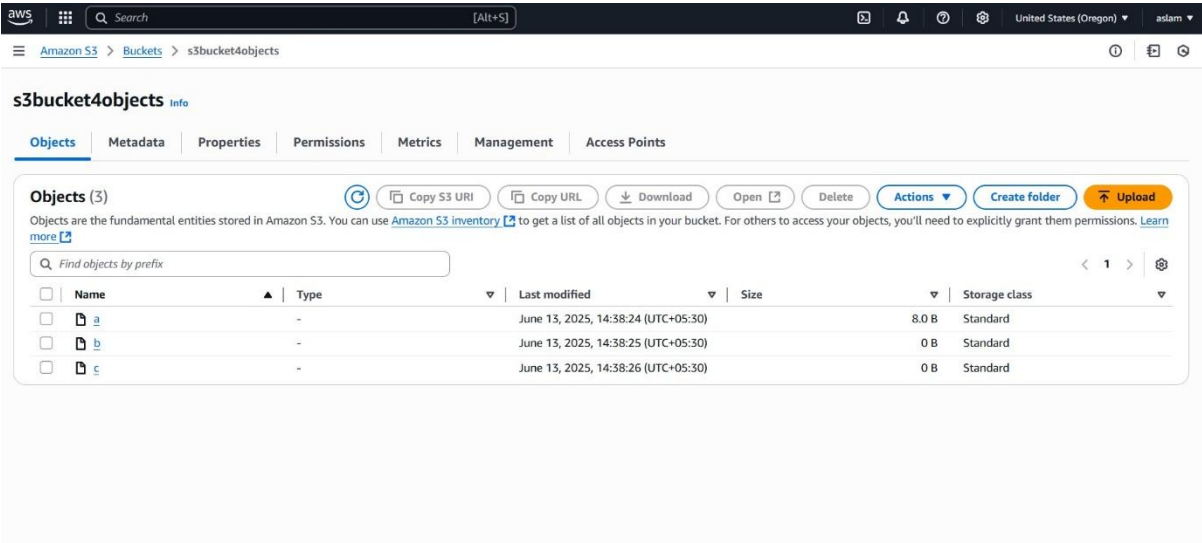
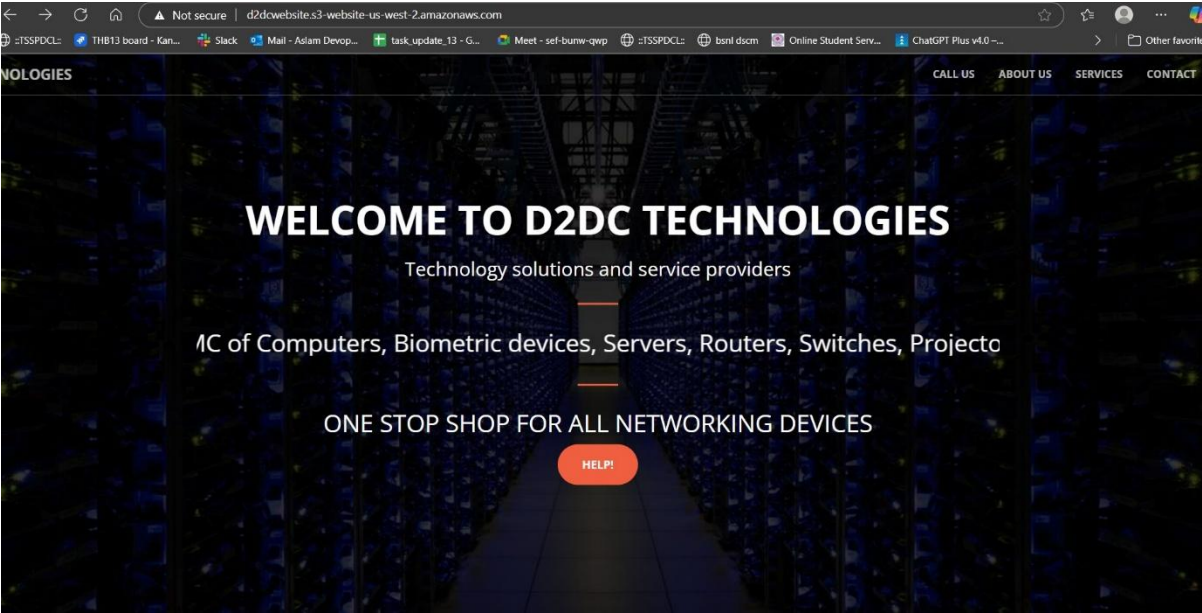


1) Create s3 bucket and upload some objects to s3.

