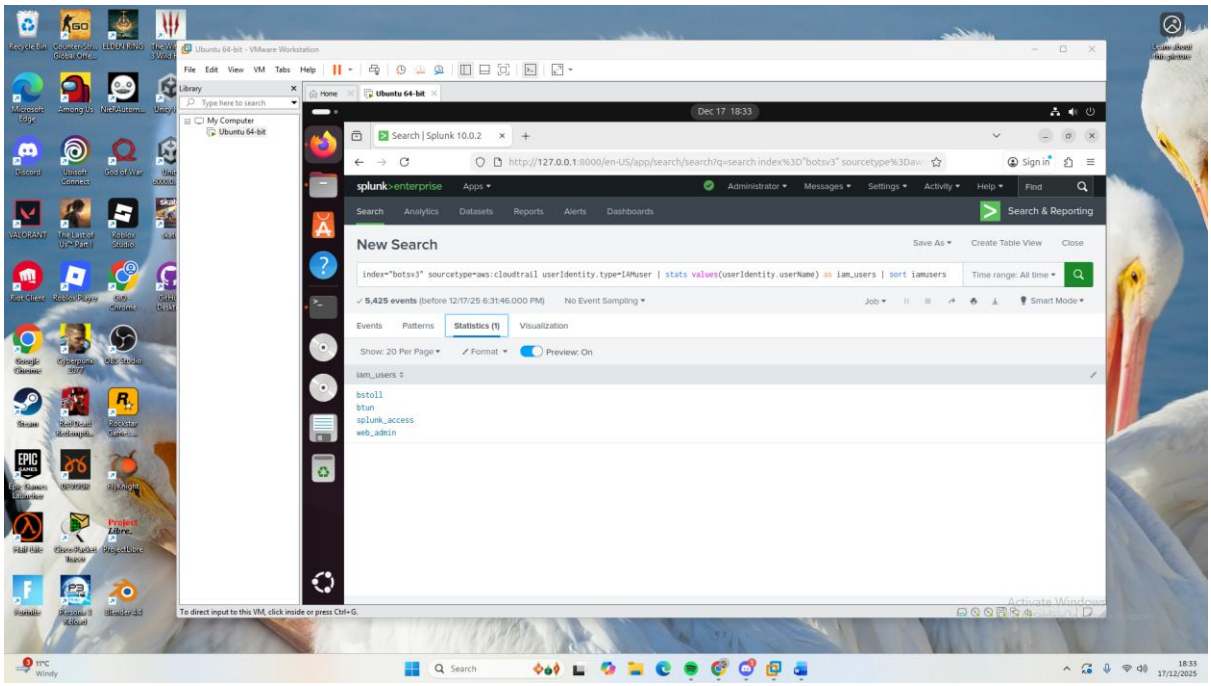
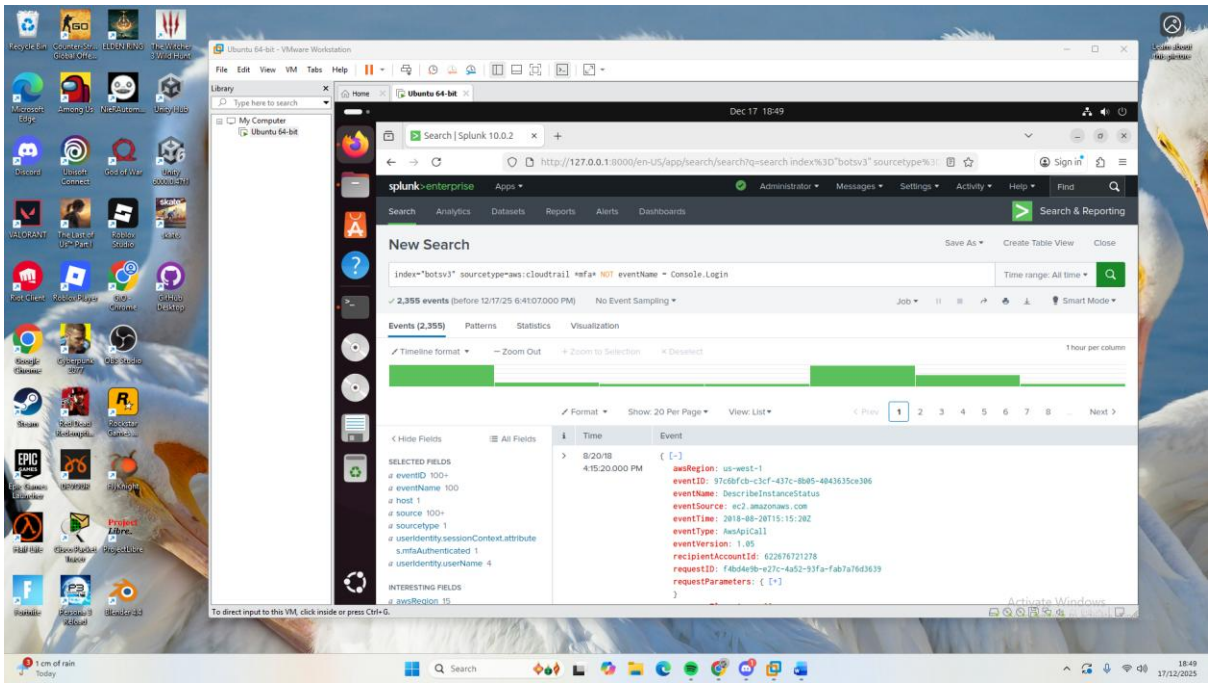
