

Deliverables (Students must submit)

Deliverable A — “Audit Evidence Pack” (one folder)

学生は audit-pack/ フォルダを提出。

```
audit-pack/
├── 00_architecture-summary.md
├── 01_data-residency-proof.txt
├── 02_edge-proof-cloudfront.txt
├── 03_waf-proof.txt
├── 04_cloudtrail-change-proof.txt
├── 05_network-corridor-proof.txt
└── evidence.json (Malgus scripts output)
```

Deliverable B — One paragraph “auditor narrative”

“この設計が APPI 的に安全で、なぜ DB を海外に置けないか”を 8～12 行で説明。

Verification Commands (CLI proof students can paste)

1) Data residency proof (RDS only in Tokyo)

Tokyo: RDS exists

```
aws rds describe-db-instances --region ap-northeast-1 \
--query
"DBInstances[].{DB:DBInstanceIdentifier,AZ:AvailabilityZone,Region:'ap-northeast-1',Endpoint:Endpoint.Address}"
```

```
~ $ aws rds describe-db-instances --region ap-northeast-1 \
> --query "DBInstances[].{DB:DBInstanceIdentifier,AZ:AvailabilityZone,Region:'ap-northeast-1',Endpoint:Endpoint.Address}"
[
  {
    "DB": "terraform-20260204011443940200000006",
    "AZ": "ap-northeast-1c",
    "Region": "ap-northeast-1",
    "Endpoint": "terraform-20260204011443940200000006.c1o4ykyoarkz.ap-northeast-1.rds.amazonaws.com"
  }
]
```

São Paulo: No RDS

```
aws rds describe-db-instances --region sa-east-1 \
--query "DBInstances[].DBInstanceIdentifier"
~ $
>
[]
~ $
```

- 2) Edge proof (CloudFront logs show cache + access)
Students capture request headers:

curl -I <https://chewbacca-growls.com/api/public-feed>

```
(asmodeus@Asmodeus) - [~/.../Armageddon/Lab 3/Lab-3/Japan]
$ curl -I https://unshieldedhollow.click/
HTTP/2 200
content-type: text/html; charset=utf-8
content-length: 93
date: Thu, 05 Feb 2026 02:42:03 GMT
server: Werkzeug/2.2.3 Python/3.7.16
x-cache: Miss from cloudfront
via: 1.1 e310f7e63a4f82a466ec0d5a5d825aa8.cloudfront.net (CloudFront)
x-amz-cf-pop: MIA3-P7
x-amz-cf-id: C7zdmGPXI7mDfA7CRRL83oAA0hHSIoCvQyjcwQiXVg9diE2S7Jl20w==

(asmodeus@Asmodeus) - [~/.../Armageddon/Lab 3/Lab-3/Japan]
$
```

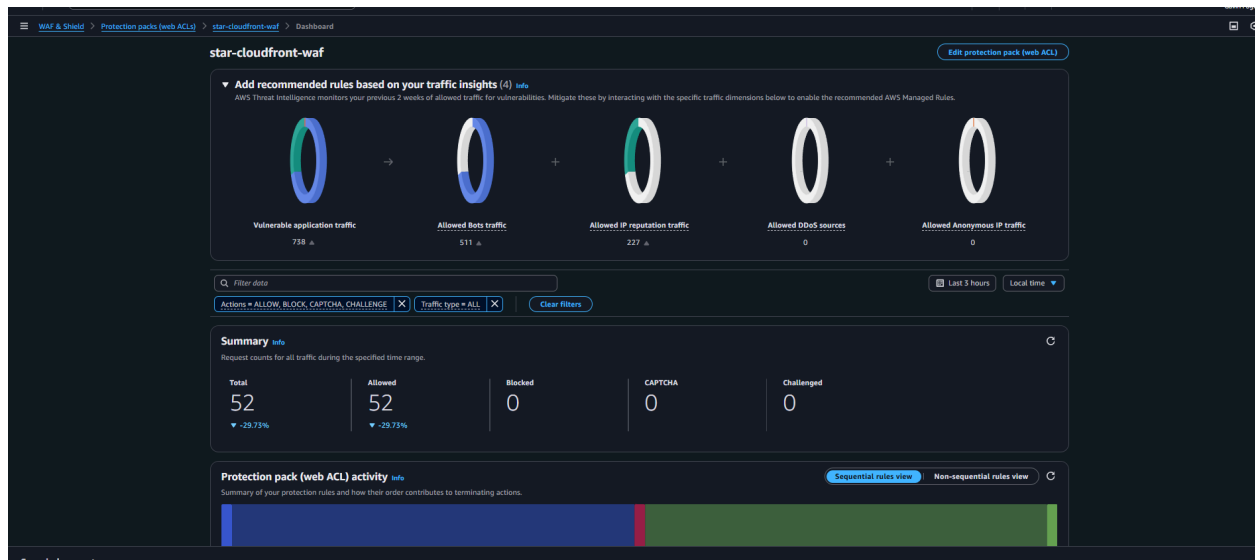
And/or submit CloudFront standard log evidence (Hit/Miss/RefreshHit)

- 3) WAF proof

Provide:

WAF log snippet or Insights summary

WAF logging destination options are documented

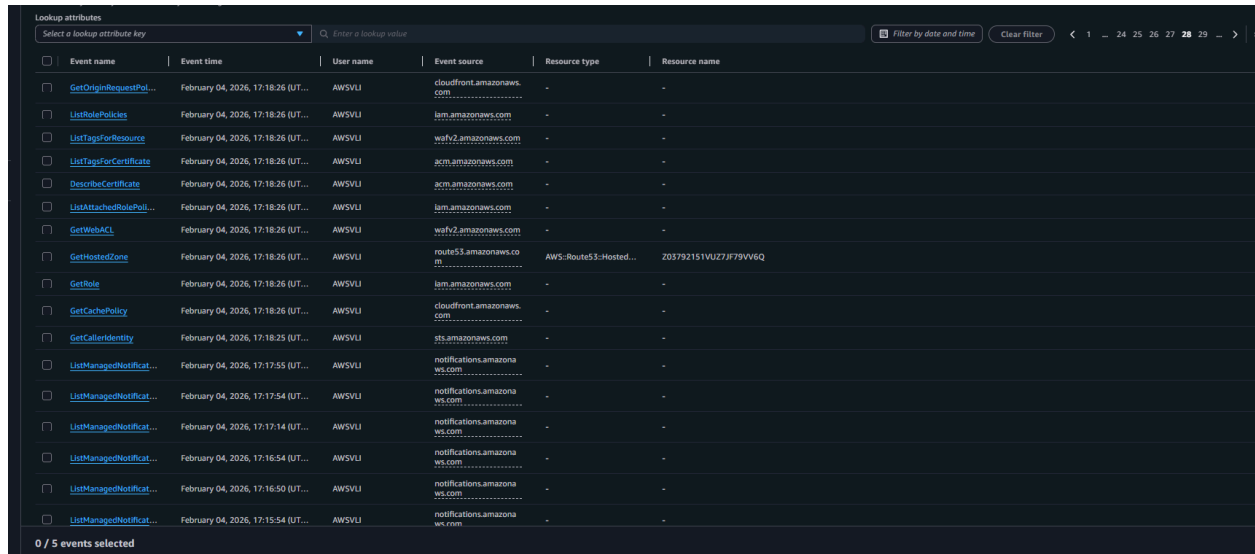


4) Change proof (CloudTrail)

CloudTrail has event history with a 90-day immutable record of management events

Students capture:

--> “who changed SG / TGW route / WAF / CloudFront config”



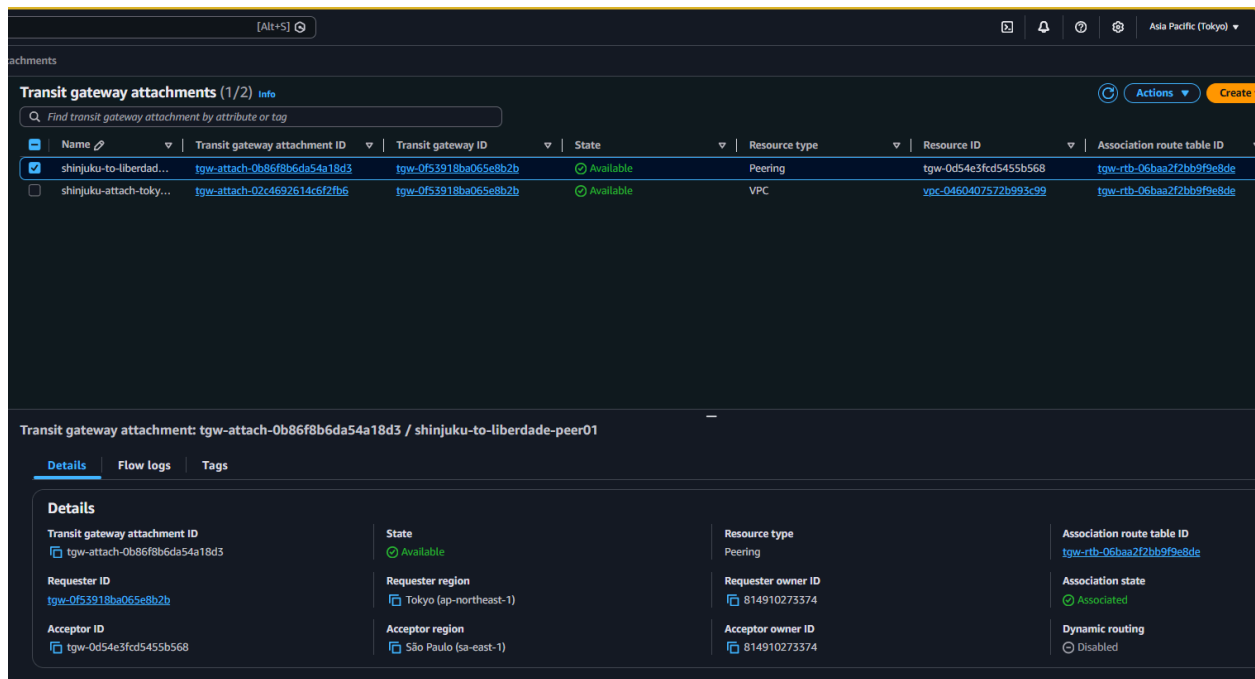
| Event name | Event time | User name | Event source | Resource type | Resource name |
|-------------------------|------------------------------------|-----------|--------------------------|-------------------------|------------------------|
| GetOriginRequestPol... | February 04, 2026, 17:18:26 (UT... | AWSVLI | cloudfront.amazonaws.com | - | - |
| ListRolePolicies | February 04, 2026, 17:18:26 (UT... | AWSVLI | iam.amazonaws.com | - | - |
| ListTagsForResource | February 04, 2026, 17:18:26 (UT... | AWSVLI | wafv2.amazonaws.com | - | - |
| ListTagsForCertificate | February 04, 2026, 17:18:26 (UT... | AWSVLI | acm.amazonaws.com | - | - |
| DescribeCertificate | February 04, 2026, 17:18:26 (UT... | AWSVLI | acm.amazonaws.com | - | - |
| ListAttachedRolePol... | February 04, 2026, 17:18:26 (UT... | AWSVLI | iam.amazonaws.com | - | - |
| GetWebACL | February 04, 2026, 17:18:26 (UT... | AWSVLI | wafv2.amazonaws.com | - | - |
| GetHostedZone | February 04, 2026, 17:18:26 (UT... | AWSVLI | route53.amazonaws.co | AWS::Route53::Hosted... | Z03792151VUZ7JF79V4V6Q |
| GetRole | February 04, 2026, 17:18:26 (UT... | AWSVLI | iam.amazonaws.com | - | - |
| GetCachePolicy | February 04, 2026, 17:18:26 (UT... | AWSVLI | cloudfront.amazonaws.com | - | - |
| GetCallerIdentity | February 04, 2026, 17:18:25 (UT... | AWSVLI | sts.amazonaws.com | - | - |
| ListManagedNotificat... | February 04, 2026, 17:17:55 (UT... | AWSVLI | notifications.amazona | - | - |
| ListManagedNotificat... | February 04, 2026, 17:17:54 (UT... | AWSVLI | notifications.amazona | - | - |
| ListManagedNotificat... | February 04, 2026, 17:17:14 (UT... | AWSVLI | notifications.amazona | - | - |
| ListManagedNotificat... | February 04, 2026, 17:16:54 (UT... | AWSVLI | notifications.amazona | - | - |
| ListManagedNotificat... | February 04, 2026, 17:16:50 (UT... | AWSVLI | notifications.amazona | - | - |
| ListManagedNotificat... | February 04, 2026, 17:15:54 (UT... | AWSVLI | notifications.amazona | - | - |

