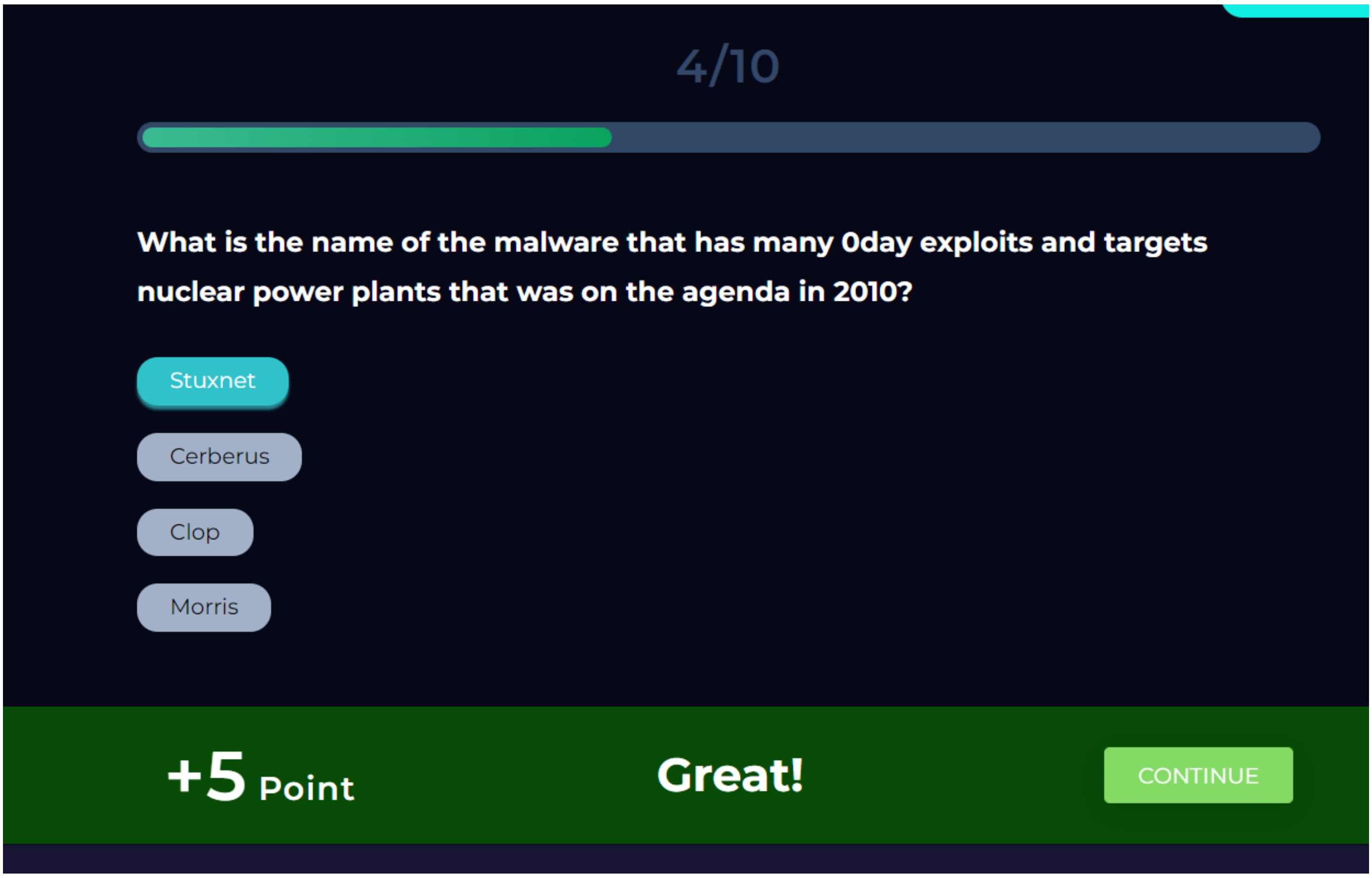
3/10

What is the type of malware that is increasing in popularity and encrypts the files on the victim device and demands ransom?

- RAT
- Trojen
- [✓ Ransomware]
- Worm

+5 Point

Great!



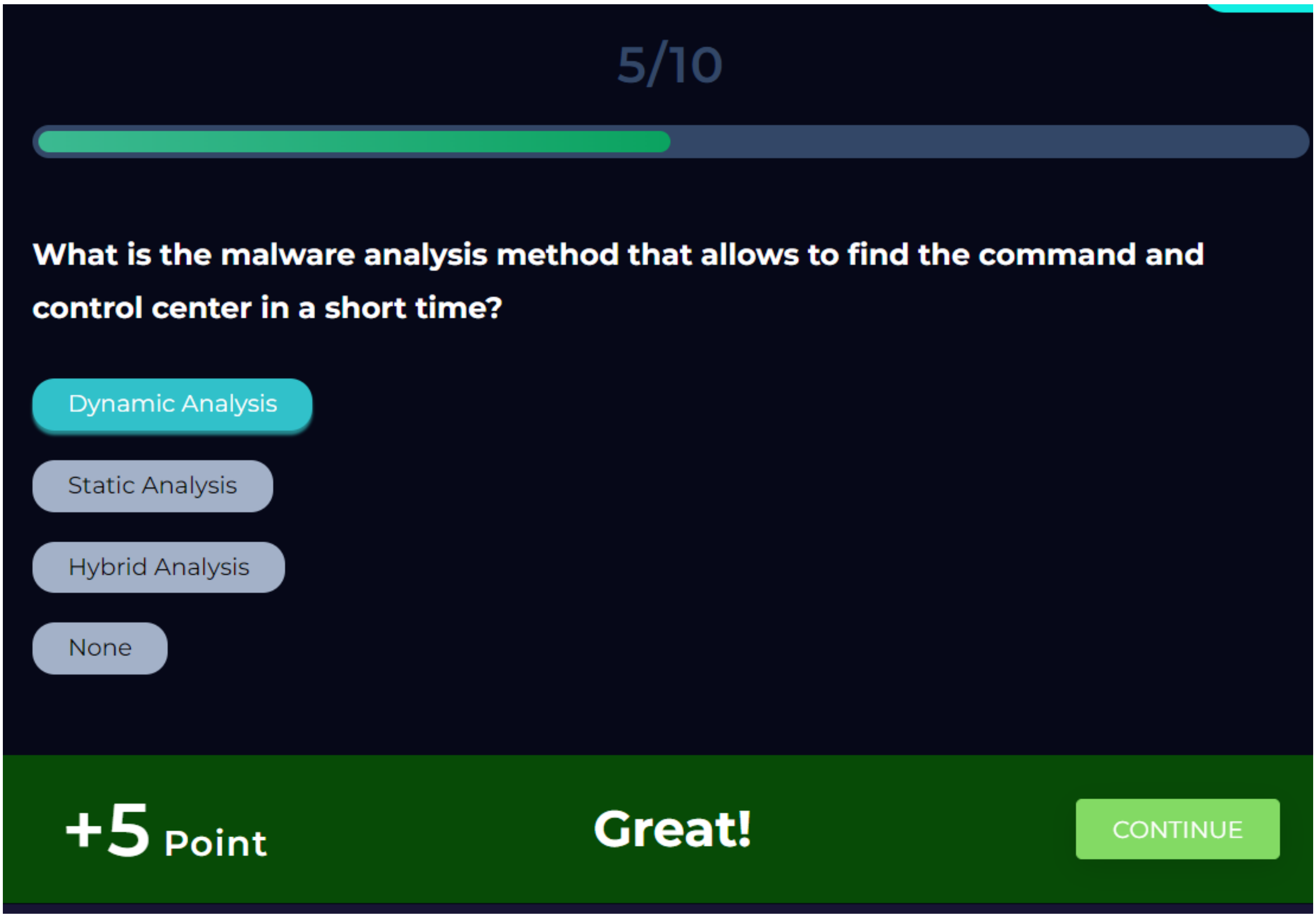
4/10

What is the name of the malware that has many 0day exploits and targets nuclear power plants that was on the agenda in 2010?