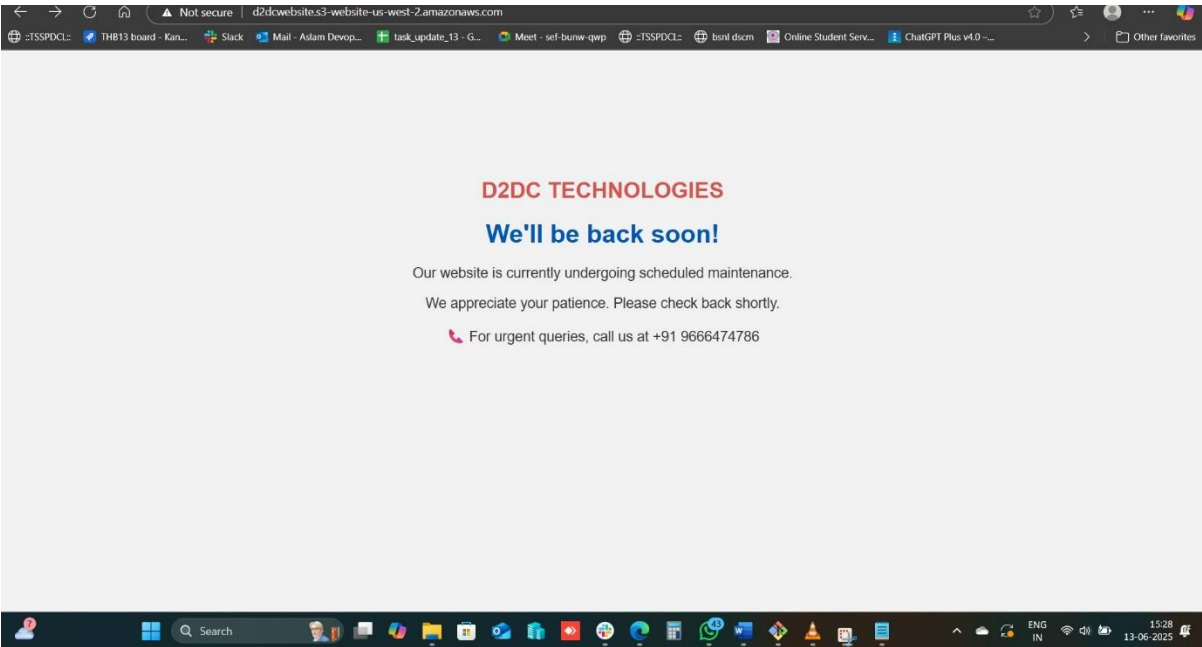


2) Deploy static website in s3 bucket.