5) Network corridor proof (TGW)

Students prove:

TGW attachments exist in both regions
routes point cross-region CIDRs to TGW

Tokyo



| Name | Transit gateway attachment ID | Transit gateway ID | State | Resource type | Resource ID | Association route table ID |
|--------------------------|-------------------------------|-----------------------|-----------|---------------|-----------------------|----------------------------|
| shinjuku-to-liberdade... | tgw-attach-0b86f8b6da54a18d3 | tgw-0f53918ba065e8b2b | Available | Peering | tgw-0d54e3cd5455b568 | tgw-rtb-06baa2f2bb9f9e8de |
| shinjuku-attach-toky... | tgw-attach-02c4692614c6f2fb6 | tgw-0f53918ba065e8b2b | Available | VPC | vpc-0460407572b993c99 | tgw-rtb-06baa2f2bb9f9e8de |

Transit gateway attachment: tgw-attach-0b86f8b6da54a18d3 / shinjuku-to-liberdade-peer01

| Details | Flow logs | Tags |
|---|---|--|
| Details Transit gateway attachment ID tgw-attach-0b86f8b6da54a18d3 Requester ID tgw-0f53918ba065e8b2b Acceptor ID tgw-0d54e3cd5455b568 | State Available Requester region Tokyo (ap-northeast-1) Acceptor region São Paulo (sa-east-1) | Resource type Peering Requester owner ID 814910273374 Acceptor owner ID 814910273374 Association state Associated Dynamic routing Disabled |

Sao-Paulo

Transit gateway attachments (1/2) Info

Find transit gateway attachment by attribute or tag

| Name | Transit gateway attachment ID | Transit gateway ID | State | Resource type | Resource ID | Association route table ID |
|------------------------|-------------------------------|-----------------------|-----------|---------------|-----------------------|----------------------------|
| liberdade-accept-pe... | tgw-attach-0b86f8b6da54a18d3 | tgw-0d54e3fcd5455b568 | Available | Peering | tgw-0f53918ba065e8b2b | tgw-rtb-0906255e29dc2f011 |
| liberdade-attach-sp... | tgw-attach-0a3aeb7e1f2546862 | tgw-0d54e3fcd5455b568 | Available | VPC | vpc-04ab35425c530e20a | tgw-rtb-0906255e29dc2f011 |

Transit gateway attachment: tgw-attach-0b86f8b6da54a18d3 / liberdade-accept-peer01

