INFO39207 Advanced Information Systems
Forensics and Electronic Discovery

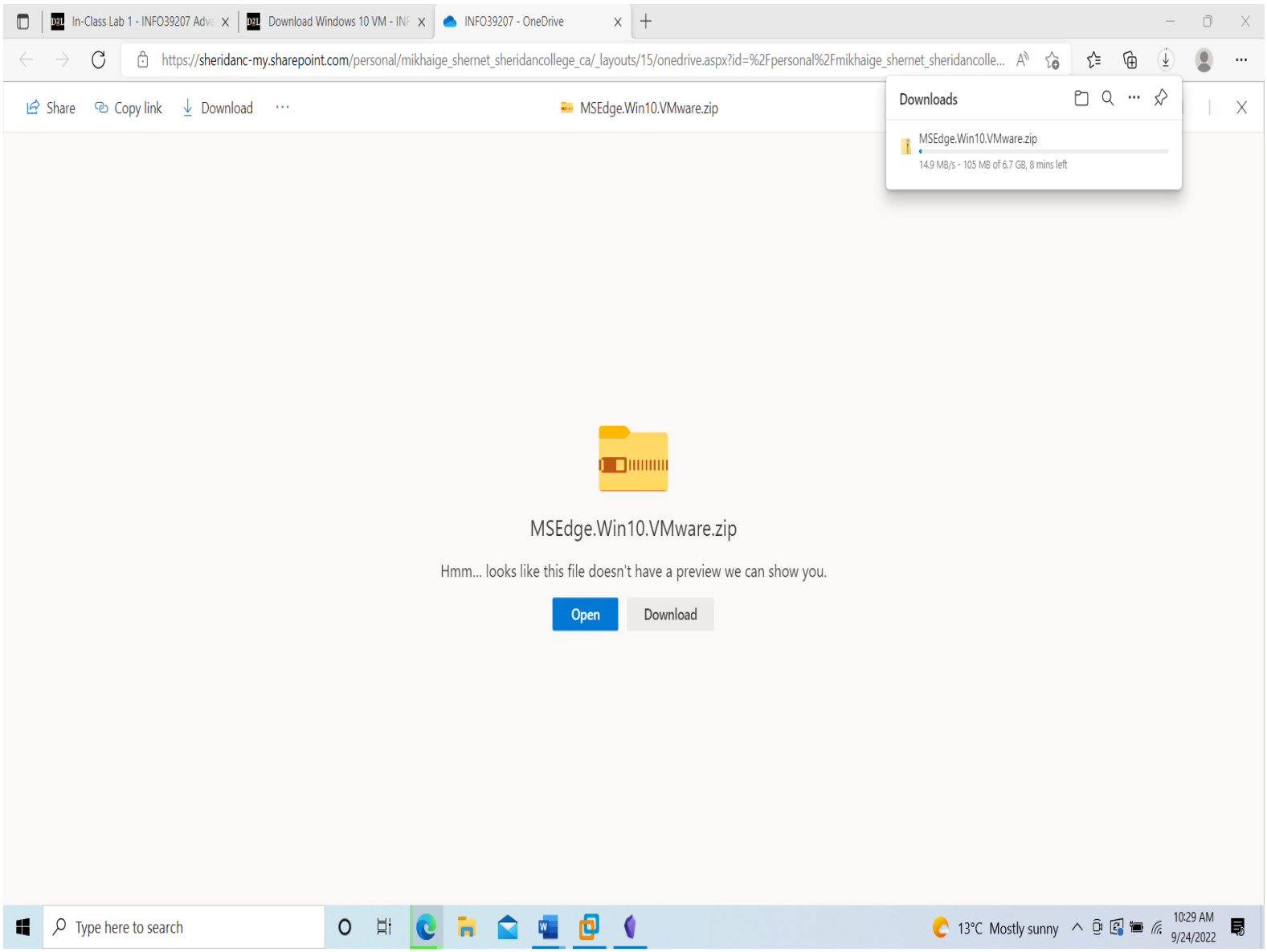
Submitted By:Chris Miele
Submitted To:Prof GM

Table of Contents

Lab 1

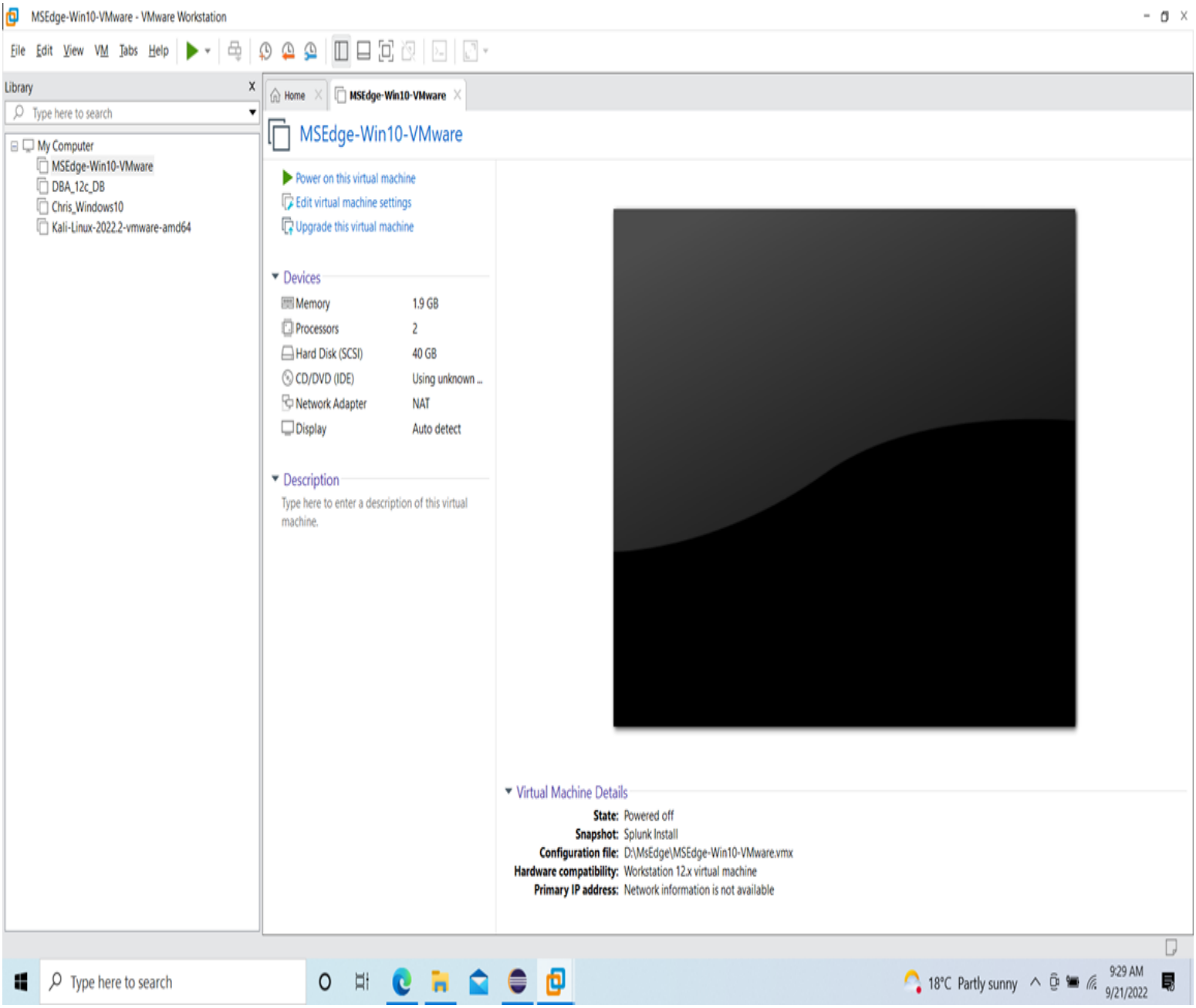
MS-Win10 Download

Figure 1: Downloading MSEdge.Win10



Import MS-Win10

Figure 2: Import Vm File -> Open -> Choose MSEdge-Win10-Vmware.



MS-Win10 New User

Figure 3: Type Settings in search -> Accounts -> Family & Other Accounts -> Click + -> Add My Student # 991609577 Assign Administrator to Account.

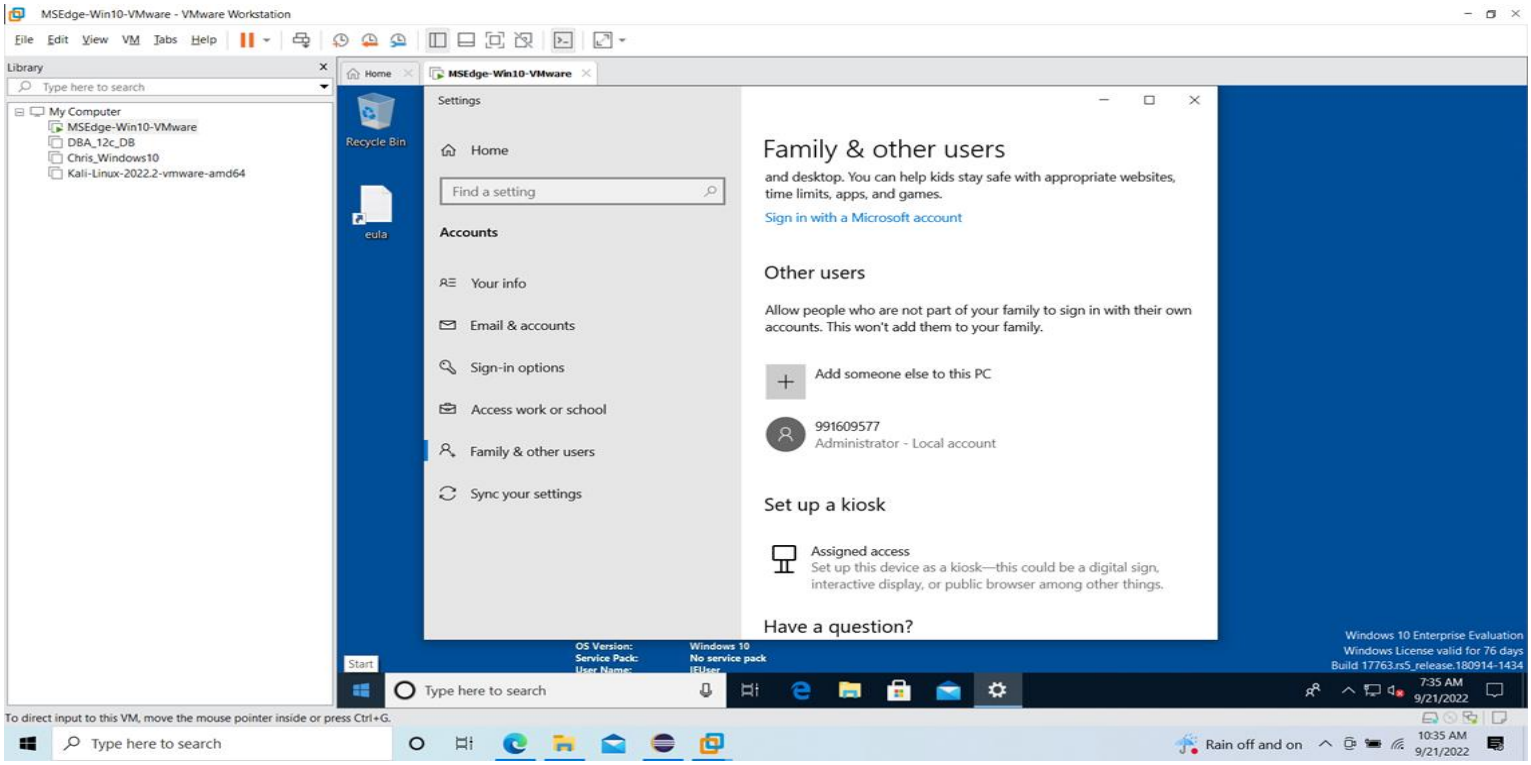


Figure 4: Sign Out -> Sign In using My Student #991609577.

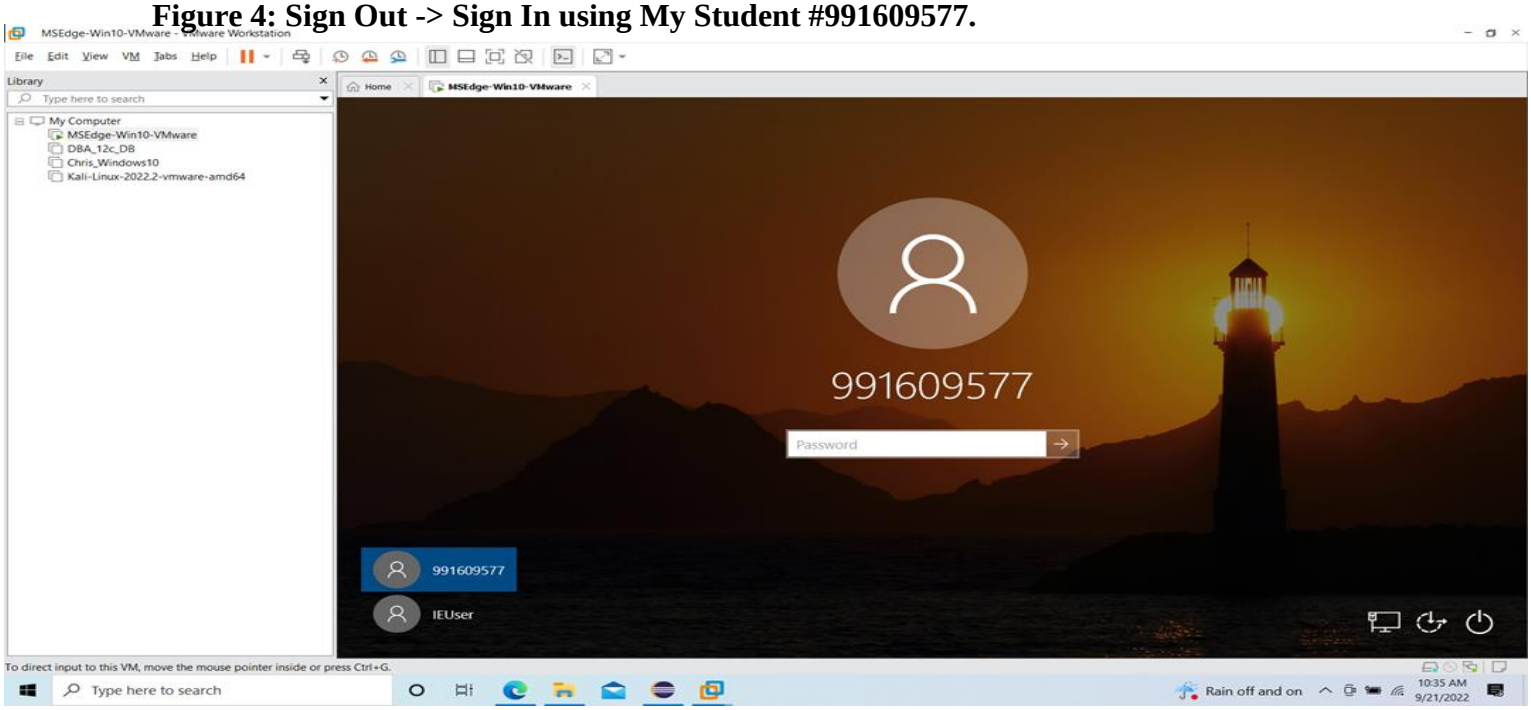
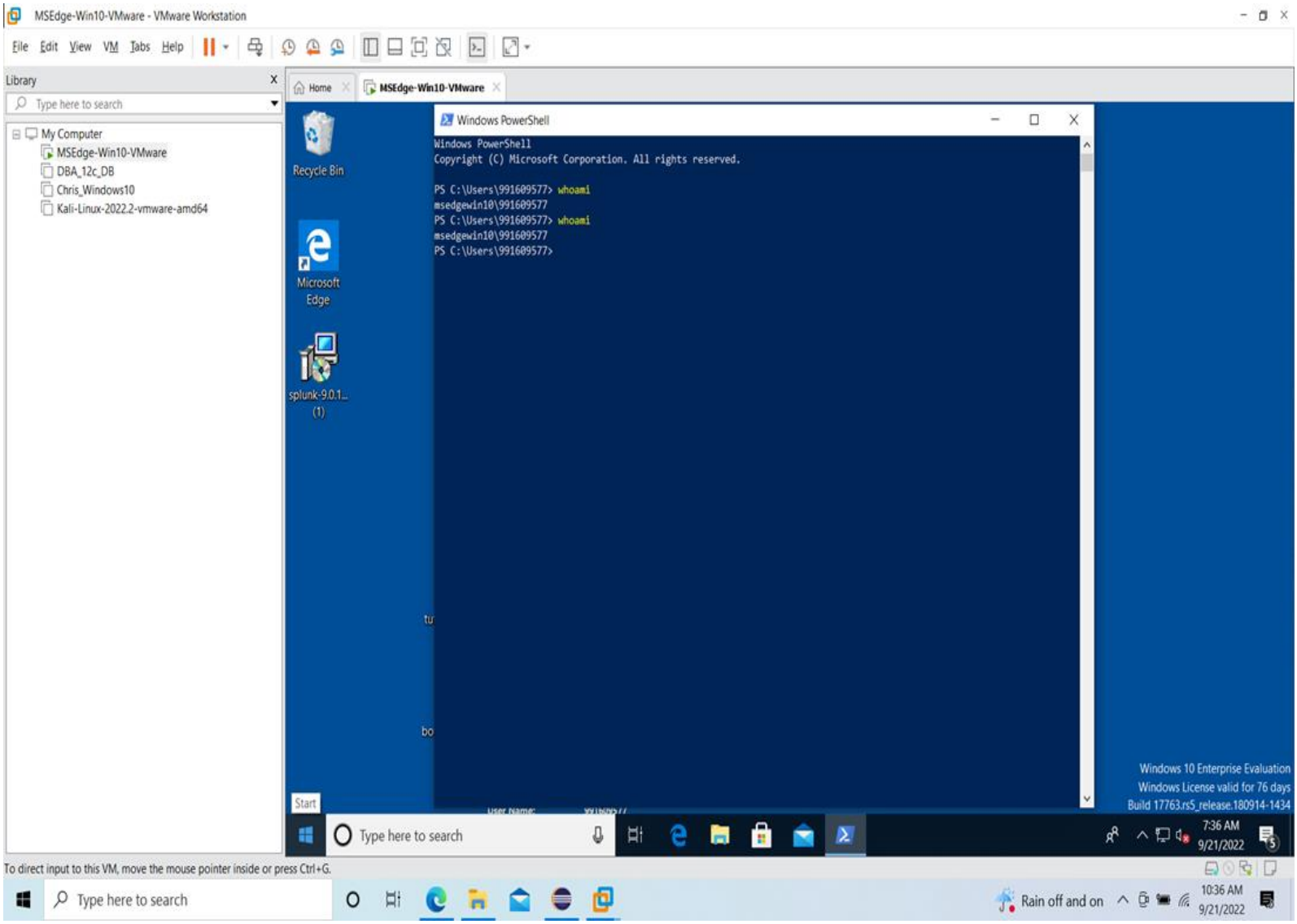
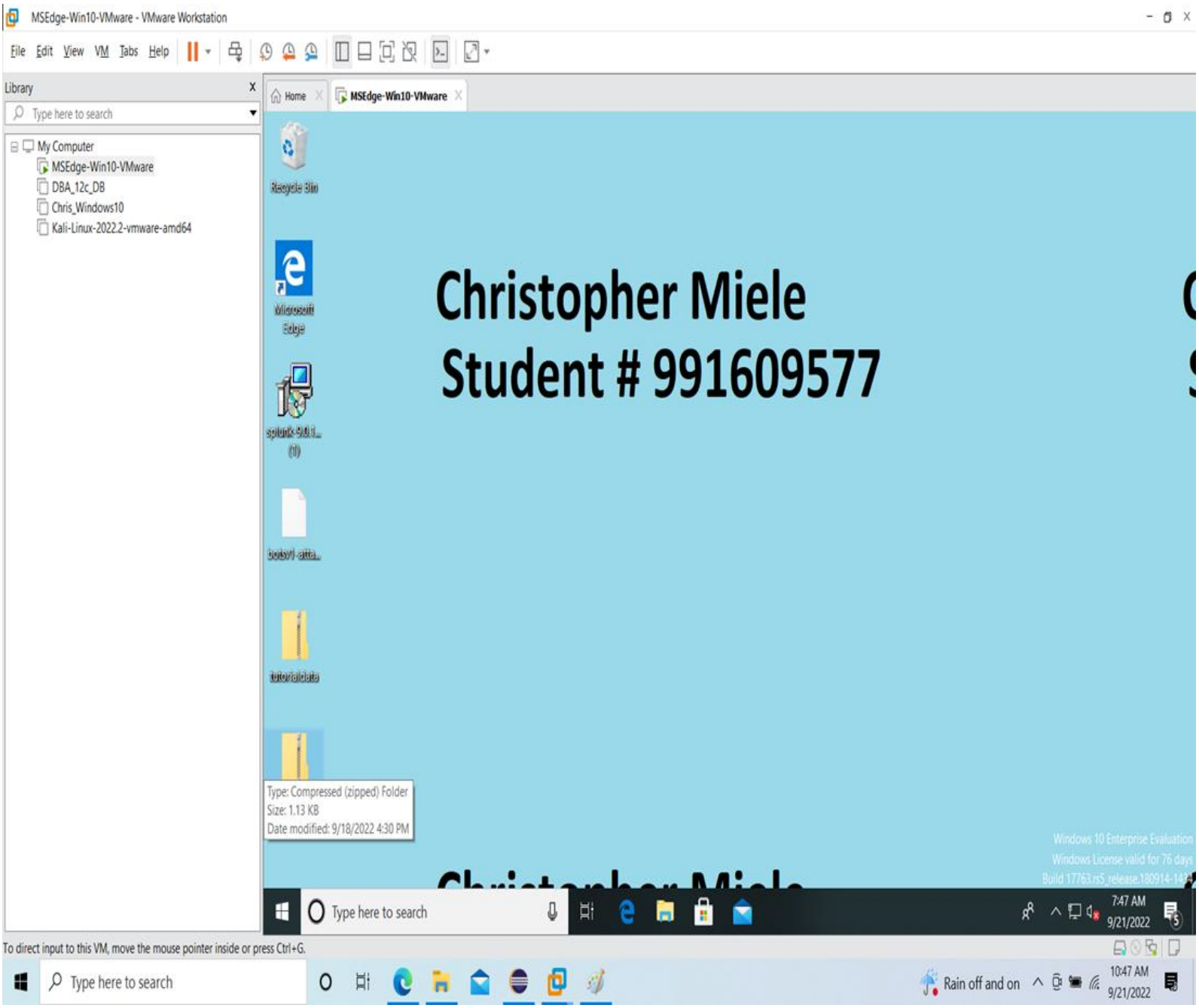


Figure 5: Powershell -> Type whoami -> Confirm Signed In My Student #991609577



MS-Win10 Desktop Background

Figure 6: Confirming Desktop Background.



MS-Win10 Disable(AV, Firewall, Updates)

Figure 7: Settings -> Update and Security -> Windows Security Virus Threat Protection-> Manage Settings Turn Everything Off.

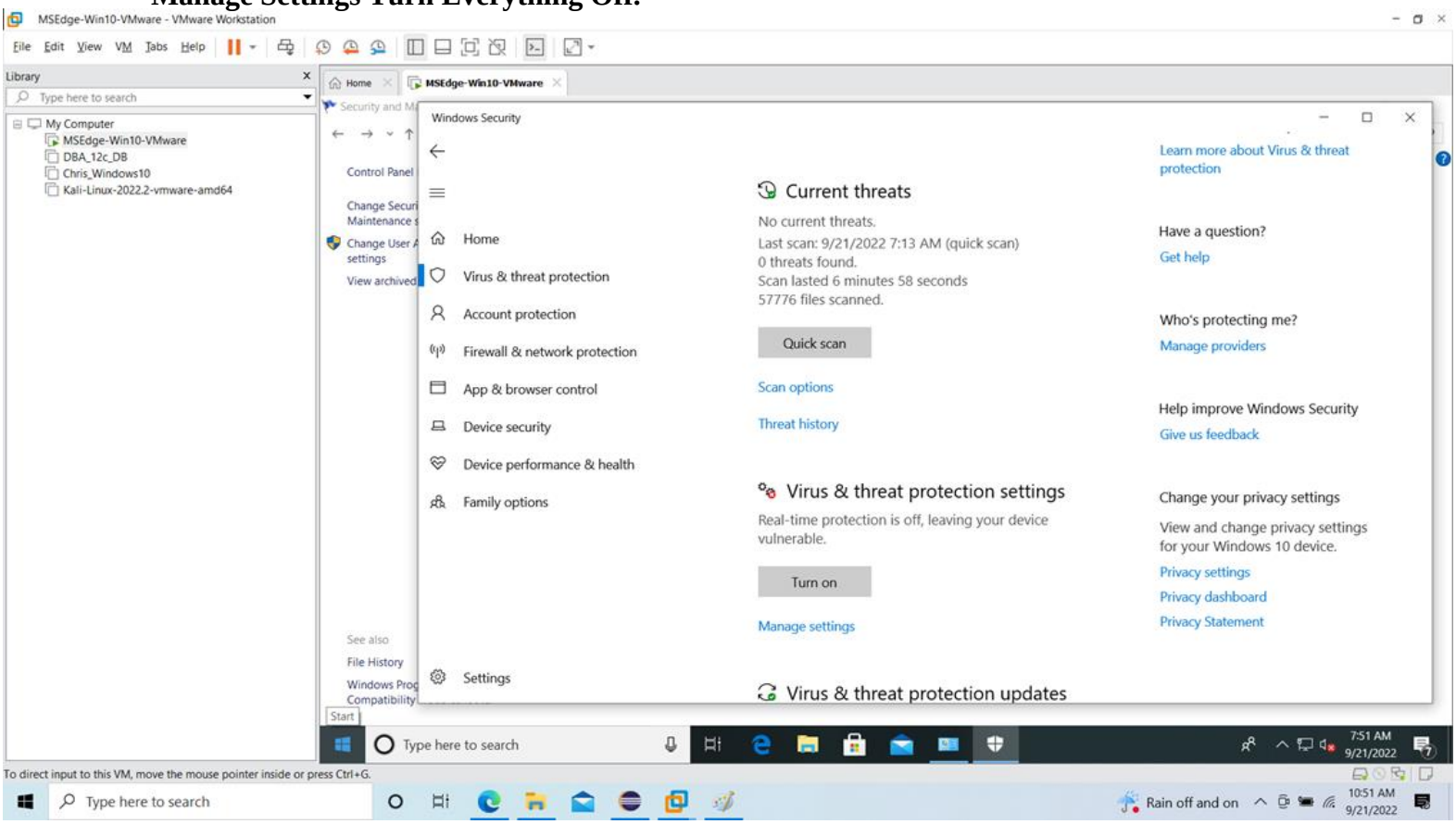


Figure 8: Settings -> Update and Security -> Firewall & Network Protection -> Click Domain Network/Private Network/Public Network -> Turn Off.

