Digital Forensics (IFS4102) Lab 7: Network and Internet Forensics

Lab Objectives

In this lab, you will perform several **network** and **Internet forensics tasks** on a target machine. More specifically, given an acquired file system and captured network-traffic logs of the target machine, you want:

1. To find out some **network configuration settings** of the machine.
2. *(Optional)* To analyze captured **network-traffic logs** using **Wireshark**.
3. To extract and analyze **objects** from network-traffic logs using two **Network Forensic Analysis Tools (NFATs)**:
    a. **NetworkMiner**;
    b. *(Optional)* **Xplico**.
4. To analyze the **web cache** and **history** of Chrome and Firefox browsers.

Task 1 (Win-FWS): Finding out Network Configuration Settings of a Target Windows Machine

Notes:

- We want to perform an **offline registry analysis** to find out some ***network configuration settings*** of a target machine. For this purpose, we will use a registry analysis tool called **MiTeC Windows Registry Recovery (WRR)**.
- Please download a set of sample registry files, which were previously also used in your Lab 5 (Windows forensics), from: https://drive.google.com/file/d/133bLl7TYqDyCG9eSfuDcIKhbwqiKxJil/view?usp=sharing. Its MD5 value is b527b6a8a4a395aac8afb6c59cf4b15e.

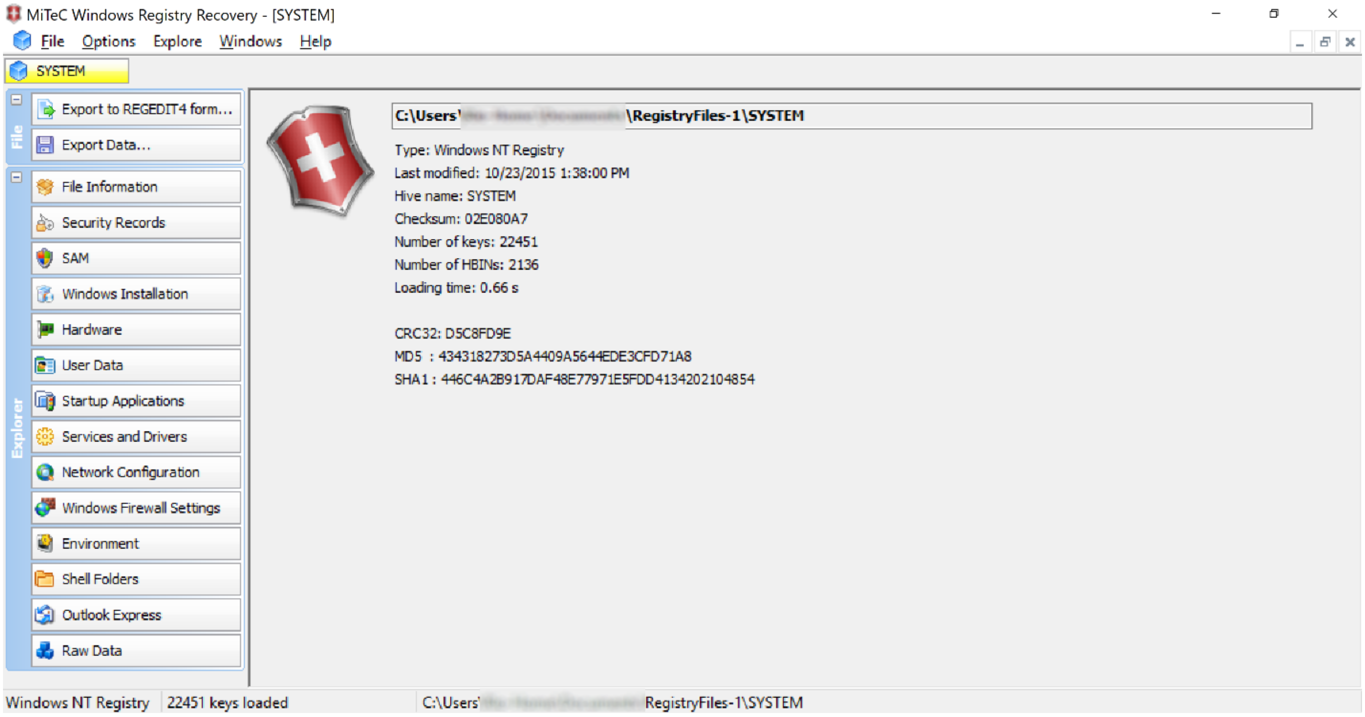
Steps:

1. Download **Windows Registry Recovery (WRR)** from http://www.mitec.cz/wrr.html, and extract its zip file.

2. Launch WRR.

3. From the main menu, select "File" and then "Open". After that, choose the `SYSTEM` registry file from the downloaded registry file set.

   WRR will show the information of the registry hive file as shown below.



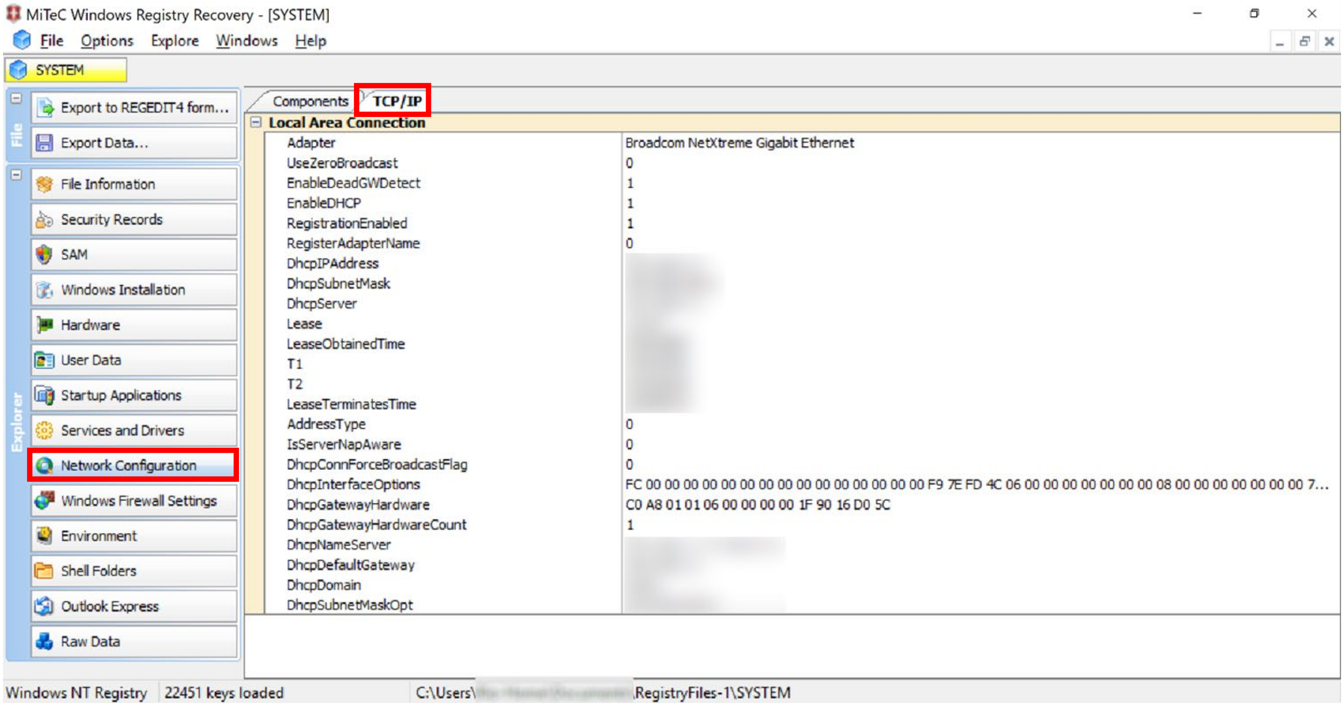
```
C:\Users\[redacted]\RegistryFiles-1\SYSTEM

Type: Windows NT Registry
Last modified: 10/23/2015 1:38:00 PM
Hive name: SYSTEM
Checksum: 02E080A7
Number of keys: 22451
Number of HBINs: 2136
Loading time: 0.66 s

CRC32: D5C8FD9E
MD5  : 434318273D5A4409A5644EDE3CFD71A8
SHA1 : 446C4A2B917DAF48E77971E5FDD4134202104854
```

```
Windows NT Registry    22451 keys loaded    C:\Users\[redacted]RegistryFiles-1\SYSTEM
```

4. Now, on the menu list on the left pane of the window, click the "**Network Configuration**" button as highlighted below. Then, on the right pane, click the "**TCP/IP**" tab. Some network information from the registry will be shown as below.