Details Flow logs Tags

Details

| | | | |
|--|---|---|--|
| Transit gateway attachment ID tgw-attach-0b86f8b6da54a18d3 | State Available | Resource type Peering | Association route table ID tgw-rtb-0906255e29dc2f011 |
| Requester ID tgw-0f53918ba065e8b2b | Requester region Tokyo (ap-northeast-1) | Requester owner ID 814910273374 | Association state Associated |
| Acceptor ID tgw-0d54e3fcd5455b568 | Acceptor region São Paulo (sa-east-1) | Acceptor owner ID 814910273374 | |

6) AWS CLI verification (students can prove the bucket/logs exist)

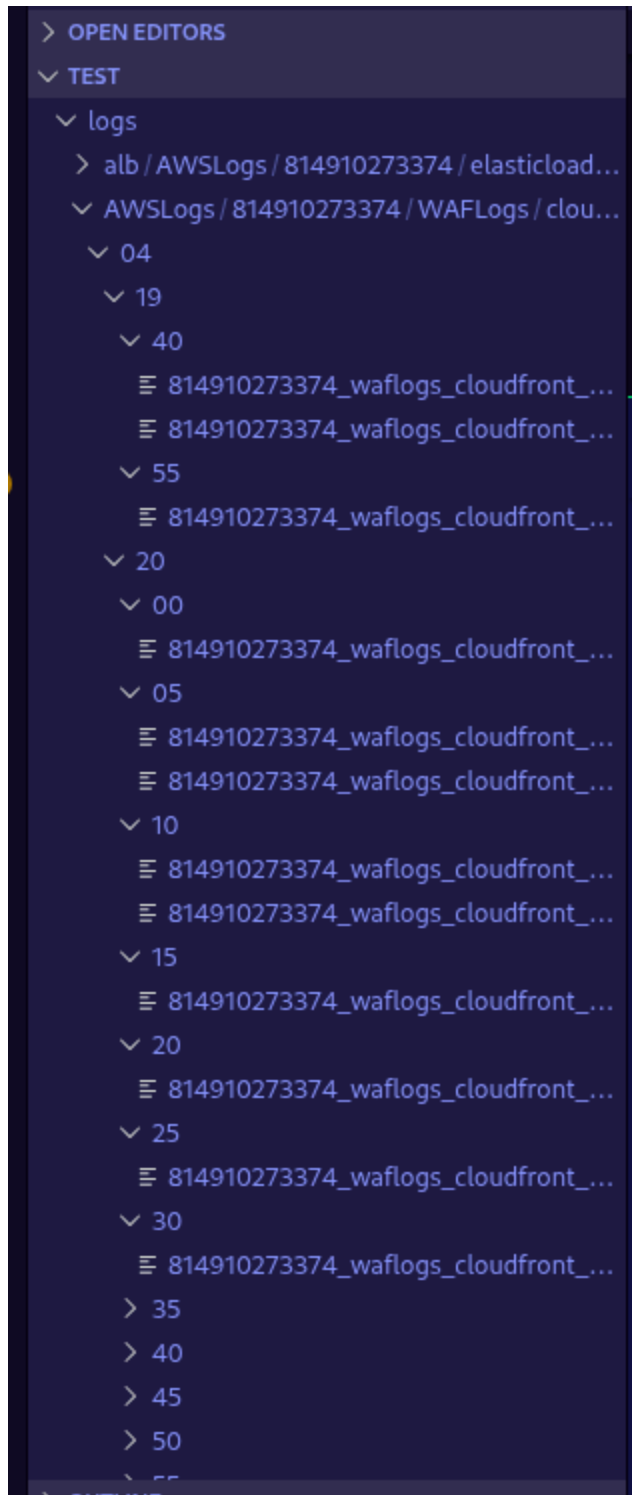
```
aws s3 ls s3://Class_Lab3/
```

```
# If logs are under a folder/prefix:
```

```
aws s3 ls s3://aws-alb-logs-sa-east-1-star1-814910273374/ --recursive | tail -n 20
```

```
asmodeus@Asmodeus: ~/Armaggeddon/Lab_3/Lab-3/Japan
$ aws s3 ls s3://aws-alb-logs-sa-east-1-star1-814910273374/ --recursive | tail -n 20
2026-02-04 16:40:04 1125 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T21002_54.232.74.66_1vscsf3.log.g
2026-02-04 16:40:04 371 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T21002_54.233.248.94_69001021.log.g
2026-02-04 16:15:08 396 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T21152_54.233.248.94_3zv0bmcf.log.g
2026-02-04 16:39:08 392 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T21302_54.232.74.66_569cotfb.log.g
2026-02-04 16:35:08 669 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T21352_54.232.74.66_1oihjnra.log.g
2026-02-04 16:35:08 1318 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T21352_54.233.248.94_46449dk7.log.g
2026-02-04 16:55:09 394 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T21552_54.232.74.66_1x7nj5x7.log.g
2026-02-04 16:55:08 388 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T21552_54.233.248.94_g7e0dios.log.g
2026-02-04 17:10:09 484 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T22102_54.232.74.66_3k1uuvj.log.g
2026-02-04 17:10:08 810 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T22102_54.233.248.94_ev4fw28c.log.g
2026-02-04 17:15:09 530 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T22152_54.232.74.66_260gdikm.log.g
2026-02-04 17:15:08 593 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T22152_54.233.248.94_4joh295r.log.g
2026-02-04 17:35:09 392 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T22352_54.233.248.94_4whteom.log.g
2026-02-04 17:49:09 786 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T22402_54.232.74.66_2vich0u.log.g
2026-02-04 16:30:10 380 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T23302_54.233.248.94_hbh1e3r.log.g
2026-02-04 18:40:10 550 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T23402_54.232.74.66_3jt1ttqj.log.g
2026-02-04 18:40:11 420 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T23402_54.233.248.94_2c74ctbd.log.g
2026-02-04 18:45:10 426 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T23452_54.232.74.66_3x38hfqp.log.g
2026-02-04 18:45:11 848 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T23452_54.233.248.94_5zxj37g7.log.g
2026-02-04 18:55:11 422 alb/AWSLogs/814910273374/elasticloadbalancing/sa-east-1/2026/02/04/814910273374_elasticloadbalancing_sa-east-1_app.LoadExternal.10e5401d827c5ea4_20260204T23552_54.233.248.94_6mzxnyvy.log.g
```