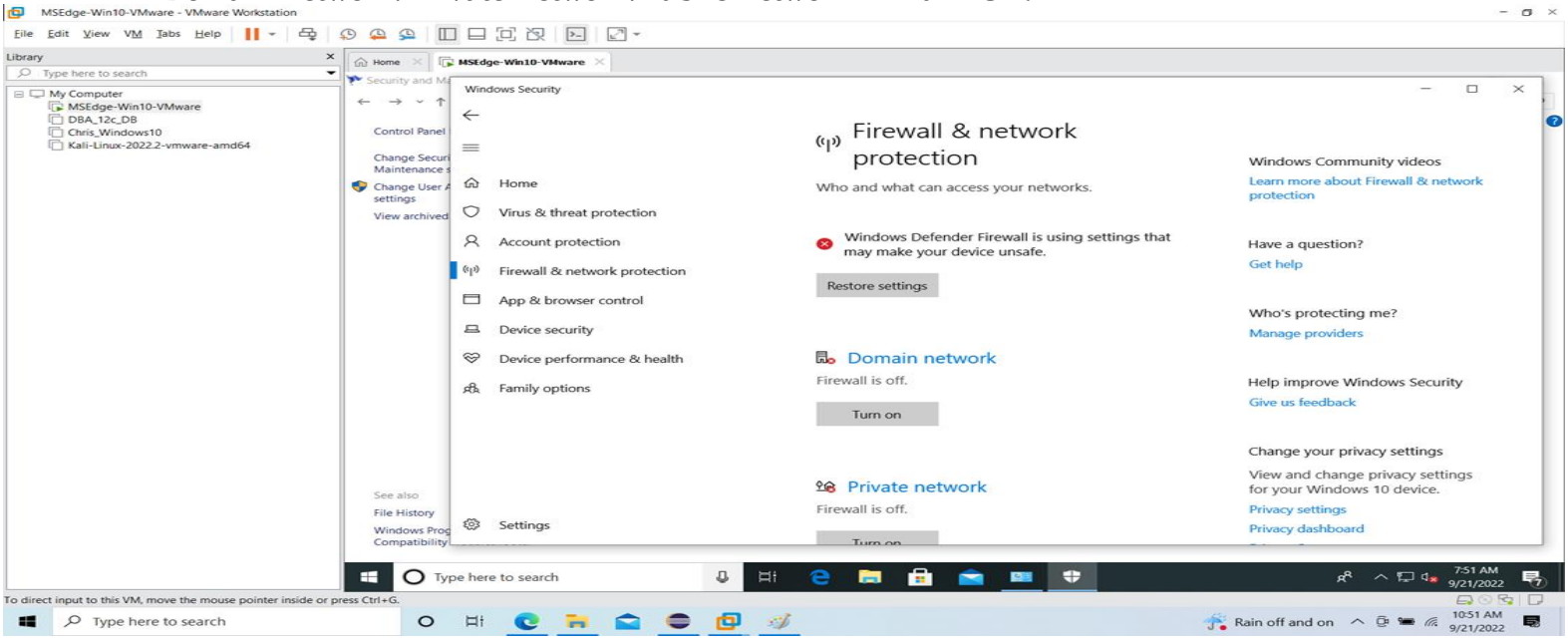


Figure 9: Settings -> Update and Security -> Firewall & Network Protection -> Click Domain Network/Private Network/Public Network -> Turn Off.

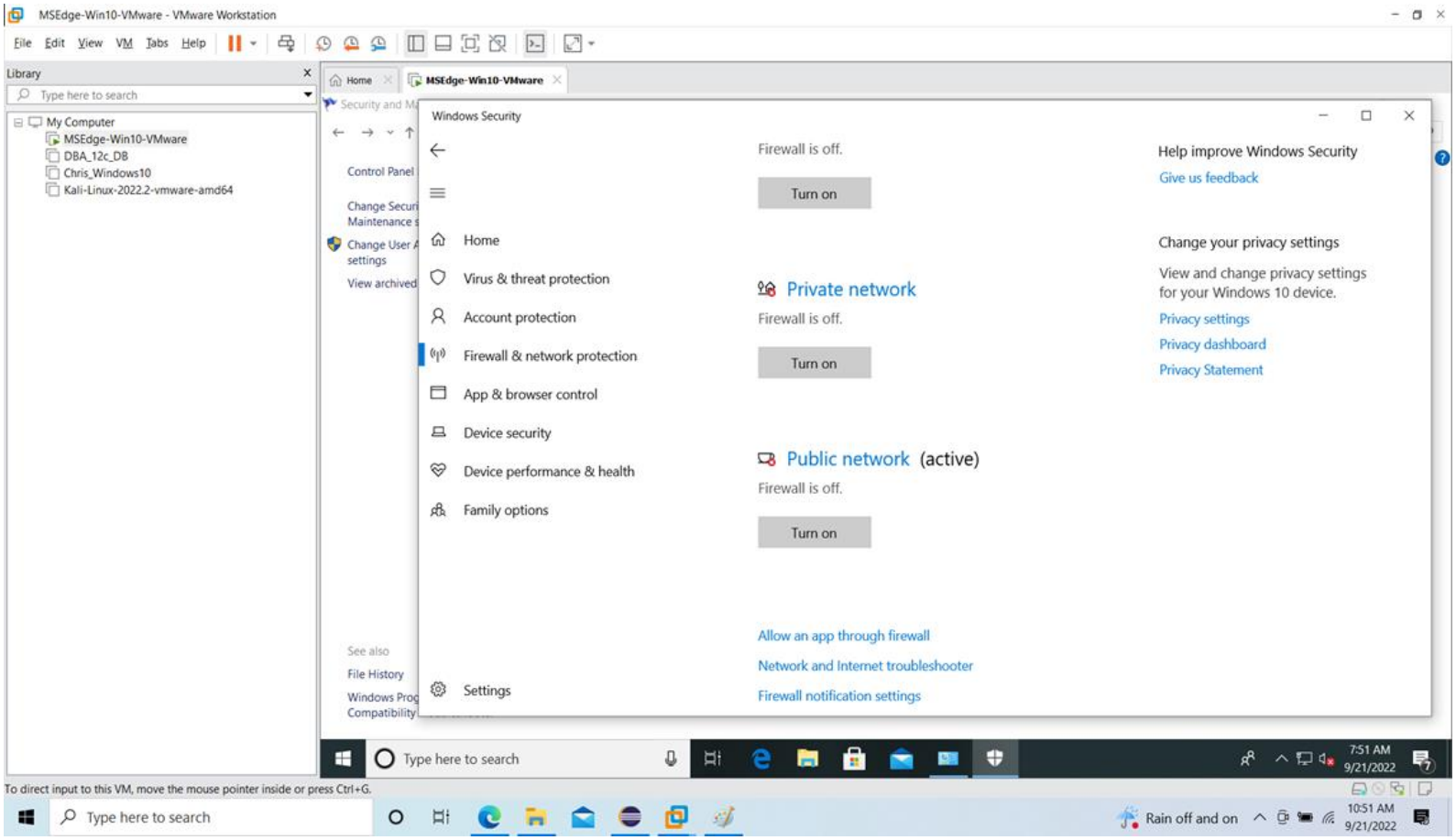
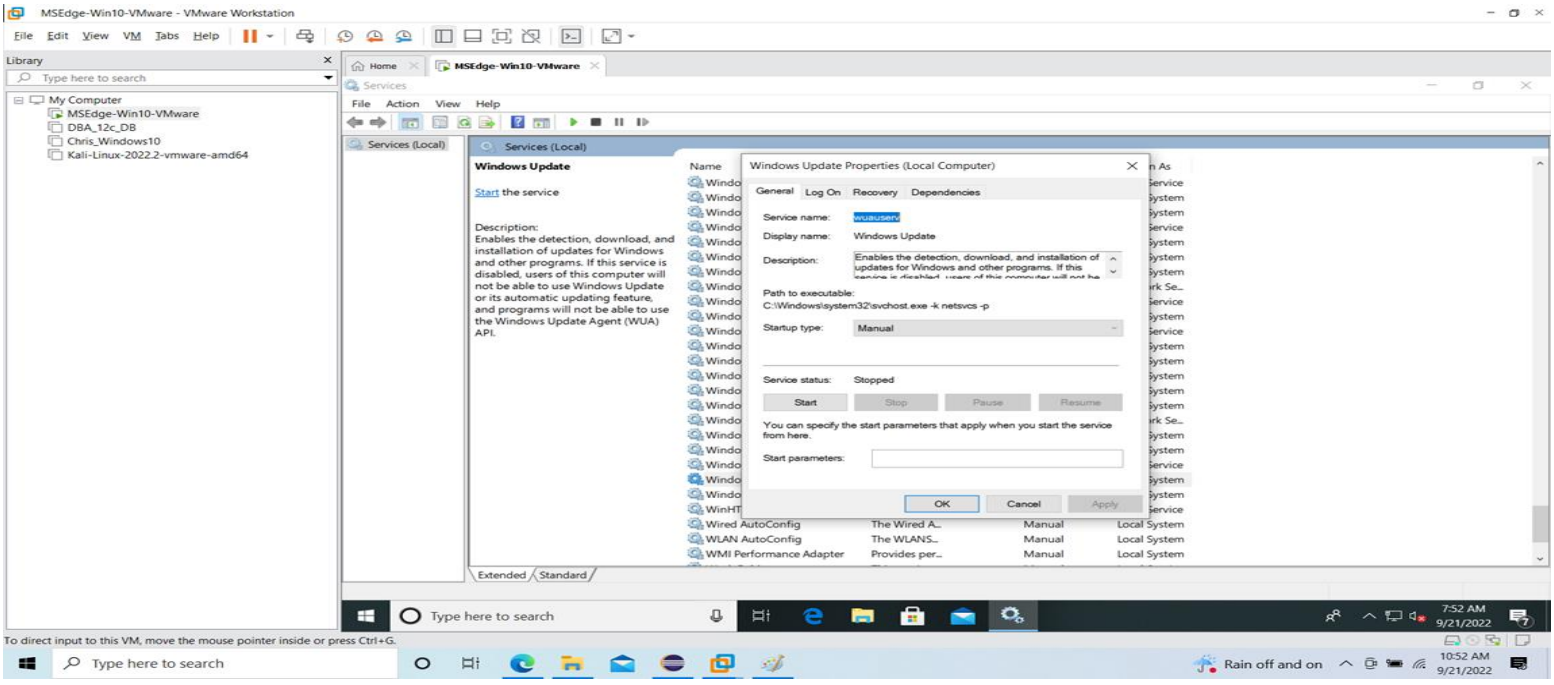
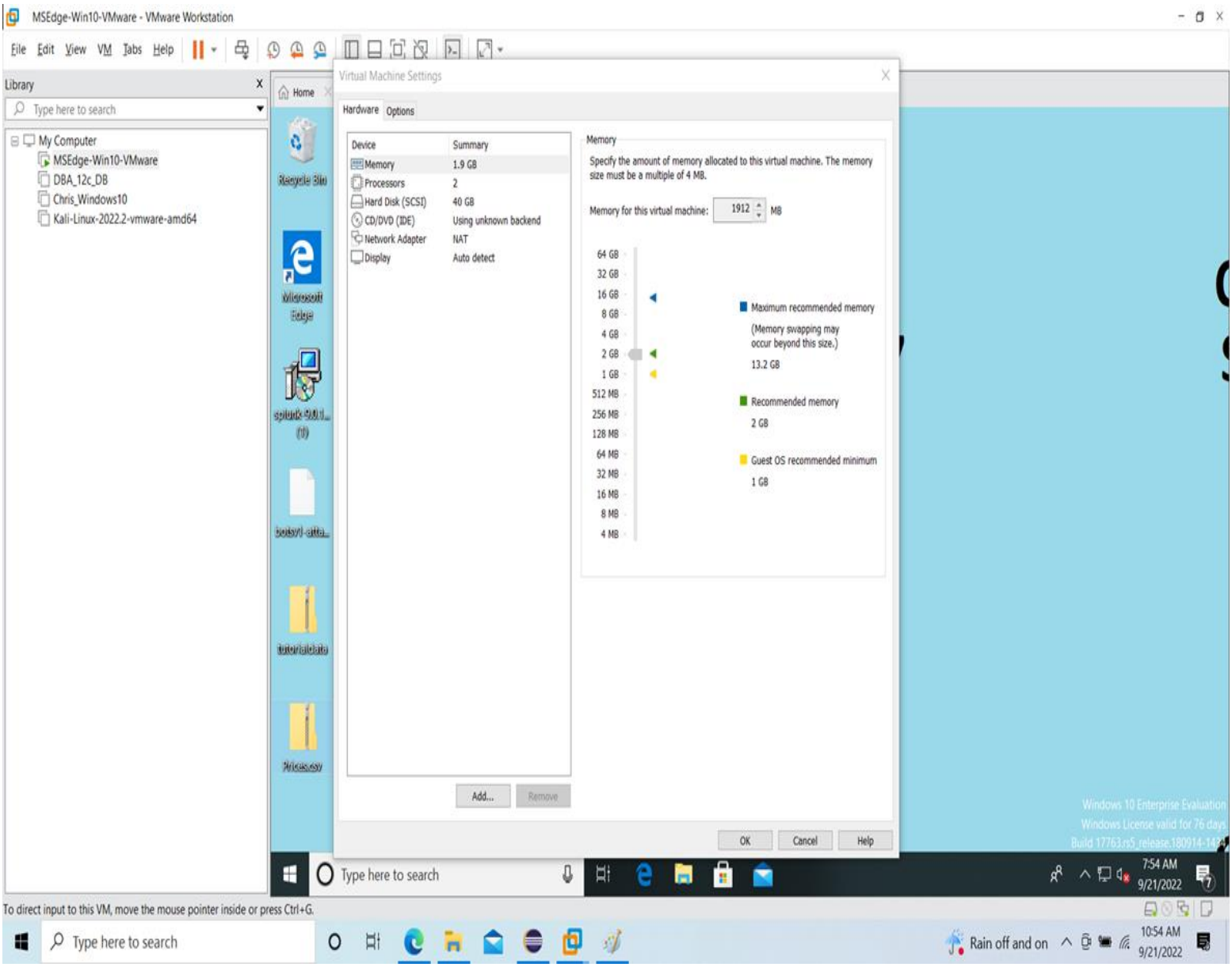


Figure 10: Services -> Windows Updates Properties(Local Computer) -> Stop Updates.



MS-Win10 VM NAT/Disk Space

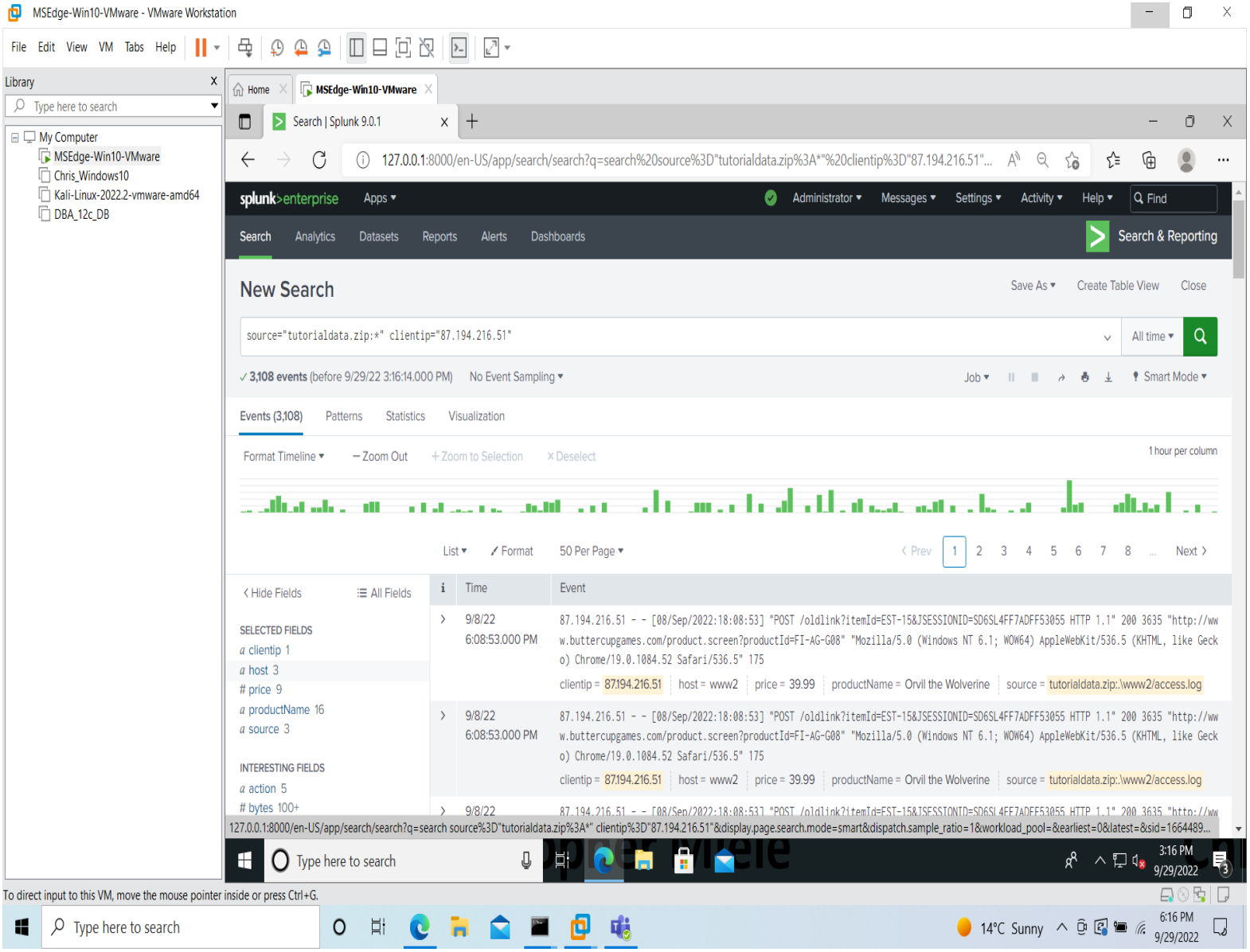
Figure 11: Click MSEdge-Win10-VMWare -> VM -> Settings -> Hardware.



Lab 2

Splunk Search

Figure 12: Run search on tutorialdata.zip specify client ip address as a filter.



Boss of SOC Walkthrough

Figure 13: Upload bots-attack-only.tgz
Explain: Splunk Add Data Upload the botsv1-attack-only.tgz

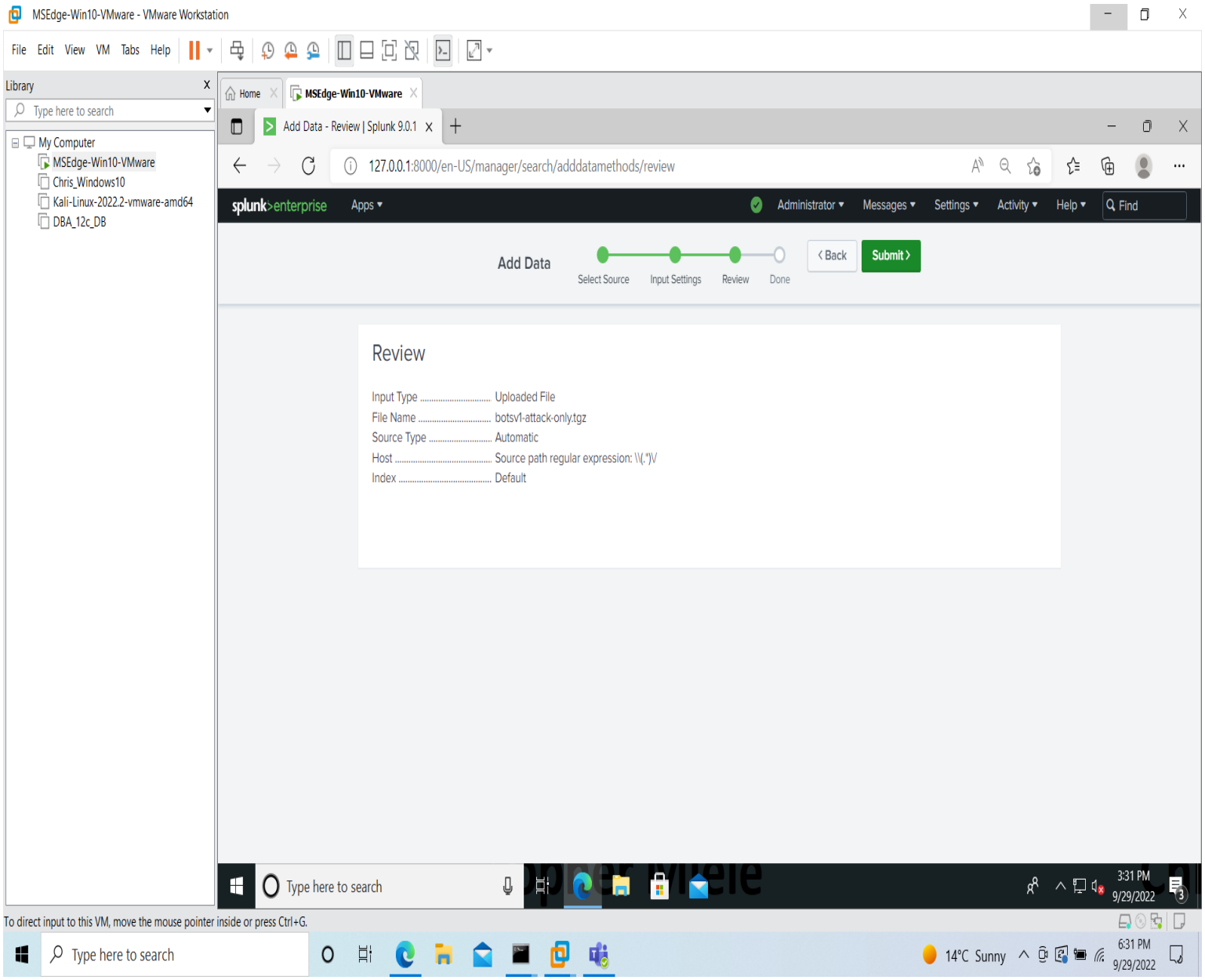


Figure 14: Q2 What is the likely IP address of someone from the Po1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?
Command: source="botsv1-attack-only.tgz:*" imreallynotbatman.com srcip="40.80.148.42"
Explain: The command above allows you to search(Query) tgz file using the parameters imreallynotbatman and srcip.

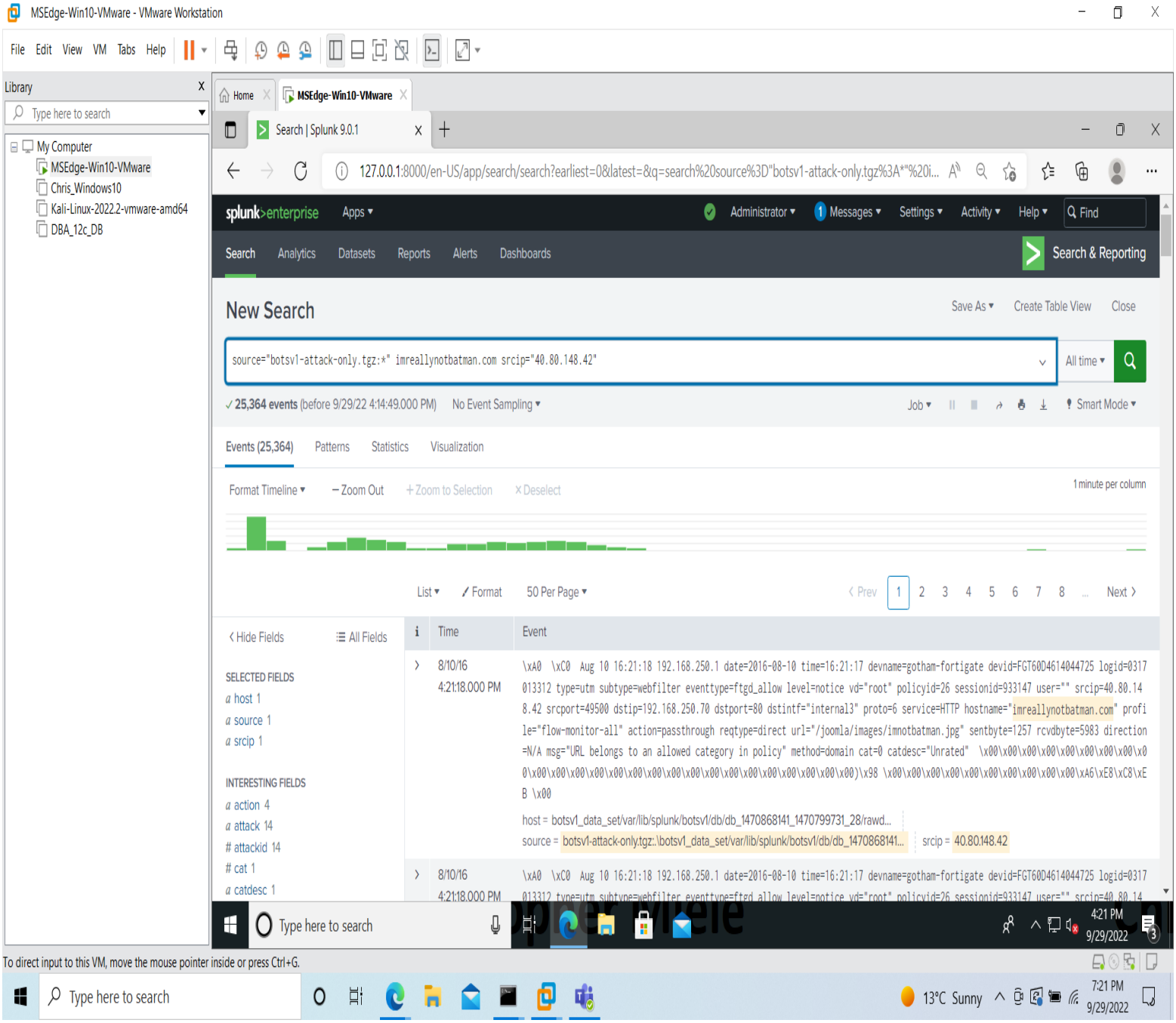


Figure 15: Q3 What company created the web vulnerability scanner used by Po1s0n1vy? Type the company name. (For example, “Microsoft” or “Oracle”)
Command: source="botsv1-attack-only.tgz:*" imreallynotbatman.com srcip="40.80.148.42"
Answer: Acunetix
Explain: Searching tgz file using the parameters imreallynotbatman.com and source ip(Attacker) to find the Web Vulnerability Scanner Information.