Local Area Connection

Adapter	Broadcom NetXtreme Gigabit Ethernet
UseZeroBroadcast	0
EnableDeadGWDetect	1
EnableDHCP	1
RegistrationEnabled	1
RegisterAdapterName	0
DhcpIPAddress	[redacted]
DhcpSubnetMask	[redacted]
DhcpServer	[redacted]
Lease	[redacted]
LeaseObtainedTime	[redacted]
T1	[redacted]
T2	[redacted]
LeaseTerminatesTime	[redacted]
AddressType	0
IsServerNapAware	0
DhcpConnForceBroadcastFlag	0
DhcpInterfaceOptions	FC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F9 7E FD 4C 06 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 7...
DhcpGatewayHardware	C0 A8 01 01 06 00 00 00 00 1F 90 16 D0 5C
DhcpGatewayHardwareCount	1
DhcpNameServer	[redacted]
DhcpDefaultGateway	[redacted]
DhcpDomain	[redacted]
DhcpSubnetMaskOpt	[redacted]

Windows NT Registry | 22451 keys loaded | C:\Users\[redacted]RegistryFiles-1\SYSTEM

5. Inspect the shown information. Answer the following questions:

   a. What was the IP address of the machine, which was assigned via DHCP, together with its netmask?

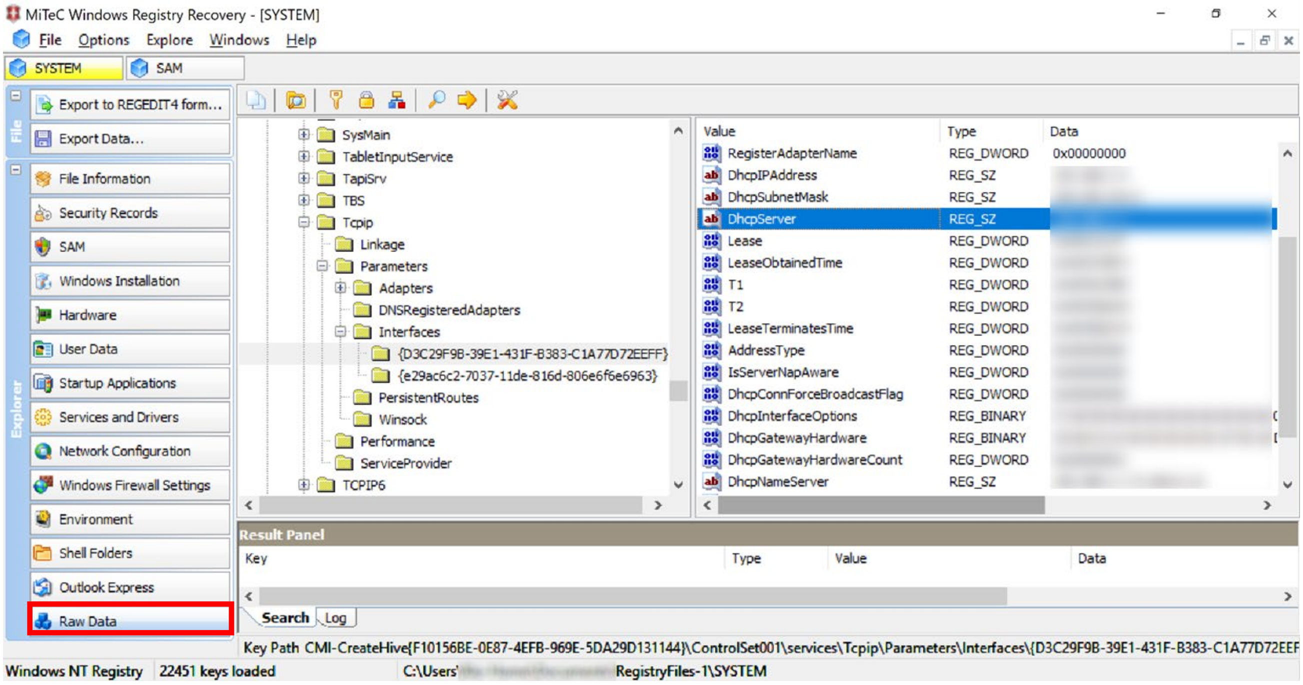
   b. When was the IP address lease obtained by the machine (in human-readable time format)?

   c. *When would the IP address lease expire/terminate (in human-readable time format)?

   d. *What were the IP addresses of the DHCP server and default gateway?

6. As an alternative method, you can also access raw registry values that store the setting information. On the menu list on the left pane of the window, click the “**Raw Data**” button. Then, navigate to `SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces`.

   Check the data of some relevant registry values there as shown below.

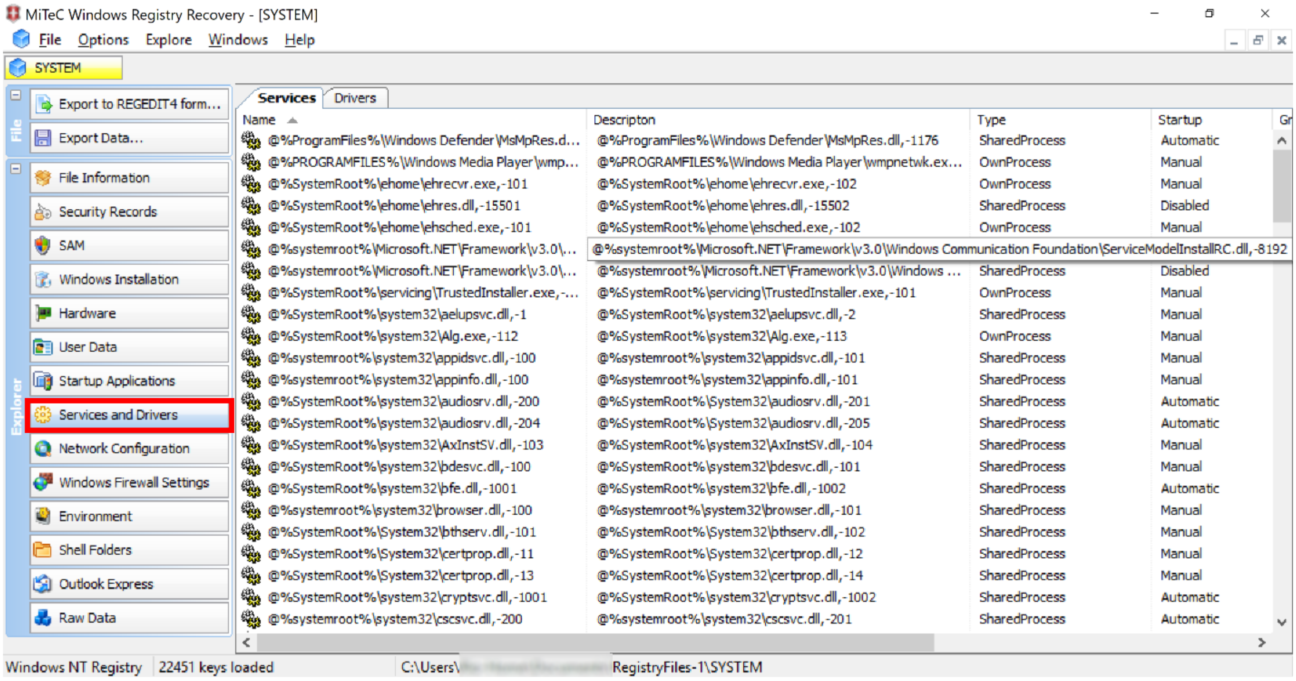


Value	Type	Data
RegisterAdapterName	REG_DWORD	0x00000000
DhcpIPAddress	REG_SZ	[redacted]
DhcpSubnetMask	REG_SZ	[redacted]
DhcpServer	REG_SZ	[redacted]
Lease	REG_DWORD	[redacted]
LeaseObtainedTime	REG_DWORD	[redacted]
T1	REG_DWORD	[redacted]
T2	REG_DWORD	[redacted]
LeaseTerminatesTime	REG_DWORD	[redacted]
AddressType	REG_DWORD	[redacted]
IsServerNapAware	REG_DWORD	[redacted]
DhcpConnForceBroadcastFlag	REG_DWORD	[redacted]
DhcpInterfaceOptions	REG_BINARY	[redacted]
DhcpGatewayHardware	REG_BINARY	[redacted]
DhcpGatewayHardwareCount	REG_DWORD	[redacted]
DhcpNameServer	REG_SZ	[redacted]

Key Path CMI-CreateHive{F10156BE-0E87-4EFB-969E-5DA29D131144}\ControlSet001\services\Tcpip\Parameters\Interfaces\{D3C29F9B-39E1-431F-B383-C1A77D72EEF