Download one file manually (sanity check):



```
aws s3 cp s3://aws-waf-logs-sa-east-1-star1-814910273374/ logs.gz .
```

Script 1 — `malgus_residency_proof.py`
Creates a “DB only in Tokyo” proof file.

```
terminal Help
malgus_residency_proof.py x malgus_tgw_corridor_proof.py malgus_cloudfront_log_explainer.py
malgus_residency_proof.py
1  #!/usr/bin/env python3
2  import boto3, json
3
4  # Reason why Darth Malgus would be pleased with this script.
5  # Malgus wants proof, not opinions: "Show me the database lives ONLY in Tokyo."
6  # Reason why this script is relevant to your career.
7  # Auditors demand evidence bundles. Automating compliance proofs is real-world SRE/SEC work.
8  # How you would talk about this script at an interview.
9  # "I automated data residency verification by checking RDS inventory across regions and exporting an audit artifact."
10
11 def list_rds(region):
12     rds = boto3.client("rds", region_name=region)
13     resp = rds.describe_db_instances()
14     out = []
15     for d in resp.get("DBInstances", []):
16         out.append({
17             "region": region,
18             "id": d["DBInstanceIdentifier"],
19             "az": d.get("AvailabilityZone"),
20             "endpoint": d.get("Endpoint", {}).get("Address")
21         })
22     return out
23
24 def main():
25     tokyo = list_rds("ap-northeast-1")
26     sp = list_rds("sa-east-1")
27
28 PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS GITLENS AZURE
29 python3 -i import boto3, json; print(boto3.__doc__)
30 (venv)-(asmodeus@Asmodeus) - [~/Armageddon/Lab 3/Lab-3/Test]
31 $ python malgus_residency_proof.py
32 {
33   "tokyo_rds": [
34     {
35       "region": "ap-northeast-1",
36       "id": "terraform-20260204162055696600000006",
37       "az": "ap-northeast-1c",
38       "endpoint": "terraform-20260204162055696600000006.clo4kyoarkz.ap-northeast-1.rds.amazonaws.com"
39     }
40   ],
41   "saopaulo_rds": [],
42   "assertion": "PASS"
43 }
44 (venv)-(asmodeus@Asmodeus) - [~/Armageddon/Lab 3/Lab-3/Test]
45 $
```

Script 2 — malgus_tgw_corridor_proof.py

```

• (venv)~(asmodeus@Asmodeus)-[~/Armageddon/Lab 3/Lab-3/Test]
$ python malgus_tgw_corridor_proof.py
{
  "tokyo": {
    "region": "ap-northeast-1",
    "transit_gateways": [
      {
        "TransitGatewayId": "tgw-0f53918ba065e8b2b",
        "TransitGatewayArn": "arn:aws:ec2:ap-northeast-1:814910273374:transit-gateway/tgw-0f53918ba065e8b2b",
        "State": "available",
        "OwnerId": "814910273374",
        "Description": "shinjuku-tgw01 (Tokyo hub)",
        "CreationTime": "2026-02-04 16:20:36+00:00",
        "Options": {
          "AmazonSideAsn": 64512,
          "AutoAcceptSharedAttachments": "disable",
          "DefaultRouteTableAssociation": "disable",
          "DefaultRouteTablePropagation": "disable",
          "VpnEcmpSupport": "enable",
          "DnsSupport": "enable",
          "SecurityGroupReferencingSupport": "disable",
          "MulticastSupport": "disable",
          "EncryptionSupport": {
            "EncryptionState": "disabled"
          }
        },
        "Tags": [
          {
            "Key": "Name",
            "Value": "shinjuku-tgw01"
          }
        ]
      }
    ],
    "attachments": [
      {
        "TransitGatewayAttachmentId": "tgw-attach-0b86f8b6da54a18d3",
        "TransitGatewayId": "tgw-0f53918ba065e8b2b",
        "TransitGatewayOwnerId": "814910273374",
        "ResourceOwnerId": "814910273374",
        "ResourceType": "peering",
        "ResourceId": "tgw-0d54e3fcd5455b568",
        "State": "available",
        "Association": {
          "TransitGatewayRouteTableId": "tgw-rtb-06baa2f2bb9f9e8de",
          "State": "associated"
        },
        "CreationTime": "2026-02-04 17:34:11+00:00",
        "Tags": [
          {
            "Key": "Name",
            "Value": "shinjuku-to-liberdade-peer01"
          }
        ]
      }
    ]
  }
}