Configured one website using online template available



Configured error page also

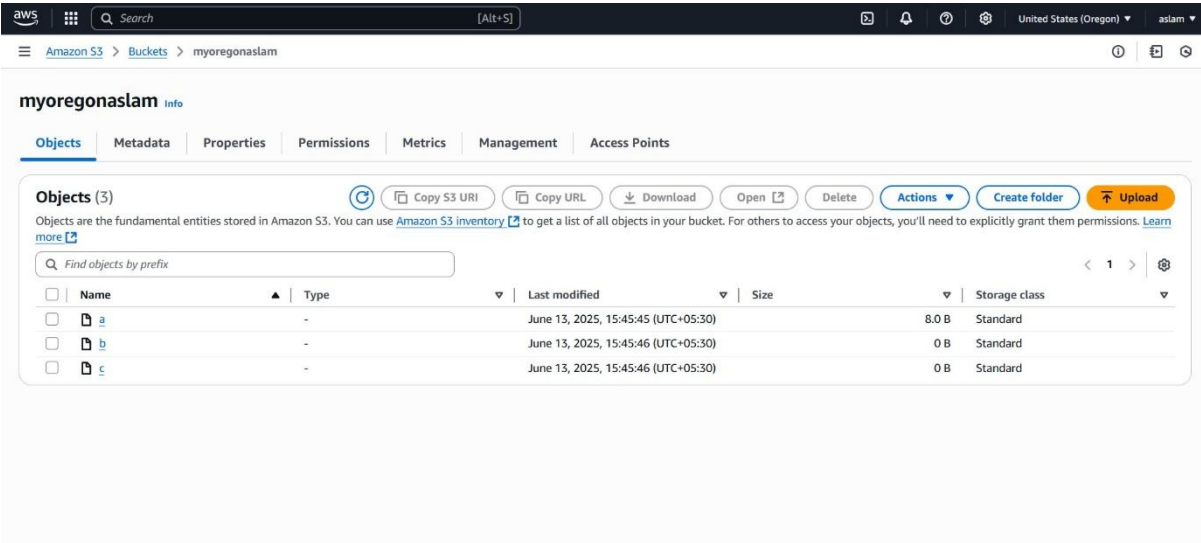


Link for verification

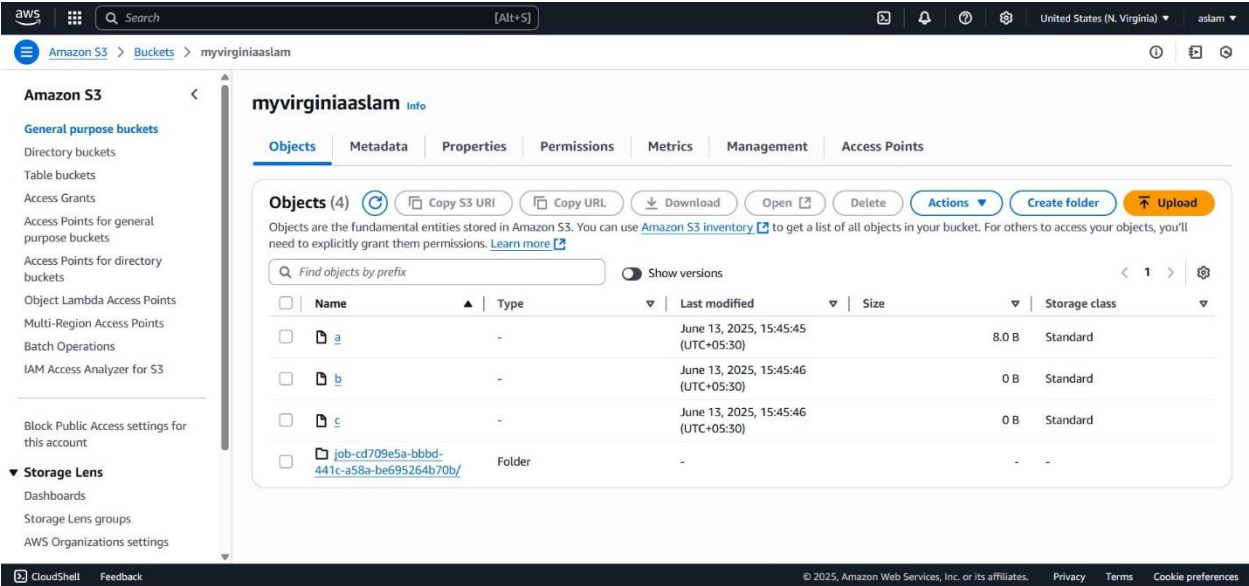
http://d2dcwebsite.s3-website-us-west-2.amazonaws.com

3) Enable cross region replication on s3 buckets.