Windows NT Registry 22451 keys loaded C:\Users\[redacted]RegistryFiles-1\SYSTEM

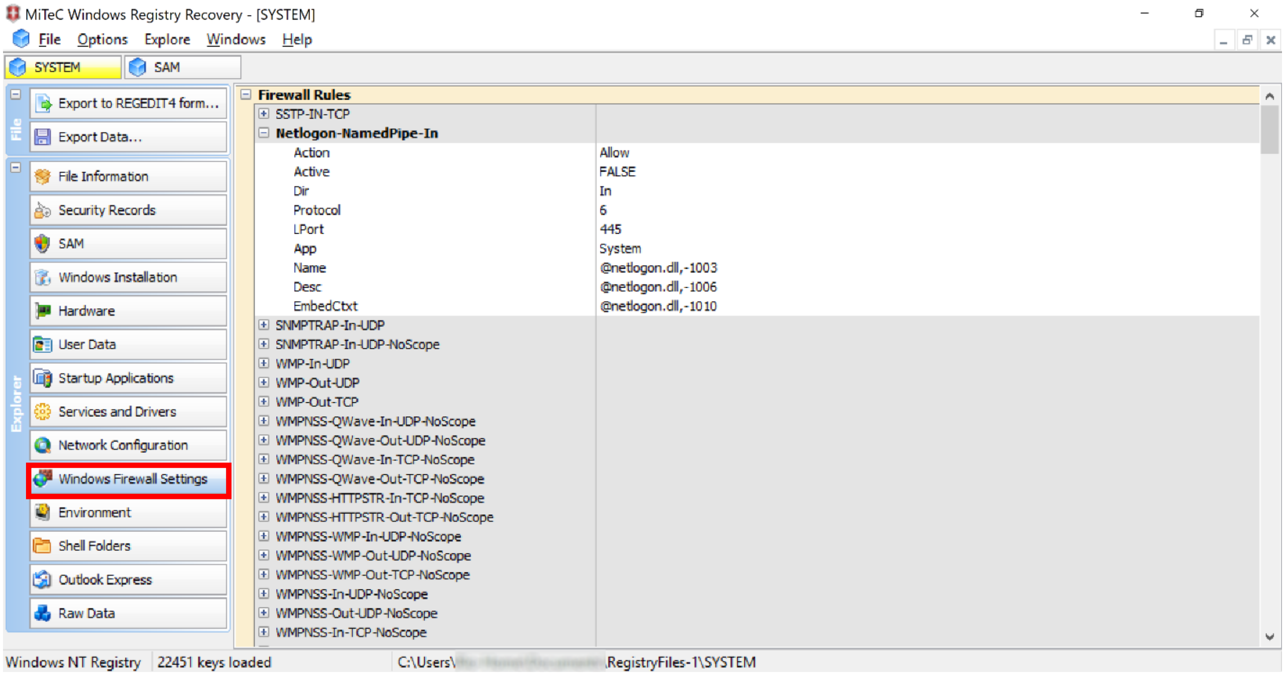
7. Now, on the menu list on the left pane of the window, click the "**Services and Drivers**" button to inspect the **list of services**. Have a look on the listed entries like the ones shown below.



Name	Descripton	Type	Startup
@%ProgramFiles%\Windows Defender\MsMpRes.d...	@%ProgramFiles%\Windows Defender\MsMpRes.dll,-1176	SharedProcess	Automatic
@%PROGRAMFILES%\Windows Media Player\wmp...	@%PROGRAMFILES%\Windows Media Player\wmpnetwk.ex...	OwnProcess	Manual
@%SystemRoot%\ehome\ehrecvr.exe,-101	@%SystemRoot%\ehome\ehrecvr.exe,-102	OwnProcess	Manual
@%SystemRoot%\ehome\ehres.dll,-15501	@%SystemRoot%\ehome\ehres.dll,-15502	SharedProcess	Disabled
@%SystemRoot%\ehome\ehsched.exe,-101	@%SystemRoot%\ehome\ehsched.exe,-102	OwnProcess	Manual
@%systemroot%\Microsoft.NET\Framework\v3.0\...	@%systemroot%\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\ServiceModelInstallRC.dll,-8192		
@%systemroot%\Microsoft.NET\Framework\v3.0\...	@%systemroot%\Microsoft.NET\Framework\v3.0\Windows ...	SharedProcess	Disabled
@%SystemRoot%\servicing\TrustedInstaller.exe,-...	@%SystemRoot%\servicing\TrustedInstaller.exe,-101	OwnProcess	Manual
@%SystemRoot%\system32\aelupsvc.dll,-1	@%SystemRoot%\system32\aelupsvc.dll,-2	SharedProcess	Manual
@%SystemRoot%\system32\Alg.exe,-112	@%SystemRoot%\system32\Alg.exe,-113	OwnProcess	Manual
@%systemroot%\system32\appidsvc.dll,-100	@%systemroot%\system32\appidsvc.dll,-101	SharedProcess	Manual
@%systemroot%\system32\appinfo.dll,-100	@%systemroot%\system32\appinfo.dll,-101	SharedProcess	Manual
@%SystemRoot%\system32\audiosrv.dll,-200	@%SystemRoot%\System32\audiosrv.dll,-201	SharedProcess	Automatic
@%SystemRoot%\system32\audiosrv.dll,-204	@%SystemRoot%\System32\audiosrv.dll,-205	SharedProcess	Automatic
@%SystemRoot%\system32\AxInstSV.dll,-103	@%SystemRoot%\system32\AxInstSV.dll,-104	SharedProcess	Manual
@%SystemRoot%\system32\bdesvc.dll,-100	@%SystemRoot%\system32\bdesvc.dll,-101	SharedProcess	Manual
@%SystemRoot%\system32\bfe.dll,-1001	@%SystemRoot%\system32\bfe.dll,-1002	SharedProcess	Automatic
@%systemroot%\system32\browser.dll,-100	@%systemroot%\system32\browser.dll,-101	SharedProcess	Manual
@%SystemRoot%\System32\bthserv.dll,-101	@%SystemRoot%\System32\bthserv.dll,-102	SharedProcess	Manual
@%SystemRoot%\System32\certprop.dll,-11	@%SystemRoot%\System32\certprop.dll,-12	SharedProcess	Manual
@%SystemRoot%\System32\certprop.dll,-13	@%SystemRoot%\System32\certprop.dll,-14	SharedProcess	Manual
@%SystemRoot%\system32\cryptsvc.dll,-1001	@%SystemRoot%\system32\cryptsvc.dll,-1002	SharedProcess	Automatic
@%systemroot%\system32\cscsvc.dll,-200	@%systemroot%\system32\cscsvc.dll,-201	SharedProcess	Automatic

Windows NT Registry 22451 keys loaded C:\Users\[redacted]RegistryFiles-1\SYSTEM

8. Lastly, on the menu list on the left pane of the window, click the "**Windows Firewall Settings**" button. Have a look on the listed **host firewall settings**.

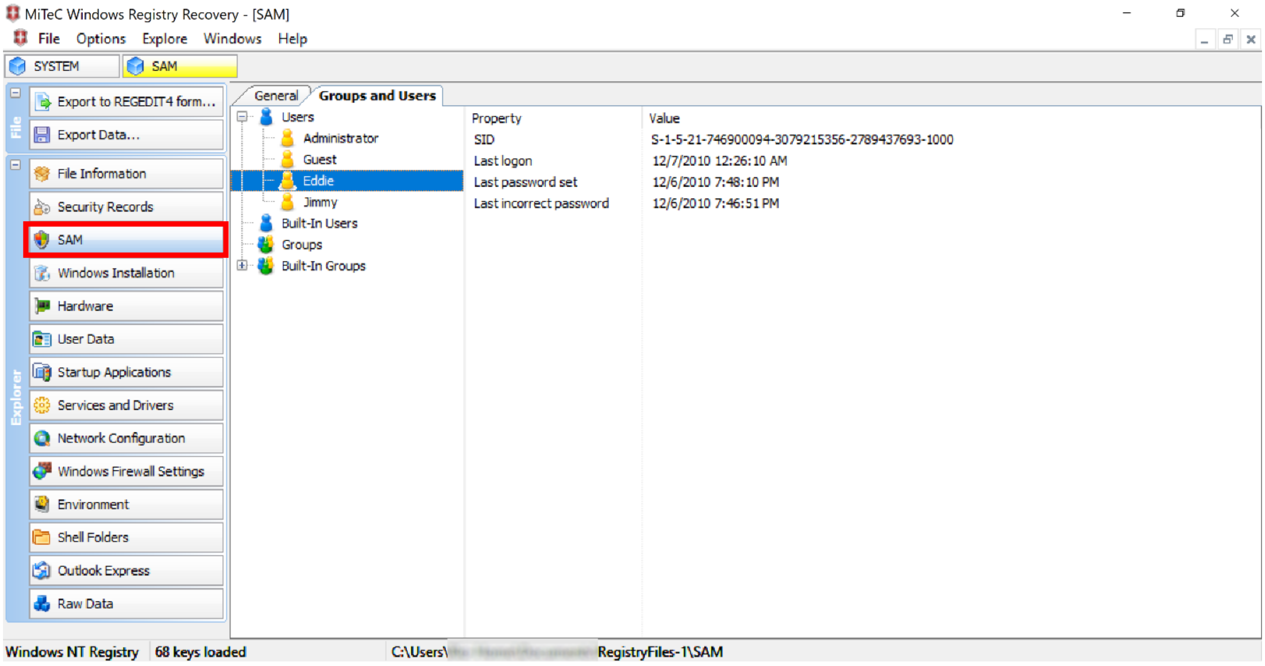


```
Firewall Rules
 SSTP-IN-TCP
 Netlogon-NamedPipe-In
    Action        Allow
    Active        FALSE
    Dir           In
    Protocol      6
    LPort         445
    App           System
    Name          @netlogon.dll,-1003
    Desc          @netlogon.dll,-1006
    EmbedCtxt     @netlogon.dll,-1010
 SNMPTRAP-In-UDP
 SNMPTRAP-In-UDP-NoScope
 WMP-In-UDP
 WMP-Out-UDP
 WMP-Out-TCP
 WMPNSS-QWave-In-UDP-NoScope
 WMPNSS-QWave-Out-UDP-NoScope
 WMPNSS-QWave-In-TCP-NoScope
 WMPNSS-QWave-Out-TCP-NoScope
 WMPNSS-HTTPSTR-In-TCP-NoScope
 WMPNSS-HTTPSTR-Out-TCP-NoScope
 WMPNSS-WMP-In-UDP-NoScope
 WMPNSS-WMP-Out-UDP-NoScope
 WMPNSS-WMP-Out-TCP-NoScope
 WMPNSS-In-UDP-NoScope
 WMPNSS-Out-UDP-NoScope
 WMPNSS-In-TCP-NoScope
```

Windows NT Registry | 22451 keys loaded | C:\Users\[redacted]RegistryFiles-1\SYSTEM

9. Using WRR, you can additionally check other pieces of information on the target machine, such as its **SAM users and groups**. For this, from the main menu, select “File” then “Open”, and choose the downloaded `SAM` file.