```

```

        "Value": "shinjuku-to-liberdade-peer01"
    }
},
{
    "TransitGatewayAttachmentId": "tgw-attach-02c4692614c6f2fb6",
    "TransitGatewayId": "tgw-0f53918ba065e8b2b",
    "TransitGatewayOwnerId": "814910273374",
    "ResourceOwnerId": "814910273374",
    "ResourceType": "vpc",
    "ResourceId": "vpc-0460407572b993c99",
    "State": "available",
    "Association": {
        "TransitGatewayRouteTableId": "tgw-rtb-06baa2f2bb9f9e8de",
        "State": "associated"
    },
    "CreationTime": "2026-02-04 16:20:53+00:00",
    "Tags": [
        {
            "Key": "Name",
            "Value": "shinjuku-attach-tokyo-vpc01"
        }
    ]
}
],
"saopaulo": {
    "region": "sa-east-1",
    "transit_gateways": [
        {
            "TransitGatewayId": "tgw-0d54e3fcd5455b568",
            "TransitGatewayArn": "arn:aws:ec2:sa-east-1:814910273374:transit-gateway/tgw-0d54e3fcd5455b568",
            "State": "available",
            "OwnerId": "814910273374",
            "Description": "liberdade-tgw01 (Sao Paulo spoke)",
            "CreationTime": "2026-02-04 16:44:17+00:00",
            "Options": {
                "AmazonSideAsn": 64512,
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "disable",
                "DefaultRouteTablePropagation": "disable",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "disable",
                "MulticastSupport": "disable",
                "EncryptionSupport": {
                    "EncryptionState": "disabled"
                }
            },
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "liberdade-tgw01"
                }
            ]
        }
    ]
}
}

```



```
python3 malgus_tgw_cloudtrail.py
{
  "Key": "Name",
  "Value": "liberdade-tgw01"
}
],
"attachments": [
  {
    "TransitGatewayAttachmentId": "tgw-attach-0b86f8b6da54a18d3",
    "TransitGatewayId": "tgw-0d54e3fcd5455b568",
    "TransitGatewayOwnerId": "814910273374",
    "ResourceOwnerId": "814910273374",
    "ResourceType": "peering",
    "ResourceId": "tgw-0f53918ba065e8b2b",
    "State": "available",
    "Association": {
      "TransitGatewayRouteTableId": "tgw-rtb-0906255e29dc2f011",
      "State": "associated"
    },
    "CreationTime": "2026-02-04 17:34:35+00:00",
    "Tags": [
      {
        "Key": "Name",
        "Value": "liberdade-accept-peer01"
      }
    ]
  },
  {
    "TransitGatewayAttachmentId": "tgw-attach-0a3aeb7e1f2546862",
    "TransitGatewayId": "tgw-0d54e3fcd5455b568",
    "TransitGatewayOwnerId": "814910273374",
    "ResourceOwnerId": "814910273374",
    "ResourceType": "vpc",
    "ResourceId": "vpc-04ab35425c530e20a",
    "State": "available",
    "Association": {
      "TransitGatewayRouteTableId": "tgw-rtb-0906255e29dc2f011",
      "State": "associated"
    },
    "CreationTime": "2026-02-04 16:44:45+00:00",
    "Tags": [
      {
        "Key": "Name",
        "Value": "liberdade-attach-sp-vpc01"
      }
    ]
  }
]
}
}

(venv)-(asmodeus@Asmodeus) - [~/../Armageddon/Lab 3/Lab-3/Test]
```

Shows TGW attachments + routes that form the “legal corridor”.

Script 3 — malgus_cloudtrail_last_changes.py

Pulls recent CloudTrail events for “who changed what”.

--> Event history is available by default; it provides a 90-day record of management events.

Not Created Yet

Script 4 — malgus_waf_summary.py

Summarizes WAF logs (Allow vs Block) from CloudWatch Logs destination.

WAF logging destinations: CloudWatch Logs, S3, Firehose.

Not Created Yet

Script 5 — malgus_cloudfront_log_explainer.py (optional)

If you ingest CloudFront standard logs into S3, this script reads a log file and counts Hit/Miss/RefreshHit.