Created a bucket in oregon

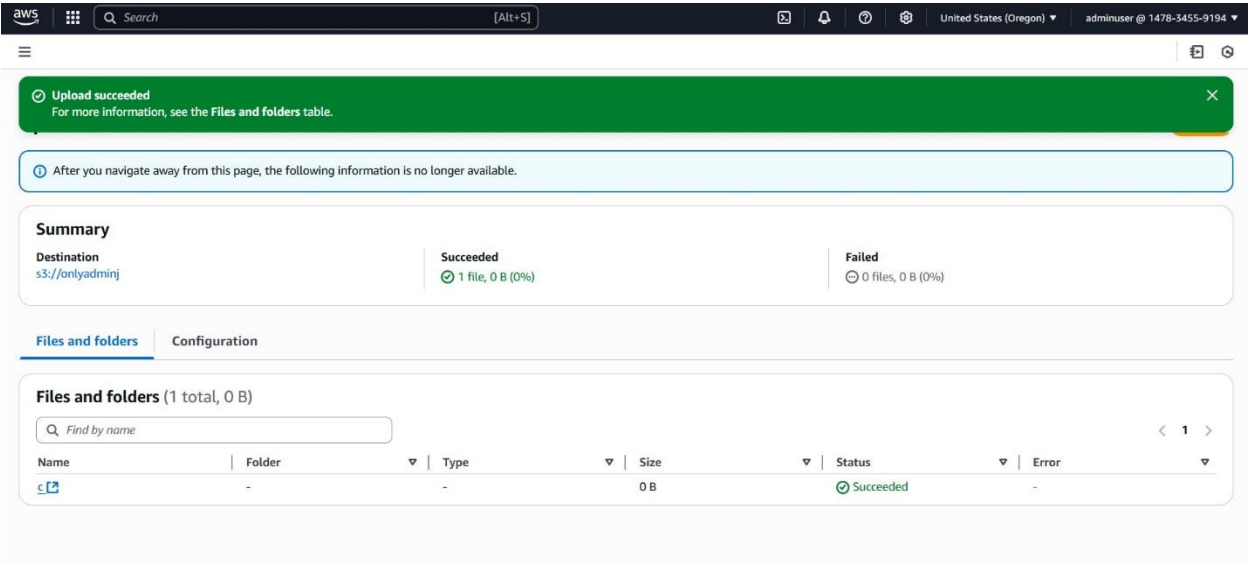


Replicated all items in bucket created in virginia



4) Configure bucket policy,only Admin user can see the objects of s3 bucket.

Only Admin user is able to access and see bucket



Normal user who has s3 readonly access

aws

Search

[Alt+S]

IAM > Users > aslam

aslam

Delete

Summary

ARN
arn:aws:iam::147834559194:user/aslam

Created
June 06, 2025, 18:25 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Today

Access key 1
AKIASE25ALLNDYRFPZT17 - Active
Used 24 hours ago. 24 hours old.

Access key 2
Create access key

Permissions

Groups

Tags

Security credentials

Last Accessed

Permissions policies (3)

Remove

Add permissions

Permissions are defined by policies attached to the user directly or through groups.

Search

Filter by Type
All types

< 1 >

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	Directly
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	Directly

Unable to see the files inside restricted bucket

aws

Search

[Alt+S]

Amazon S3 > Buckets > onlyadminj

onlyadminj

Info

Objects

Metadata

Properties

Permissions

Metrics

Management

Access Points

Objects

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

Show versions

< 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
--------------------------	------	------	---------------	------	---------------

Insufficient permissions to list objects

After you or your AWS administrator has updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about Identity and access management in Amazon S3

Diagnose with Amazon Q

Same user is able to see other buckets

aws

Search

[Alt+S]

Amazon S3 > Buckets > myvirginiaaslam

myvirginiaaslam

Info

Objects

Metadata

Properties

Permissions

Metrics

Management

Access Points

Objects (4)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

Show versions

< 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	a	-	June 13, 2025, 15:45:45 (UTC+05:30)	8.0 B	Standard
<input type="checkbox"/>	b	-	June 13, 2025, 15:45:46 (UTC+05:30)	0 B	Standard
<input type="checkbox"/>	c	-	June 13, 2025, 15:45:46 (UTC+05:30)	0 B	Standard
<input type="checkbox"/>	job-cd709e5a-bbbd-441c-a58a-be695264b70b/	Folder	-	-	-

5) Setup lifecycle policies to automatically transition or delete objects based on specific criteria.