10. On the menu list on the left pane of the window, click the “SAM” button. Then, on the right pane, click the “**Groups and Users**” tab as shown below. Inspect the shown information related to the machine’s users.



```
Users                      Property                  Value
  Administrator            SID                       S-1-5-21-746900094-3079215356-2789437693-1000
  Guest                    Last logon                12/7/2010 12:26:10 AM
  Eddie                    Last password set         12/6/2010 7:48:10 PM
  Jimmy                    Last incorrect password   12/6/2010 7:46:51 PM
Built-In Users
Groups
Built-In Groups
```

Windows NT Registry | 68 keys loaded | C:\Users\[redacted]RegistryFiles-1\SAM

[Optional] Task 2 (Win-FWS/Lin-FWS): Analyzing Captured Network Traffic Logs using WireShark

Notes:

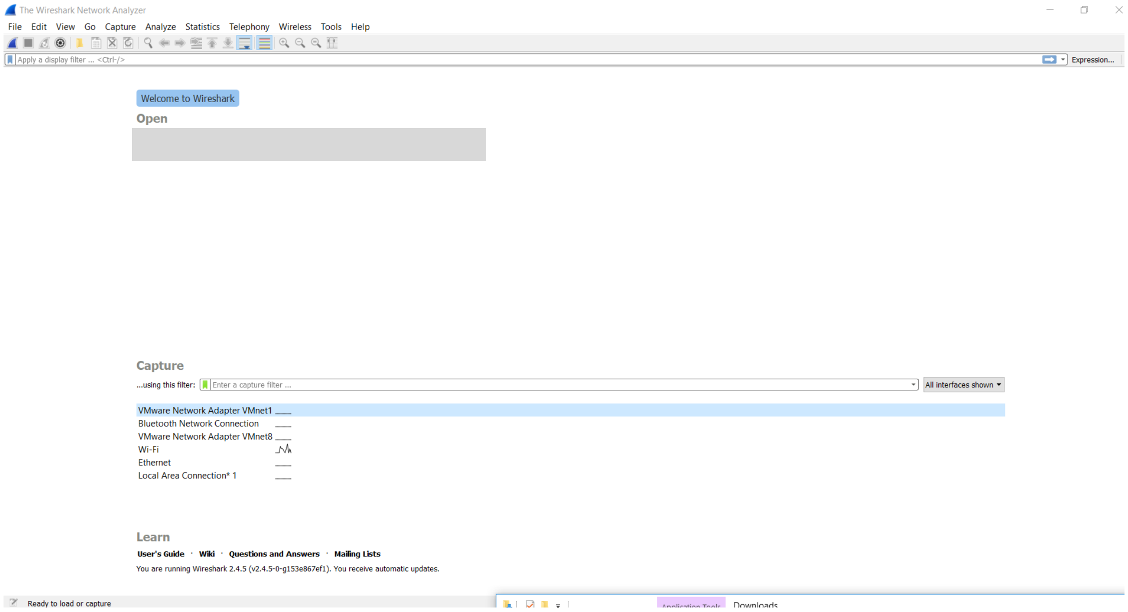
- **If it's still necessary for you to practise**, you can try analyzing **captured network-traffic logs** of a target machine. You can use a widely used **Wireshark** to analyse its PCAP files and analyze the network traffic.
- Please download three sample `.pcapng` files from: https://drive.google.com/file/d/1f2rD8FoiEAQYBtrryd583HfgWGjW9oDw/view?usp=sharing.

Task 2-1: Analyzing DNS Traffic Logs

Steps:

1. Download and install Wireshark (and its dependencies) from https://www.wireshark.org/
2. Launch Wireshark.

   You will see a main window similar to the one shown below.



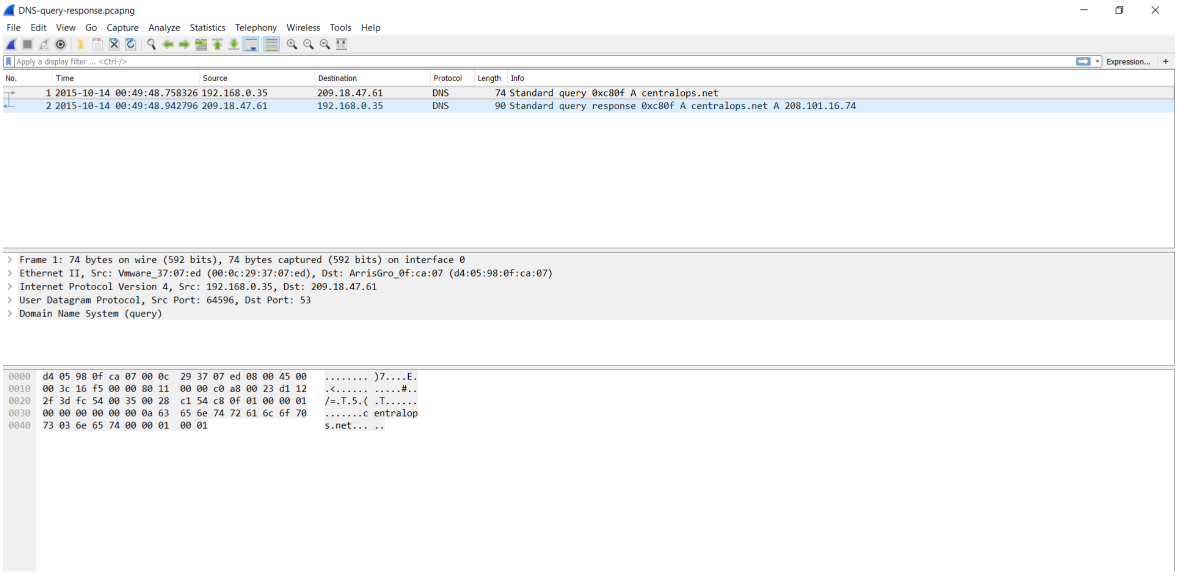
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Open
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Application Tools
Downloads

VMware Network Adapter VMnet1
Bluetooth Network Connection
VMware Network Adapter VMnet8
Wi-Fi
Ethernet
Local Area Connection* 1

You are running Wireshark 2.4.5 (v2.4.5-0-g153e867ef1). You receive automatic updates.

Ready to load or capture

3. From the main menu, select " File → Open", and then open the file named `DNS-query-response.pcapng` which you have downloaded from the shared folder. The captured packets will be opened and displayed as shown below. Clicking on a packet in the "Packet List" pane will display the details of that packet in both the "Packet Details" pane and "Packet Bytes" pane.