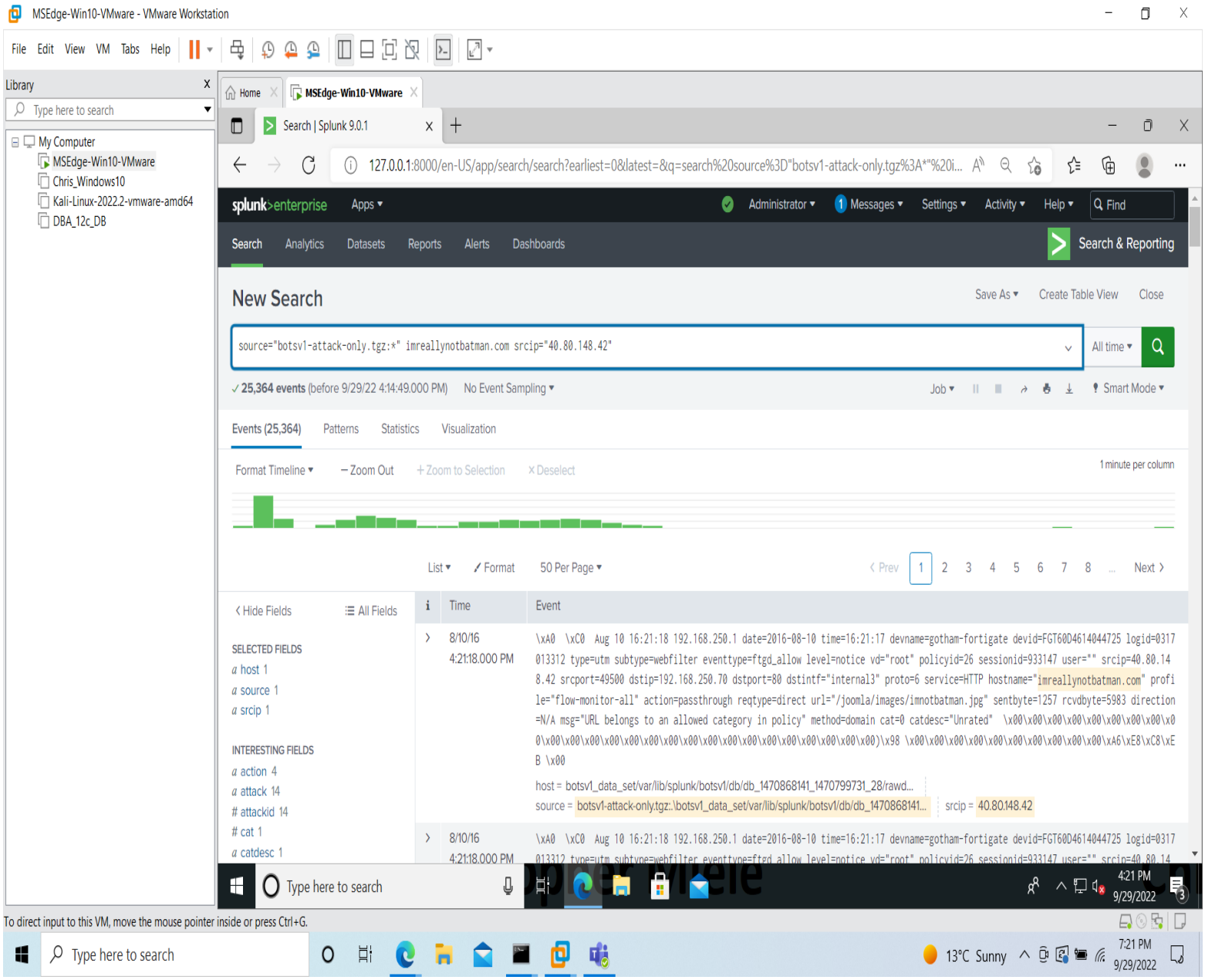


Figure 16:

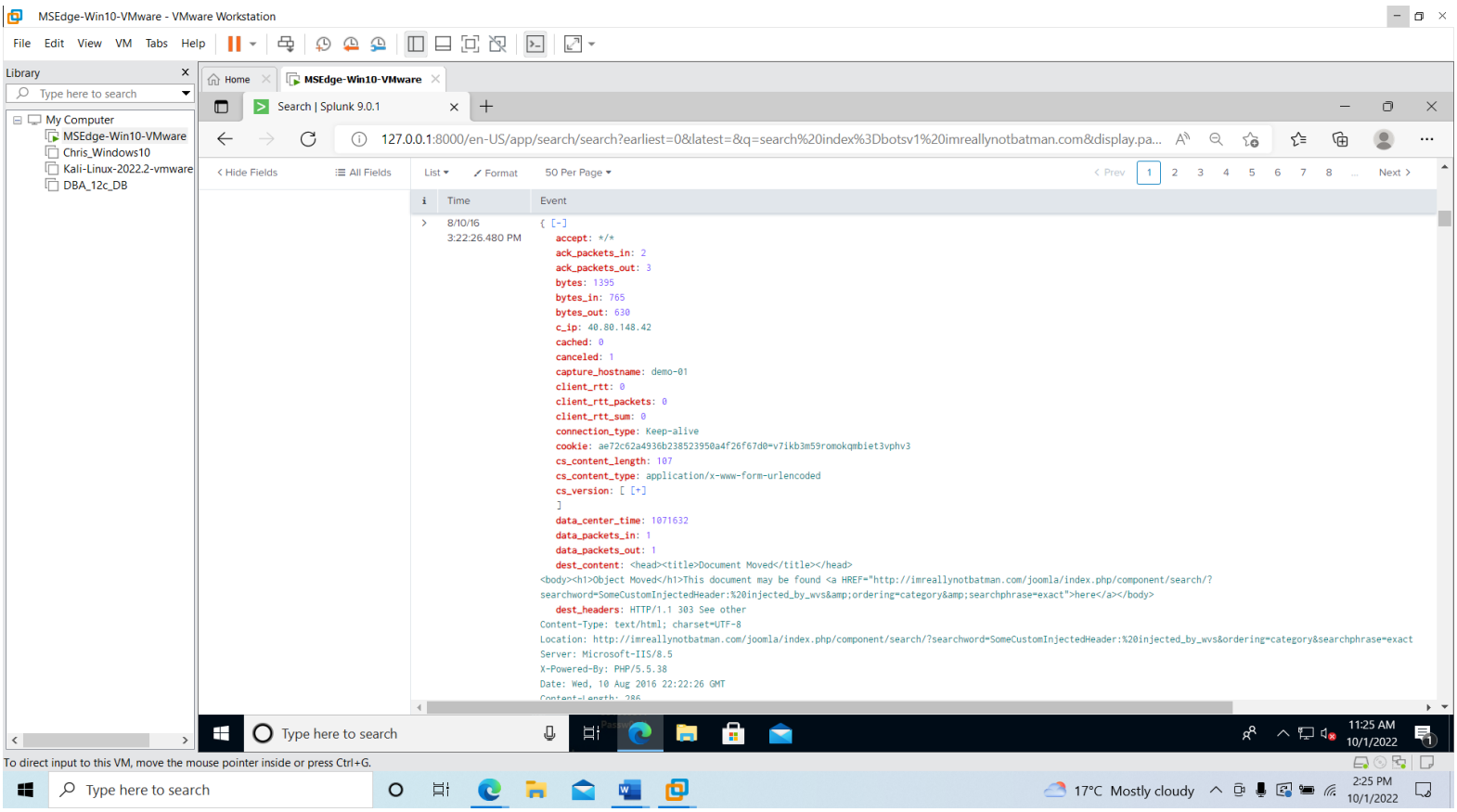


Figure 17:

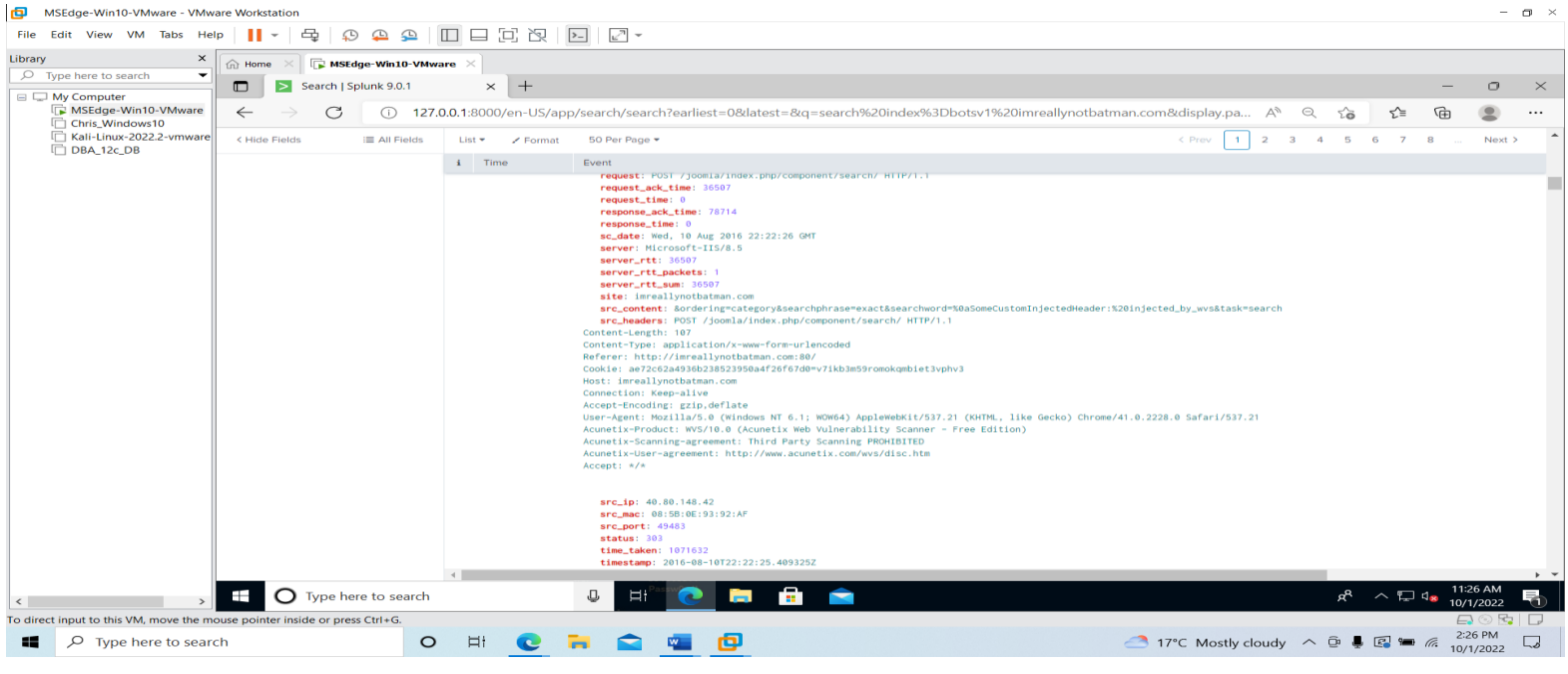


Figure 18: Q4 What Content Management System is imreallynotbatman.com likely using?
Command: index=botsv1 imreallynotbatman.com
Answer: Joomla
Explain: Searching the Index has events(bots-attack-only.tgz) the argument is imreallynotbatman.com. The Content Management System is Joomla

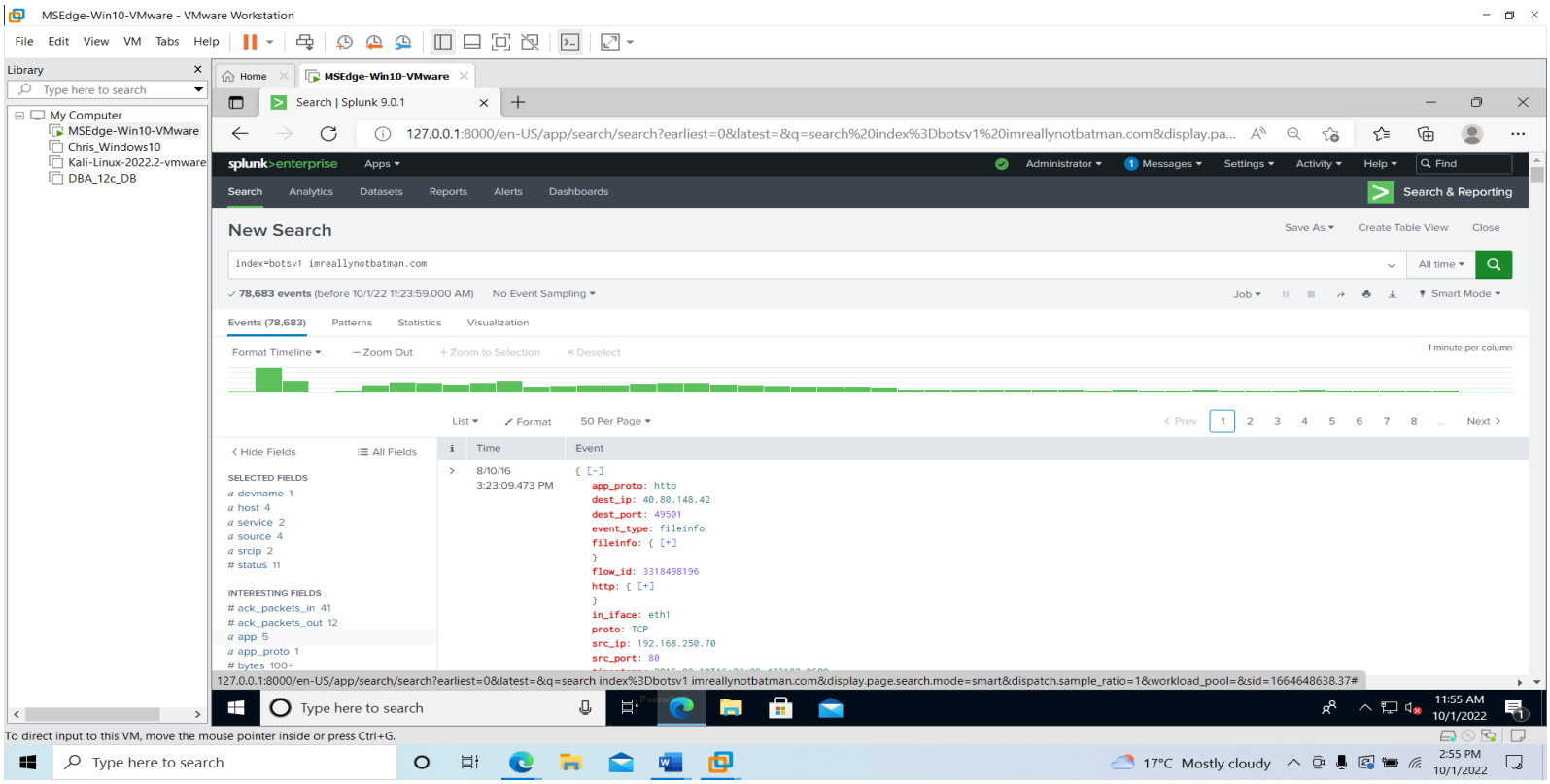


Figure 19:

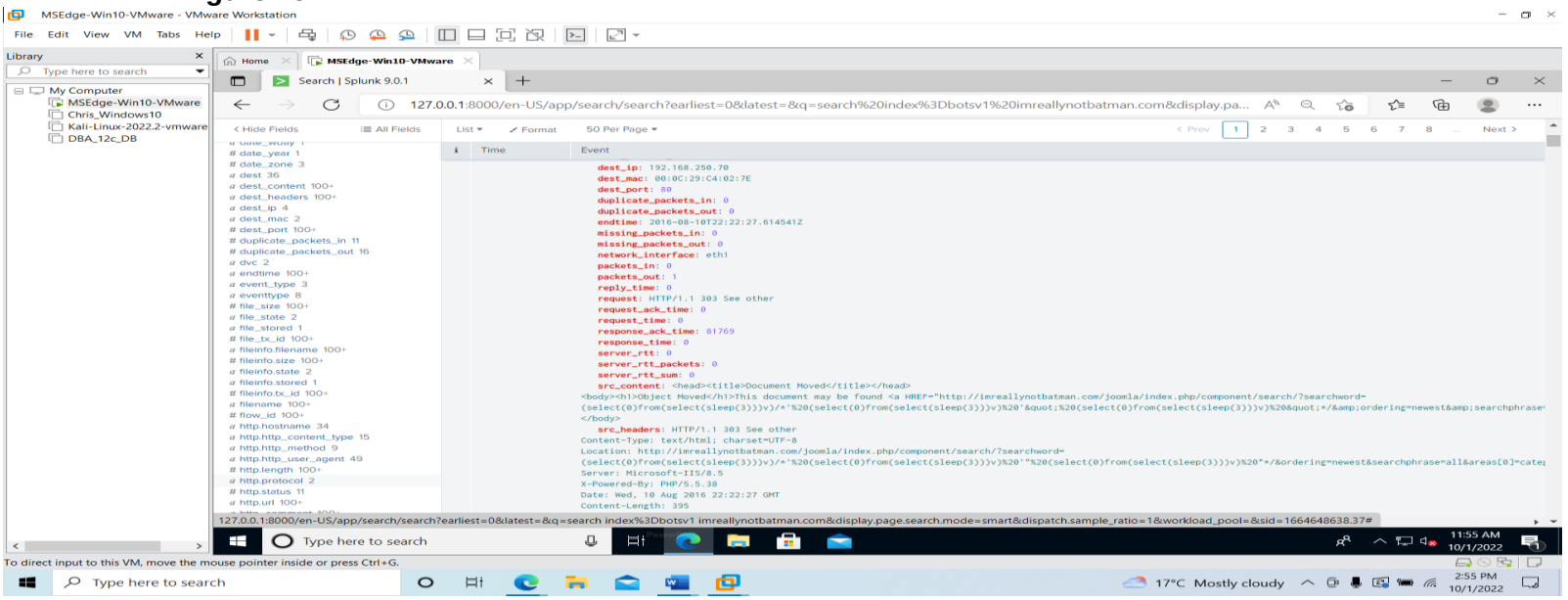


Figure 20: Q5 What name of the file that defaced the imreallynotbatman.com website?
Command: index=botsv1 c_ip=”192.168.250.70”
Answer: poison-ivy-is-coming-for-you-batman.jpeg
Explain: Search the events located in the botsv1 using the argument 192.168.250.70. The File that defaced the website is poison-ivy-is-coming-for-you-batman.jpeg.

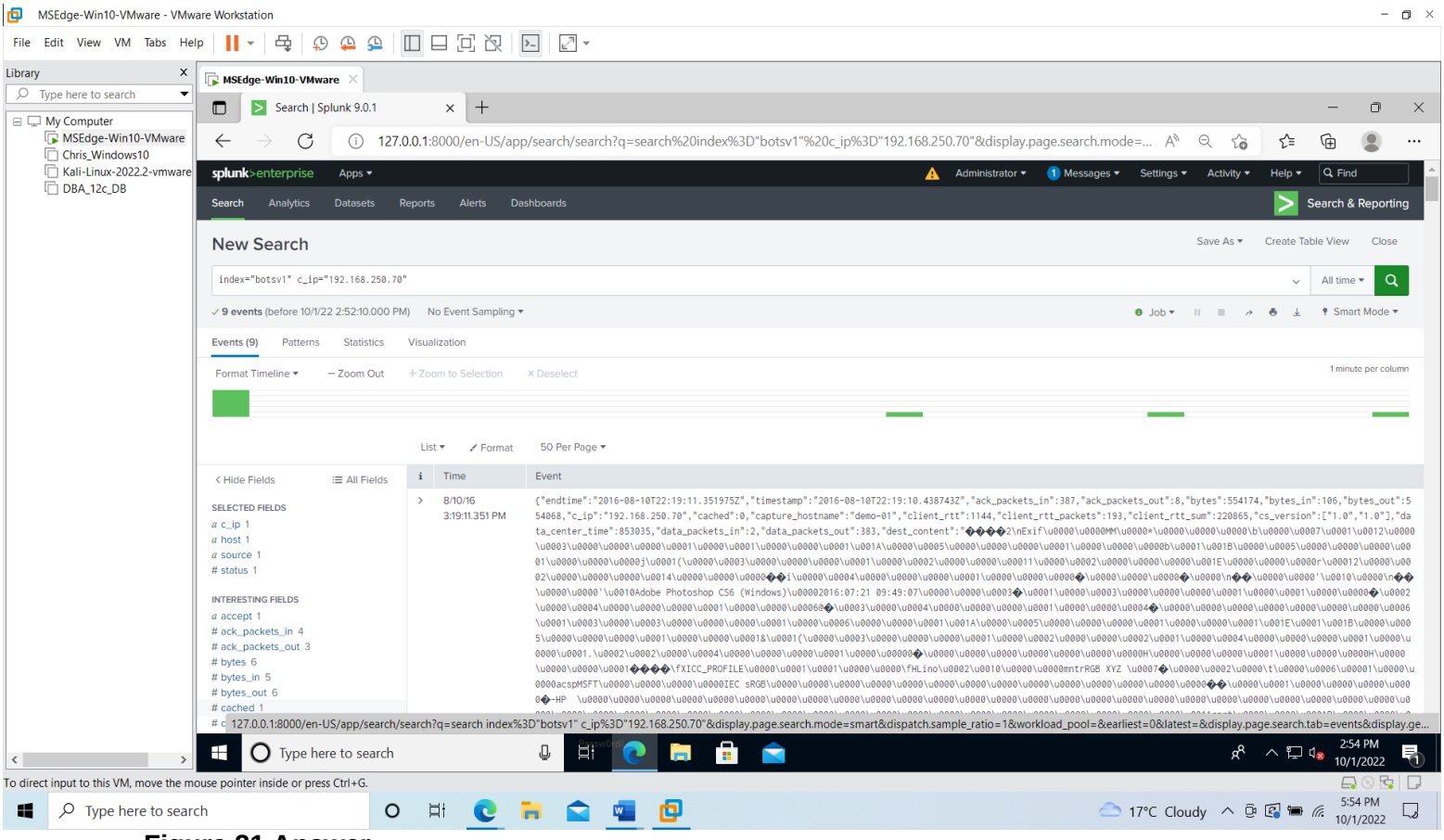


Figure 21 Answer

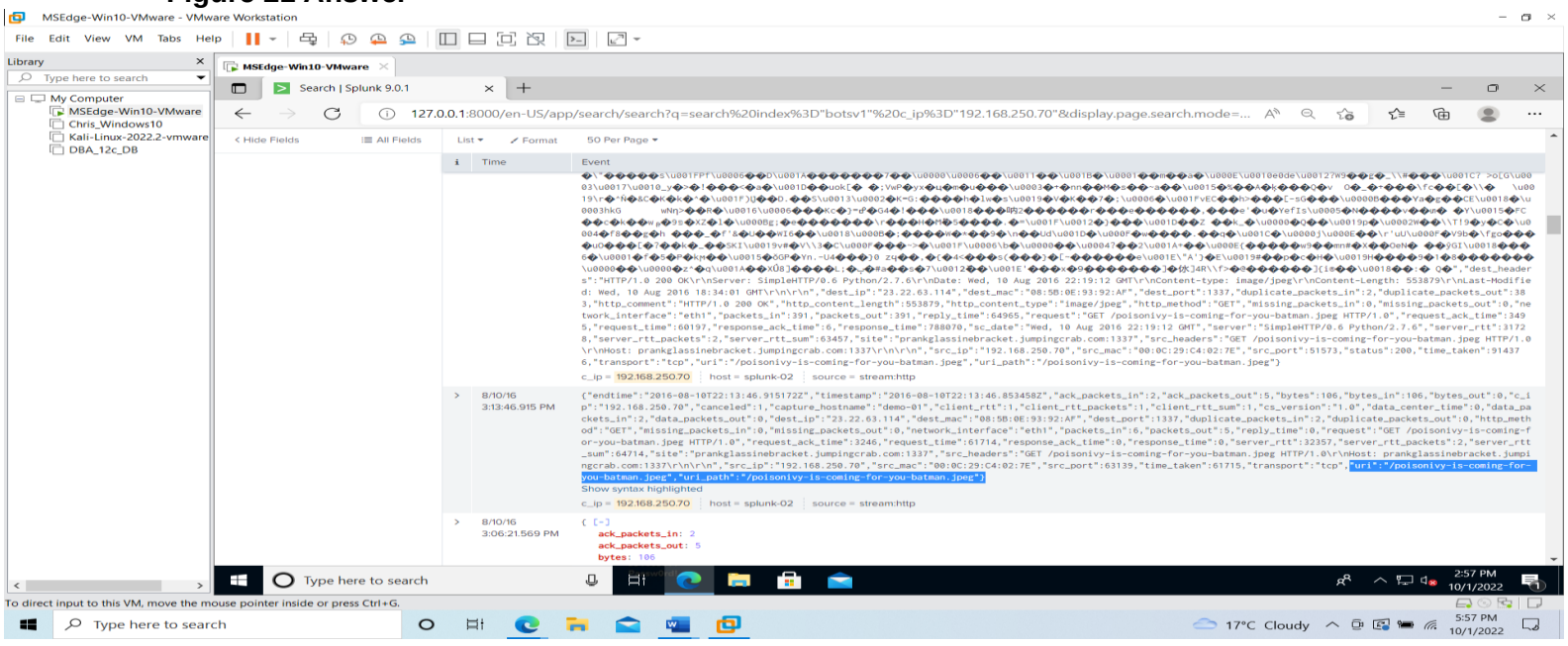


Figure 22: Q6 This attack used dynamic DNS to resolve the malicious IP. What is the Fully Qualified Domain Name (FQDN) associated with this attack?

Command: index=botsv1 c_ip="192.168.250.70"

Answer: prankglasslinebracket.jumpingcrab.com

Explain: Search the botsv1 the c_ip is the destination ip address. The fully qualified domain name is prankglasslinebracket.jumpingcrab.com

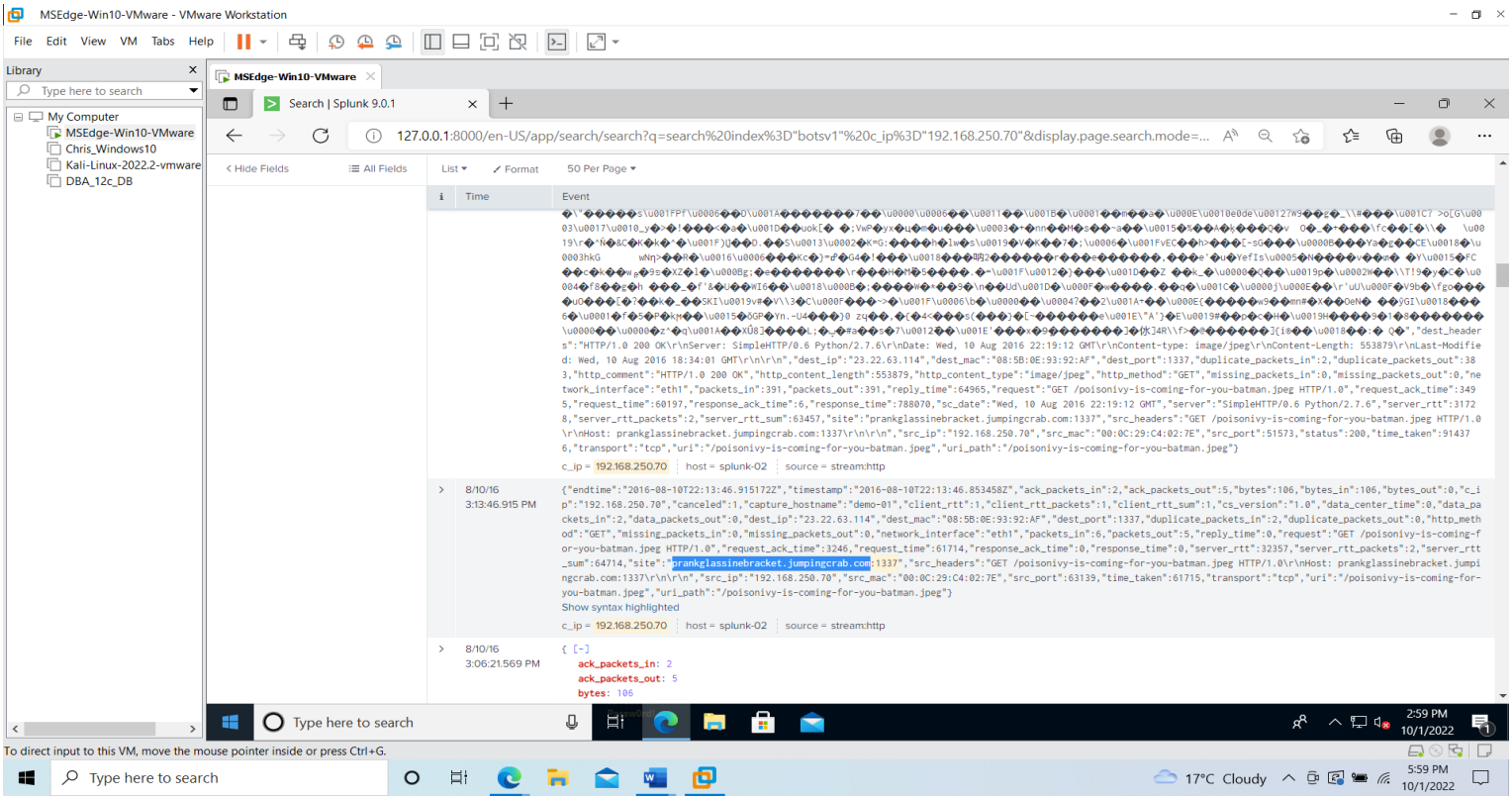


Figure 23: Q7 What IP address has Po1s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?