- [✓ Stuxnet]
- Cerberus
- Clop
- Morris

+5 Point

Great!



5/10

What is the malware analysis method that allows to find the command and control center in a short time?

[✓ Dynamic Analysis]

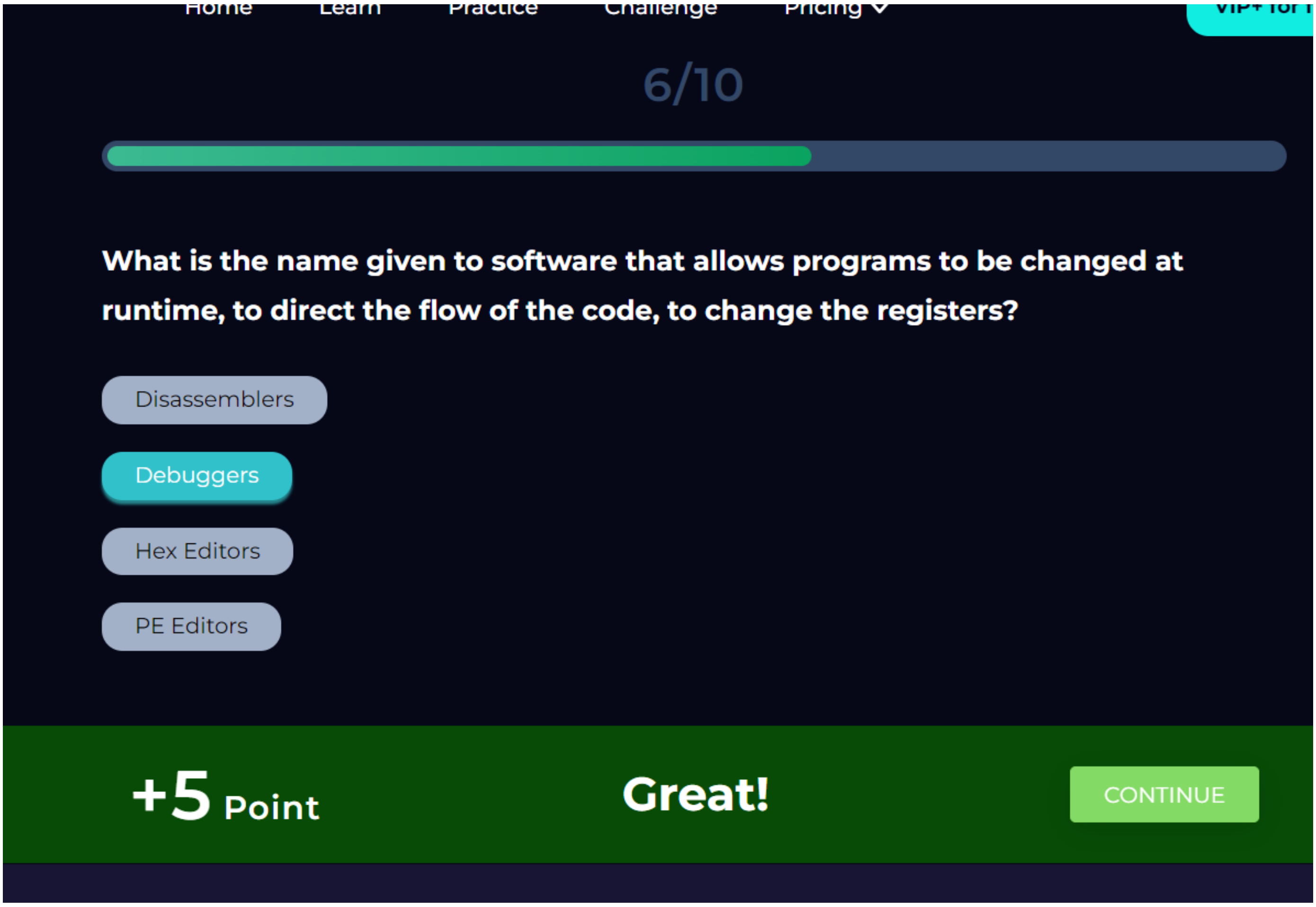
Static Analysis

Hybrid Analysis

None

+5 Point

Great!



6/10

What is the name given to software that allows programs to be changed at runtime, to direct the flow of the code, to change the registers?

Disassemblers

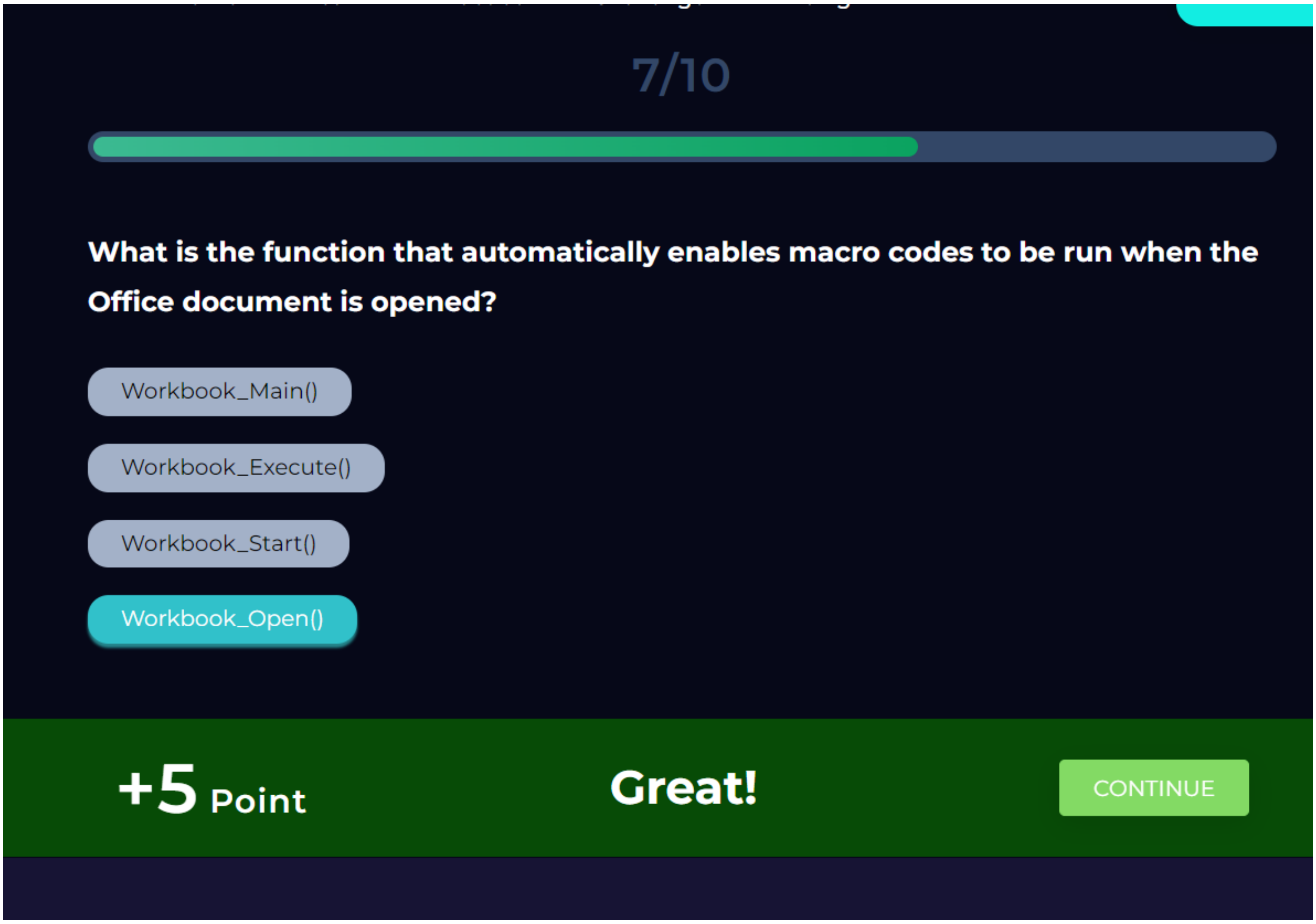
[✓ Debuggers]

Hex Editors

PE Editors

+5 Point

Great!