DNS-query-response.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

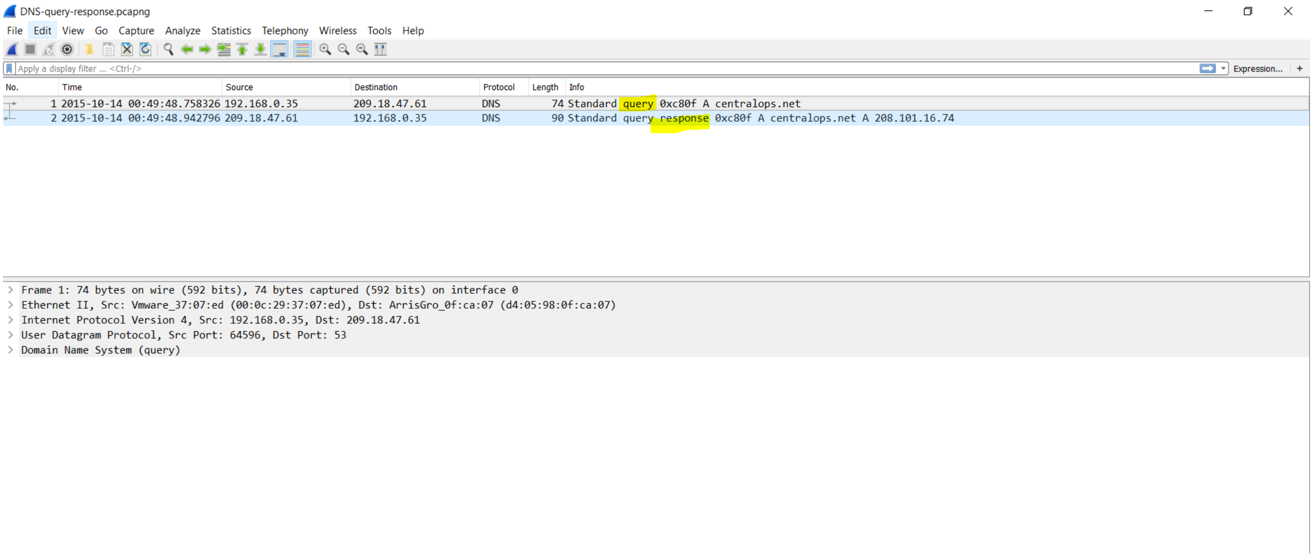
```
No.  Time                       Source         Destination    Protocol Length Info
   1 2015-10-14 00:49:48.758326 192.168.0.35   209.18.47.61   DNS          74 Standard query 0xc80f A centralops.net
   2 2015-10-14 00:49:48.942796 209.18.47.61   192.168.0.35   DNS          90 Standard query response 0xc80f A centralops.net A 208.101.16.74
```

```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Vmware_37:07:ed (00:0c:29:37:07:ed), Dst: ArrisGro_0f:ca:07 (d4:05:98:0f:ca:07)
> Internet Protocol Version 4, Src: 192.168.0.35, Dst: 209.18.47.61
> User Datagram Protocol, Src Port: 64596, Dst Port: 53
> Domain Name System (query)
```

```
0000  d4 05 98 0f ca 07 00 0c  29 37 07 ed 08 00 45 00   ........ )7....E.
0010  00 3c 16 f5 00 00 80 11  00 00 c0 a8 00 23 d1 12   .<...... .....#..
0020  2f 3d fc 54 00 35 00 28  c1 54 c8 0f 01 00 00 01   /=.T.5.( .T......
0030  00 00 00 00 00 00 0a 63  65 6e 74 72 61 6c 6f 70   .......c entralop
0040  73 03 6e 65 74 00 00 01  00 01                     s.net... ..
```

4. Analyse the details of the packet in the "Packet List" plane by clicking on Frame 1, Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System. Answer the queries below.

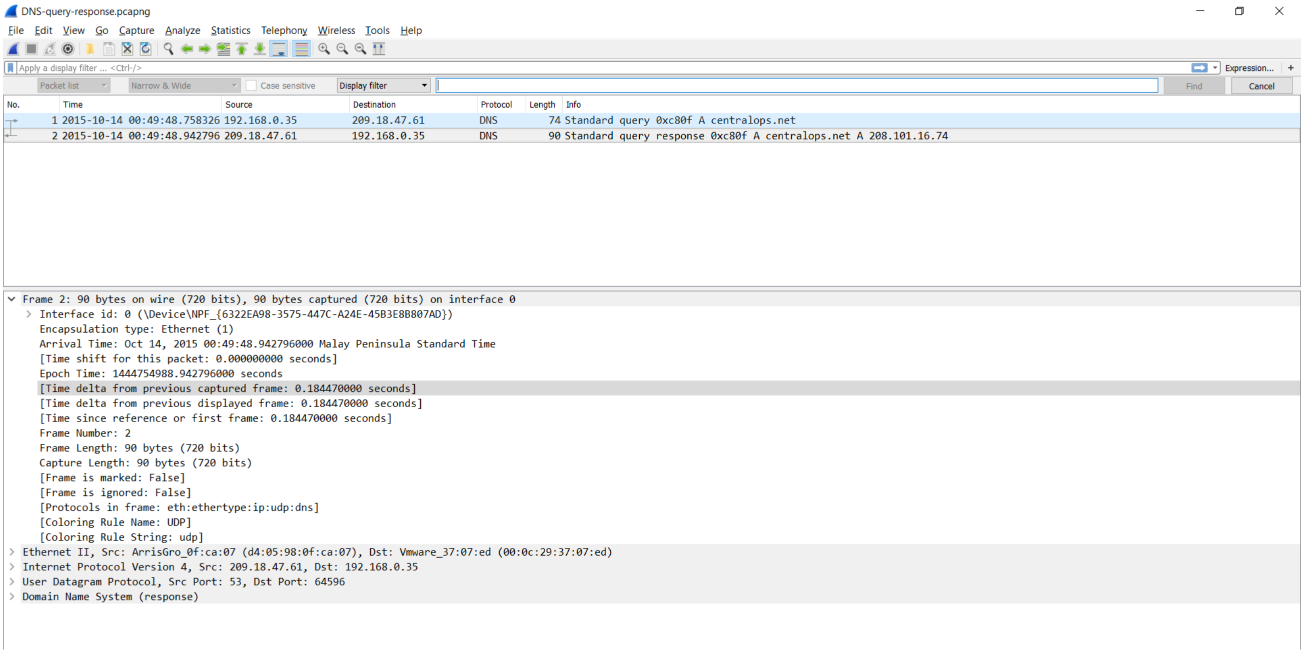
5. How many packets are involved in the DNS query?


DNS-query-response.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time                       Source         Destination    Protocol Length Info
   1 2015-10-14 00:49:48.758326 192.168.0.35   209.18.47.61   DNS          74 Standard query 0xc80f A centralops.net
   2 2015-10-14 00:49:48.942796 209.18.47.61   192.168.0.35   DNS          90 Standard query response 0xc80f A centralops.net A 208.101.16.74
```

```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Vmware_37:07:ed (00:0c:29:37:07:ed), Dst: ArrisGro_0f:ca:07 (d4:05:98:0f:ca:07)
> Internet Protocol Version 4, Src: 192.168.0.35, Dst: 209.18.47.61
> User Datagram Protocol, Src Port: 64596, Dst Port: 53
> Domain Name System (query)
```

6. How long did it take to get a response for the DNS query?


DNS-query-response.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

```
No.  Time                        Source         Destination    Protocol  Length  Info
   1 2015-10-14 00:49:48.758326 192.168.0.35   209.18.47.61   DNS           74 Standard query 0xc80f A centralops.net
   2 2015-10-14 00:49:48.942796 209.18.47.61   192.168.0.35   DNS           90 Standard query response 0xc80f A centralops.net A 208.101.16.74
```

```
Frame 2: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
  Interface id: 0 (\Device\NPF_{6322EA98-3575-447C-A24E-45B3E8B807AD})
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct 14, 2015 00:49:48.942796000 Malay Peninsula Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1444754988.942796000 seconds
  [Time delta from previous captured frame: 0.184470000 seconds]
  [Time delta from previous displayed frame: 0.184470000 seconds]
  [Time since reference or first frame: 0.184470000 seconds]
  Frame Number: 2
  Frame Length: 90 bytes (720 bits)
  Capture Length: 90 bytes (720 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:dns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
Ethernet II, Src: ArrisGro_0f:ca:07 (d4:05:98:0f:ca:07), Dst: Vmware_37:07:ed (00:0c:29:37:07:ed)
Internet Protocol Version 4, Src: 209.18.47.61, Dst: 192.168.0.35
User Datagram Protocol, Src Port: 53, Dst Port: 64596
Domain Name System (response)
```

7. What is the IP address of the host which submitted DNS query?

8. What is the IP address of the DNS server?

9. Based on the information contained in the packet details, what protocol is used for DNS query and what is the destination port?

10. What domain name was sought to be resolved by the query?

11. To what IP address did the domain name resolved to?

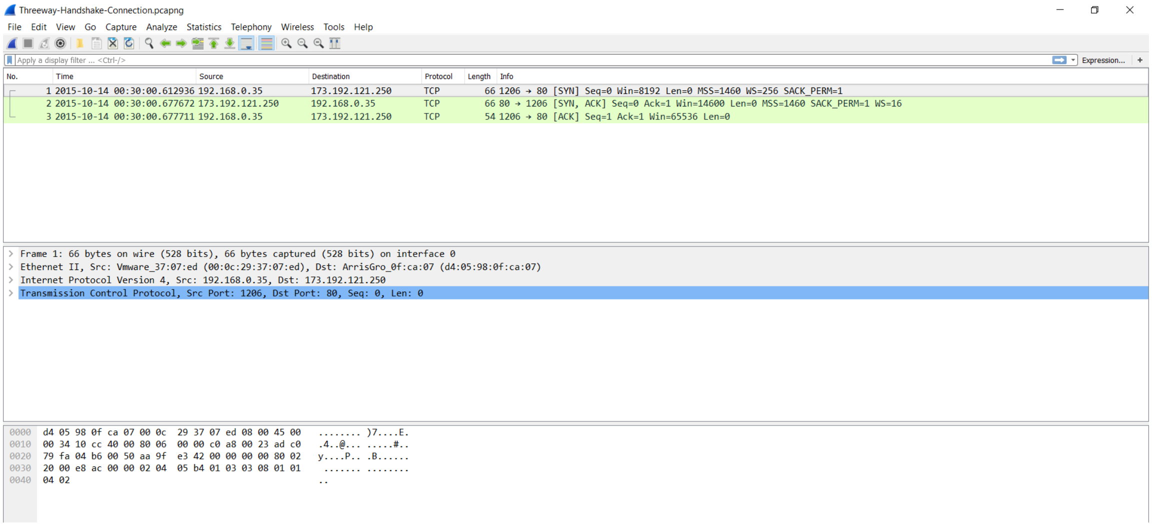
Task 2-2: Analyzing Three-Way Handshake Traffic Logs

Steps:

1. Launch Wireshark (if still needed).

2. Open the file `Threeway-handshake-connection.pcapng`.

   The captured logs will appear as shown below.


Threeway-Handshake-Connection.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time                       Source           Destination      Protocol Length Info
    1 2015-10-14 00:30:00.612936 192.168.0.35     173.192.121.250  TCP      66 1206 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    2 2015-10-14 00:30:00.677672 173.192.121.250  192.168.0.35     TCP      66 80 → 1206 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
    3 2015-10-14 00:30:00.677711 192.168.0.35     173.192.121.250  TCP      54 1206 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_37:07:ed (00:0c:29:37:07:ed), Dst: ArrisGro_0f:ca:07 (d4:05:98:0f:ca:07)
> Internet Protocol Version 4, Src: 192.168.0.35, Dst: 173.192.121.250
> Transmission Control Protocol, Src Port: 1206, Dst Port: 80, Seq: 0, Len: 0
```