Not Working

```
(venv)-(asmodeus@Asmodeus)-[~/Armageddon/Lab 3/Lab-3/Test]
$ python malgus_cloudfront_log_explainer.py
Traceback (most recent call last):
  File "/home/asmodeus/Downloads/Armageddon/Lab 3/Lab-3/Test/malgus_cloudfront_log_explainer.py", line 35, in run
    p = subprocess.run(cmd, check=True, capture_output=True, text=True)
  File "/usr/lib/python3.13/subprocess.py", line 577, in run
    raise CalledProcessError(retcode, process.args,
        output=stdout, stderr=stderr)
subprocess.CalledProcessError: Command '['aws', 's3', 'ls', 's3://Class_Lab3/', '--recursive']' returned non-zero exit status 254.

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/home/asmodeus/Downloads/Armageddon/Lab 3/Lab-3/Test/malgus_cloudfront_log_explainer.py", line 222, in <module>
    raise SystemExit(main())
  File "/home/asmodeus/Downloads/Armageddon/Lab 3/Lab-3/Test/malgus_cloudfront_log_explainer.py", line 174, in main
    keys = aws_s3_ls_recursive(args.bucket, args.prefix)
  File "/home/asmodeus/Downloads/Armageddon/Lab 3/Lab-3/Test/malgus_cloudfront_log_explainer.py", line 48, in aws_s3_ls_recursive
    out = run(["aws", "s3", "ls", uri, "--recursive"])
  File "/home/asmodeus/Downloads/Armageddon/Lab 3/Lab-3/Test/malgus_cloudfront_log_explainer.py", line 41, in run
    raise RuntimeError(f"Command failed: {' '.join(cmd)}\n{msg}")
RuntimeError: Command failed: aws s3 ls s3://Class_Lab3/ --recursive
An error occurred (NoSuchBucket) when calling the ListObjectsV2 operation: The specified bucket does not exist

(venv)-(asmodeus@Asmodeus)-[~/Armageddon/Lab 3/Lab-3/Test]
$
```

CloudFront standard logs reference Hit / RefreshHit semantics.

A) Standard logs in S3 (downloaded locally)

```
python3 malgus_cloudfront_log_explainer.py --mode standard cloudfront.log.gz
```

```
python3 malgus_cloudfront_log_explainer.py --mode standard cloudfront_part1.log
cloudfront_part2.log
```

```
malgus_residency_proof.py malgus_tgw_corridor_proof.py malgus_cloudfront_log_explainer.py x
malgus_cloudfront_log_explainer.py
25 import sys
26 import tempfile
27 from collections import Counter
28 from typing import Dict, List, Optional
29
30 TARGETS = {"Hit", "Miss", "RefreshHit"}
31
32 def run(cmd: List[str]) -> str:
33     """Run a command and return stdout: raise with clear error if it fails."""

[asmodeus@Asmodeus] ~/Armageddon/Lab 3/Lab-3/Test
$ python malgus_cloudfront_log_explainer.py logs/
usage: malgus_cloudfront_log_explainer.py [-h] [--bucket BUCKET] [--prefix PREFIX] [--latest LATEST] [--keep]
malgus_cloudfront_log_explainer.py: error: unrecognized arguments: logs/

[asmodeus@Asmodeus] ~/Armageddon/Lab 3/Lab-3/Test
$ python malgus_cloudfront_log_explainer.py \
  --bucket aws-waf-logs-sa-east-1-star1-814910273374 \
  --prefix AWSLogs/814910273374/

Found 54 objects. Analyzing latest 3:
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/30/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0630Z_cbe269c8.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/35/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0635Z_241e8144.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/50/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0650Z_e6c3cff4.log.gz

=== CloudFront Cache Outcome Report (Standard Logs) ===
Core total (Hit/Miss/RefreshHit): 0
All counted lines/notes: 14

Core outcomes:
Hit          0 (0.0% of core)
Miss         0 (0.0% of core)
RefreshHit   0 (0.0% of core)

Other outcomes / parsing notes (top 20):
Other:(missing_fields_header) 14

Interpretation (ops):
• High Hit% usually means lower latency & lower origin load.
• High Miss% suggests caching policy mismatch, uncacheable headers, query-string/cookie variance, or origin Cache-Control behavior.
• RefreshHit means CloudFront revalidated with origin and served cached content (often good).
```

B) Real-time logs as JSON lines

```
python3 malgus_cloudfront_log_explainer.py --mode realtime realtime_logs.jsonl
```

```
[asmodeus@Asmodeus] ~/Armageddon/Lab 3/Lab-3/Test
$ python malgus_cloudfront_log_explainer.py \
  --bucket aws-waf-logs-sa-east-1-star1-814910273374 \
  --prefix AWSLogs/814910273374/
  --mode realtime \
  realtime_logs.jsonl

Found 54 objects. Analyzing latest 3:
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/30/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0630Z_cbe269c8.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/35/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0635Z_241e8144.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/50/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0650Z_e6c3cff4.log.gz

=== CloudFront Cache Outcome Report (Standard Logs) ===
Core total (Hit/Miss/RefreshHit): 0
All counted lines/notes: 14

Core outcomes:
Hit          0 (0.0% of core)
Miss         0 (0.0% of core)
RefreshHit   0 (0.0% of core)

Other outcomes / parsing notes (top 20):
Other:(missing_fields_header) 14

Interpretation (ops):
• High Hit% usually means lower latency & lower origin load.
• High Miss% suggests caching policy mismatch, uncacheable headers, query-string/cookie variance, or origin Cache-Control behavior.
• RefreshHit means CloudFront revalidated with origin and served cached content (often good).
```

Final Lab Assumptions (Locked)