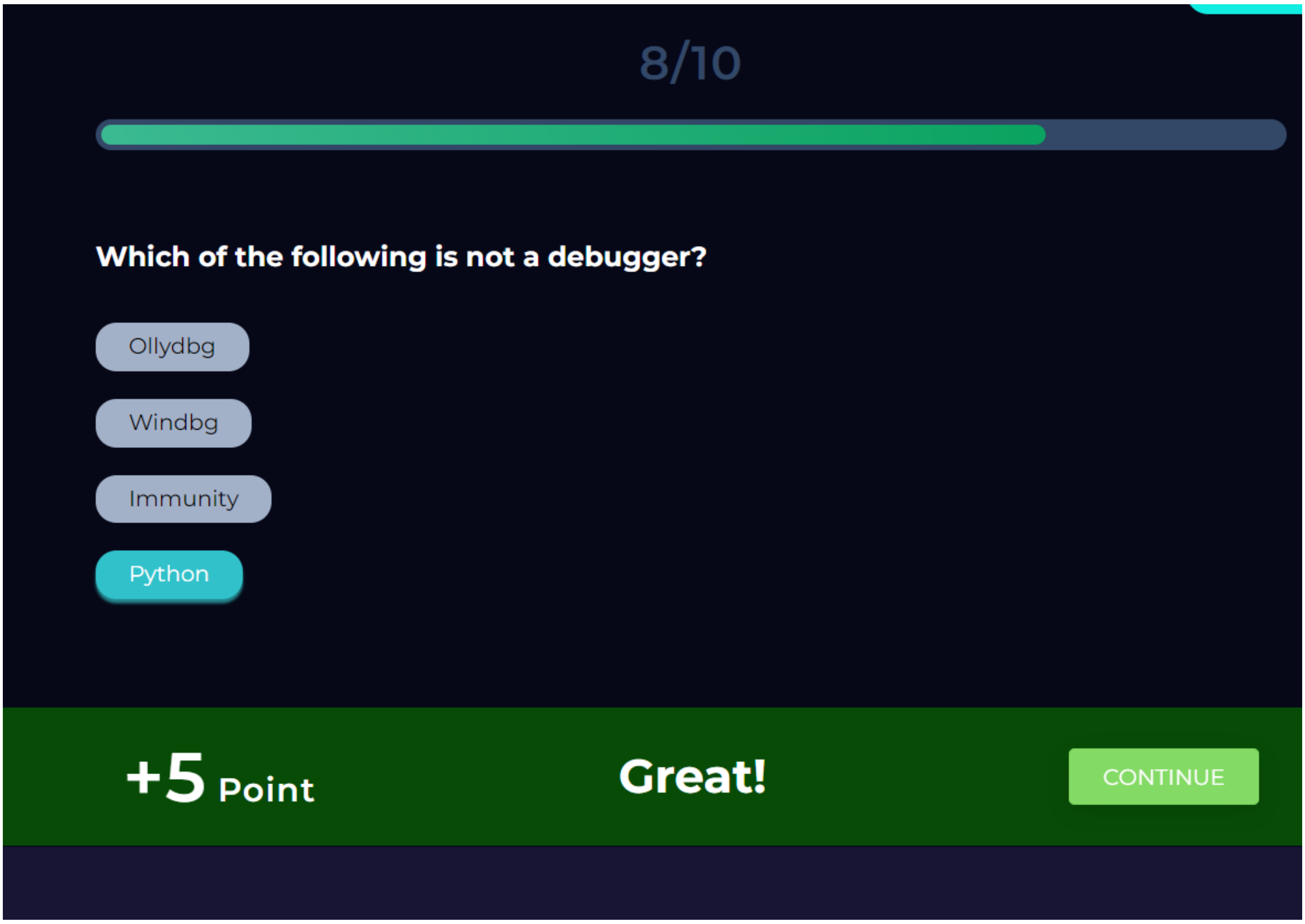
7/10

What is the function that automatically enables macro codes to be run when the Office document is opened?

- Workbook_Main()
- Workbook_Execute()
- Workbook_Start()
- [✓ Workbook_Open()]

+5 Point

Great!



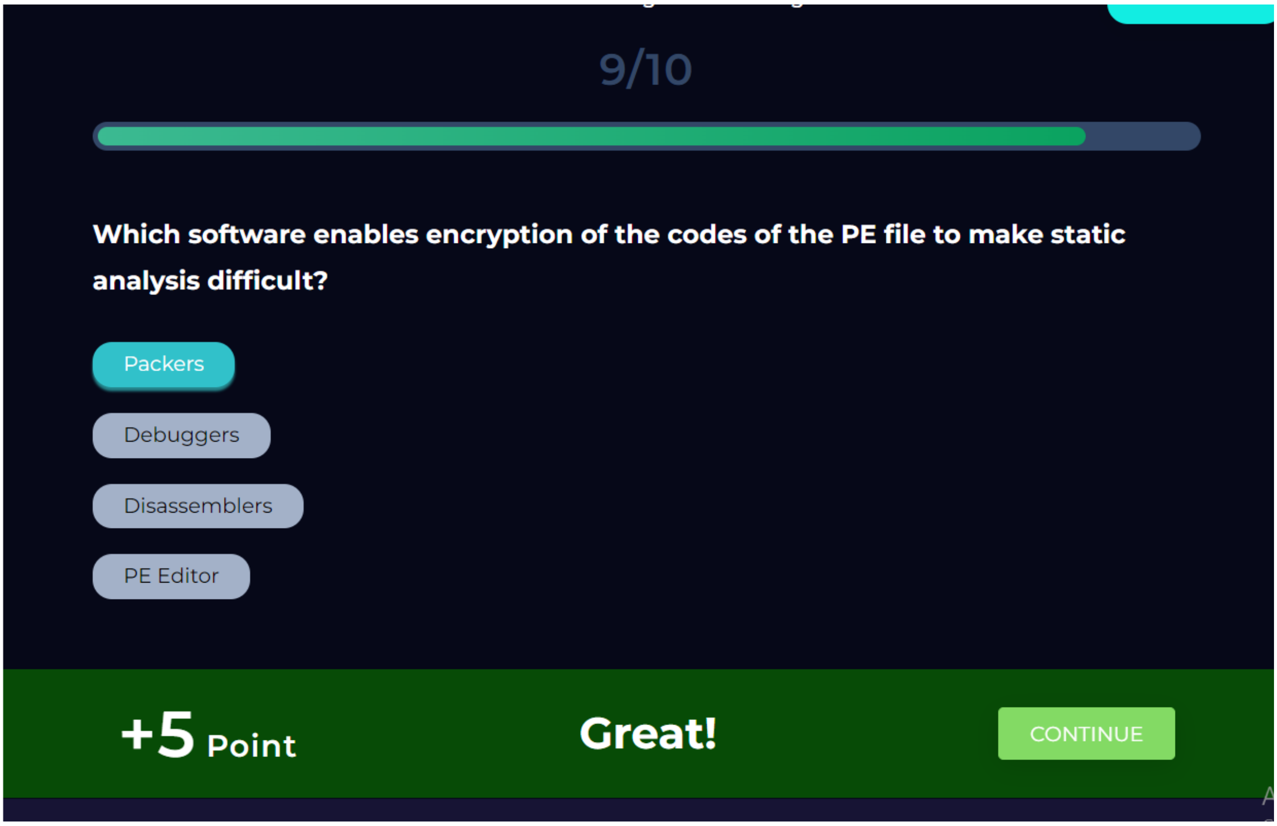
8/10

Which of the following is not a debugger?

- Ollydbg
- Windbg
- Immunity
- [✓ Python]

+5 Point

Great!