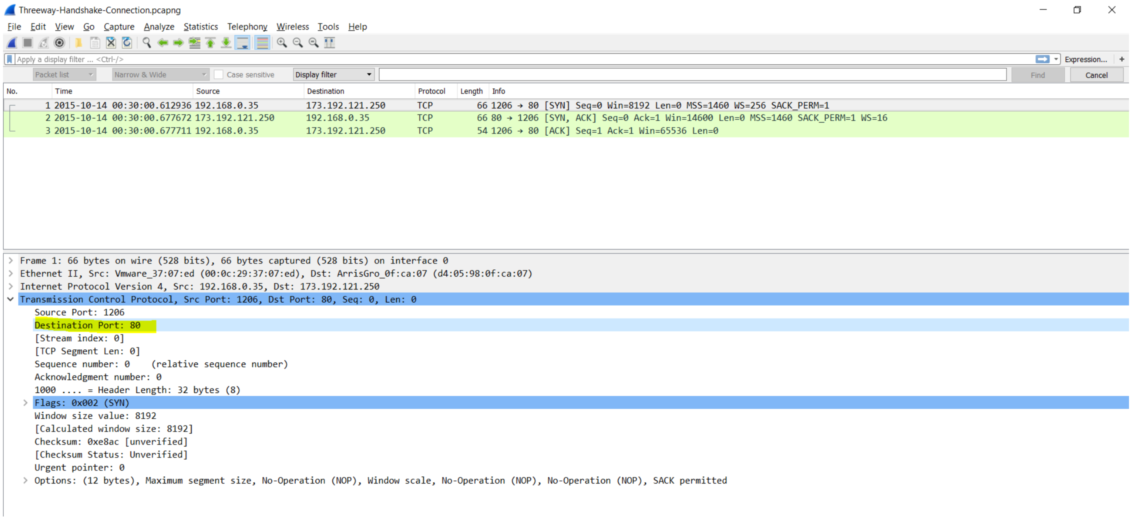
```
0000  d4 05 98 0f ca 07 00 0c  29 37 07 ed 08 00 45 00   ........ )7....E.
0010  00 34 10 cc 40 00 80 06  00 00 c0 a8 00 23 ad c0   .4..@... .....#..
0020  79 fa 04 b6 00 50 aa 9f  e3 42 00 00 00 00 80 02   y....P.. .B......
0030  20 00 e8 ac 00 00 02 04  05 b4 01 03 03 08 01 01    ....... ........
0040  04 02                                              ..
```

3. Inspect the packets to answer the following questions.

4. What is the IP address of the host initiating the TCP handshake,

   and what is the IP address of the host that responds to the initial request.

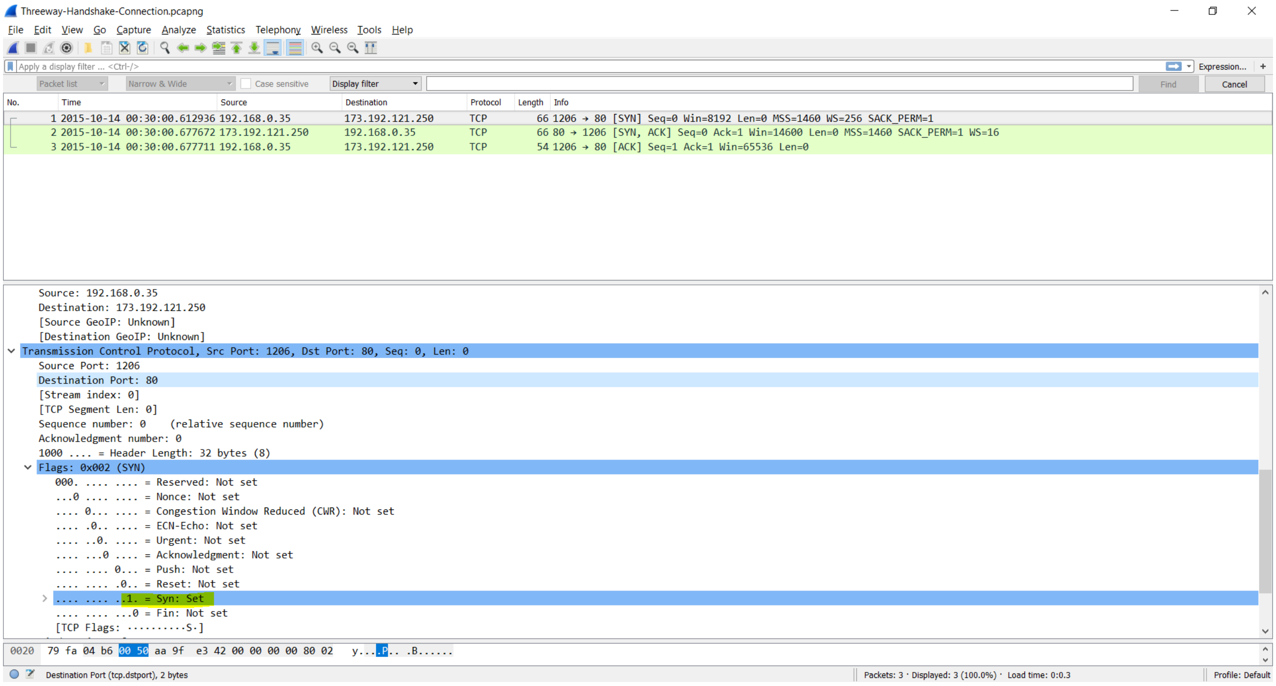
5. What possible type was the server to which the connection being established?


Threeway-Handshake-Connection.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

```
No.   Time                       Source           Destination      Protocol Length Info
    1 2015-10-14 00:30:00.612936 192.168.0.35     173.192.121.250  TCP      66 1206 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    2 2015-10-14 00:30:00.677672 173.192.121.250  192.168.0.35     TCP      66 80 → 1206 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
    3 2015-10-14 00:30:00.677711 192.168.0.35     173.192.121.250  TCP      54 1206 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_37:07:ed (00:0c:29:37:07:ed), Dst: ArrisGro_0f:ca:07 (d4:05:98:0f:ca:07)
> Internet Protocol Version 4, Src: 192.168.0.35, Dst: 173.192.121.250
v Transmission Control Protocol, Src Port: 1206, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 1206
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0xe8ac [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
```

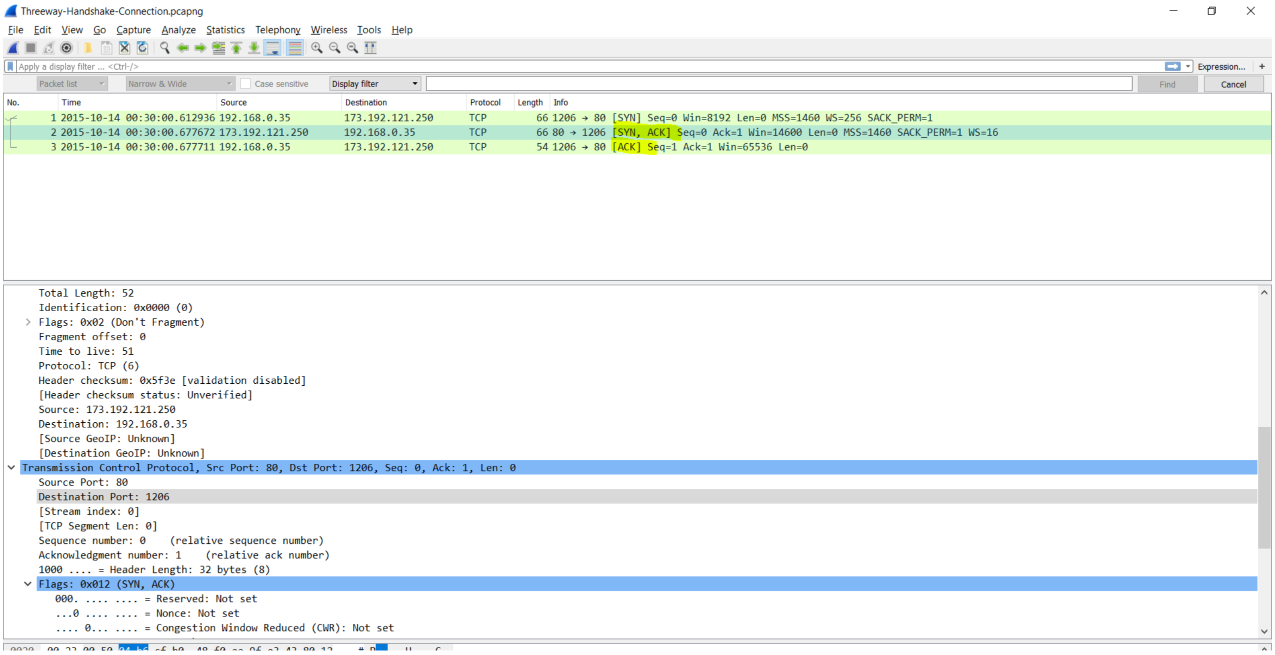
6. Based on the information in the packet details pane, which flag is set on the first packet of the conducted TCP three-way handshake?