S3 Bucket: Class_Lab3

CloudFront Logs Prefix: Chwebacca-logs/ ← intentionally misspelled

AWS Account ID: 200819971986

Running Scripts:

```
python3 malgus_cloudfront_log_explainer.py --latest 5
```

```
(asmodeus@Asmodeus) - [~/Armageddon/Lab 3/Lab-3/Test]
└─$ python3 malgus_cloudfront_log_explainer.py --latest 5 \
--bucket aws-waf-logs-sa-east-1-star1-814910273374 \
--prefix AWSLogs/814910273374/

Found 54 objects. Analyzing latest 5:
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/10/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0610Z_fe8d4625.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/20/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0620Z_109a42da.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/30/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0630Z_cbe269c8.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/35/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0635Z_241e8144.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/50/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0650Z_e6c3cff4.log.gz

=== CloudFront Cache Outcome Report (Standard Logs) ===
Core total (Hit/Miss/RefreshHit): 0
All counted lines/notes: 25

Core outcomes:
Hit          0 (0.0% of core)
Miss         0 (0.0% of core)
RefreshHit   0 (0.0% of core)

Other outcomes / parsing notes (top 20):
Other:(missing_fields_header) 25

Interpretation (ops):
• High Hit% usually means lower latency & lower origin load.
• High Miss% suggests caching policy mismatch, uncacheable headers, query-string/cookie variance, or origin Cache-Control behavior.
• RefreshHit means CloudFront revalidated with origin and served cached content (often good).
```

```
python3 malgus_cloudfront_log_explainer.py --prefix cloudfront-logs/ --latest 10
```

```
(asmodeus@Asmodeus) - [~/Armageddon/Lab 3/Lab-3/Test]
└─$ python3 malgus_cloudfront_log_explainer.py --latest 10 \
--bucket aws-waf-logs-sa-east-1-star1-814910273374 \
--prefix AWSLogs/814910273374/

Found 54 objects. Analyzing latest 10:
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/04/05/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0405Z_ca148f56.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/04/20/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0420Z_0d97c9c6.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/04/25/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0425Z_7de9a87a.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/04/55/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0455Z_74652635.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/05/25/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0525Z_7c7f5ada.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/10/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0610Z_fe8d4625.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/20/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0620Z_109a42da.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/30/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0630Z_cbe269c8.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/35/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0635Z_241e8144.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/50/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T0650Z_e6c3cff4.log.gz

=== CloudFront Cache Outcome Report (Standard Logs) ===
Core total (Hit/Miss/RefreshHit): 0
All counted lines/notes: 52

Core outcomes:
Hit          0 (0.0% of core)
Miss         0 (0.0% of core)
RefreshHit   0 (0.0% of core)

Other outcomes / parsing notes (top 20):
Other:(missing_fields_header) 52

Interpretation (ops):
• High Hit% usually means lower latency & lower origin load.
• High Miss% suggests caching policy mismatch, uncacheable headers, query-string/cookie variance, or origin Cache-Control behavior.
• RefreshHit means CloudFront revalidated with origin and served cached content (often good).
```

```
python3 malgus_cloudfront_log_explainer.py --prefix cloudfront-logs/ --latest 5 --keep
```

```
(asmodeus@Asmodeus) - [~/Armageddon/Lab 3/Lab-3/Test]
$ python malgus_cloudfront_log_explainer.py --latest 5 --keep \
  --bucket aws-waf-logs-sa-east-1-star1-814910273374 \
  --prefix AWSLogs/814910273374/

Found 54 objects. Analyzing latest 5:
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/10/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T06102_fe8d4625.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/20/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T06202_109a42da.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/30/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T06302_cbe269c8.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/35/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T06352_241e8144.log.gz
- s3://aws-waf-logs-sa-east-1-star1-814910273374/AWSLogs/814910273374/WAFLogs/cloudfront/star-cloudfront-waf/2026/02/05/06/50/814910273374_waflogs_cloudfront_star-cloudfront-waf_20260205T06502_e6c3cff4.log.gz

=== CloudFront Cache Outcome Report (Standard Logs) ===
Core total (Hit/Miss/RefreshHit): 0
All counted lines/notes: 25

Core outcomes:
Hit      0 (0.0% of core)
Miss     0 (0.0% of core)
RefreshHit 0 (0.0% of core)

Other outcomes / parsing notes (top 20):
Other:(missing_fields_header) 25

Interpretation (ops):
• High Hit% usually means lower latency & lower origin load.
• High Miss% suggests caching policy mismatch, uncacheable headers, query-string/cookie variance, or origin Cache-Control behavior.
• RefreshHit means CloudFront revalidated with origin and served cached content (often good).

Kept downloaded files in: /tmp/malgus_cf_0_iwbv61

(asmodeus@Asmodeus) - [~/Armageddon/Lab 3/Lab-3/Test]
$
```

From stdin (nice for pipelines)

```
zcat cloudfront.log.gz | python3 malgus_cloudfront_log_explainer.py --mode standard -
```

Where “Hit / Miss / RefreshHit” come from (student-facing truth)

In standard CloudFront logs, you usually read the field:

x-edge-result-type (primary)

sometimes also x-edge-response-result-type

Values commonly include: Hit, Miss, RefreshHit, plus other states like Error, LimitExceeded, etc.

That’s why the script reports “Other:*” — so students don’t blindly ignore unusual outcomes.