Command: index="botsv1" imreallynotbatman srcip="23.22.63.114"

Answer: 23.22.63.114

Explain: Search the botsv1 the arguments are website name imreallynotbatman and the source ip address is attack wayne enterprises. To confirm this lookup ip in virustotal(Get info about IP Address/Domain/Hashes/etc).

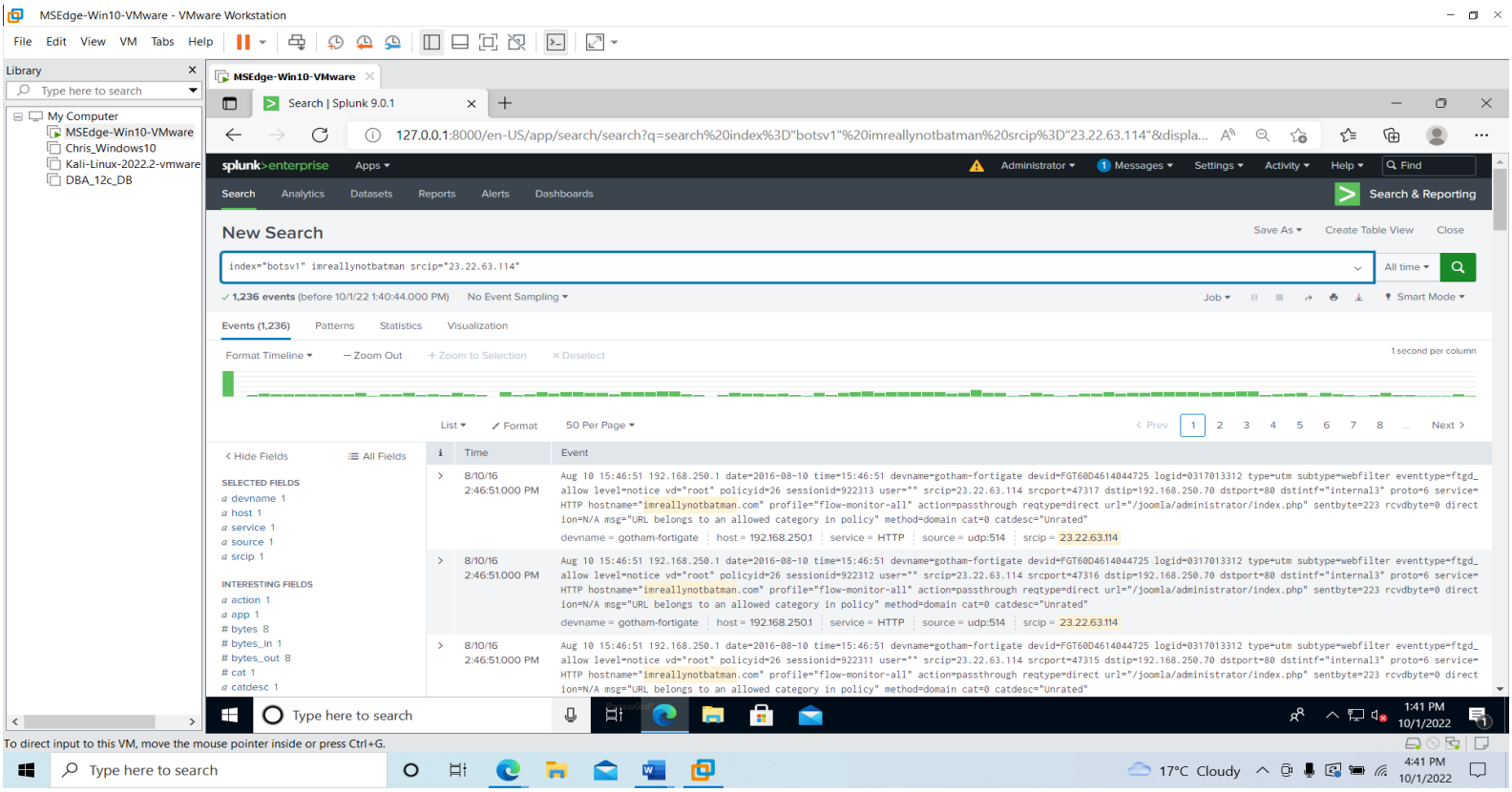


Figure 24 Answer

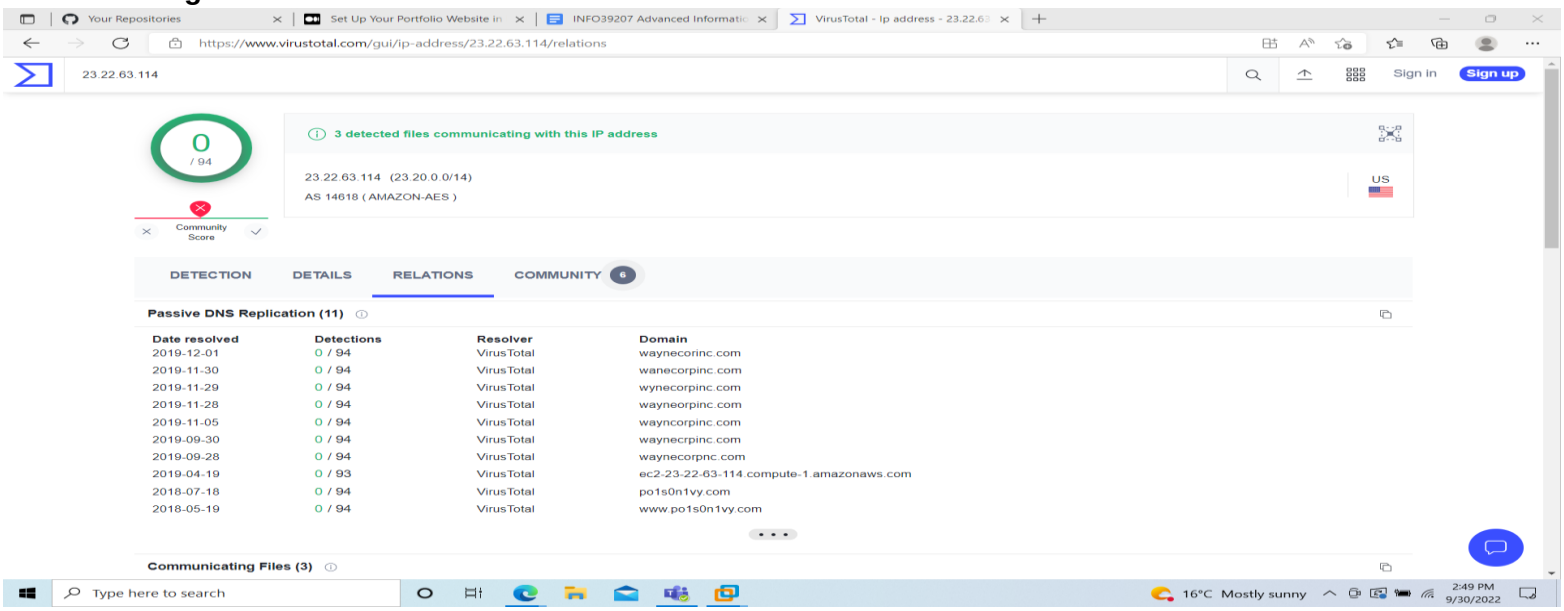


Figure 25: Q10 What is the name of the executable uploaded by Po1son1vy? Please include the file extension. (For example, “notepad.exe” or “favicon.ico”?
Command: index="botsv1" dest_ip="192.168.250.70" sourcetype="stream:http" "multipart/form-data"
Answer: 3791.exe
Explain: The Command will search the botsv1 events. The arguments are Destination IP the traffic is http(Hyper Text Transfer Protocol). The executable that was uploaded was 3791.exe.

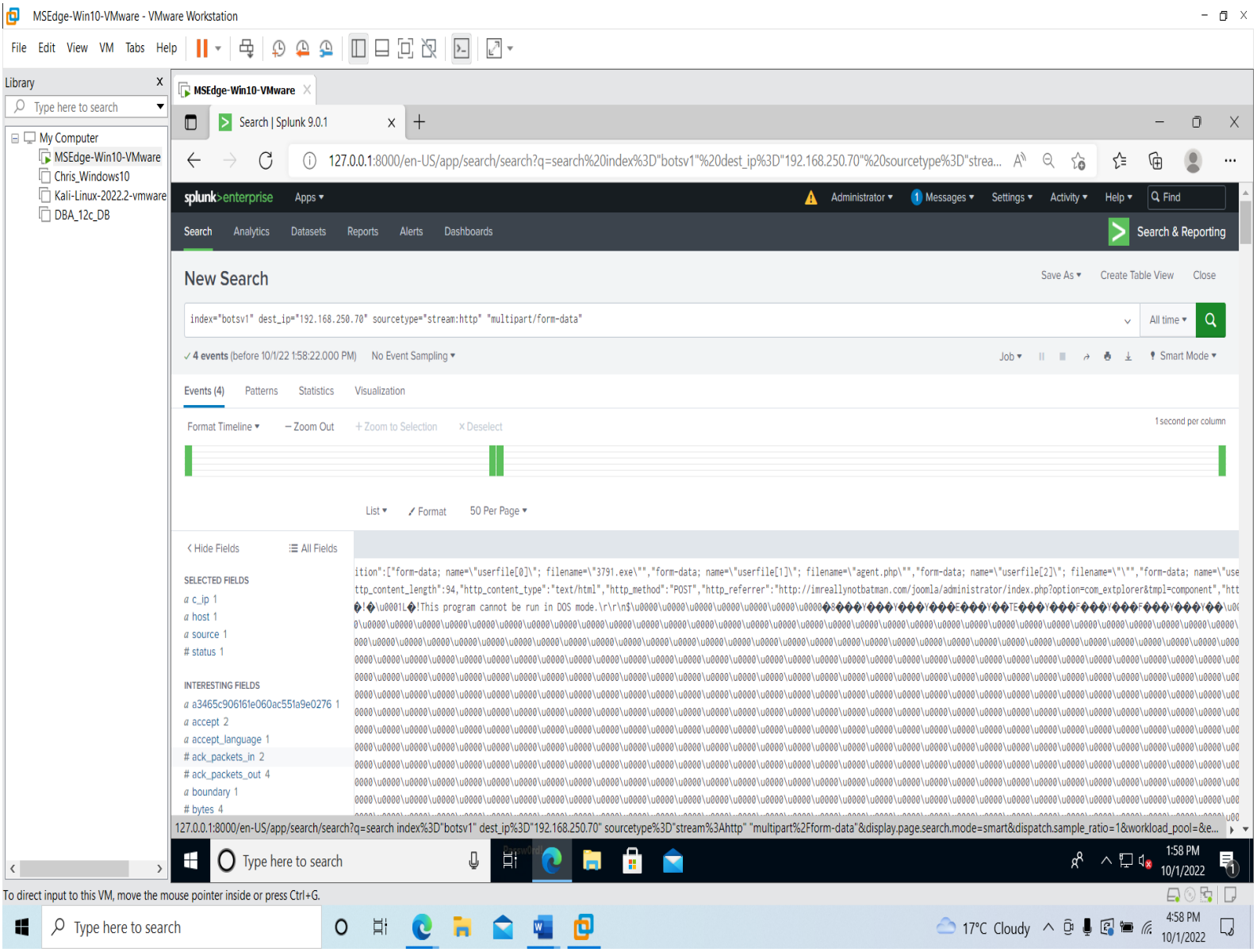


Figure 26: Question 11: What is the MD5 hash of the executable uploaded?

Command: index=”botsv1” 3791.exe md5

Answer: AAE3F5A29935E6ABCC2C2754D12A9AF0

Explain: The index is botsv1 the command you run is 3791.exe command line, the md5 is the argument to find a search.

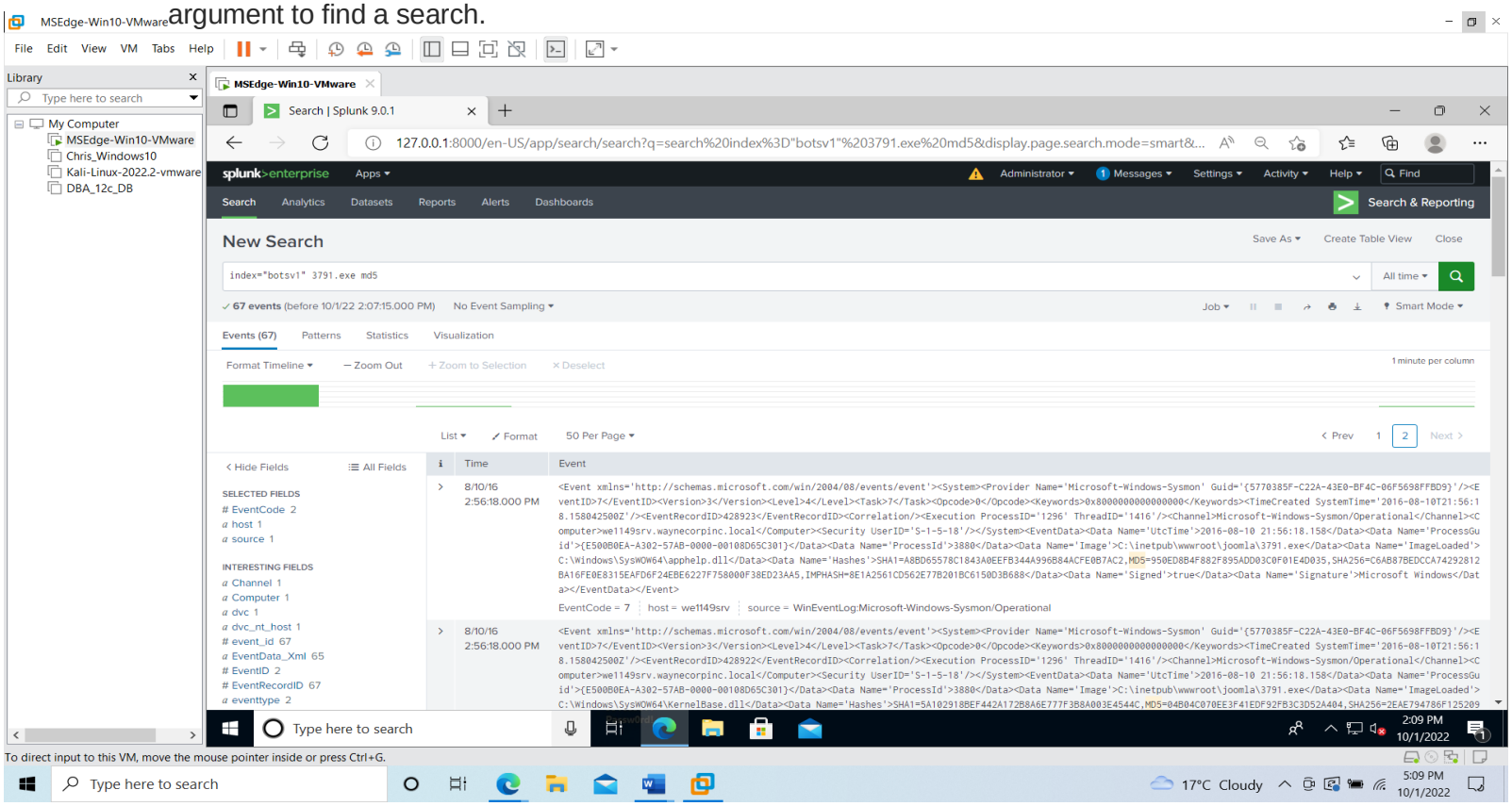


Figure 27 Answer

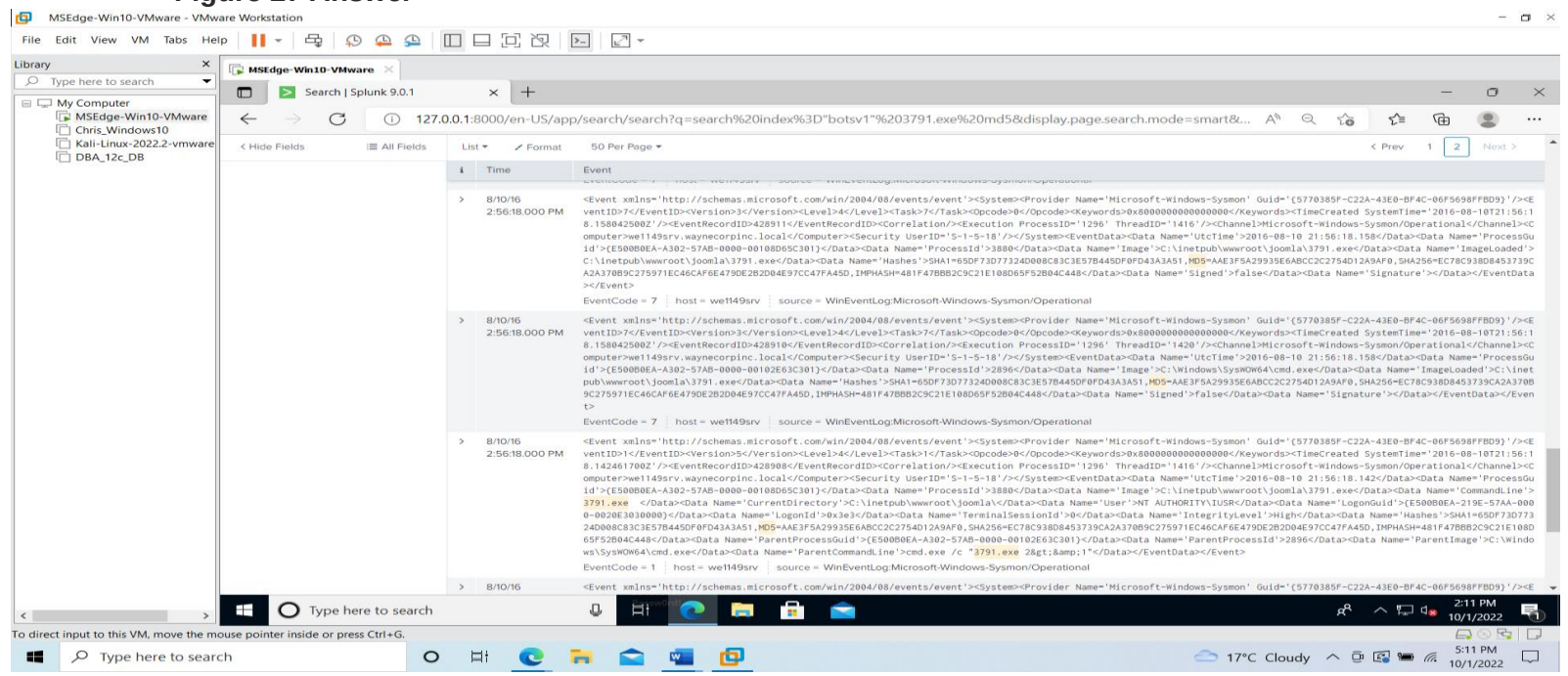


Figure 28: Question 15: What was the first brute force password used?
Command: index="botsv1" sourcetype=stream:http imreallynotbatman.com http_method=POST | stats count by src_ip, form_data, timestamp
Answer: 2016-08-10T21:45:14.774439Z
Explain: Indexes botsv1 the sourcetype is http traffic you are looking for on the website imreallynotbatman.com the POST sends data to the server.

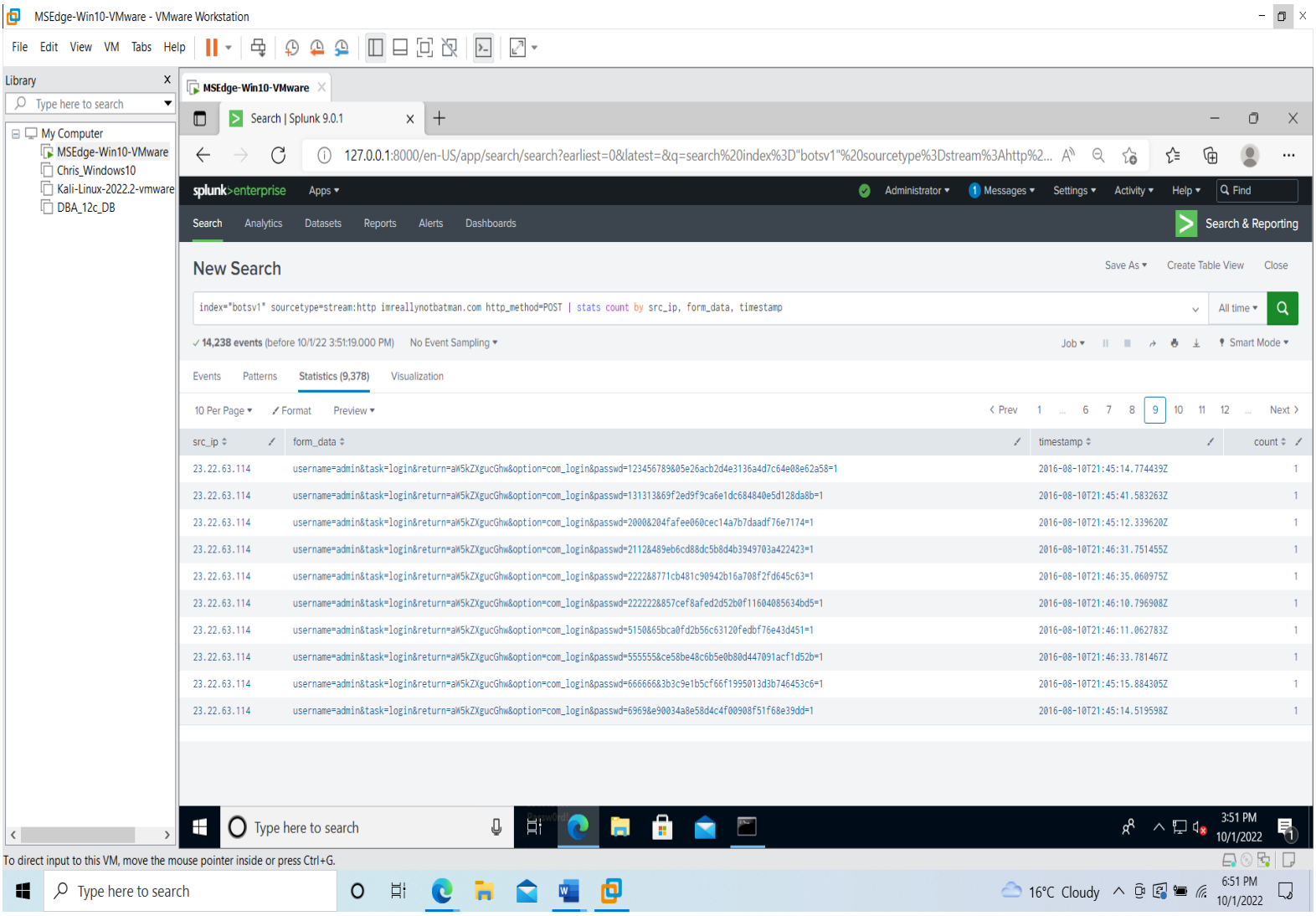


Figure 29: Question 16 One of the passwords in the brute force attack is James Brodsky's Favorite Cold Play Song.
Command: index="botsv1" sourcetype=stream:http imreallynotbatman.com http_method=POST yellow | stats count by src_ip, form_data
Answer: Yellow
Explain: The command searches botsv1 for traffic http on the website imreallynotbatman.com the method is POST(Send Data Server). Yellow is one of the brute force passwords.

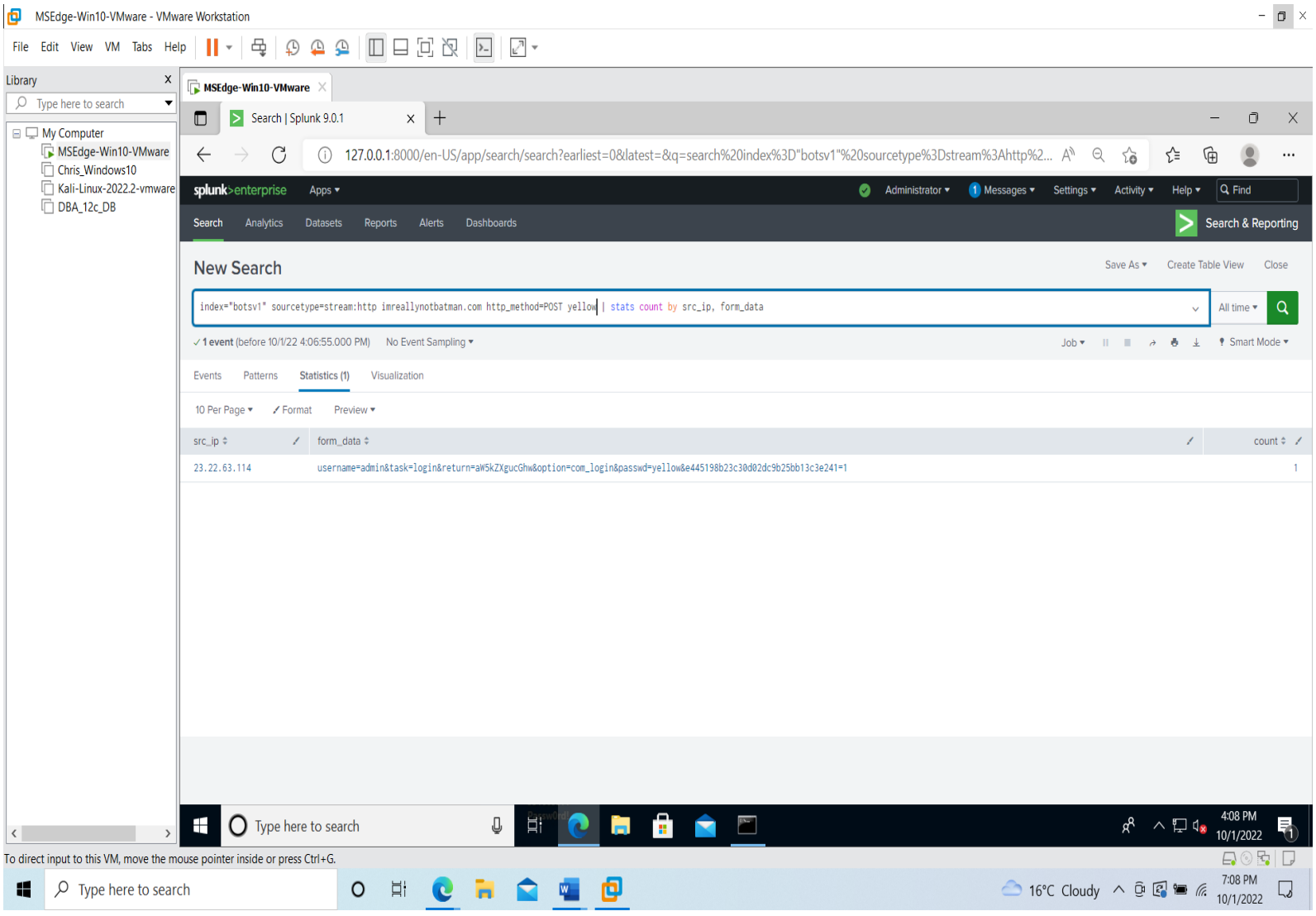


Figure 30: Question 17 What was the correct password for admin access to the content management system running “imreallynotbatman.com”?
Command: index="botsv1" sourcetype=stream:http form_data=*username*passwd* |stats count by src_ip, form_data, timestamp
Answer: batman
Explain: Search botsv1 for http traffic and the website form inputs you are looking for is username and passwords.