Threeway-Handshake-Connection.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

```
No.  Time                        Source          Destination     Protocol Length Info
   1 2015-10-14 00:30:00.612936 192.168.0.35    173.192.121.250 TCP      66 1206 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   2 2015-10-14 00:30:00.677672 173.192.121.250 192.168.0.35    TCP      66 80 → 1206 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
   3 2015-10-14 00:30:00.677711 192.168.0.35    173.192.121.250 TCP      54 1206 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
    Source: 192.168.0.35
    Destination: 173.192.121.250
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 1206, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 1206
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ··········S·]
0020  79 fa 04 b6 00 50 aa 9f  e3 42 00 00 00 00 80 02   y....P.. .B......
Destination Port (tcp.dstport), 2 bytes    Packets: 3 · Displayed: 3 (100.0%) · Load time: 0:0.3    Profile: Default
```

7. Based on the information in the packet list plane, which are the flags for the second and third packets of the conducted TCP three-way handshake?


Threeway-Handshake-Connection.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

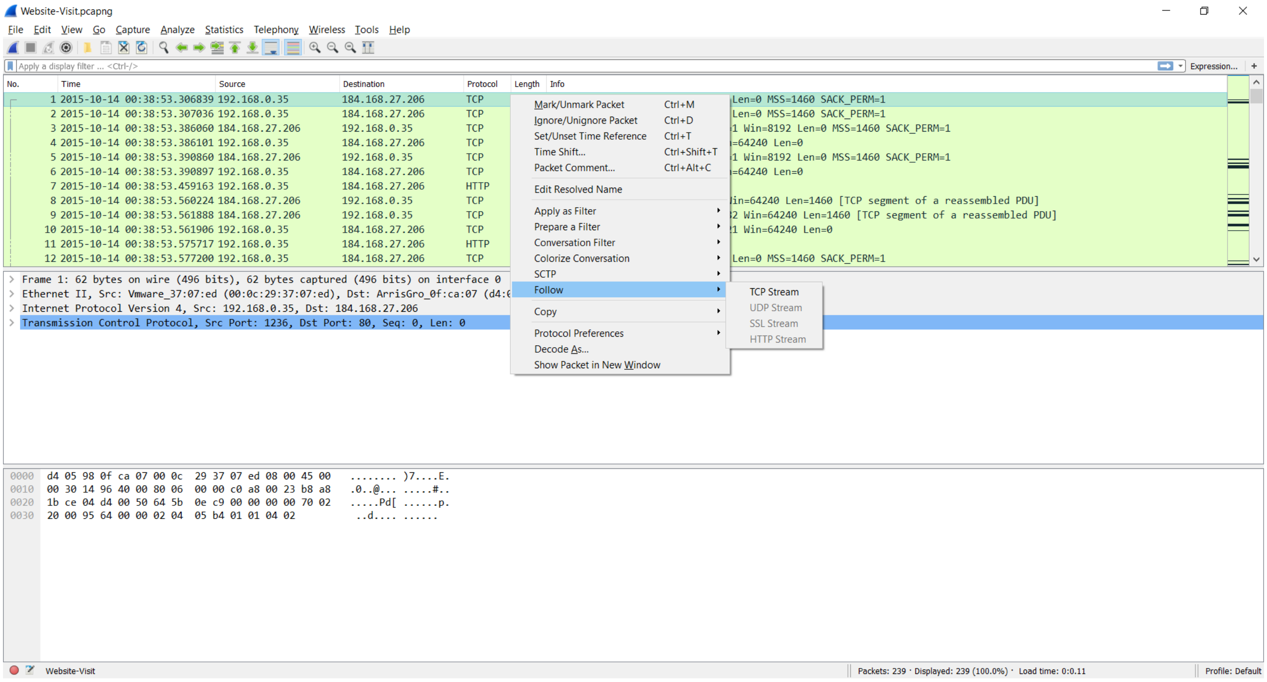
```
No.  Time                        Source          Destination     Protocol Length Info
   1 2015-10-14 00:30:00.612936 192.168.0.35    173.192.121.250 TCP      66 1206 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   2 2015-10-14 00:30:00.677672 173.192.121.250 192.168.0.35    TCP      66 80 → 1206 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
   3 2015-10-14 00:30:00.677711 192.168.0.35    173.192.121.250 TCP      54 1206 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
    Total Length: 52
    Identification: 0x0000 (0)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 51
    Protocol: TCP (6)
    Header checksum: 0x5f3e [validation disabled]
    [Header checksum status: Unverified]
    Source: 173.192.121.250
    Destination: 192.168.0.35
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80, Dst Port: 1206, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1206
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
```

Task 2-3: Analyzing Website-Visit Traffic Logs

Steps:

1. Launch Wireshark (if still needed).
2. Open the file `Website-visit.pcapng`.
3. In the Packet List pane, right-click on the first packet, and then select “Follow TCP stream” from the pull-down menu as shown below.


Website-Visit.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
HTTP Stream
Website-Visit
Packets: 239 · Displayed: 239 (100.0%) · Load time: 0:0.11
Profile: Default

```
No.   Time                       Source          Destination     Protocol  Length  Info
   1 2015-10-14 00:38:53.306839 192.168.0.35    184.168.27.206  TCP       Len=0 MSS=1460 SACK_PERM=1
   2 2015-10-14 00:38:53.307036 192.168.0.35    184.168.27.206  TCP       Len=0 MSS=1460 SACK_PERM=1
   3 2015-10-14 00:38:53.386060 184.168.27.206  192.168.0.35    TCP       1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
   4 2015-10-14 00:38:53.386101 192.168.0.35    184.168.27.206  TCP       =64240 Len=0
   5 2015-10-14 00:38:53.390860 184.168.27.206  192.168.0.35    TCP       1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
   6 2015-10-14 00:38:53.390897 192.168.0.35    184.168.27.206  TCP       =64240 Len=0
   7 2015-10-14 00:38:53.459163 192.168.0.35    184.168.27.206  HTTP
   8 2015-10-14 00:38:53.560224 184.168.27.206  192.168.0.35    TCP       in=64240 Len=1460 [TCP segment of a reassembled PDU]
   9 2015-10-14 00:38:53.561888 184.168.27.206  192.168.0.35    TCP       2 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
  10 2015-10-14 00:38:53.561906 192.168.0.35    184.168.27.206  TCP       1 Win=64240 Len=0
  11 2015-10-14 00:38:53.575717 192.168.0.35    184.168.27.206  HTTP
  12 2015-10-14 00:38:53.577200 192.168.0.35    184.168.27.206  TCP       Len=0 MSS=1460 SACK_PERM=1
```

```
> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
> Ethernet II, Src: Vmware_37:07:ed (00:0c:29:37:07:ed), Dst: ArrisGro_0f:ca:07 (d4:0
> Internet Protocol Version 4, Src: 192.168.0.35, Dst: 184.168.27.206
> Transmission Control Protocol, Src Port: 1236, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  d4 05 98 0f ca 07 00 0c  29 37 07 ed 08 00 45 00   ........ )7....E.
0010  00 30 14 96 40 00 80 06  00 00 c0 a8 00 23 b8 a8   .0..@... .....#..
0020  1b ce 04 d4 00 50 64 5b  0e c9 00 00 00 00 70 02   .....Pd[ ......p.
0030  20 00 95 64 00 00 02 04  05 b4 01 01 04 02          ..d.... ......
```

4. Inspect the results, and answer the following questions.
   a. What is the name of the website that was visited?
   b. Was the connection to the website successful from the server’s point of view?
   c. What kind of web platform is being used to host the server?
   d. When was this webpage last updated by web author/provider?
   e. When was this particular webpage accessed?

Task 3: Extracting and Analyzing Objects from Network-Traffic Logs using Network Forensic Analysis Tools

Notes:

- In the next two sub-tasks, you want to extract and analyze objects/artefacts from captured network-traffic logs using two popular **Network Forensic Analysis Tools** (NFATs): **NetworkMiner** and **Xplico**.