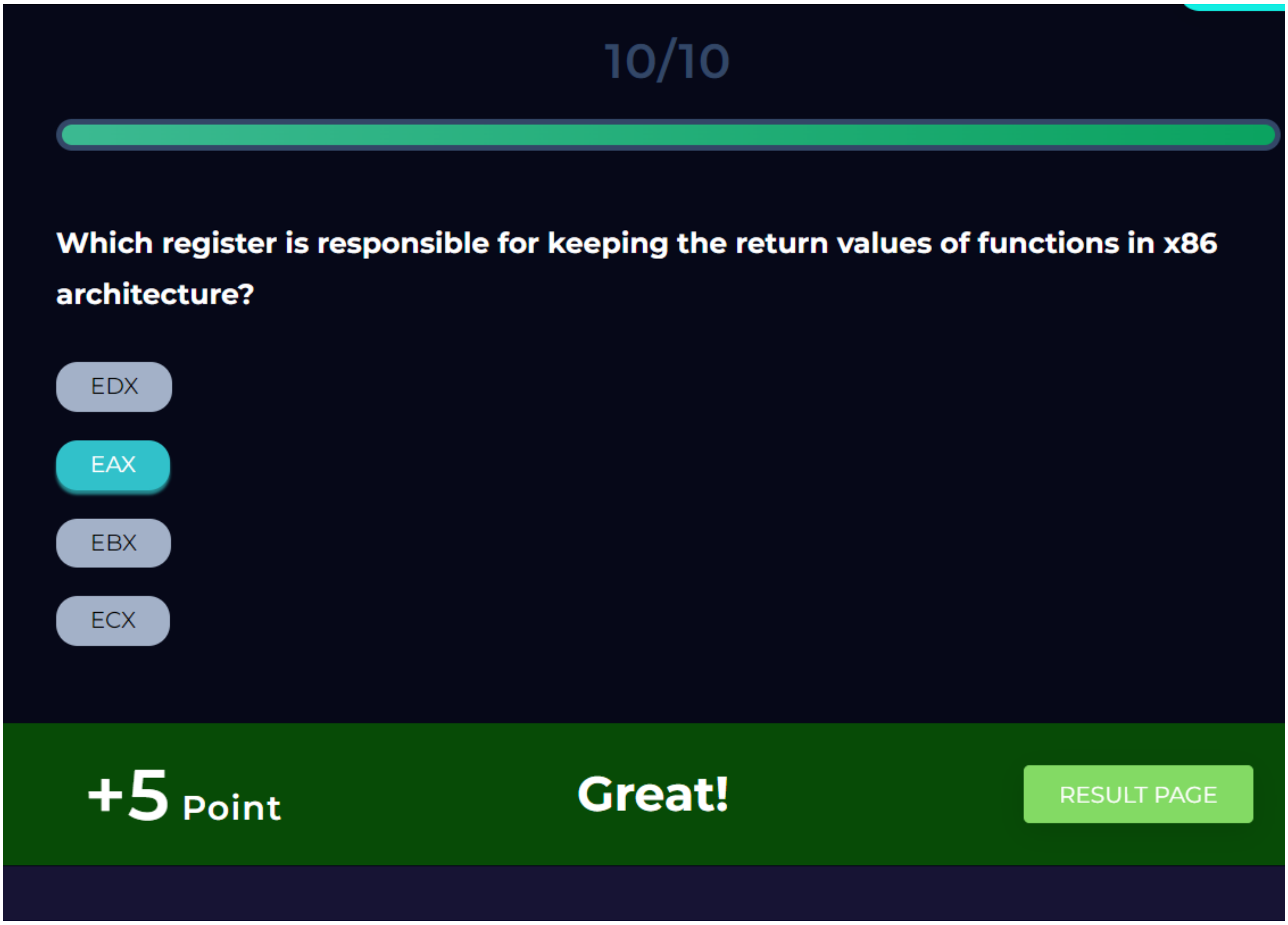
Which software enables encryption of the codes of the PE file to make static analysis difficult?

[✓ Packers]

Debuggers

Disassemblers

PE Editor



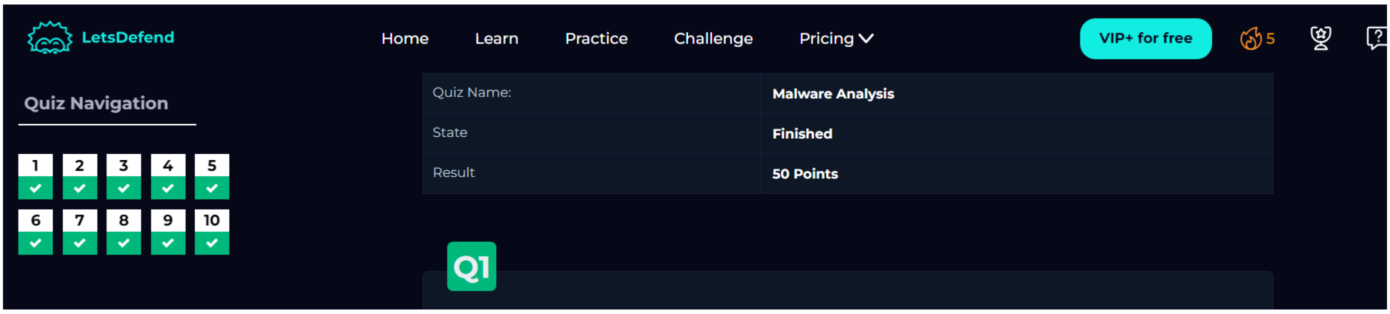
Which register is responsible for keeping the return values of functions in x86 architecture?

EDX

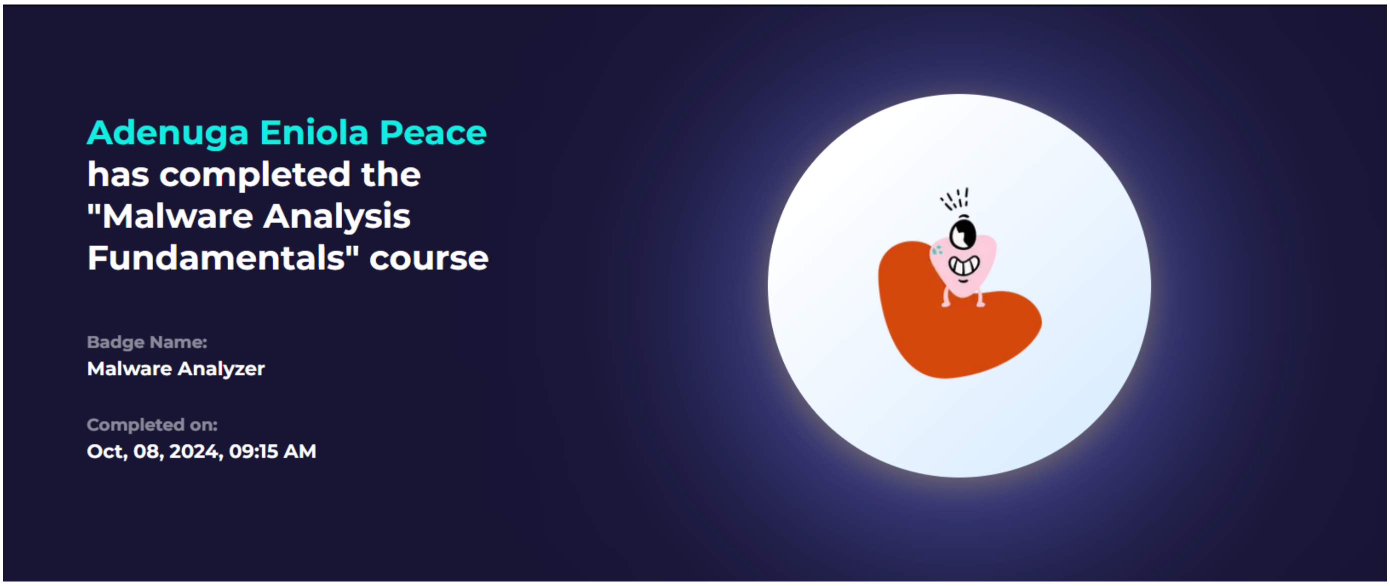
[✓ EAX]