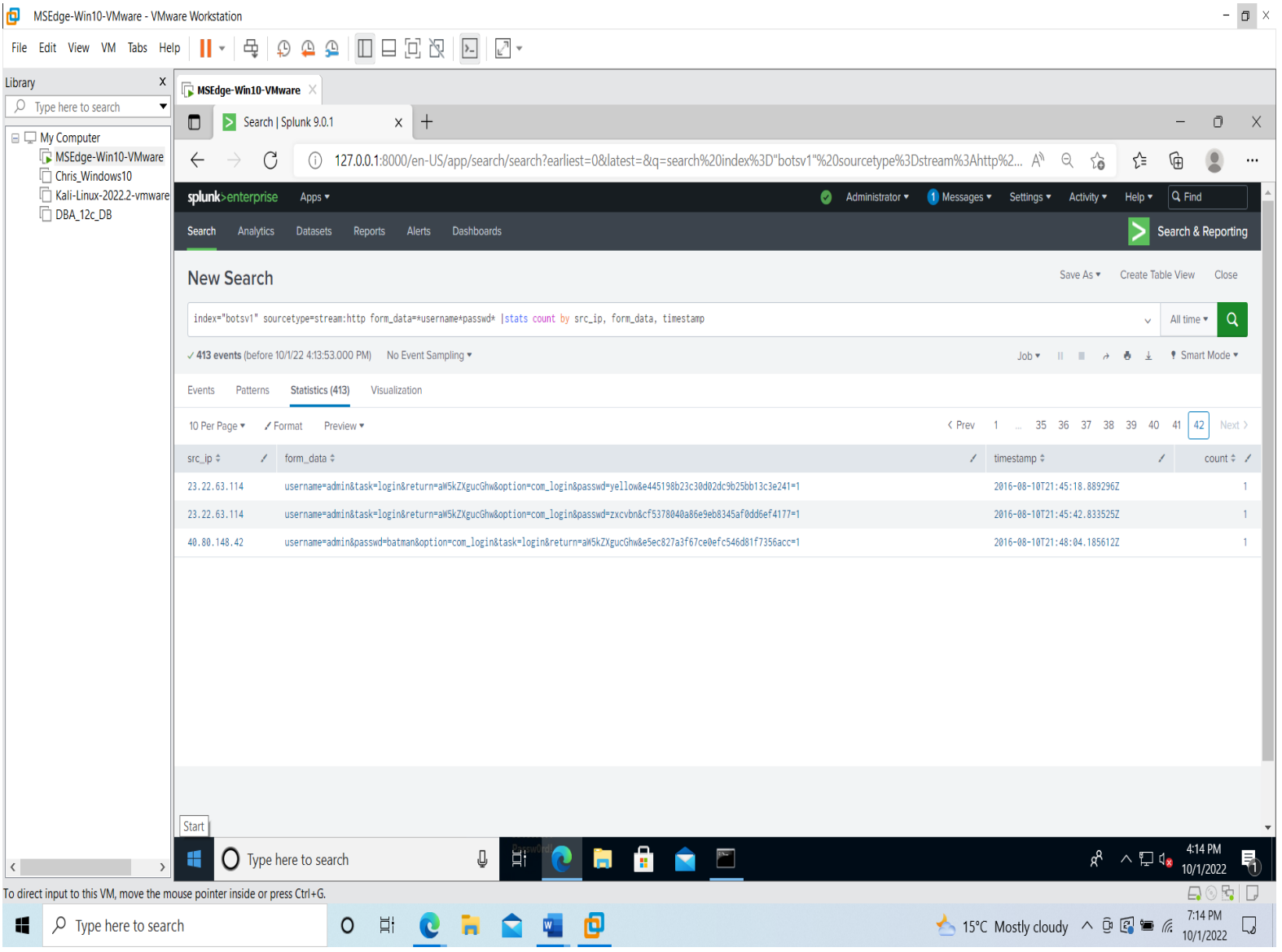


Figure 31: Question 18 What was the average password length used in the password brute forcing attempt?

Command: index="botsv1" sourcetype=stream:http form_data=*username*passwd*
| rex field=form_data "&passwd=(?<password>[\w\d]+)&"
| eval lenpword=len(password)
| stats avg(lenpword) as avglen

Answer: 6.179710144927537

Explain: Search botsv1 the arguments are http traffic, form inputs usernames, passwords. You are searching for the average password length used in brute forcing attempt.

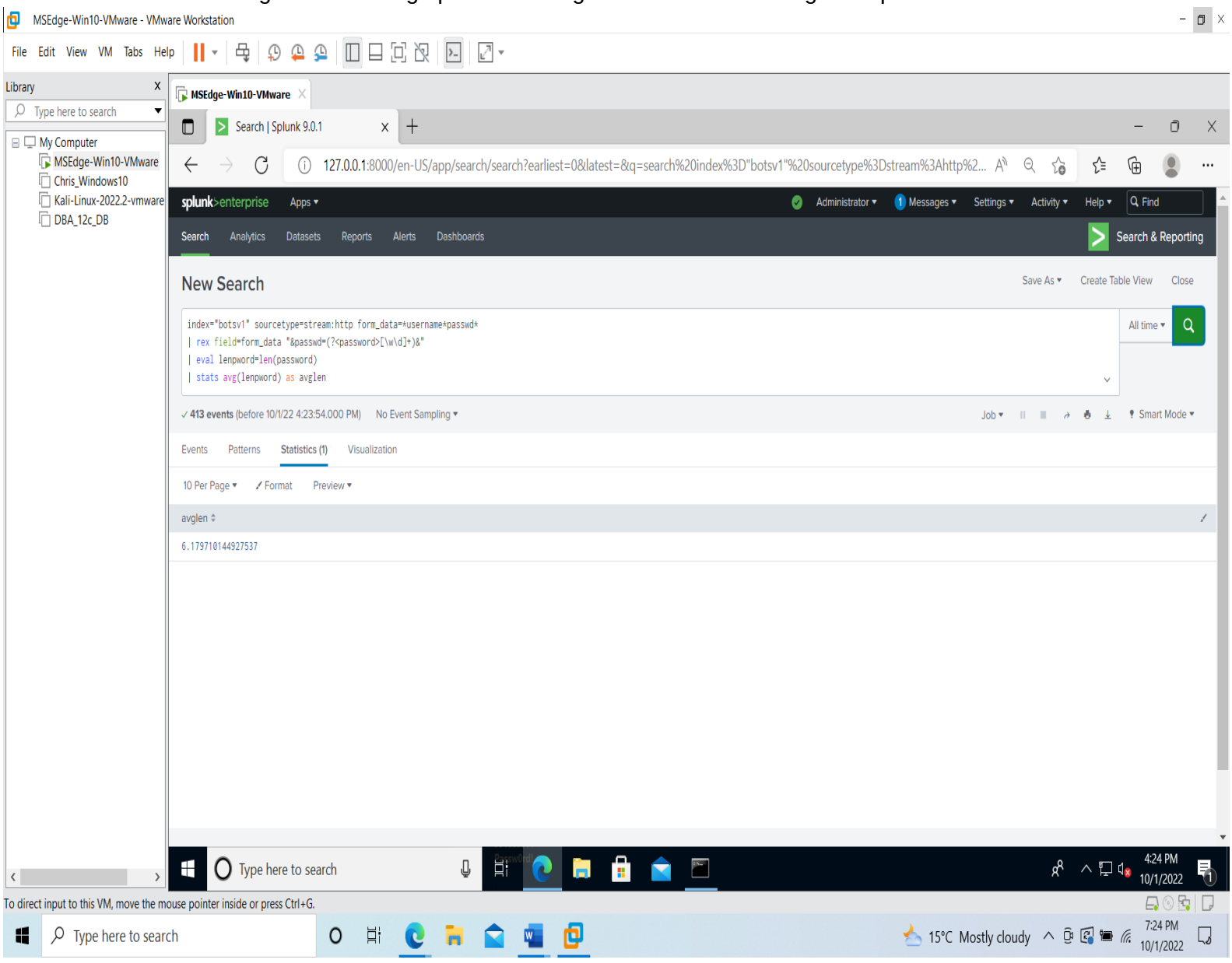


Figure 31: Question 19 How many seconds elapsed between the brute force password scan identified the correct password and the compromised login?

Command: index="botsv1" sourcetype=stream:http form_data=*username*passwd*
| rex field=form_data "&passwd=(?<password>[\w\d]+)&"
| search password = "batman"

Answer: 92.17

Explain: Search botsv1 for http traffic and form data username, password. The correct password was batman. You minus the Times and get the result of 92.17

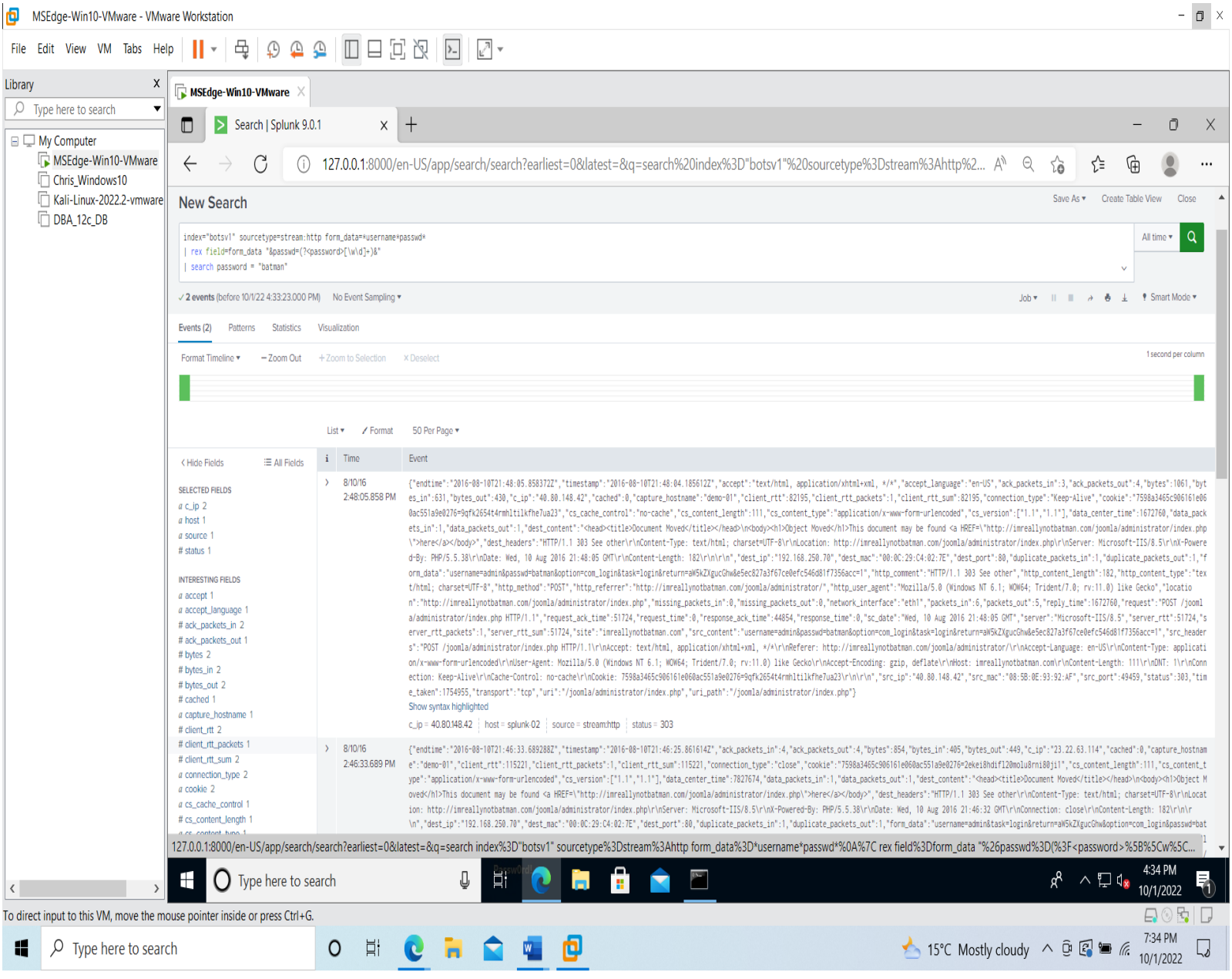


Figure 32: Question 20 How many unique passwords were attempted in the brute force attempt?

Command: index="botsv1" sourcetype=stream:http form_data=*username*passwd* | rex field=form_data "&passwd=(?<password>[\w\d]+)&"

Answer: 412

Explain: Search botsv1 the arguments are http traffic, form data is username and password. The &passwd is any type of password that means the regular expression requirements.

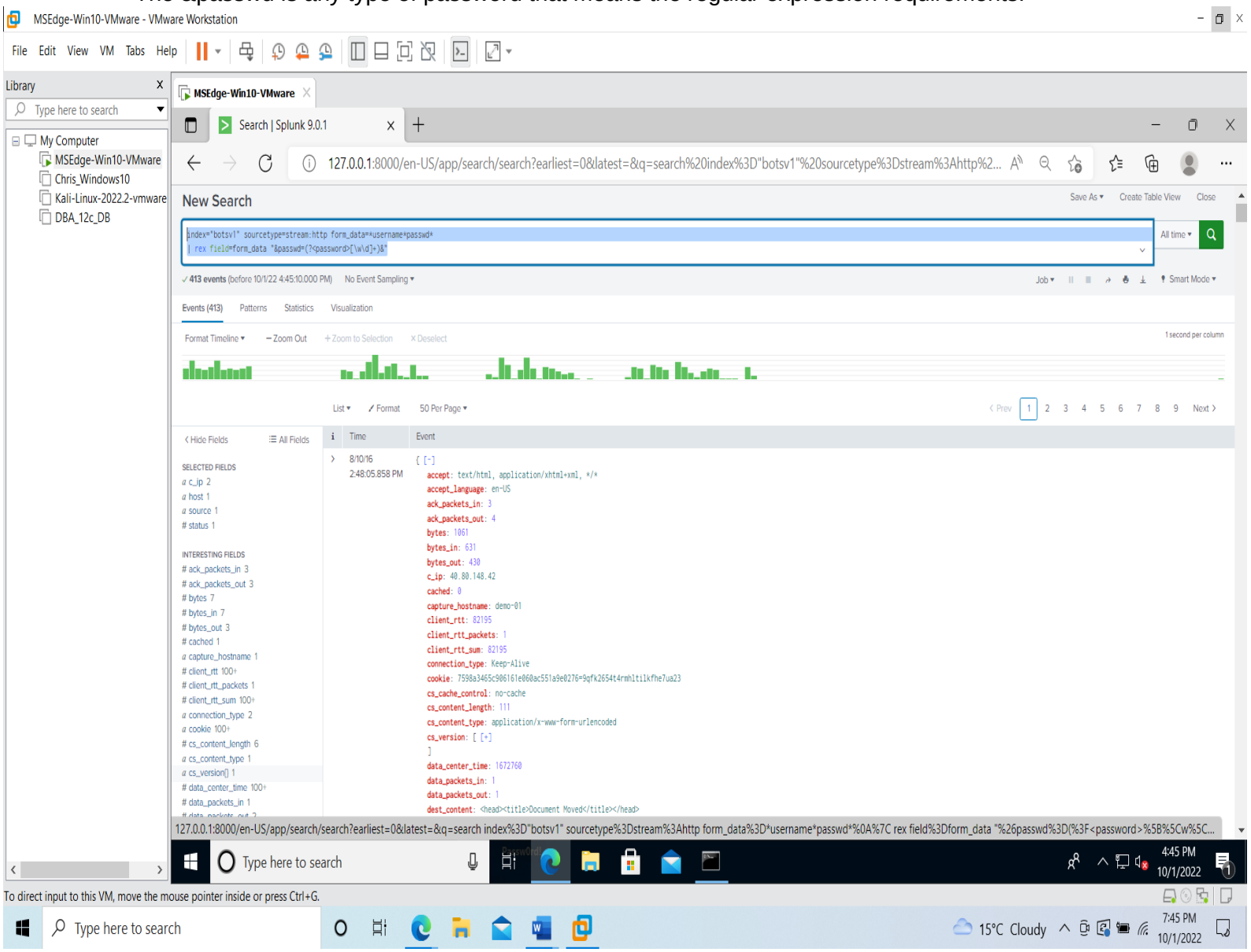


Figure 33: Question 21 What was the most likely IP of we8105desk in 24AUG2016?
Command: index="botsv1" we8105desk
| stats count by src_ip
Answer: 192.168.250.100
Explain Search botsv1 the argument is we8105desk and you are determining what ip address is associated with we8105desk on the date of Aug 24 2016.

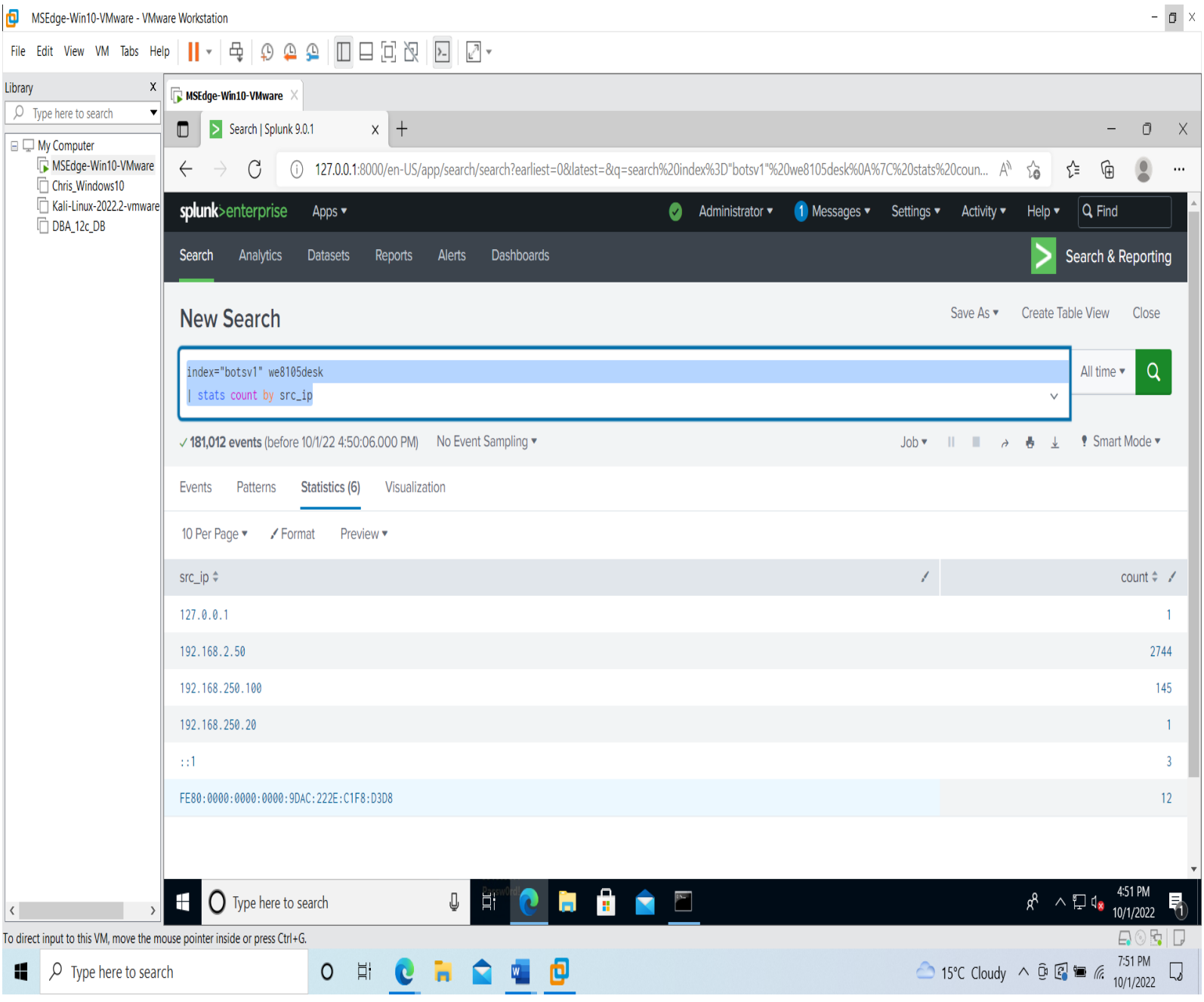


Figure 34: Question 22 Amongst the Suricata signatures that detected the Cerber Malware, which one alerted the fewest number of times?
Command: index="botsv1" host="suricata-ids.waynecorpinc.local" cerber
Answer: 2816763
Explain: Obtain search info about botsv1 the host is suricata ids information the cerber is the malware.

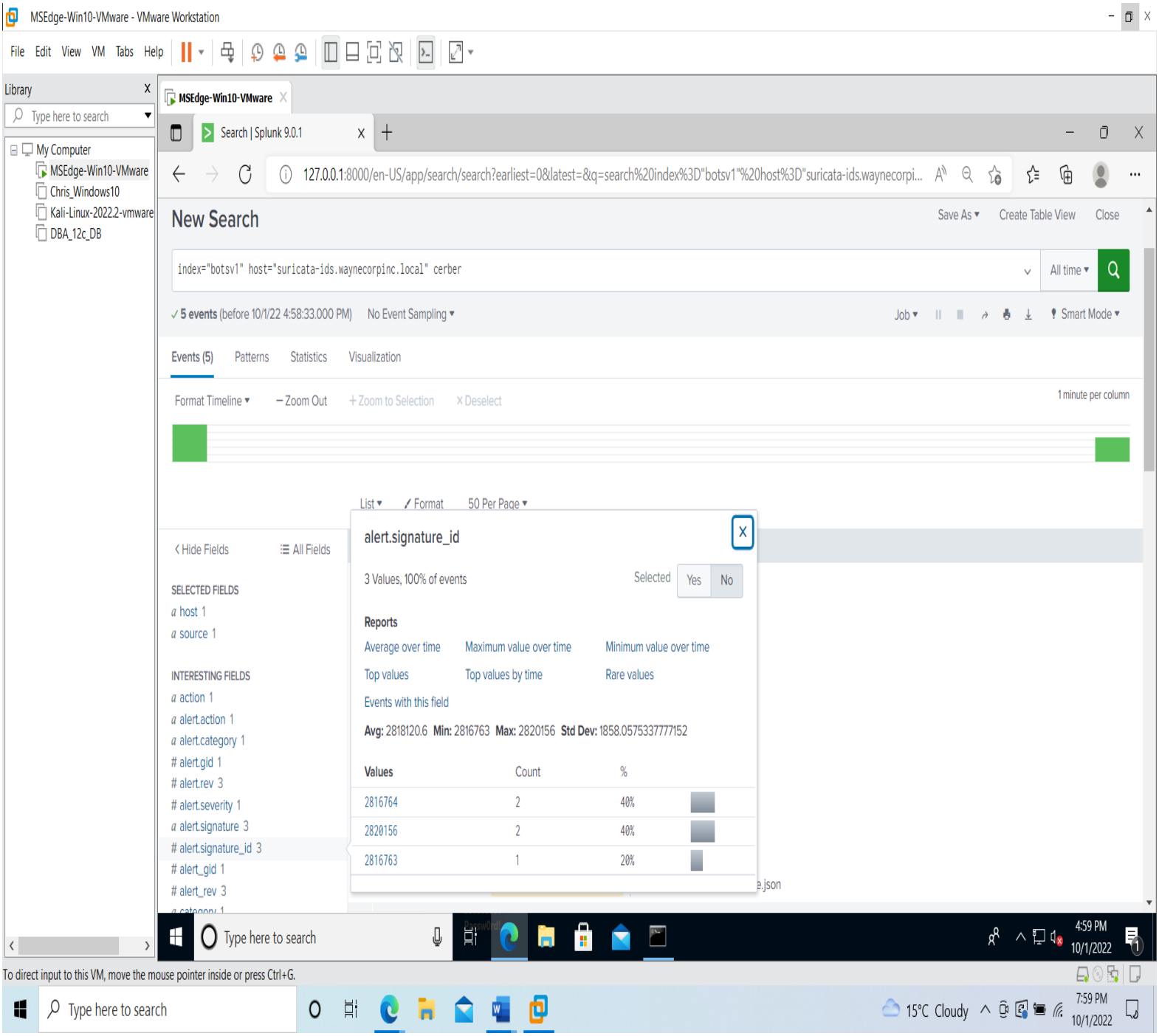


Figure 35: Question 26 What is the name of the USB key inserted by Bob Smith?
Command: index="botsv1" sourcetype=winregistry friendlyname
Answer: MIRANDA-PRI
Explain: Search botsv1 the source is winregistry freindlyname is one of the directories.

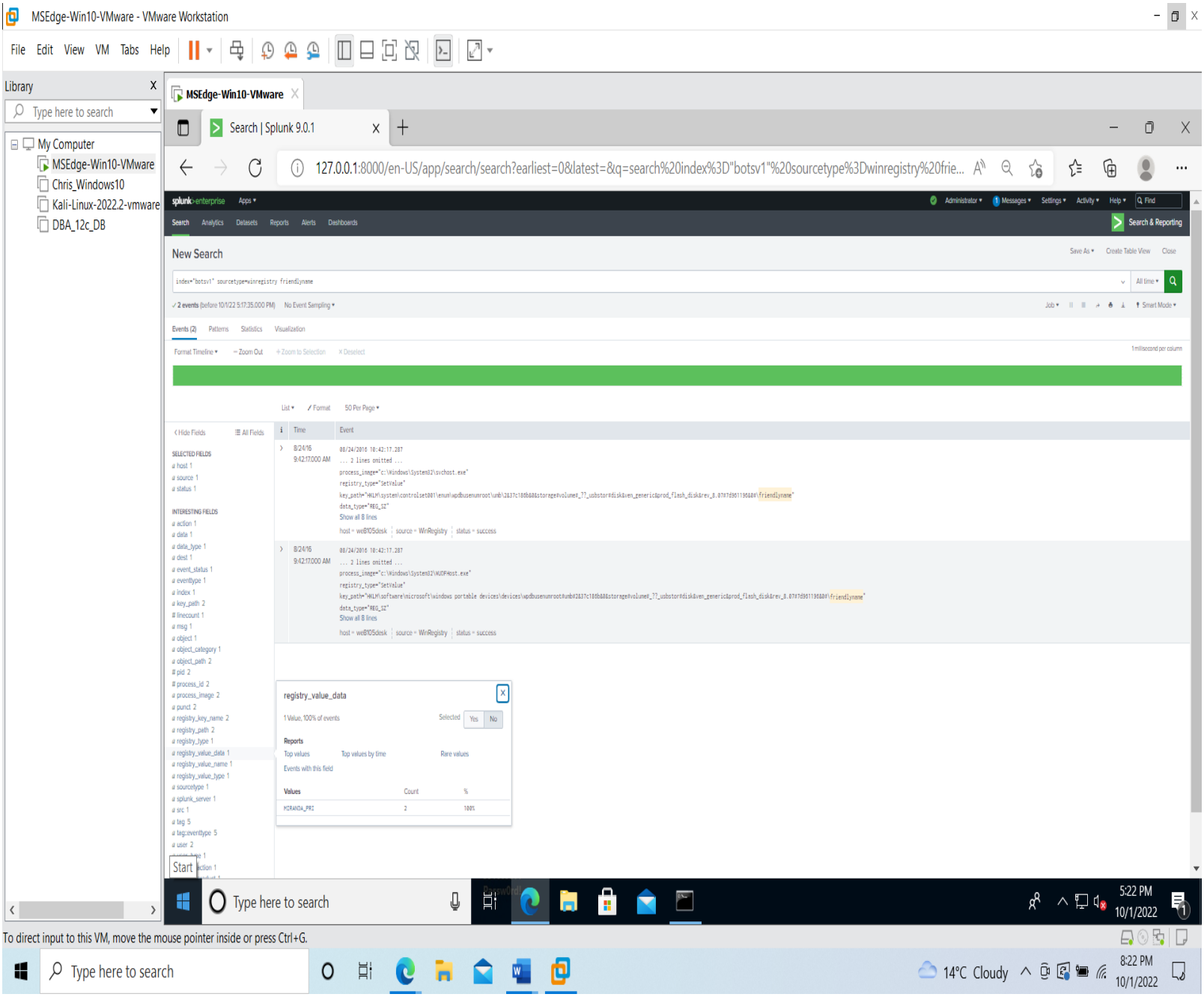


Figure 36: Question 27 Bob Smith's workstation (we8105desk) was connected to a file server during the ransomware outbreak what is the IP address of the file server?
Command: index="botsv1" sourcetype="stream:smb" src_ip=192.168.250.100 | stats count by path
Answer: 192.168.250.20
Explain: search botsv1 the source is smb traffic, the source ip is 192.168.250.100 you are determining the ip address of the file server.