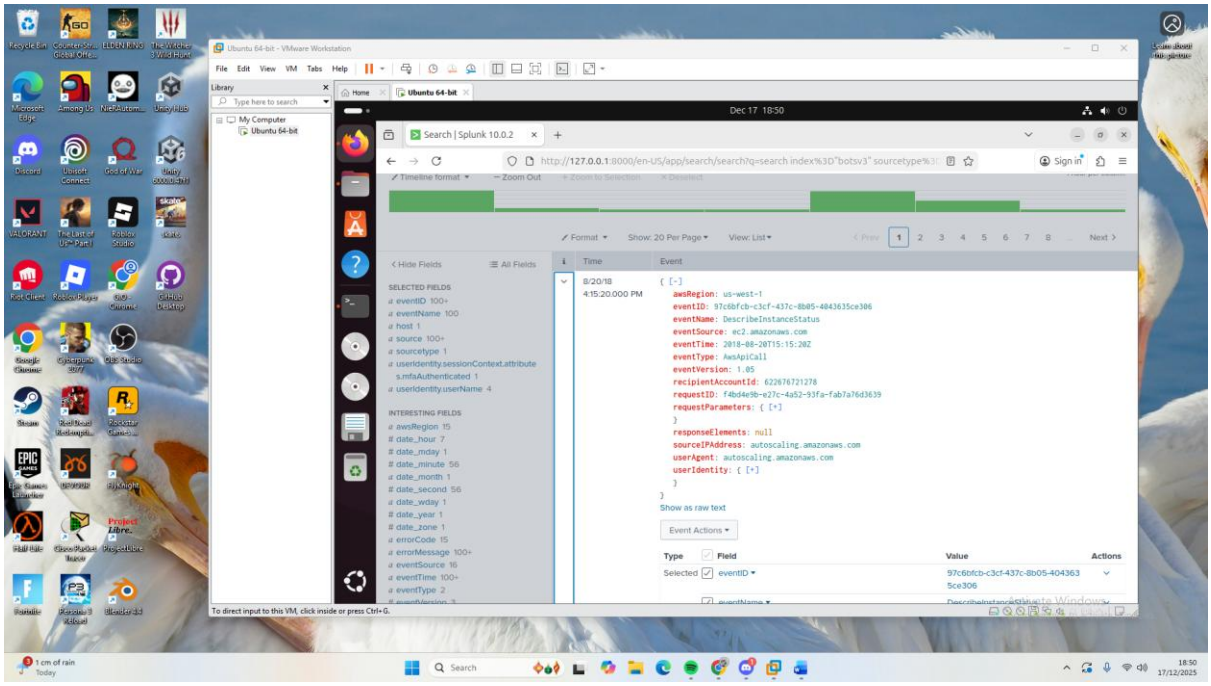
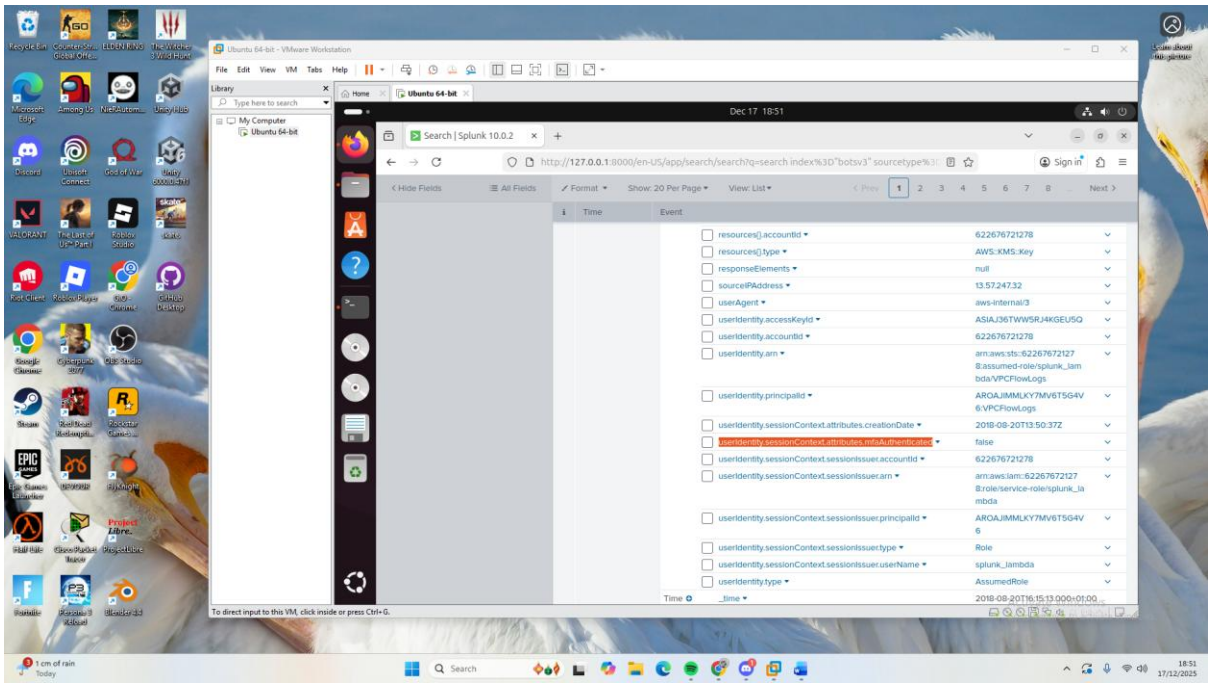
Question 1