EBX

ECX



Quiz Name:	Malware Analysis
State	Finished
Result	50 Points

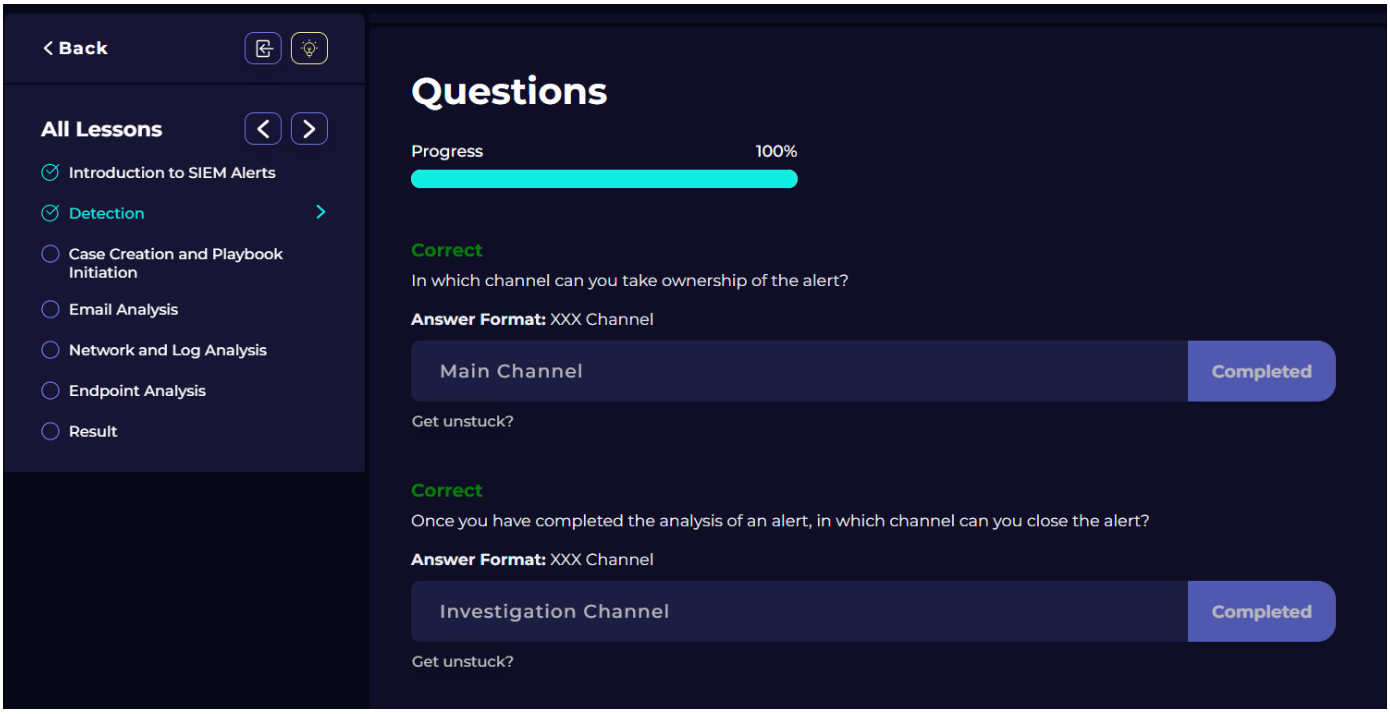


Adenuga Eniola Peace has completed the "Malware Analysis Fundamentals" course

Badge Name:
Malware Analyzer

Completed on:
Oct, 08, 2024, 09:15 AM

QUESTION 3- SIEM



Questions

Progress 100%

Correct

In which channel can you take ownership of the alert?

Answer Format: XXX Channel

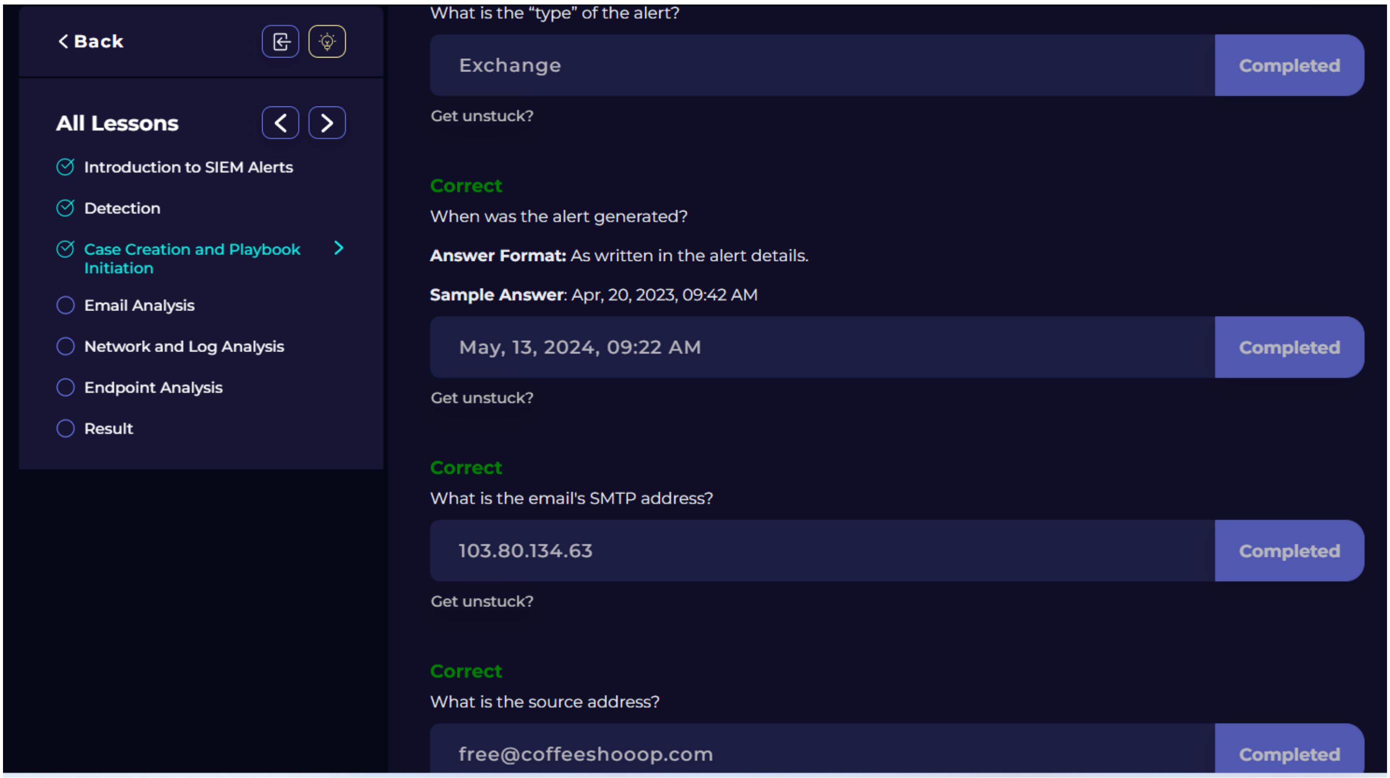
Main Channel

Correct

Once you have completed the analysis of an alert, in which channel can you close the alert?

Answer Format: XXX Channel

Investigation Channel



What is the "type" of the alert?

Exchange

Correct

When was the alert generated?

Answer Format: As written in the alert details.