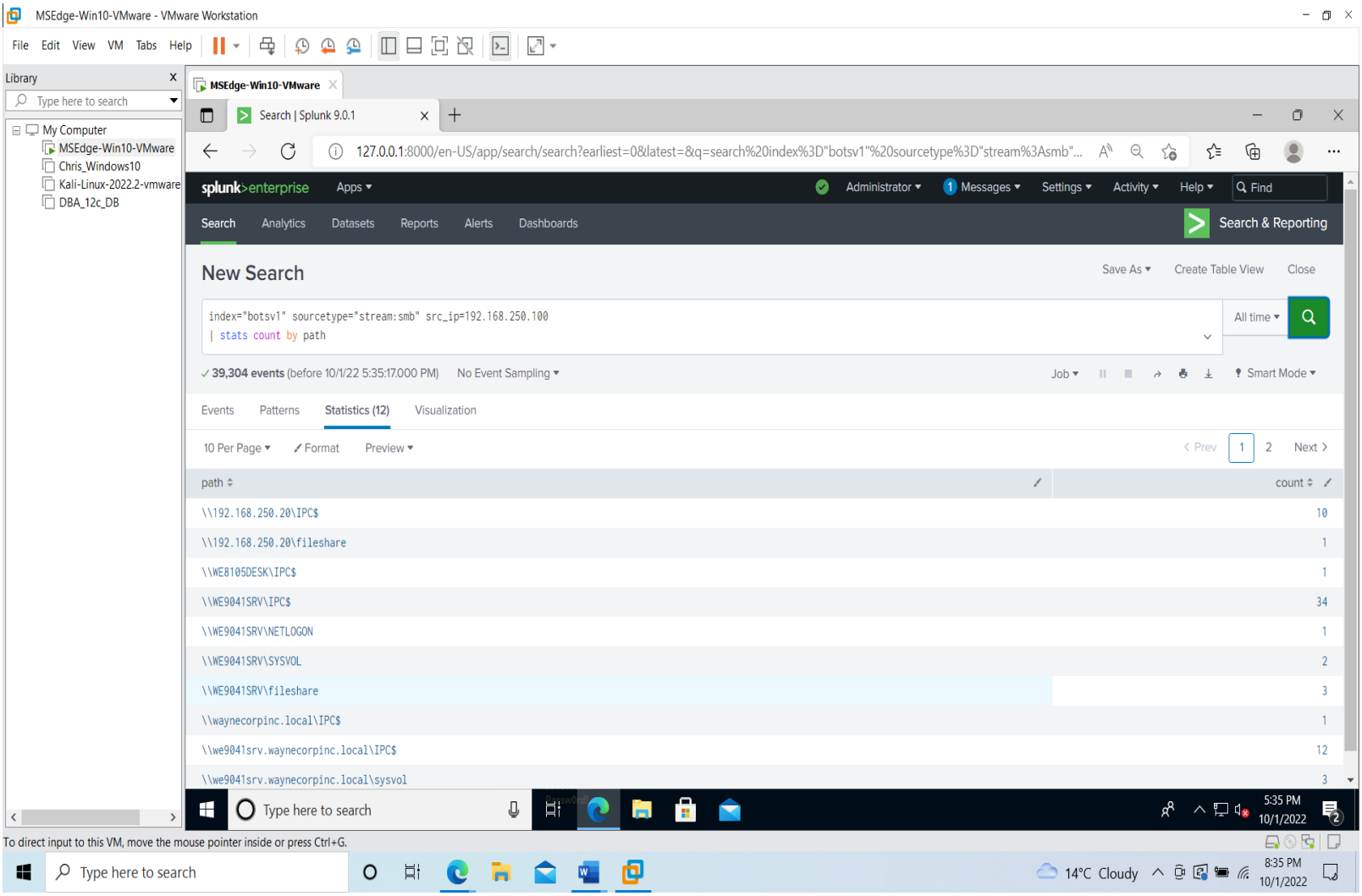


Figure 37: Question 28 How many Distinct PDFs did the ransomware encrypt on the remote file server?

Command: index="botsv1" .pdf
| stats dc(Relative_Target_Name)

Answer: 258

Explain: Search botsv1 for pdfs on file server. 258 files were encrypted.

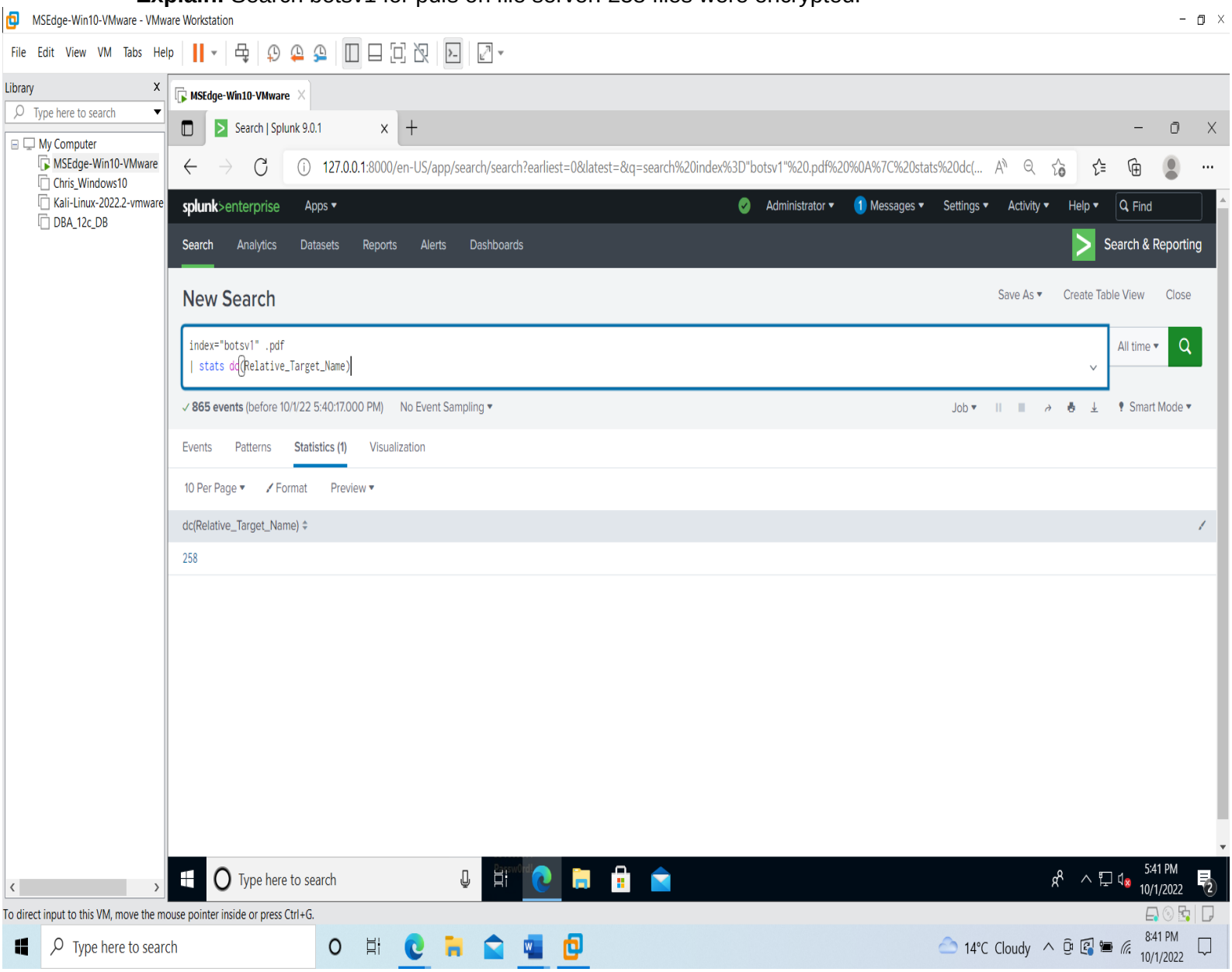
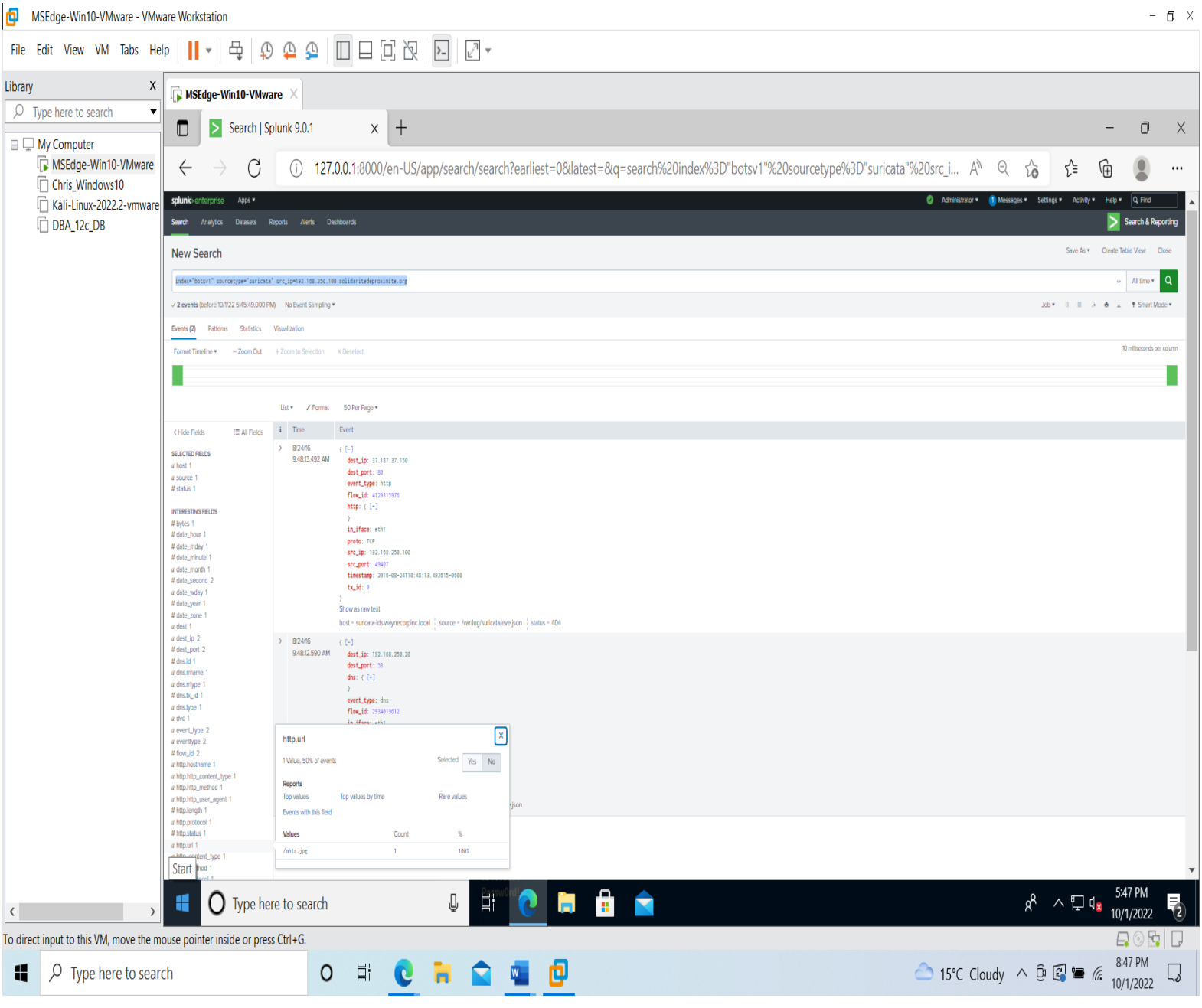


Figure 38: Question 31 The malware downloads a file that contains the Cerber ransomware crypto code. What is the name of that file?
Command: index="botsv1" sourcetype="suricata" src_ip=192.168.250.100 solidaritedeproximite.org
Answer: mhtr.jpg Explain: Search botsv1 for source suricata(IDS) source ip 192.168.250.100 and the url is solidaritedeproximite.org.



Lab 3

Event Log

Figure 39: Administrator Windows Powershell -> New-EventLog -LogName “Application” -Source “Chris Miele”.

Write-EventLog -LogName “Application” -Source “Chris Miele” -EventID 3908 -Message “Lab 3”.

Explain: Create PowerShell script to create a new event log the source Chris Miele(Must do this first before you write event log). Then you must Write the event log, the Event ID is 3908 and the Message is a custom message called Lab 3. This will show up in the eventlog on windows.

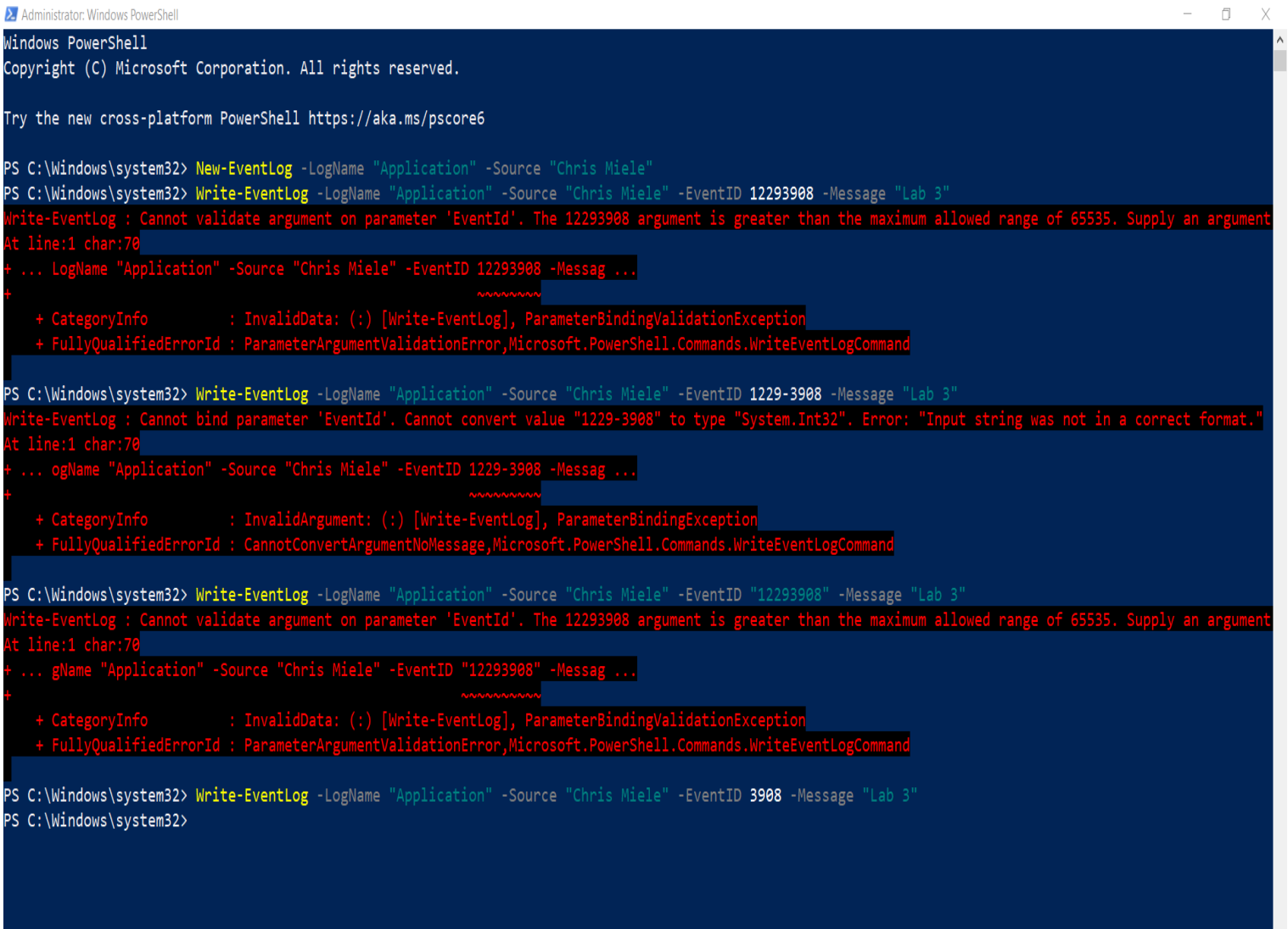


Figure 40: Settings -> Forwarding and receiving -> Receive Data -> Default Port Receive Splunk 9997.

Explain: To forward event logs from host to guest(MSEdge) you must set up the Receive port which is splunk default 9997. The receive port will receive any data coming into splunk and make a connection with the host operating system.

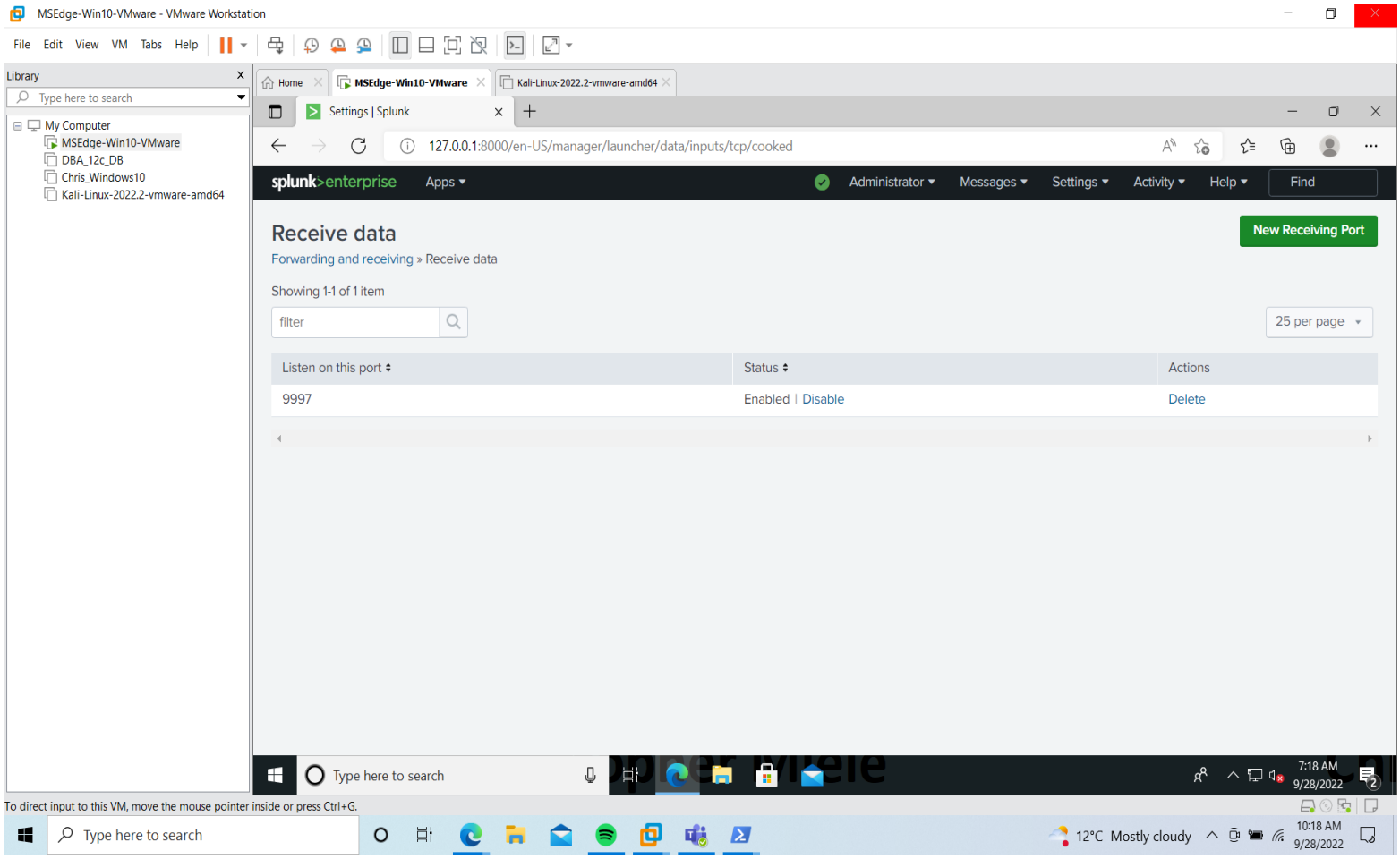


Figure 41:Settings -> Indexes(Events Coming In Sent To win10_events -> Create New Index.

Explain: Index is where you can parse Event logs to. Index makes it easier to search/Query information.

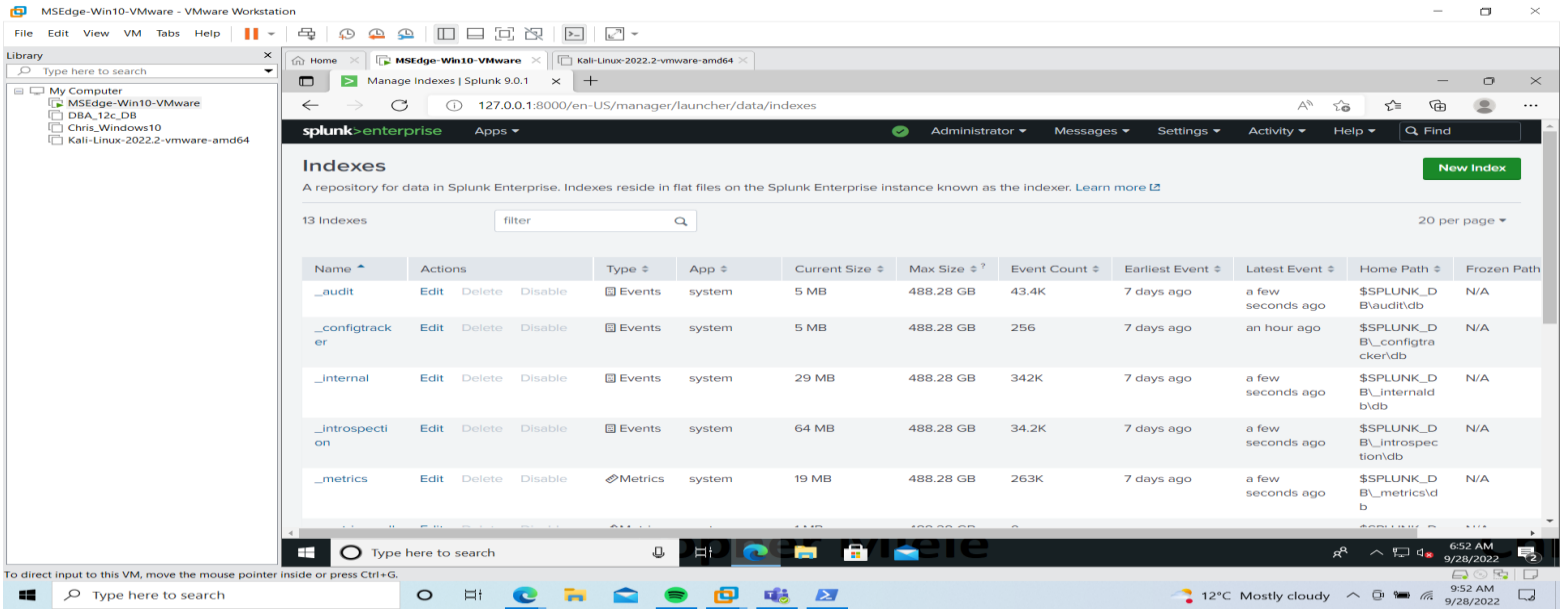


Figure 42:Verify win10_events.

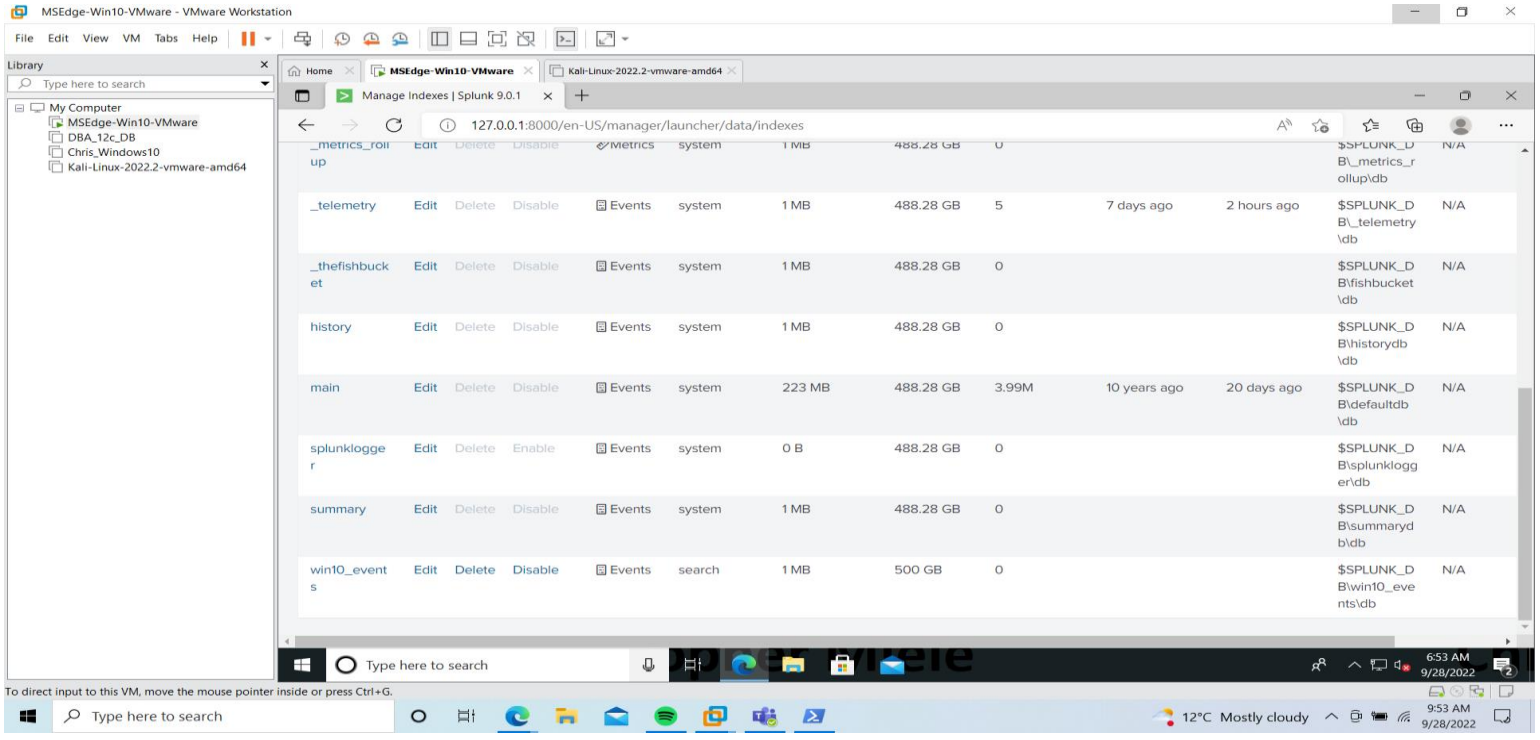


Figure 43:Download Splunk Universal Forwarder(Allows you to send Win Events Logs From Host - Guest).