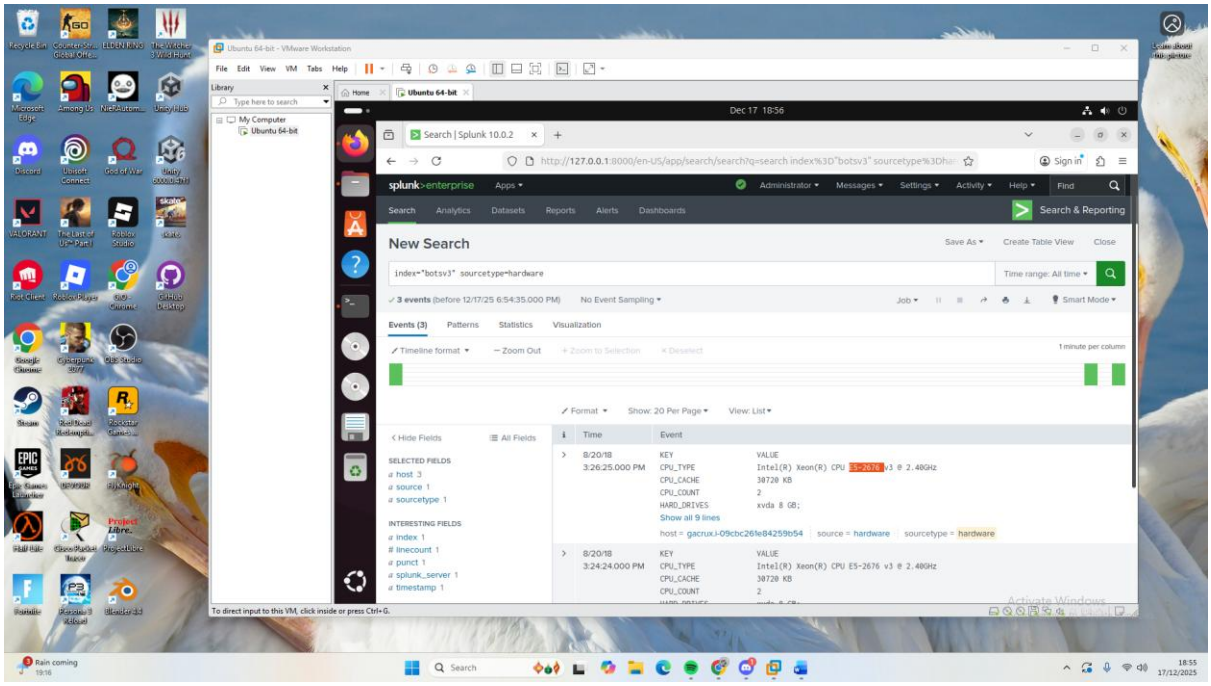

Question 2



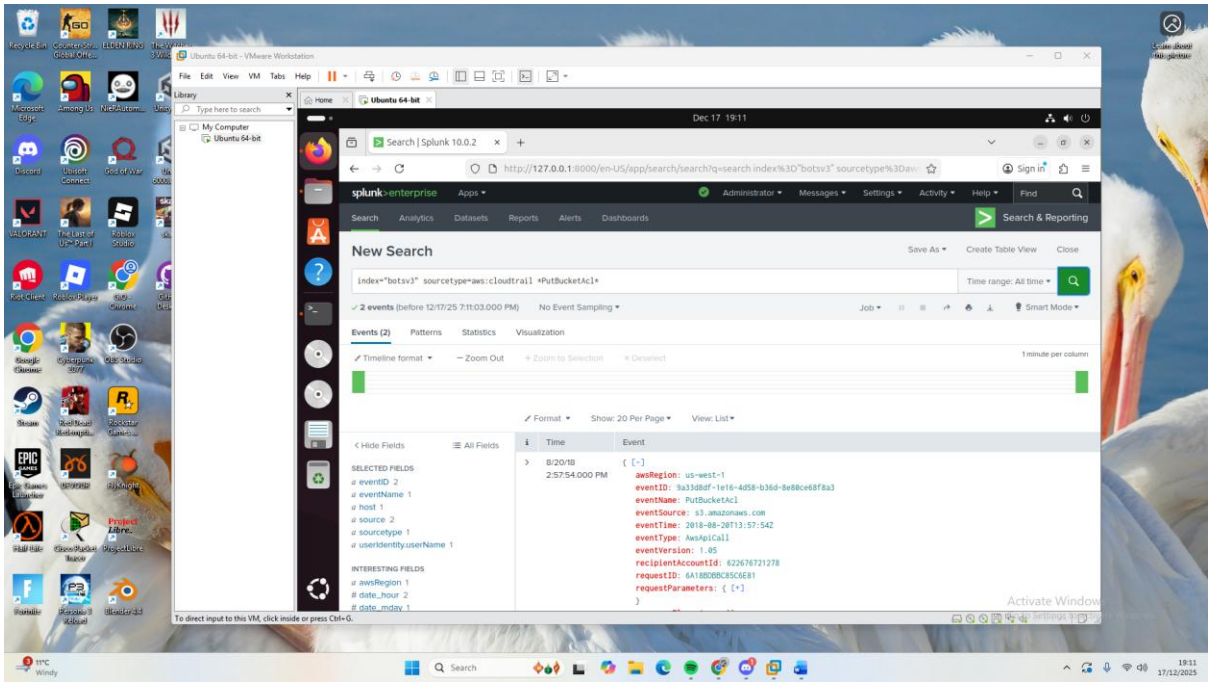

Ubuntu 64-bit - VMware Workstation
Dec 17 18:50
Search | Splunk 10.0.2
http://127.0.0.1:8000/en-US/app/search/search?q=search index%3D"botsv3" sourcetype%3D
Time
Event
8/20/18
4:15:20.000 PM
{ [-]
awsRegion: us-west-1
eventID: 97c6bfcb-c3cf-437c-8b05-4043635ce306
eventName: DescribeInstanceStatus
eventSource: ec2.amazonaws.com
eventTime: 2018-08-20T15:15:20Z
eventType: AwsApiCall
eventVersion: 1.05
recipientAccountId: 622676721278
requestID: f4bd4e9b-e27c-4a52-93fa-fab7a76d3639
requestParameters: { [+]
}
responseElements: null
sourceIPAddress: autoscaling.amazonaws.com
userAgent: autoscaling.amazonaws.com
userIdentity: { [+]
}
}
Show as raw text
Event Actions
Type
Field
Value
Actions
Selected
eventID
97c6bfcb-c3cf-437c-8b05-4043635ce306
To direct input to this VM, click inside or press Ctrl+G.