Sample Answer: Apr, 20, 2023, 09:42 AM

May, 13, 2024, 09:22 AM

Correct

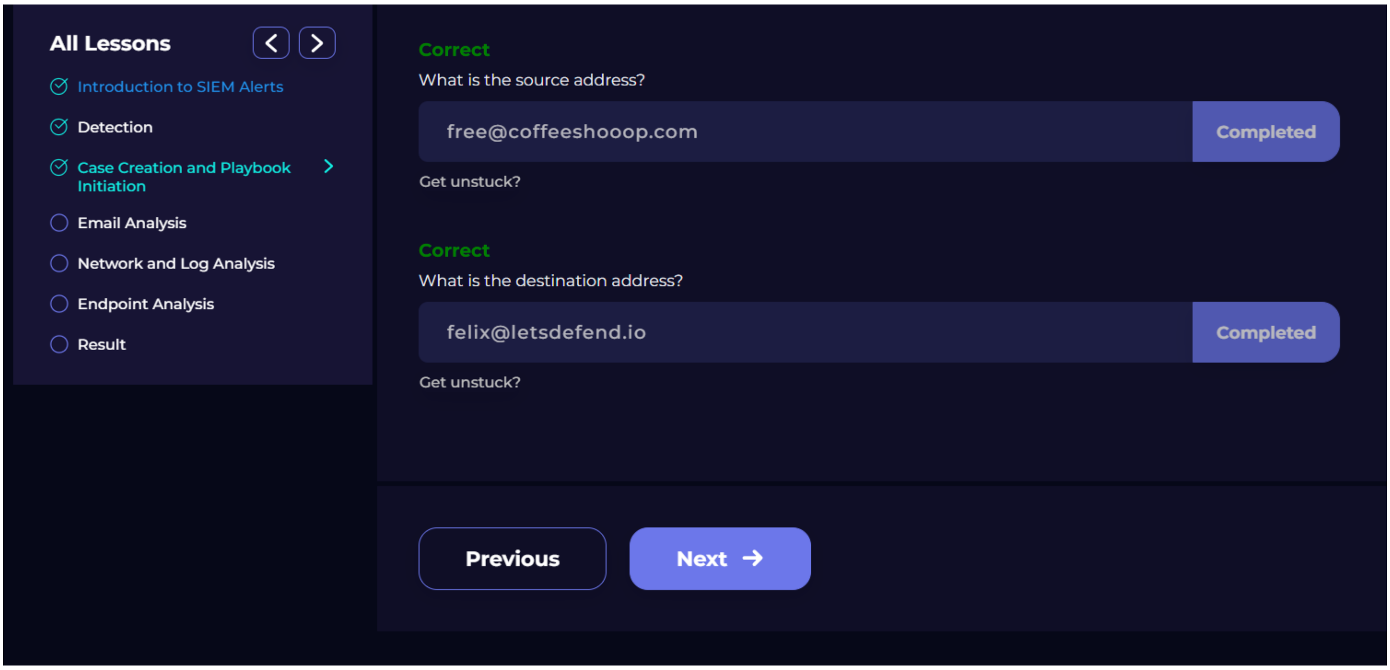
What is the email's SMTP address?

103.80.134.63

Correct

What is the source address?

free@coffeeshooop.com



Correct

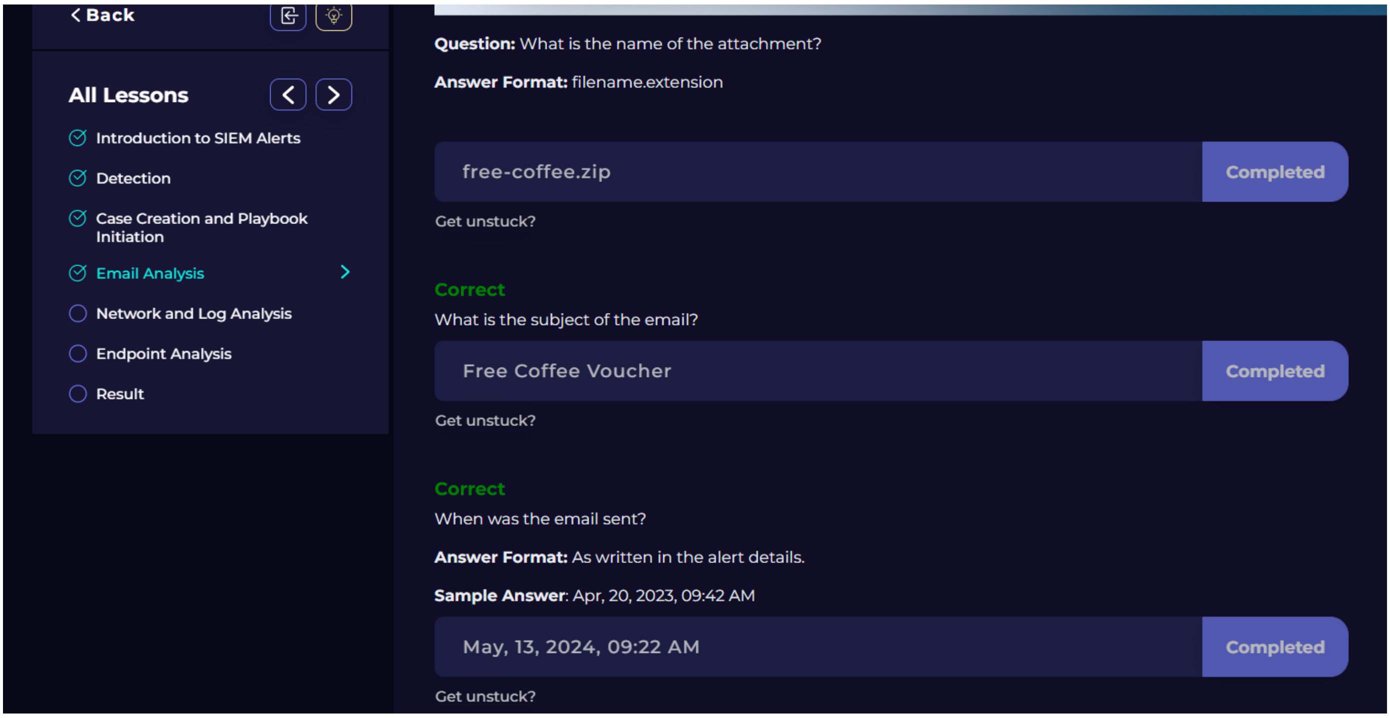
What is the source address?

free@coffeeshooop.com

Correct

What is the destination address?

felix@letsdefend.io



< Back
All Lessons
✓ Introduction to SIEM Alerts
✓ Detection
✓ Case Creation and Playbook Initiation
✓ Email Analysis
○ Network and Log Analysis
○ Endpoint Analysis
○ Result

Question: What is the name of the attachment?

Answer Format: filename.extension

free-coffee.zip | Completed

Get unstuck?

Correct

What is the subject of the email?

Free Coffee Voucher | Completed

Get unstuck?