Explain: Download Splunk Universal Forwarder to forward information from host to guestOS.

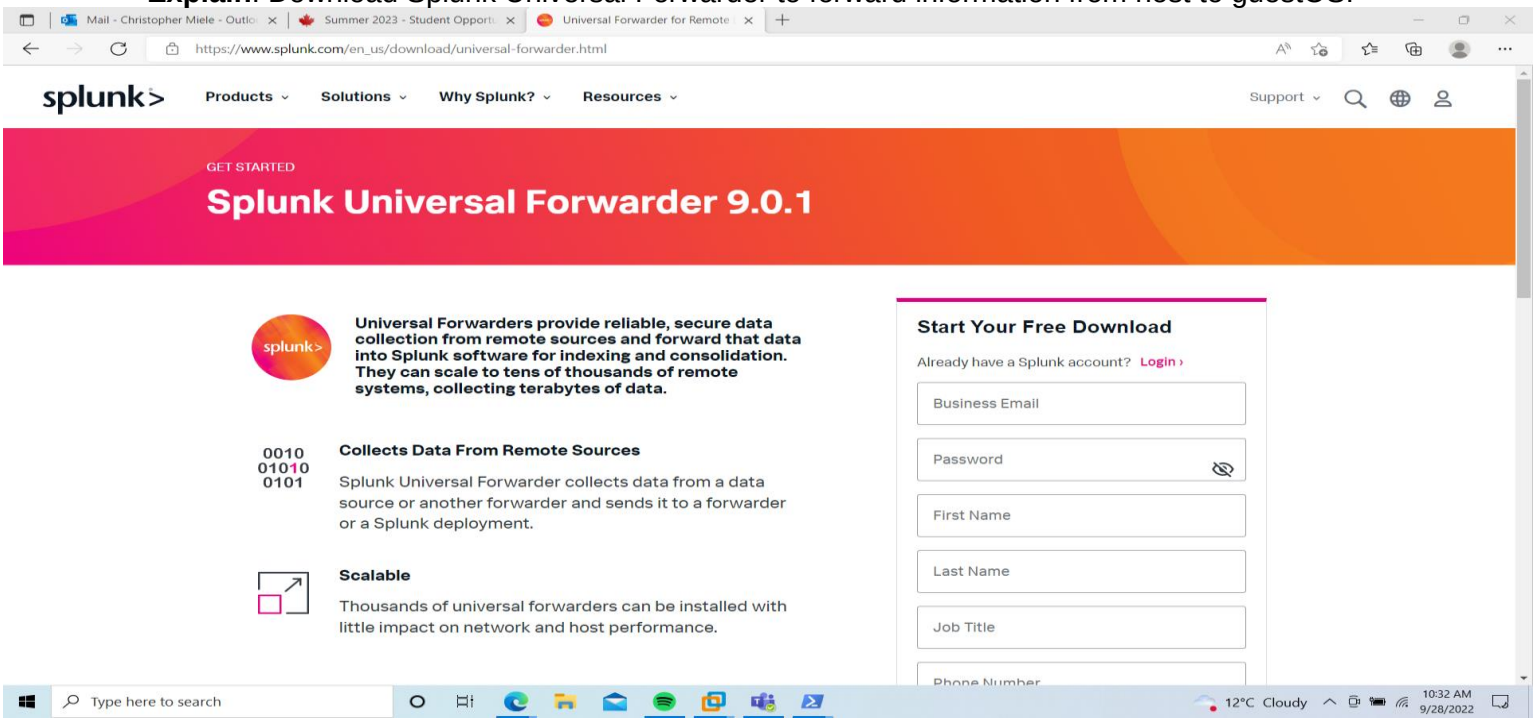


Figure 44: Type ipconfig to get VM IP Address.

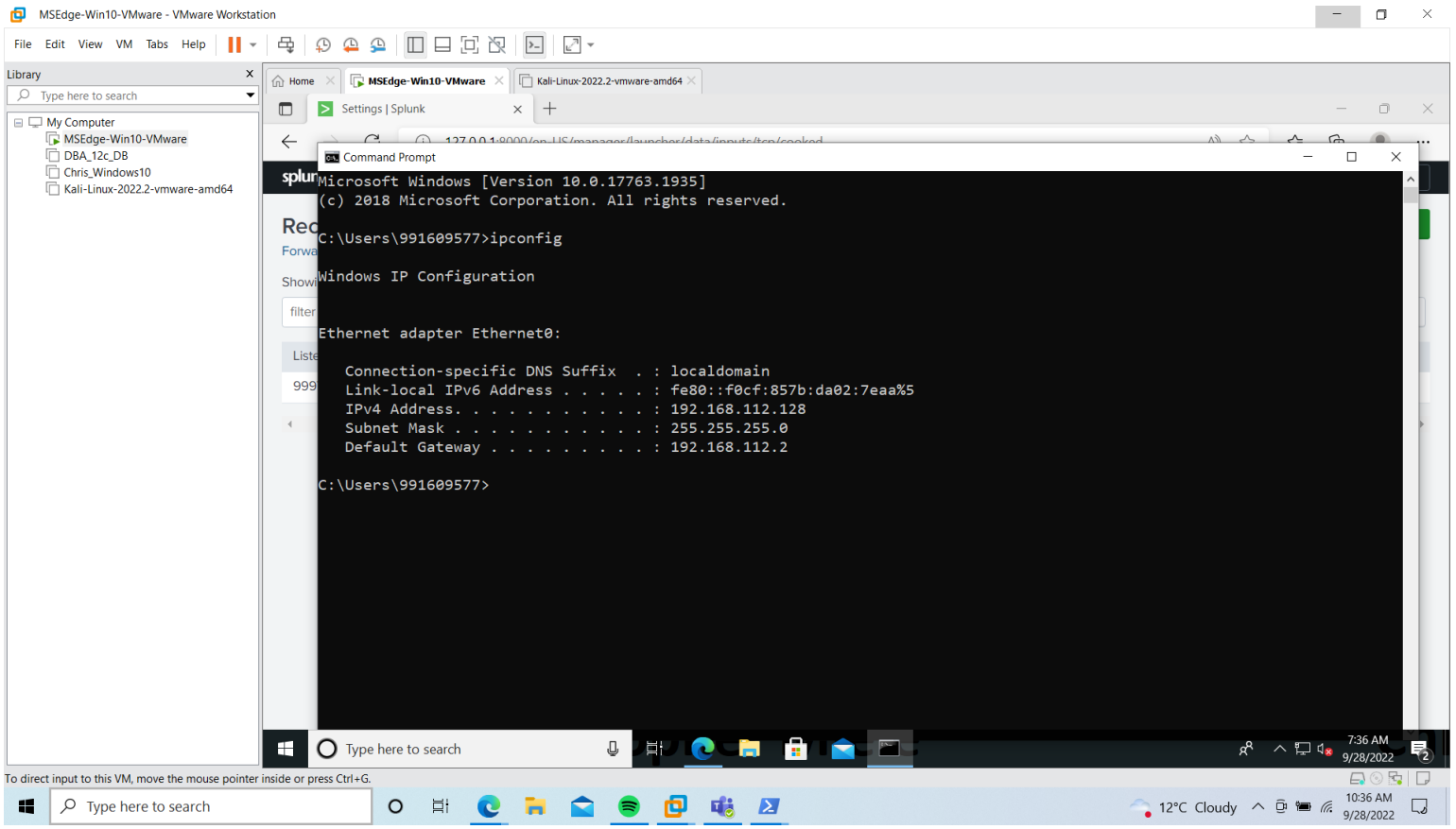


Figure 45: Run Splunk Universal Forwarder Installer.

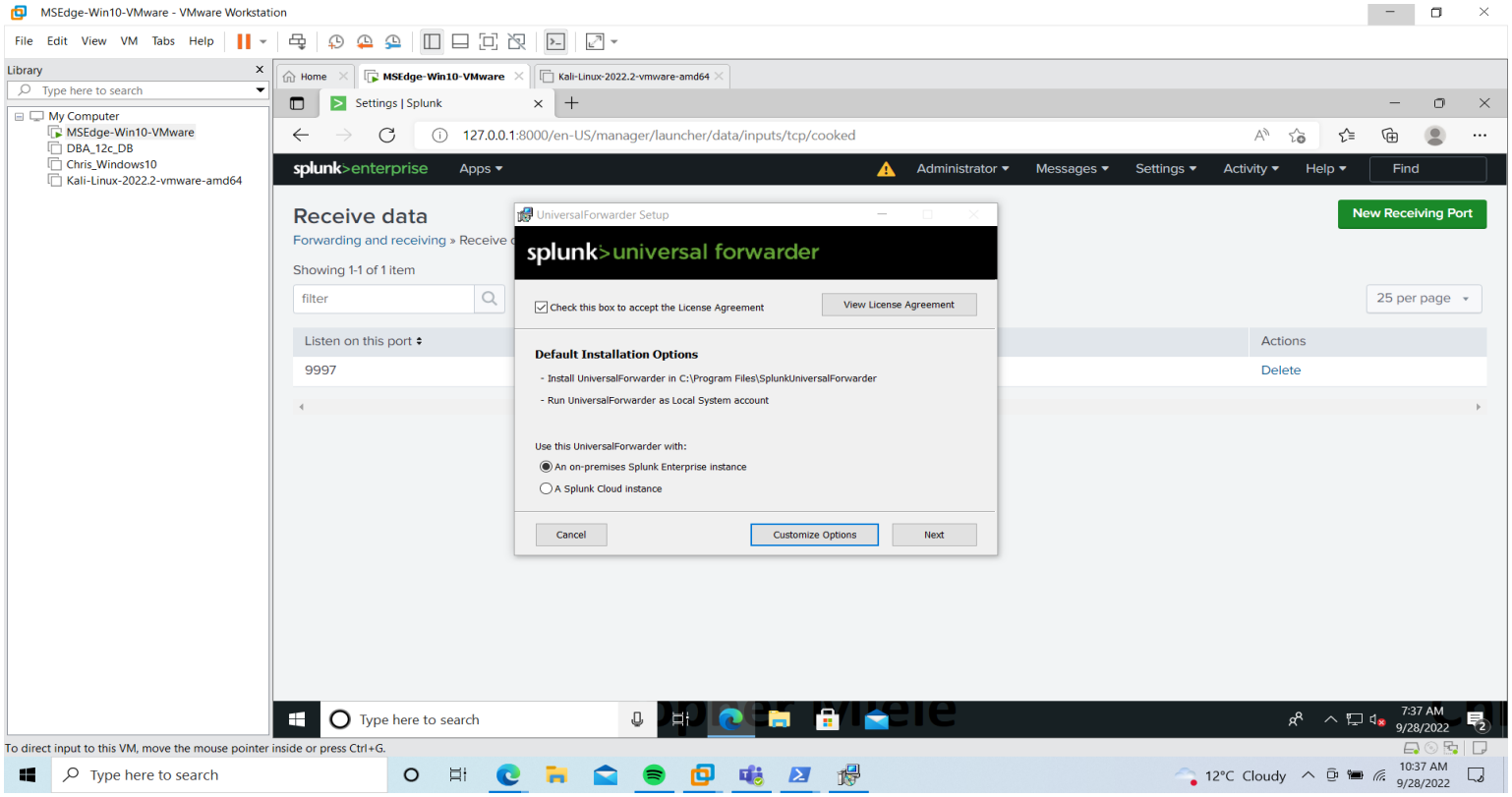


Figure 46: Insert Splunk Credentials.

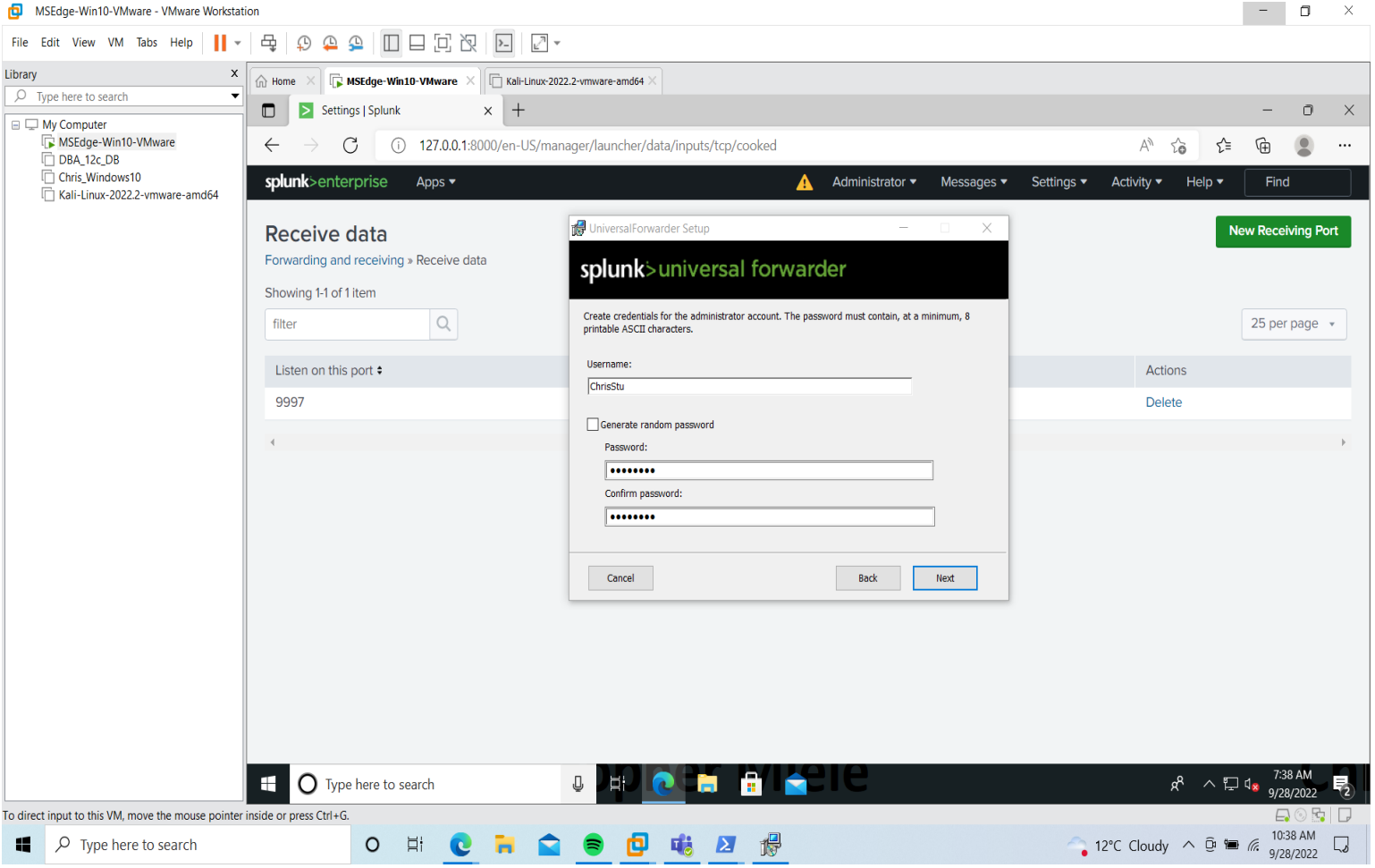


Figure 47: Deploy Server Host IP(Guest OS) VM IP “192.168.112.128” Port “8089”(Default Port Splunk)

Explain: Type in the GuestOS IP Address in the Splunk Forwarder. The port is 8089

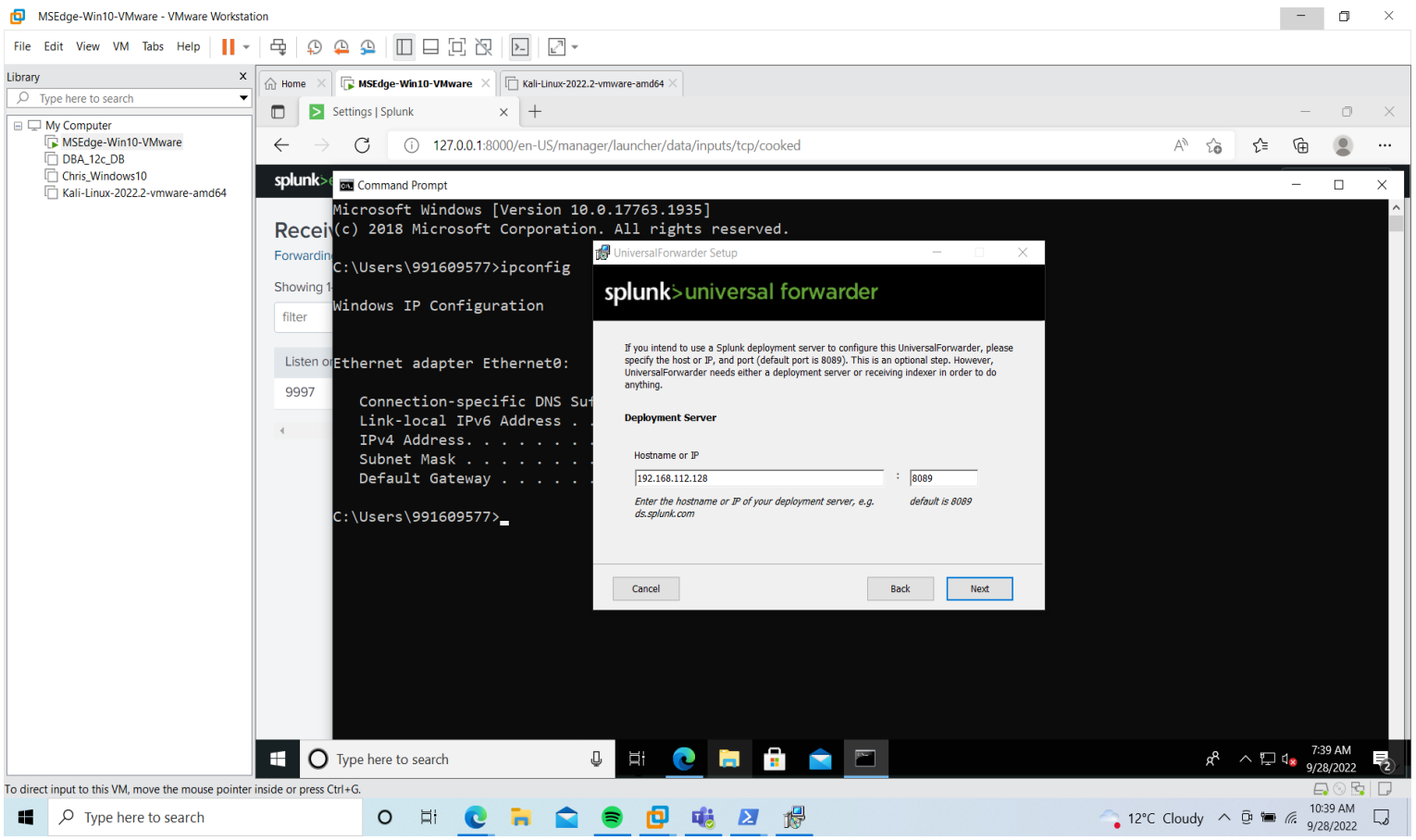


Figure 48: Receiving Indexer Host IP VM IP “192.168.112.128” Port “9997”(Default Port Splunk)

Explain: The Receiver Index is the Guest OS VM The Port is 9997. Splunk Forwarder will allow you to communicate and send logs from host to guest OS.

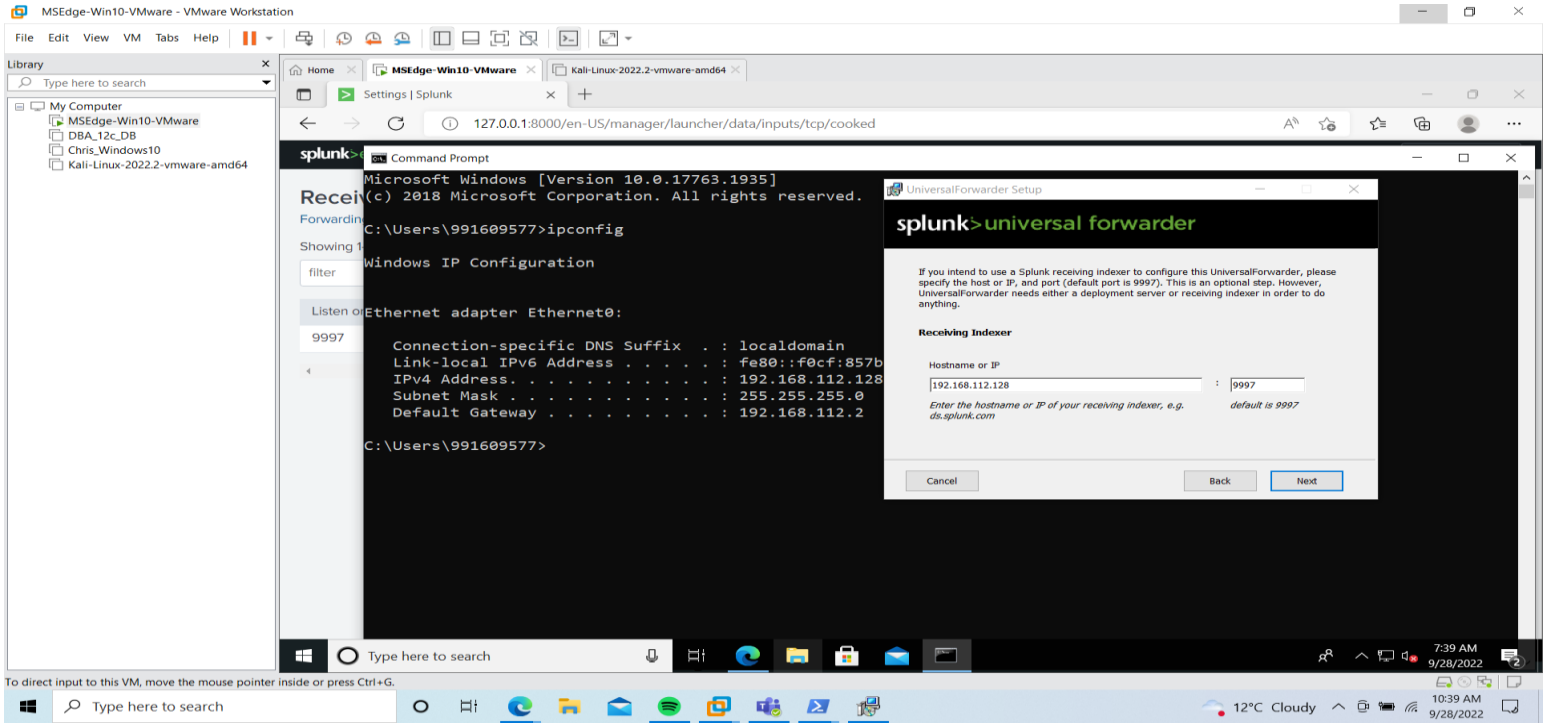


Figure 49: Finish Splunk Universal Forwarder Installer

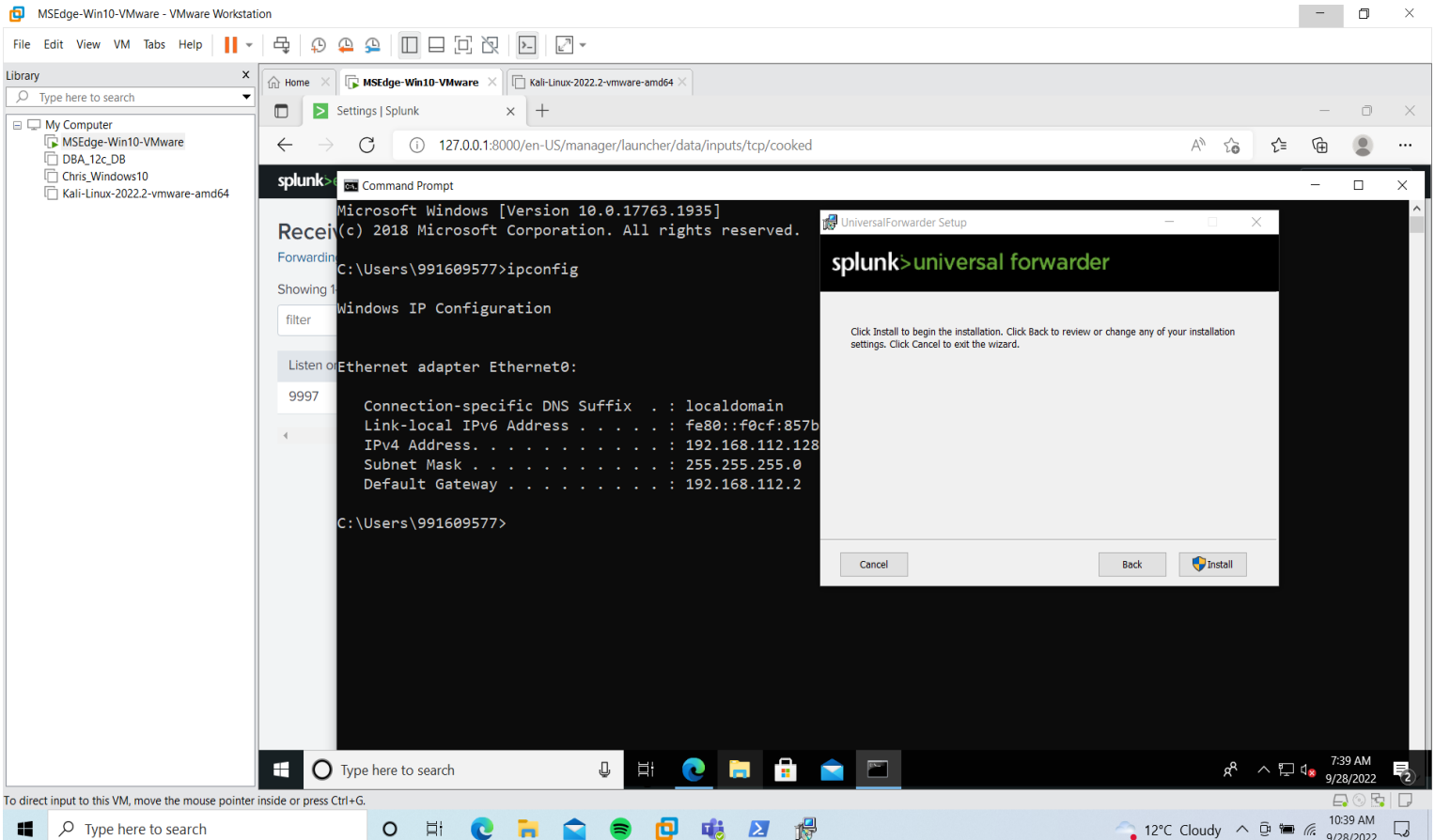


Figure 50: Add Data -> Forward.