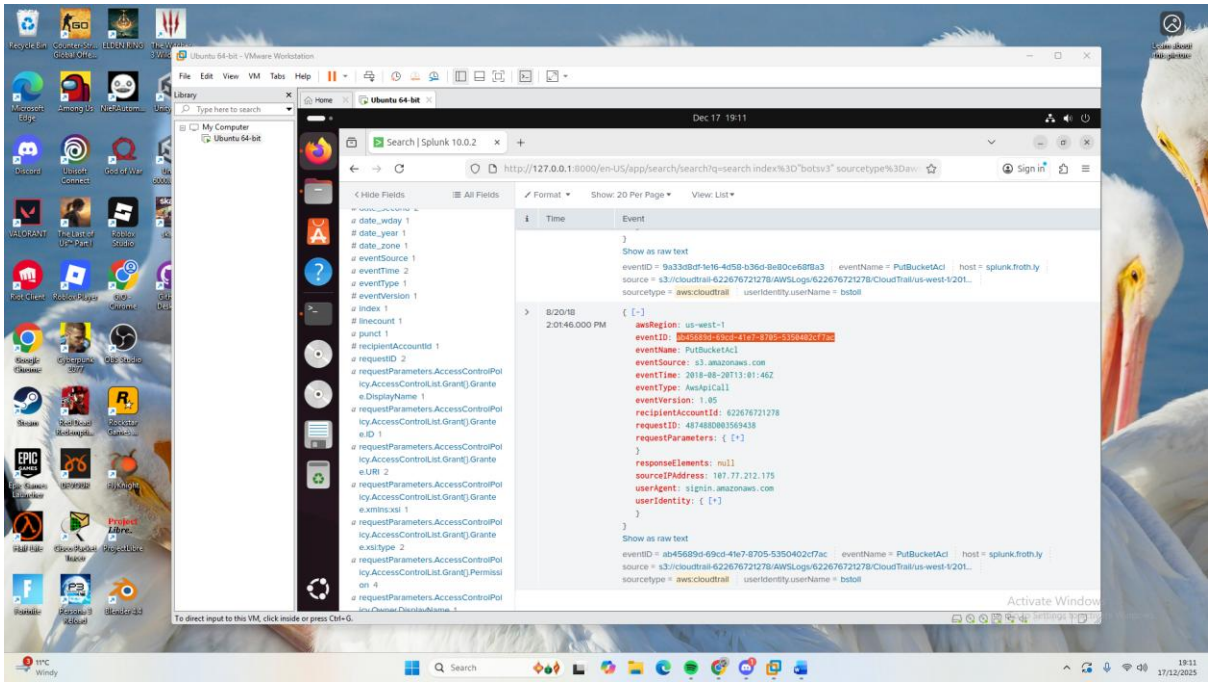

Ubuntu 64-bit - VMware Workstation
Dec 17 18:51
Search | Splunk 10.0.2
http://127.0.0.1:8000/en-US/app/search/search?q=search index%3D"botsv3" sourcetype%3D
Time
Event
resources[].accountId
622676721278
resources[].type
AWS::KMS::Key
responseElements
null
sourceIPAddress
13.57.247.32
userAgent
aws-internal/3
userIdentity.accessKeyId
ASIAJ36TWW5RJ4KGEU5Q
userIdentity.accountId
622676721278
userIdentity.arn
arn:aws:sts::622676721278:assumed-role/splunk_lambda/VPCFlowLogs
userIdentity.principalId
AROAJIMMLKY7MV6T5G4V6:VPCFlowLogs
userIdentity.sessionContext.attributes.creationDate
2018-08-20T13:50:37Z
userIdentity.sessionContext.attributes.mfaAuthenticated
false
userIdentity.sessionContext.sessionIssuer.accountId
622676721278
userIdentity.sessionContext.sessionIssuer.arn
arn:aws:iam::622676721278:role/service-role/splunk_lambda
userIdentity.sessionContext.sessionIssuer.principalId
AROAJIMMLKY7MV6T5G4V6
userIdentity.sessionContext.sessionIssuer.type
Role
userIdentity.sessionContext.sessionIssuer.userName
splunk_lambda
userIdentity.type
AssumedRole
Time
_time
To direct input to this VM, click inside or press Ctrl+G.

Question 3:

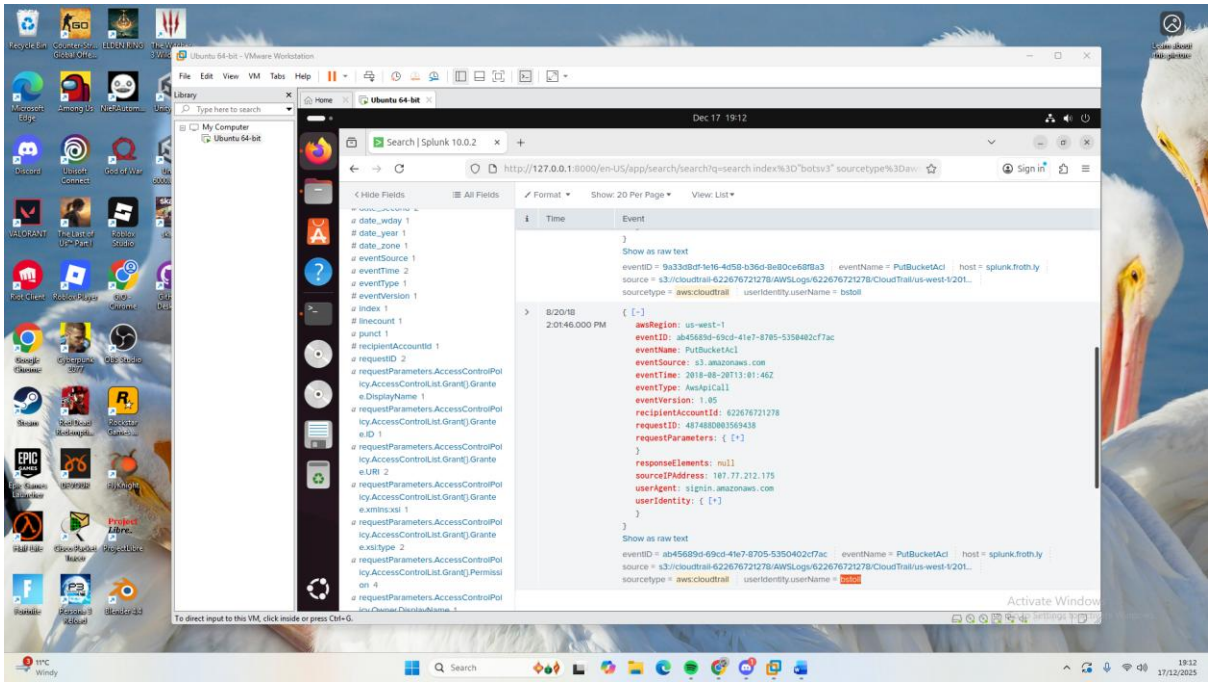

Ubuntu 64-bit - VMware Workstation
Search | Splunk 10.0.2
splunk>enterprise
New Search
index="botsv3" sourcetype=hardware
3 events (before 12/17/25 6:54:35.000 PM)
Events (3)
Patterns
Statistics
Visualization
SELECTED FIELDS
INTERESTING FIELDS
8/20/18 3:26:25.000 PM
8/20/18 3:24:24.000 PM
Dec 17 18:56

Question 4:

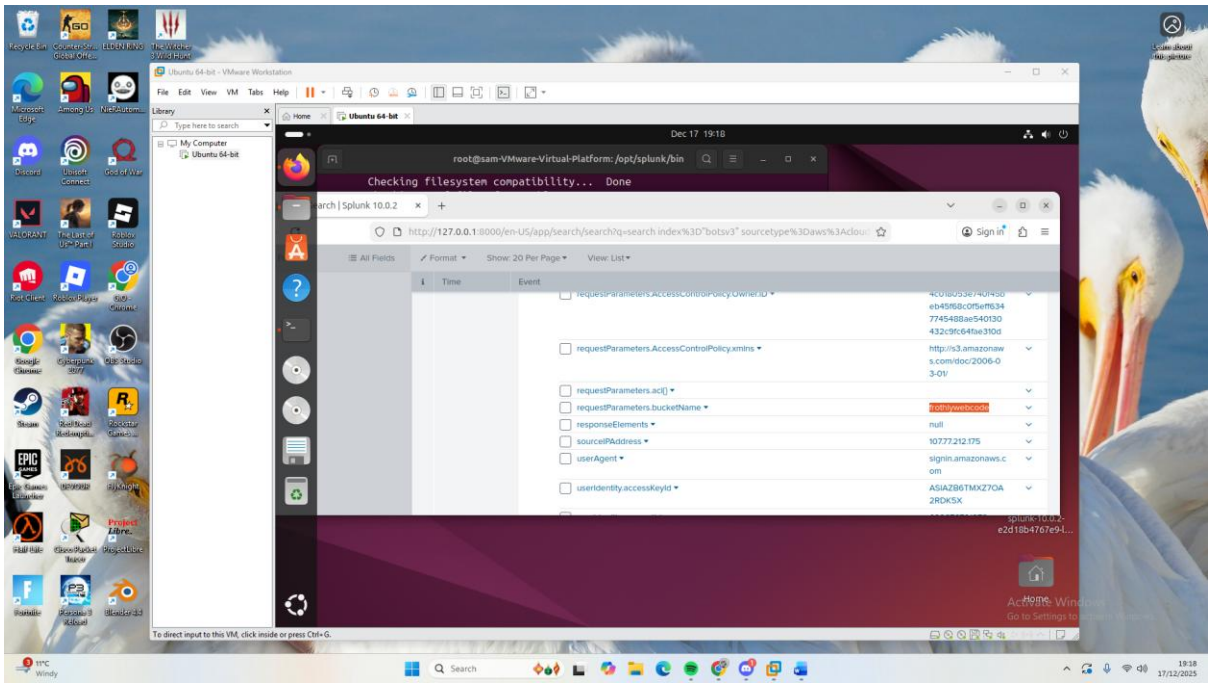

Ubuntu 64-bit - VMware Workstation
Search | Splunk 10.0.2
splunk>enterprise
New Search
index="botsv3" sourcetype=aws:cloudtrail *PutBucketAcl*
2 events (before 12/17/25 7:11:03.000 PM)
Events (2)
Patterns
Statistics
Visualization
SELECTED FIELDS
INTERESTING FIELDS
8/20/18 2:57:54.000 PM
Dec 17 19:11


Ubuntu 64-bit - VMware Workstation
Search | Splunk 10.0.2
Dec 17 19:11
8/20/18
2:01:46.000 PM
awsRegion: us-west-1
eventID: ab45689d-69cd-41e7-8705-5350402cf7ac
eventName: PutBucketAcl
eventSource: s3.amazonaws.com
eventTime: 2018-08-20T13:01:46Z
eventType: AwsApiCall
eventVersion: 1.05
recipientAccountId: 622676721278
requestID: 4874880D03569438
sourceIPAddress: 107.77.212.175
userAgent: signin.amazonaws.com
Activate Windows