Policy created

```
masla@Hplaptop MINGW64 /e
$ vi lifecycle-policy.json

masla@Hplaptop MINGW64 /e
$ aws s3api put-bucket-lifecycle-configuration \
  --bucket clibuckettt78977 \
  --lifecycle-configuration file://lifecycle-policy.json
{
  "TransitionDefaultMinimumObjectSize": "all_storage_classes_128K"
}

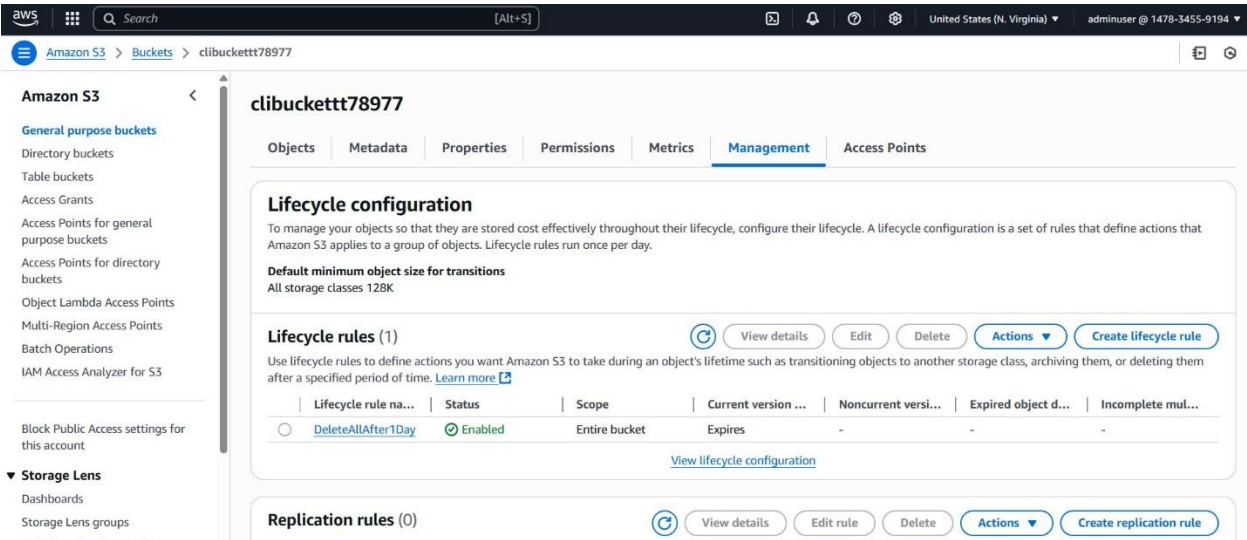
masla@Hplaptop MINGW64 /e
$ |
```

Verified using cli

```
masla@Hplaptop MINGW64 /e
$ aws s3api get-bucket-lifecycle-configuration \
  --bucket clibuckettt78977
{
  "TransitionDefaultMinimumObjectSize": "all_storage_classes_128K",
  "Rules": [
    {
      "Expiration": {
        "Days": 1
      },
      "ID": "DeleteAllAfter1Day",
      "Filter": {
        "Prefix": ""
      },
      "Status": "Enabled"
    }
  ]
}
```

```
masla@Hplaptop MINGW64 /e
$ |
```