Explain: Login to Splunk Click Splunk Forwader

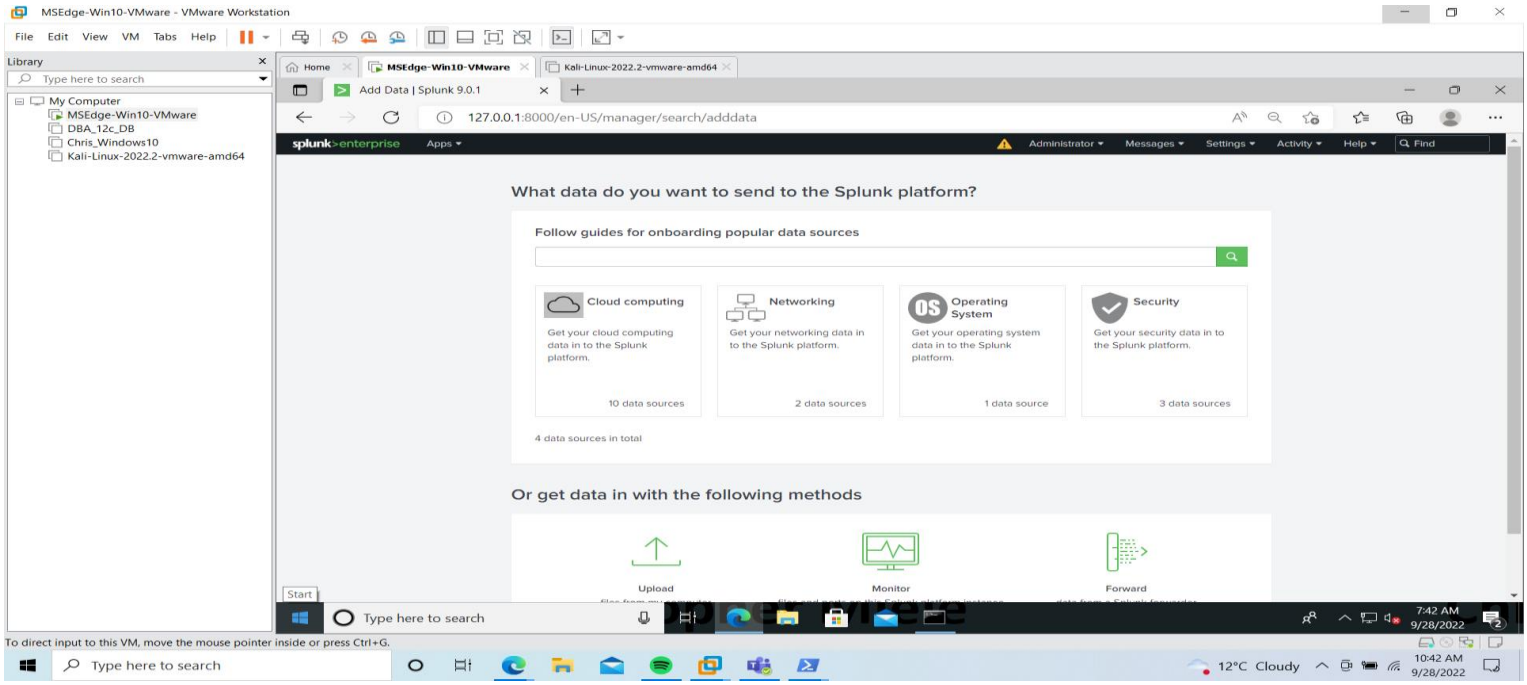


Figure 51: Verify Host Name Same As Host OS.

Explain: Compare the Host Name to Determine Same Name as Host OS

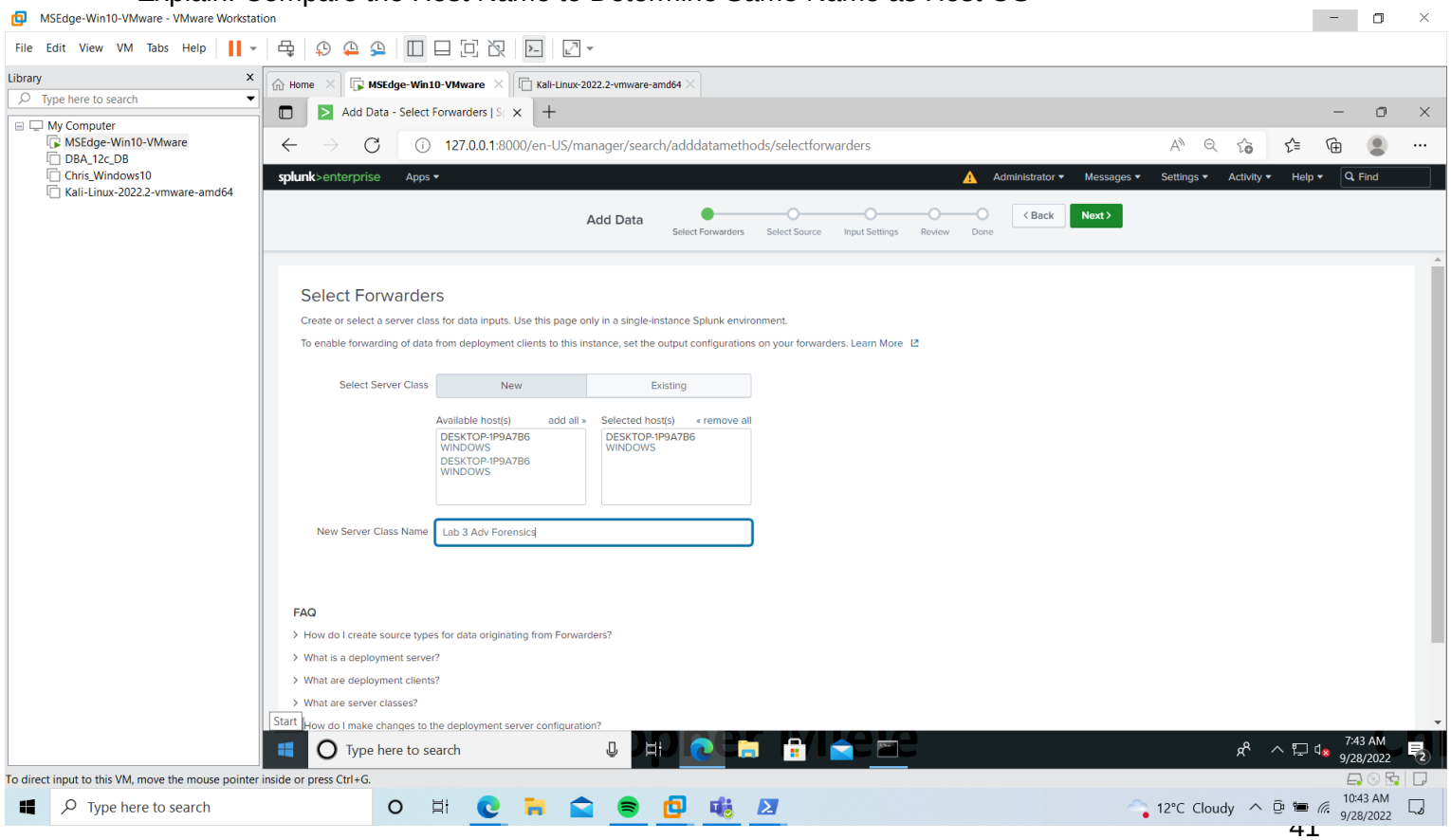


Figure 52:Run whoami in powershell Hostname matches Available Hosts Forwarders.

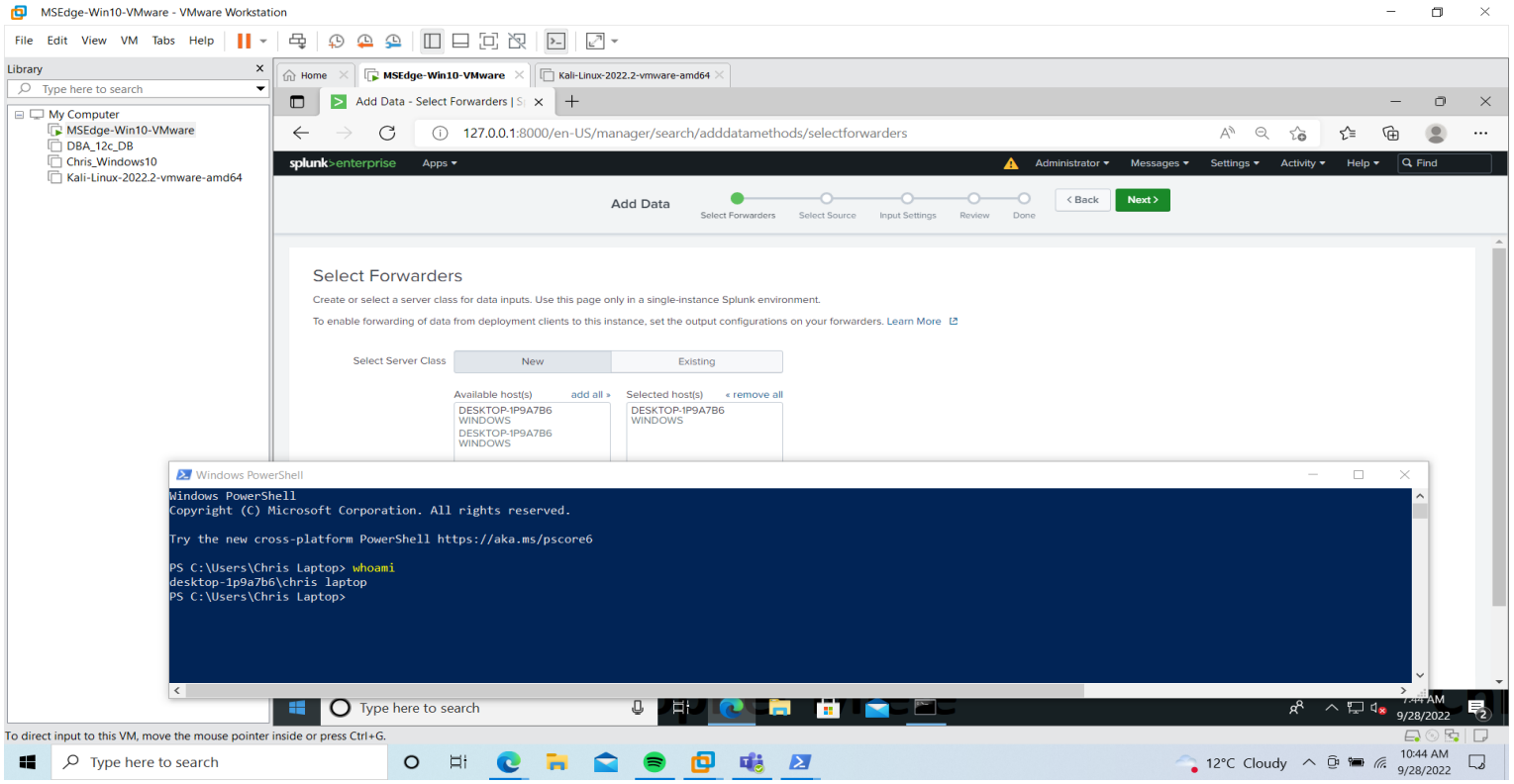


Figure 53:Add all Local Event Logs. Apps, Security, Setup, etc(Event Logs).

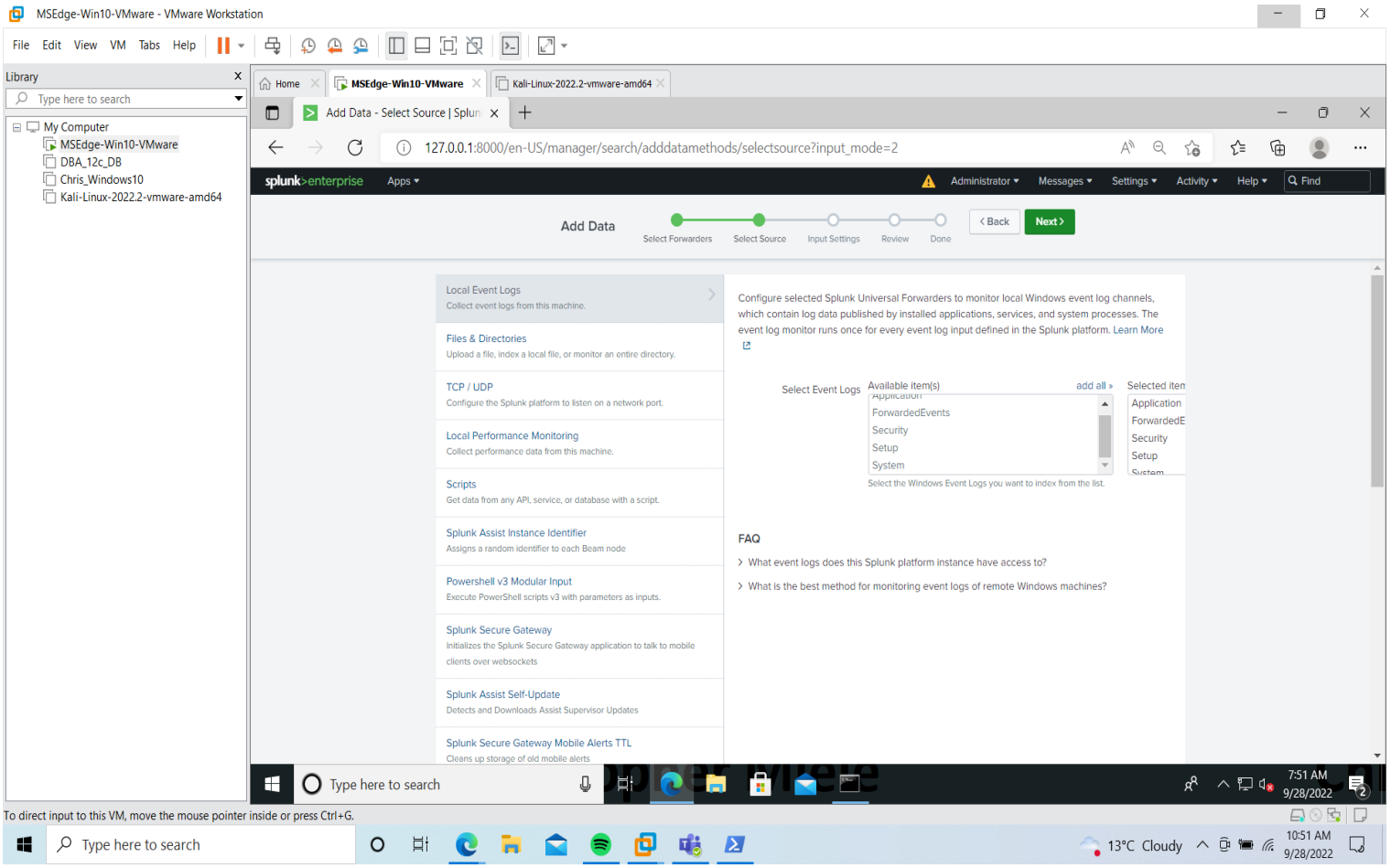


Figure 54:Choose win10_events Index(Stores Windows Event Logs) -> Review -> Search.

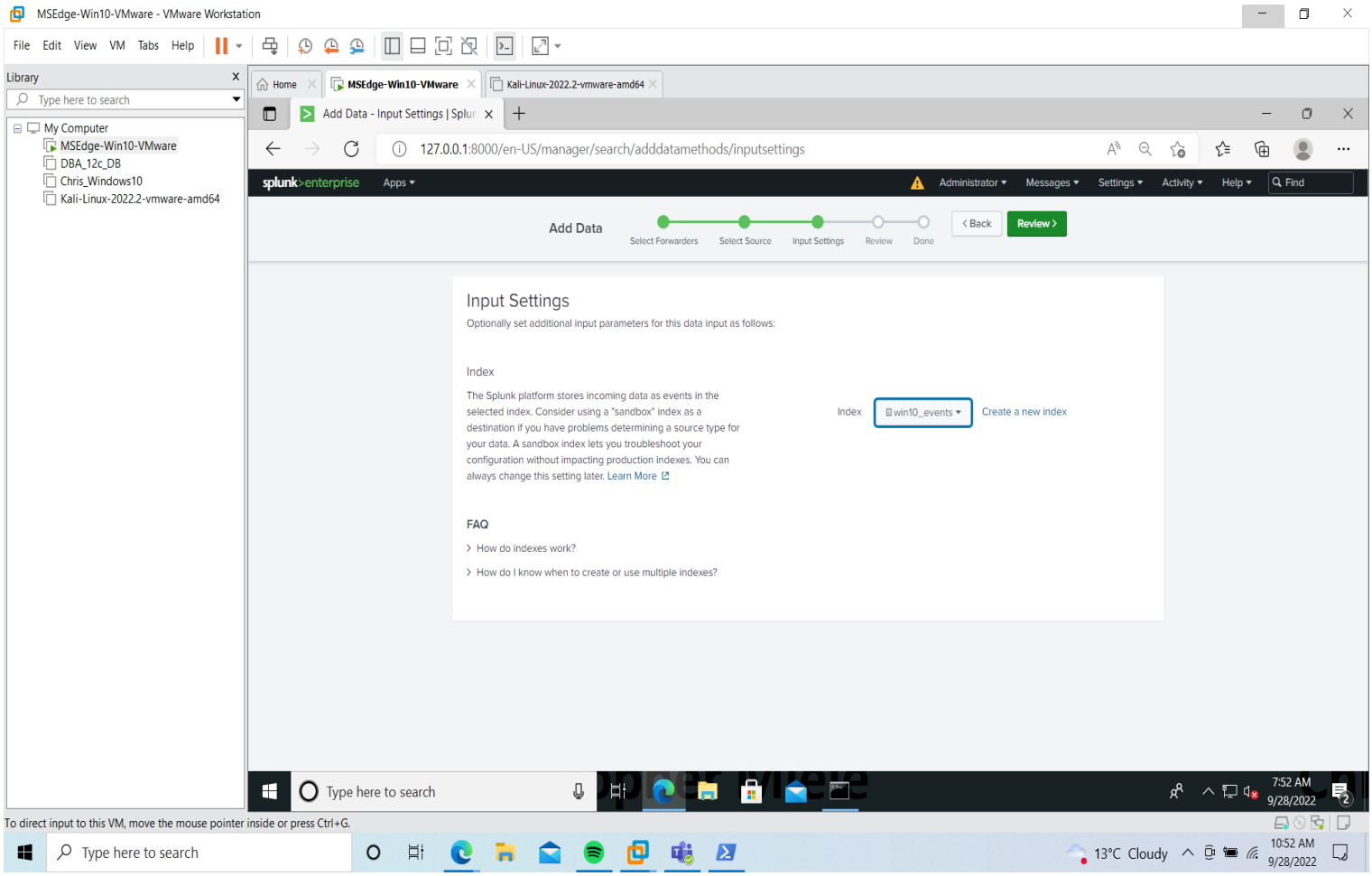
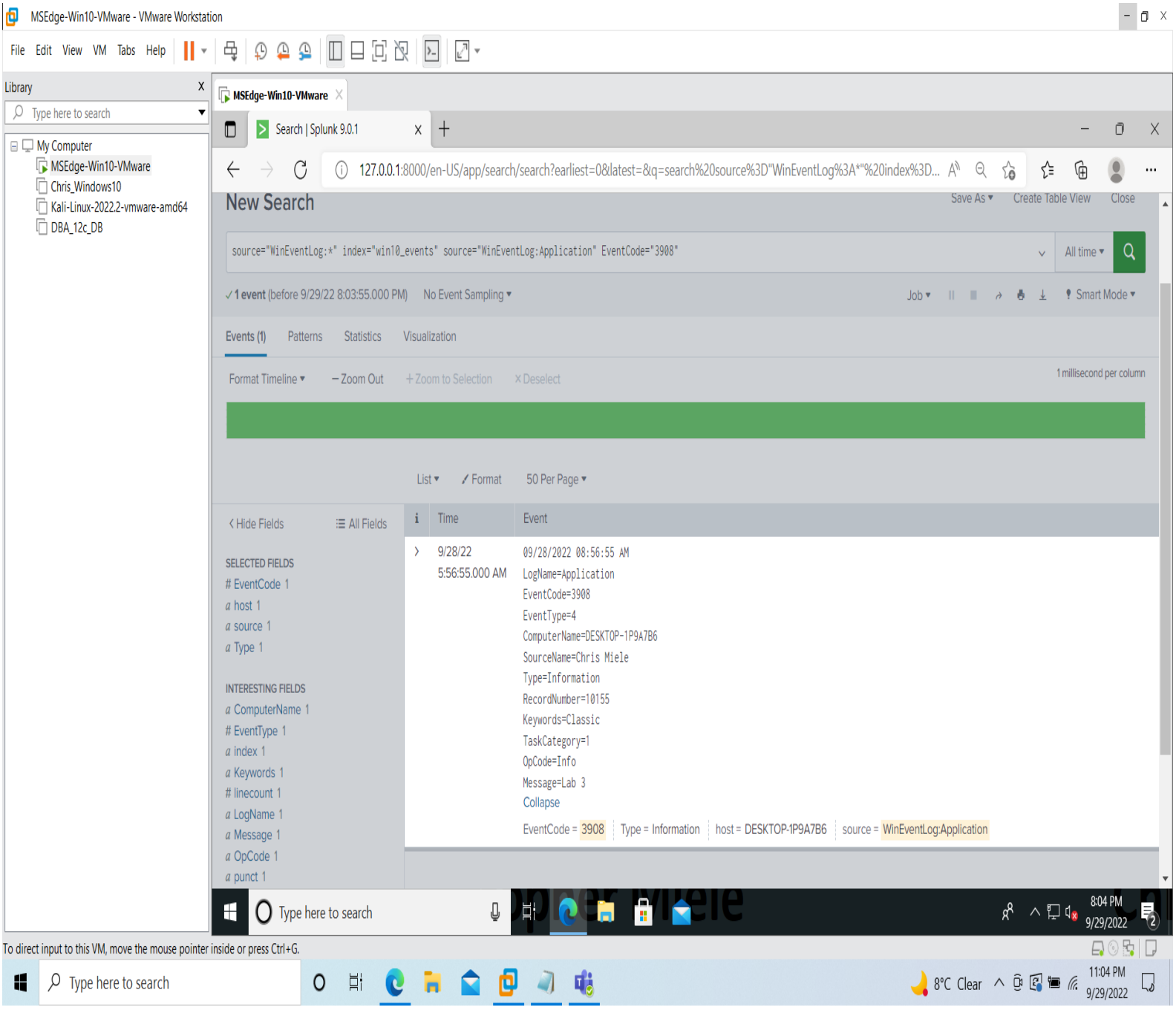


Figure 55: source="WinEventLog:*" index="win10_events" source="WinEventLog:Application" EventCode="3908"

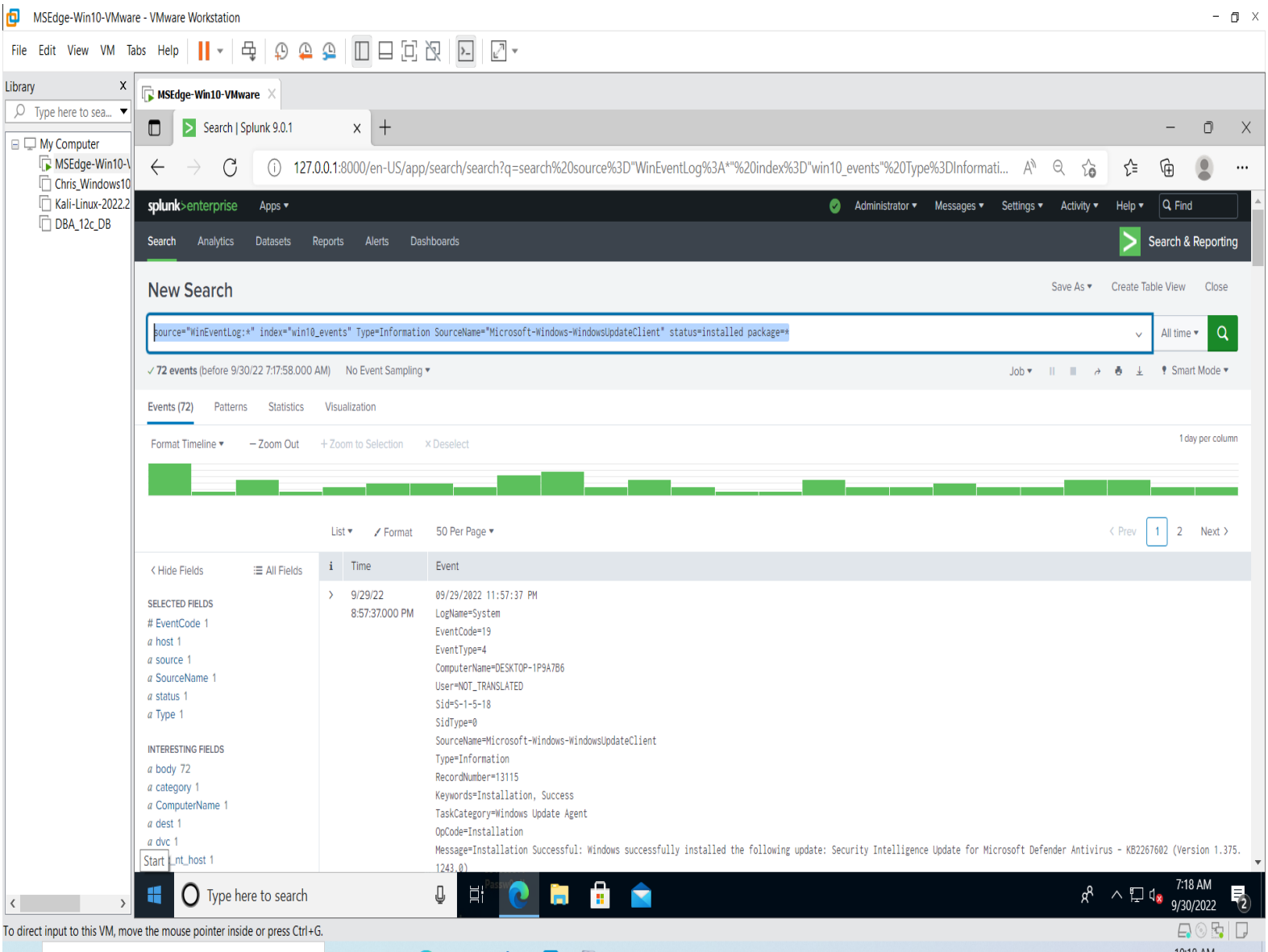
Explain: Search Windows Event Logs The Source is Application, The Event Code is 3908. This Search will confirm that the powershell event that I created is the same event in universal forwarder



Lab 4

Figure 56: source="WinEventLog:*" index="win10_events" Type=Information SourceName="Microsoft-Windows-WindowsUpdateClient" status=installed package=*

Explain: Find Updates that are downloaded on Host OS Type information, Source Windows Update Client, Status Installed Updates the Package = *(Wild card) search for different types of updates.



Reference

[1] Cyberwox, D. (2021, June 16). *Cybersecurity Detection Lab: Forwarding windows event logs to Splunk using universal forwarder*. YouTube. Retrieved September 30, 2022, from https://www.youtube.com/watch?v=yP_PFRy-pdA

[2] Satti, M. (2022, July 26). *Splunk-boss of the SOC v1 (walkthrough)*. Medium. Retrieved September 30, 2022, from https://systemweakness.com/splunk-boss-of-the-soc-v1-walkthrough-a9550cde93f5