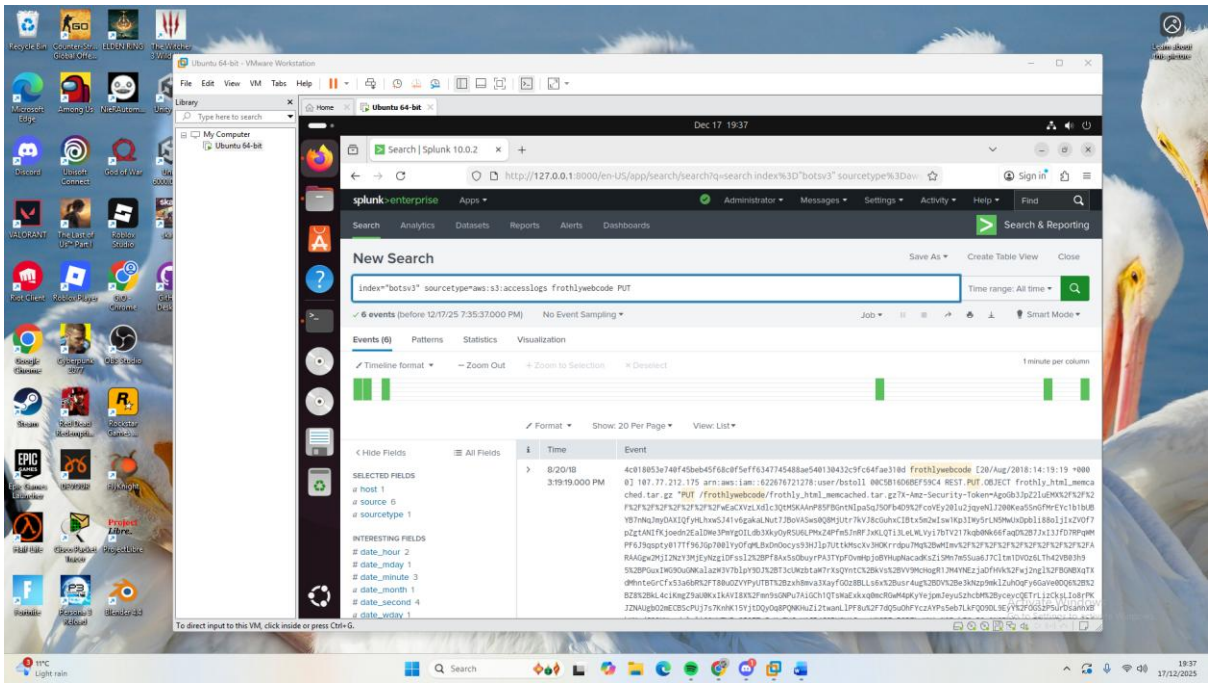
Question 5:

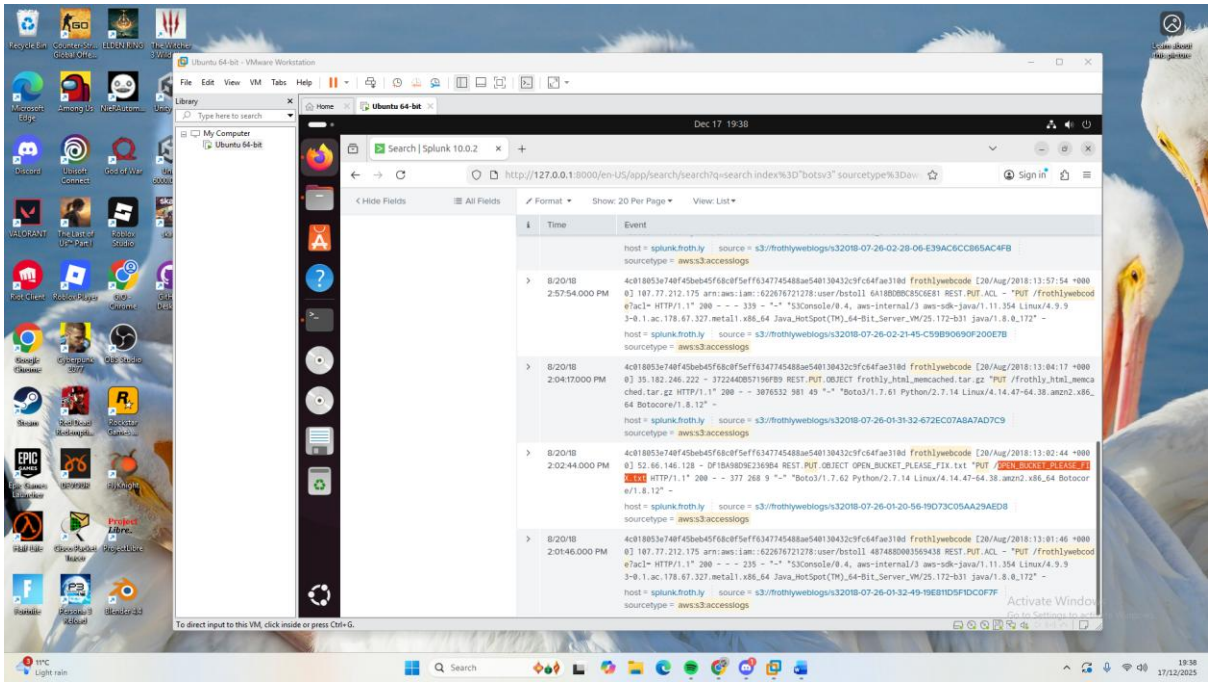

Ubuntu 64-bit - VMware Workstation
Search | Splunk 10.0.2
Dec 17 19:12
8/20/18
2:01:46.000 PM
awsRegion: us-west-1
eventID: ab45689d-69cd-41e7-8705-5350402cf7ac
eventName: PutBucketAcl
eventSource: s3.amazonaws.com
eventTime: 2018-08-20T13:01:46Z
eventType: AwsApiCall
eventVersion: 1.05
recipientAccountId: 622676721278
requestID: 4874880D03569438
sourceIPAddress: 107.77.212.175
userAgent: signin.amazonaws.com
Activate Windows

Question 6:

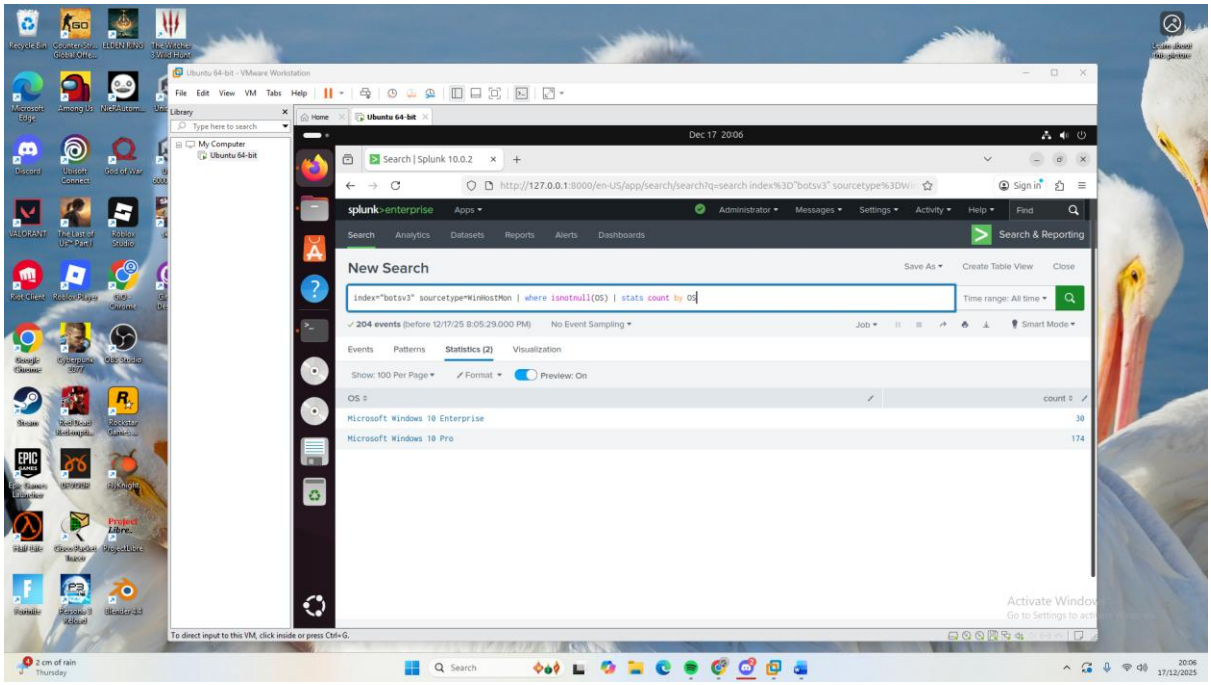


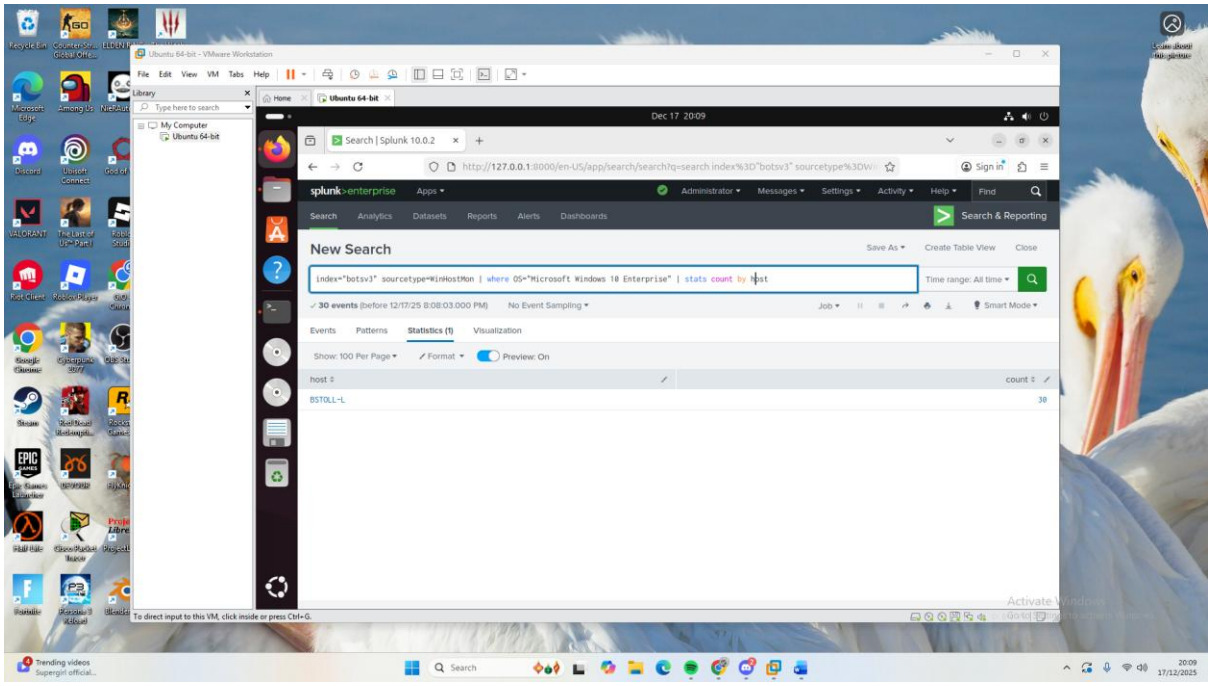

Question 7:

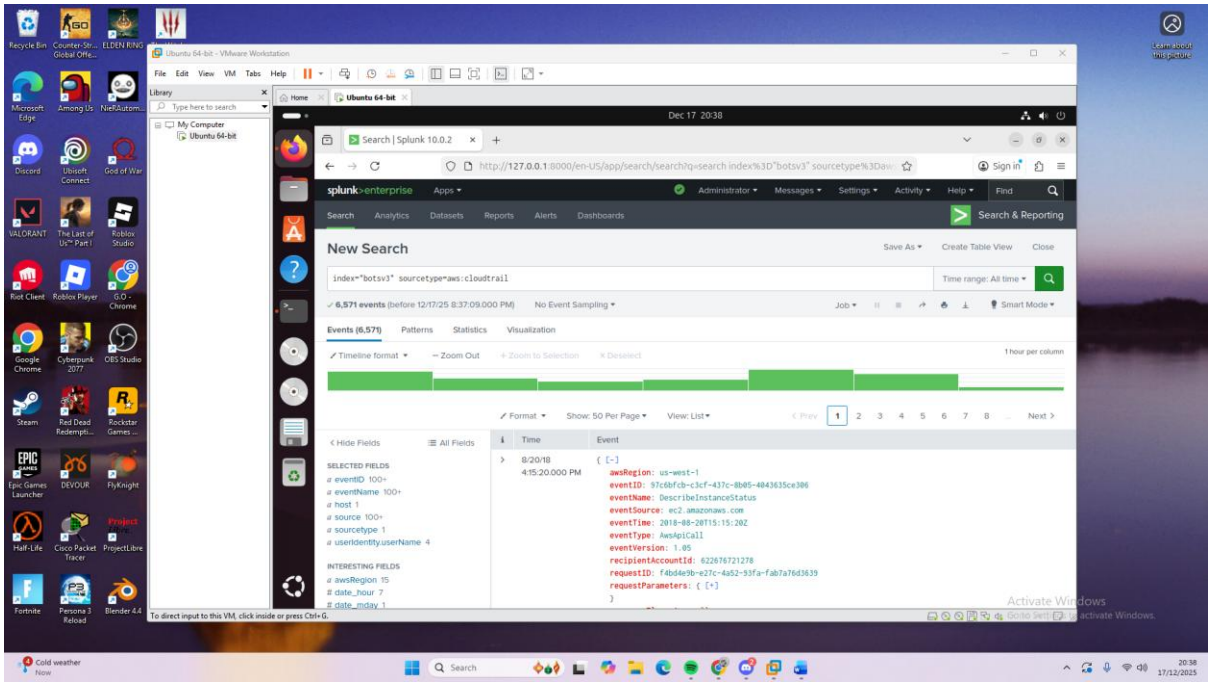


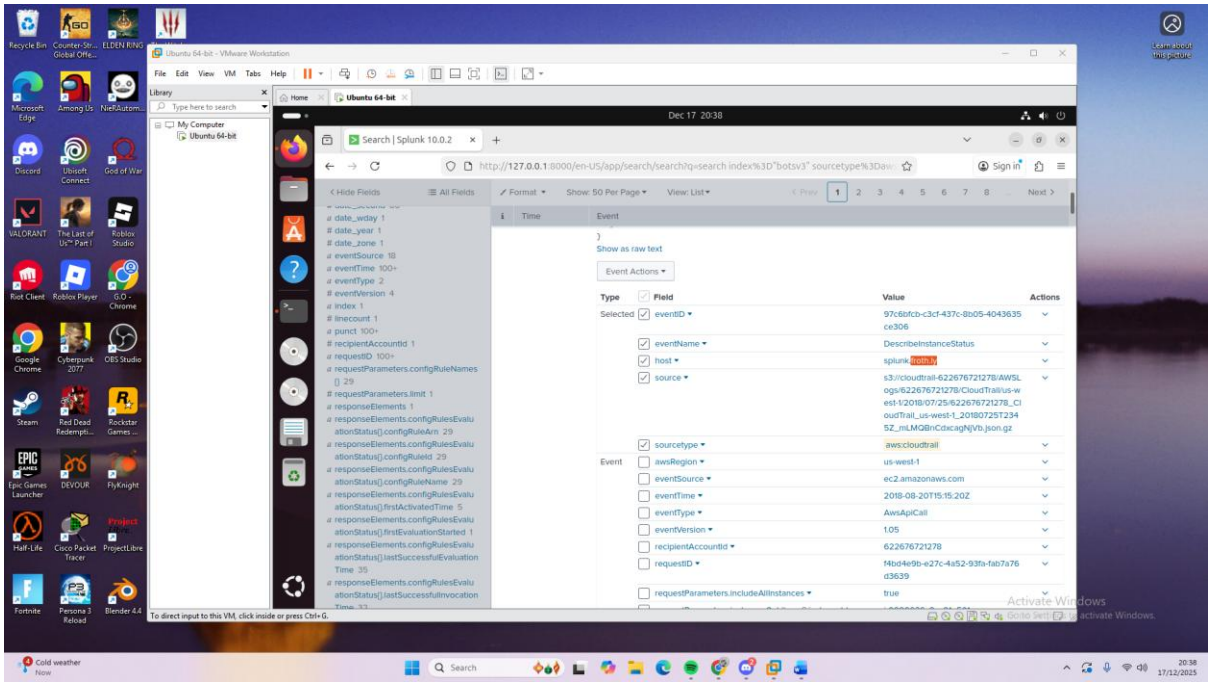


Question 8:




Ubuntu 64-bit - VMware Workstation
Dec 17 20:09
Search | Splunk 10.0.2
splunk>enterprise
New Search
index="botsv3" sourcetype="WinHostMon" | where OS="Microsoft Windows 10 Enterprise" | stats count by host
30 events (before 12/17/25 8:08:03.000 PM)
host
count
BSTOLL-L
30


Ubuntu 64-bit - VMware Workstation
Dec 17 20:38
Search | Splunk 10.0.2
splunk>enterprise
New Search
index="botsv3" sourcetype="aws:cloudtrail"
6,571 events (before 12/17/25 8:37:09.000 PM)
Events (6,571)
Patterns
Statistics
Visualization
Time
Event
8/20/18 4:15:20.000 PM
awsRegion: us-west-1
eventID: 97c6bfcb-c3cf-437c-8b05-4043635ce306
eventName: DescribeInstanceStatus
eventSource: ec2.amazonaws.com
eventTime: 2018-08-20T15:15:20Z
eventType: AwsApiCall
eventVersion: 1.05
recipientAccountId: 622676721278
requestID: f4bd4e9b-e27c-4a52-93fa-fab7a76d3639
requestParameters: { [+]


Ubuntu 64-bit - VMware Workstation
Search | Splunk 10.0.2
Dec 17 20:38
Show as raw text
Event Actions
Type
Field
Value
Actions
eventID
eventName
DescribeInstanceStatus
host
source
sourcetype
aws:cloudtrail
awsRegion
us-west-1
eventSource
ec2.amazonaws.com
eventTime
2018-08-20T15:15:20Z
eventType
AwsApiCall
eventVersion
1.05
recipientAccountId
622676721278
requestID
requestParameters.includeAllInstances
true
Activate Windows