Correct

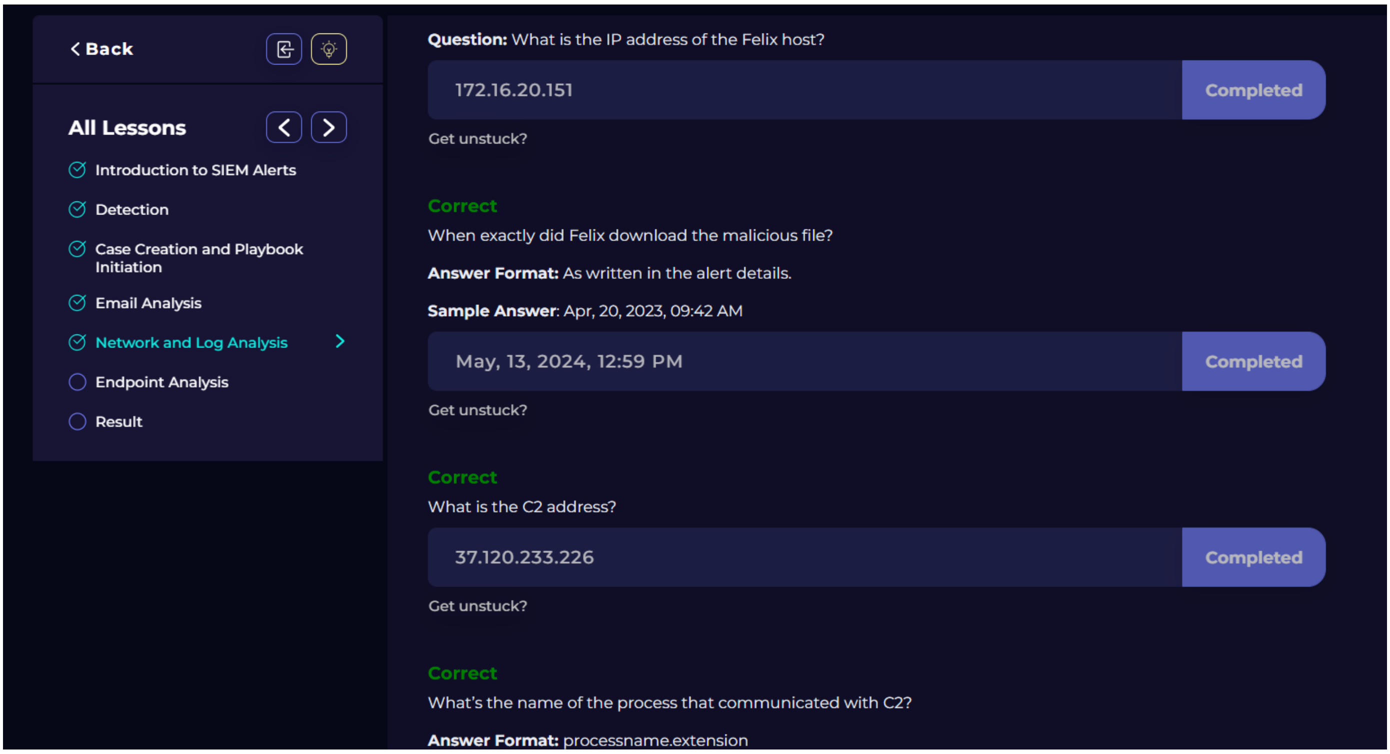
When was the email sent?

Answer Format: As written in the alert details.

Sample Answer: Apr, 20, 2023, 09:42 AM

May, 13, 2024, 09:22 AM | Completed

Get unstuck?



< Back
All Lessons
✓ Introduction to SIEM Alerts
✓ Detection
✓ Case Creation and Playbook Initiation
✓ Email Analysis
✓ Network and Log Analysis
○ Endpoint Analysis
○ Result

Question: What is the IP address of the Felix host?

172.16.20.151 | Completed

Get unstuck?

Correct

When exactly did Felix download the malicious file?

Answer Format: As written in the alert details.

Sample Answer: Apr, 20, 2023, 09:42 AM

May, 13, 2024, 12:59 PM | Completed

Get unstuck?

Correct

What is the C2 address?

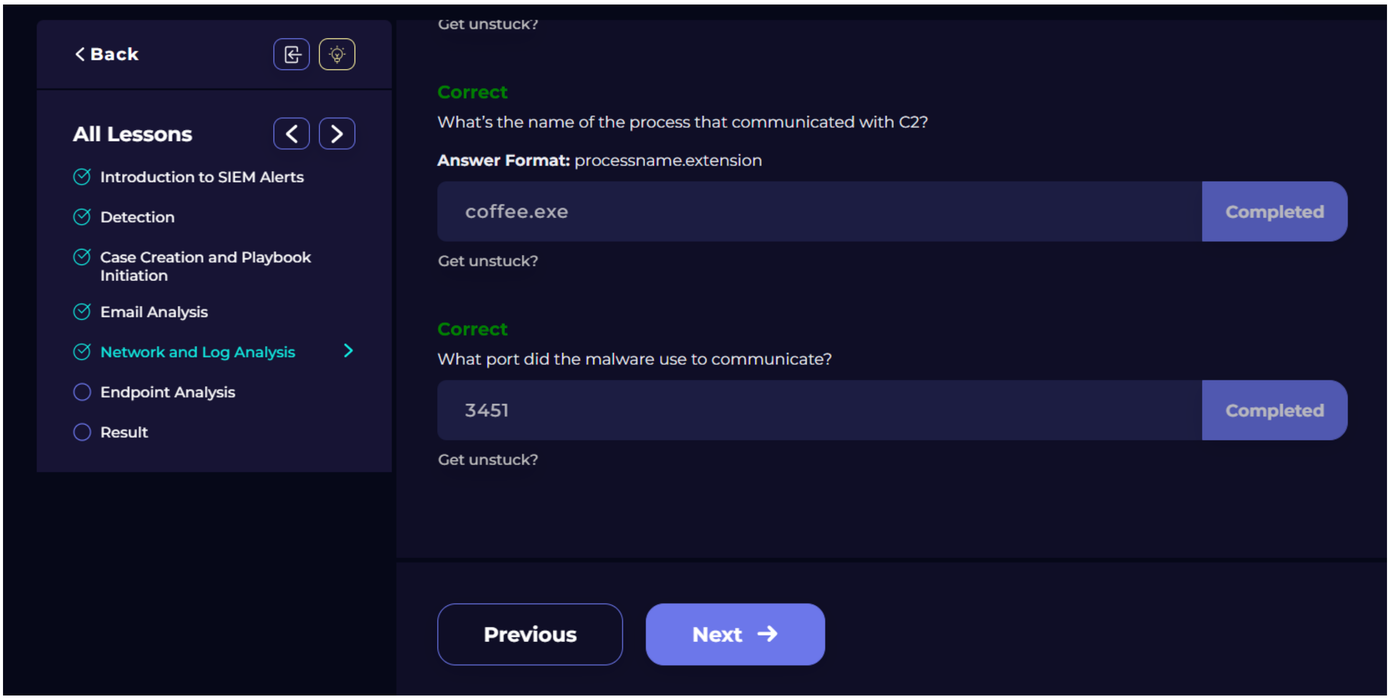
37.120.233.226 | Completed

Get unstuck?

Correct

What's the name of the process that communicated with C2?

Answer Format: processname.extension



All Lessons

- ✓ Introduction to SIEM Alerts
- ✓ Detection
- ✓ Case Creation and Playbook Initiation
- ✓ Email Analysis
- ✓ Network and Log Analysis >
- ○ Endpoint Analysis
- ○ Result

Get unstuck?

Correct

What's the name of the process that communicated with C2?

Answer Format: processname.extension

coffee.exe — Completed

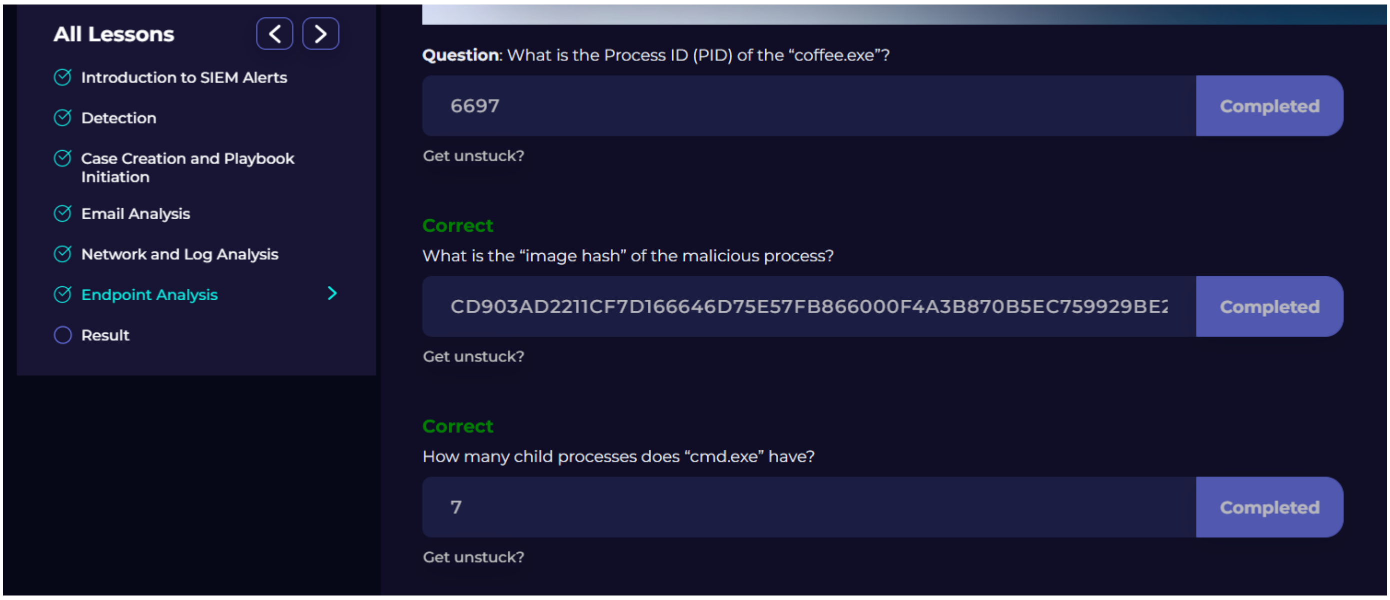
Get unstuck?