Verified using gui



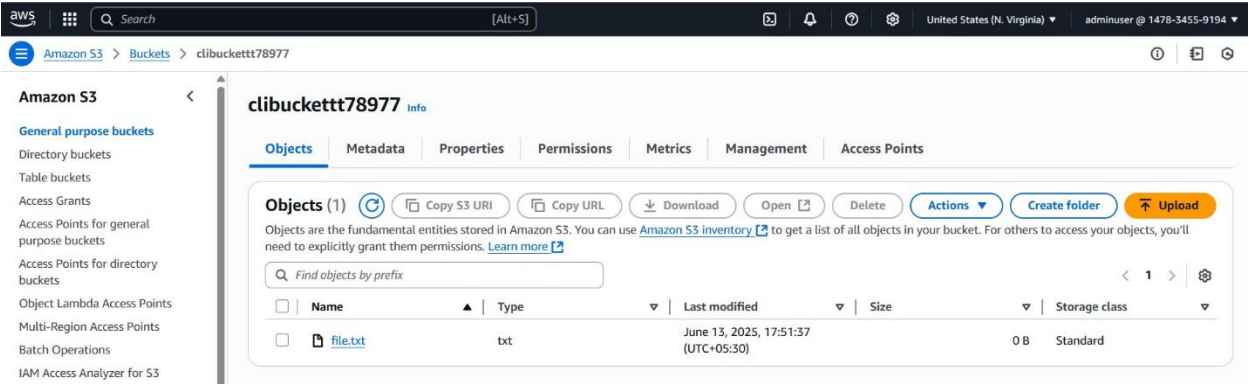
6) Push some objects in s3 using AWS CLI.

Pushed file.txt using cli

```
$
masla@Hplaptop MINGW64 /e
$ aws s3 cp "E:\file.txt" s3://clibuckettt78977/
upload: .\file.txt to s3://clibuckettt78977/file.txt

masla@Hplaptop MINGW64 /e
$
```

File.txt received in bucket



7) Write a bash script to create s3 bucket.

Written a bash script and created a bucket

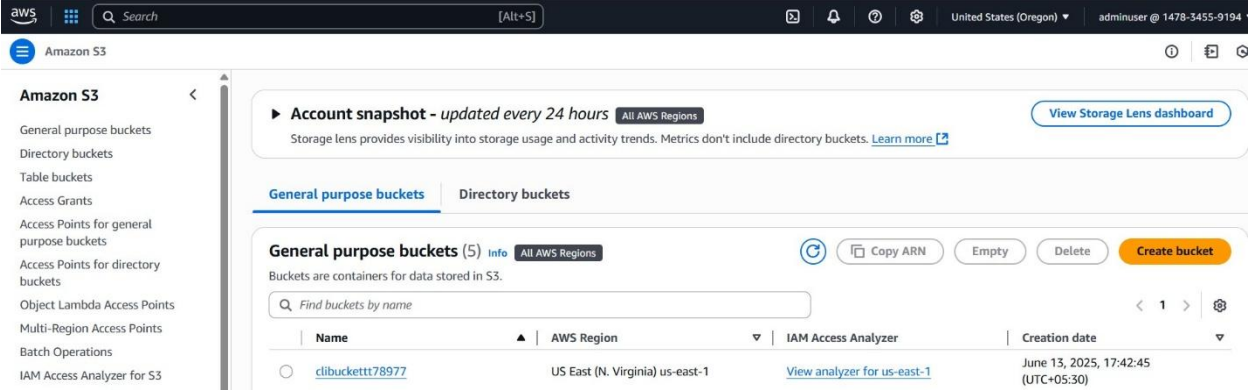
```
masla@Hplaptop MINGW64 /e/software download for aws devops/task and challanges/s3/objects for s3
$ aws configure
AWS Access Key ID [*****S30F]: AKIASE25ALLNK6MLMC3C
AWS Secret Access Key [*****Q2Ke]: 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
Default region name [us-east-1]: us-east-1
Default output format [json]: json

masla@Hplaptop MINGW64 /e/software download for aws devops/task and challanges/s3/objects for s3
$ ./seure.sh
Creating bucket: clibuckettt78977...
{
  "Location": "/clibuckettt78977"
}

Applying bucket policy...
Bucket 'clibuckettt78977' created and secured for adminuser and root only.

masla@Hplaptop MINGW64 /e/software download for aws devops/task and challanges/s3/objects for s3
$
```

verification



8) Upload one 1 gb of file to s3 using cli.

Uploading using this command

```
masla@Hplaptop MINGW64 /e
$ aws s3 cp "E:\onegbfile.zip" s3://clibuckettt78977/
upload: .\onegbfile.zip to s3://clibuckettt78977/onegbfile.zip

masla@Hplaptop MINGW64 /e
$ |
```

Uploading completed