Correct

What port did the malware use to communicate?

3451 — Completed

Get unstuck?



All Lessons

- ✓ Introduction to SIEM Alerts
- ✓ Detection
- ✓ Case Creation and Playbook Initiation
- ✓ Email Analysis
- ✓ Network and Log Analysis
- ✓ Endpoint Analysis >
- ○ Result

Question: What is the Process ID (PID) of the "coffee.exe"?

6697 — Completed

Get unstuck?

Correct

What is the "image hash" of the malicious process?

CD903AD2211CF7D166646D75E57FB866000F4A3B870B5EC759929BE2 — Completed

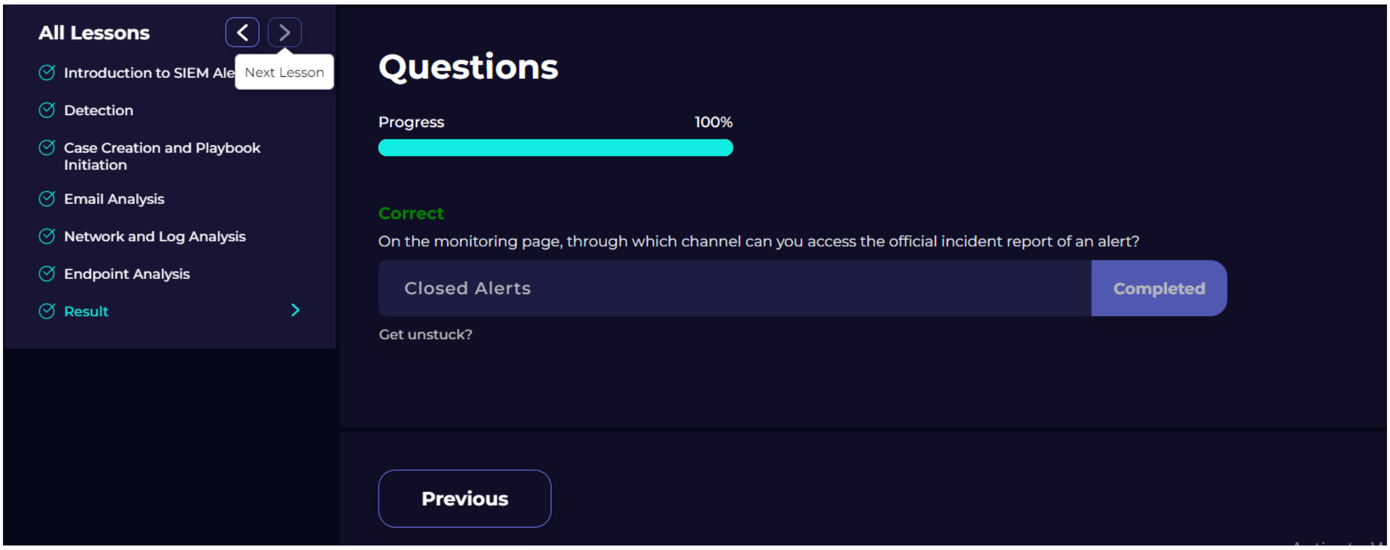
Get unstuck?

Correct

How many child processes does "cmd.exe" have?

7 — Completed

Get unstuck?



All Lessons

- ✓ Introduction to SIEM Ale
- ✓ Detection
- ✓ Case Creation and Playbook Initiation
- ✓ Email Analysis
- ✓ Network and Log Analysis
- ✓ Endpoint Analysis
- ✓ Result >

Questions

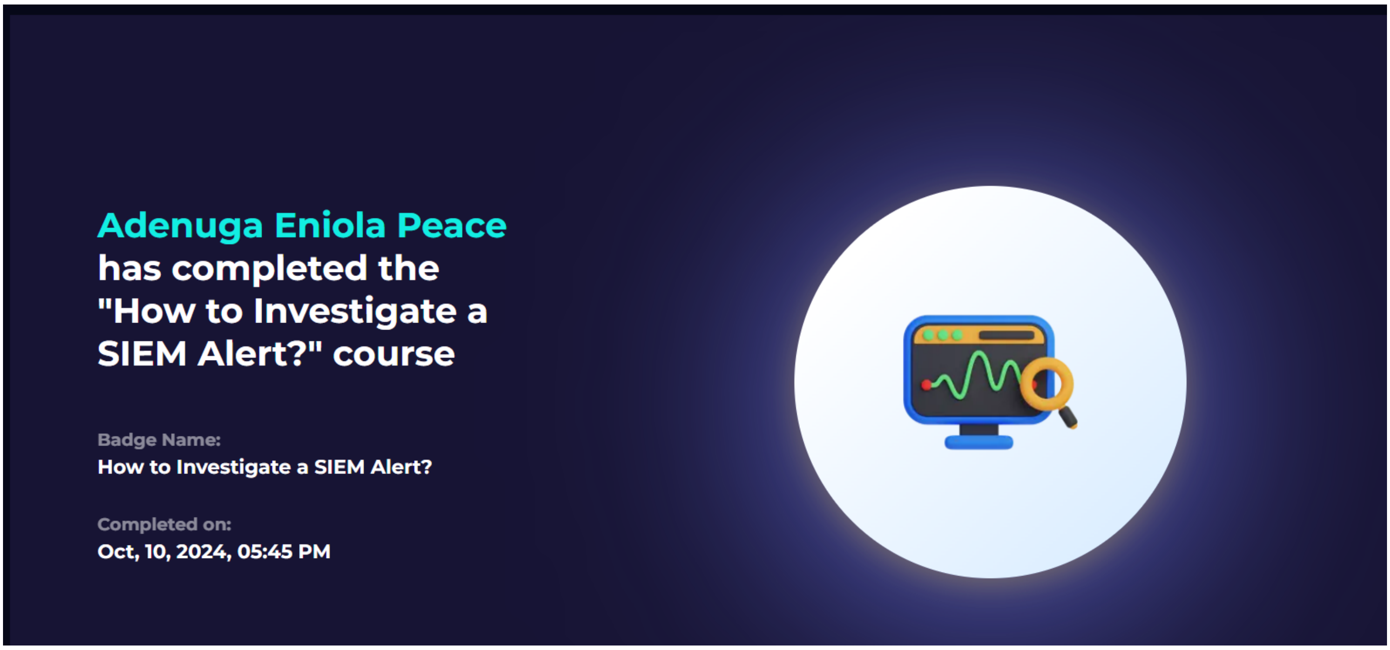
Progress 100%

Correct

On the monitoring page, through which channel can you access the official incident report of an alert?

Closed Alerts — Completed

Get unstuck?



Adenuga Eniola Peace
has completed the
"How to Investigate a
SIEM Alert?" course

Badge Name:
How to Investigate a SIEM Alert?

Completed on:
Oct, 10, 2024, 05:45 PM