Task 3-1 (Win/Lin-FWS): Extracting and Analyzing Objects from Network-Traffic Logs using NetworkMiner

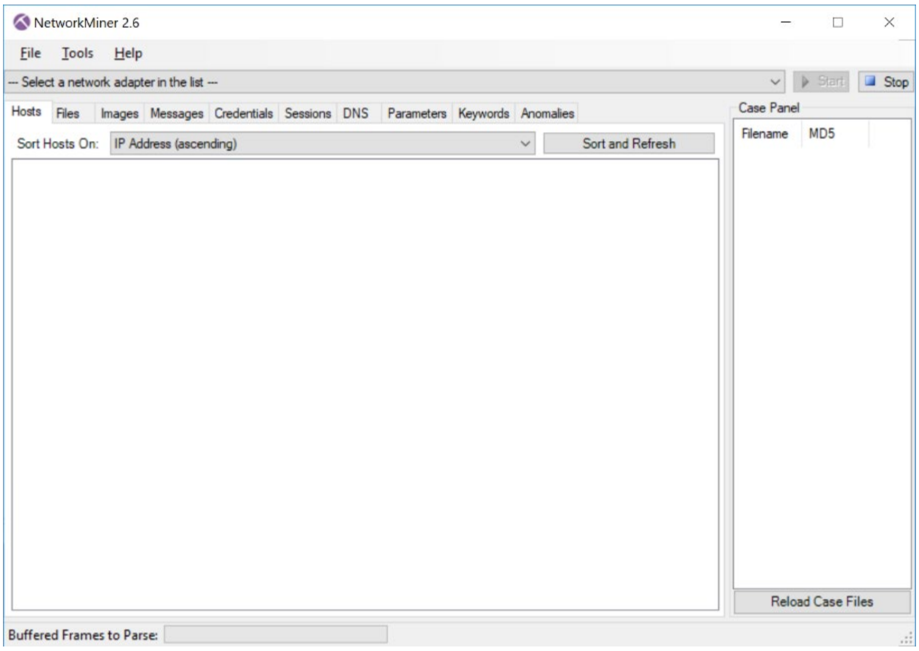
Notes:

- ***NetworkMiner*** runs on several Operating Systems. Hence, you can use either your Windows or Linux forensics workstation. The steps below, however, show how NetworkMiner runs in **Windows**.
- You can reuse the sample `.pcapng` files from Task 2. However, NetworkMiner Free Edition can't parse **PcapNG** files. Nevertheless, it can parse **PCAP** files. Hence, you can utilize a tool, e.g. Wireshark, that can convert the sample file into a PCAP file format.

Steps:

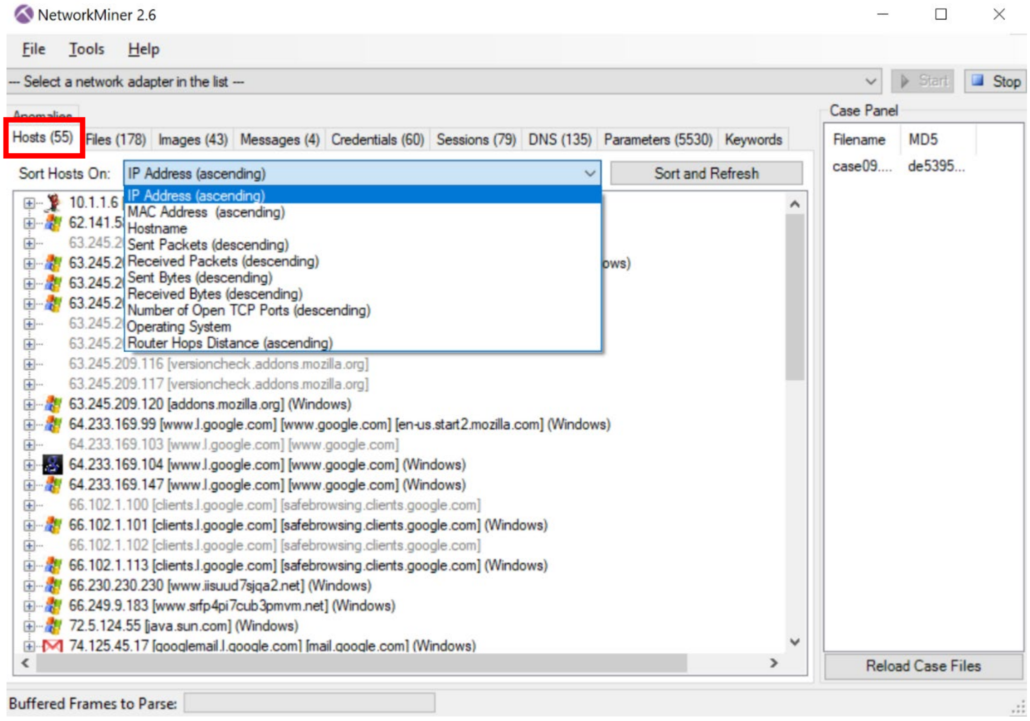
1. **Download** NetworkMiner from: https://www.netresec.com/?page=networkminer and extract its zip file. (***Note***: To install NetworkMiner on your Linux machine, you can follow the steps mentioned in https://www.netresec.com/?page=Blog&month=2014-02&post=HowTo-install-NetworkMiner-in-Ubuntu-Fedora-and-Arch-Linux).

2. Run NetworkMiner by clicking its executable until you can see its window:



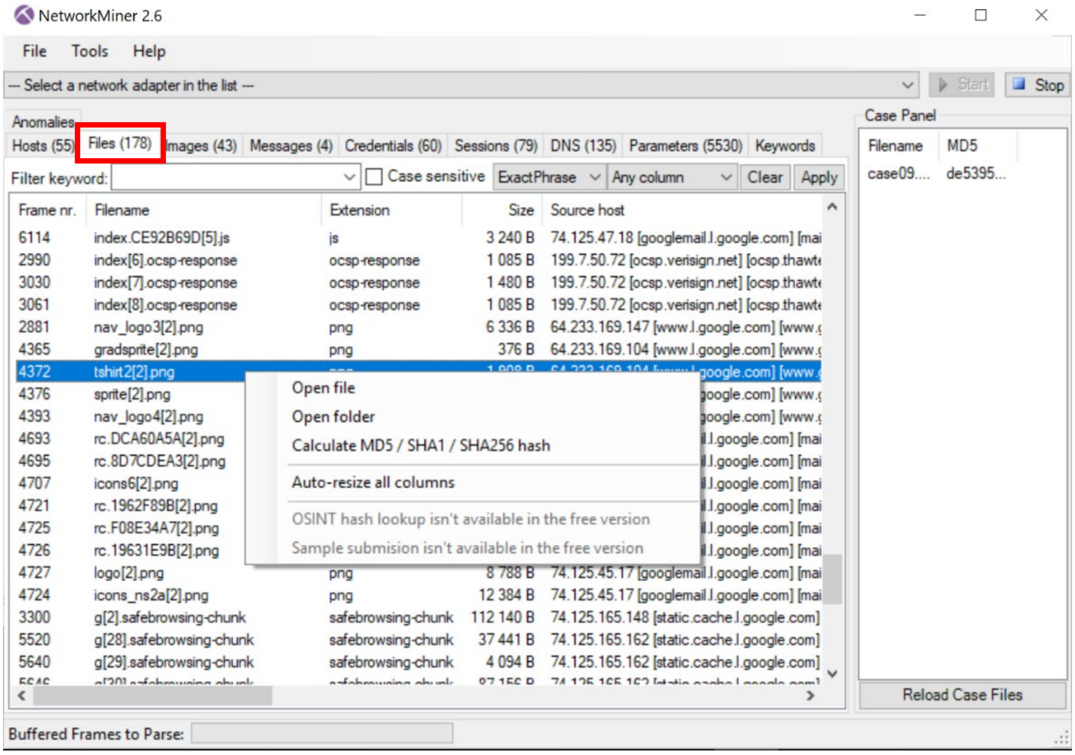
3. Select File and then open your PCAP file. NetworkMiner will process the file and, upon completion, show the mining results in its several tabs.

4. Inspect its ***Hosts* tab** as shown below. You can **sort** all the identified hosts based on various possible criteria as shown below.



```
10.1.1.6
62.141.5
63.245.2
63.245.2                                                ows)
63.245.2
63.245.2
63.245.2
63.245.2
63.245.209.116 [versioncheck.addons.mozilla.org]
63.245.209.117 [versioncheck.addons.mozilla.org]
63.245.209.120 [addons.mozilla.org] (Windows)
64.233.169.99 [www.l.google.com] [www.google.com] [en-us.start2.mozilla.com] (Windows)
64.233.169.103 [www.l.google.com] [www.google.com]
64.233.169.104 [www.l.google.com] [www.google.com] (Windows)
64.233.169.147 [www.l.google.com] [www.google.com] (Windows)
66.102.1.100 [clients.l.google.com] [safebrowsing.clients.google.com]
66.102.1.101 [clients.l.google.com] [safebrowsing.clients.google.com] (Windows)
66.102.1.102 [clients.l.google.com] [safebrowsing.clients.google.com]
66.102.1.113 [clients.l.google.com] [safebrowsing.clients.google.com] (Windows)
66.230.230.230 [www.iisuud7sjqa2.net] (Windows)
66.249.9.183 [www.srfp4pi7cub3pmvm.net] (Windows)
72.5.124.55 [java.sun.com] (Windows)
74.125.45.17 [googlemail.l.google.com] [mail.google.com] (Windows)
```

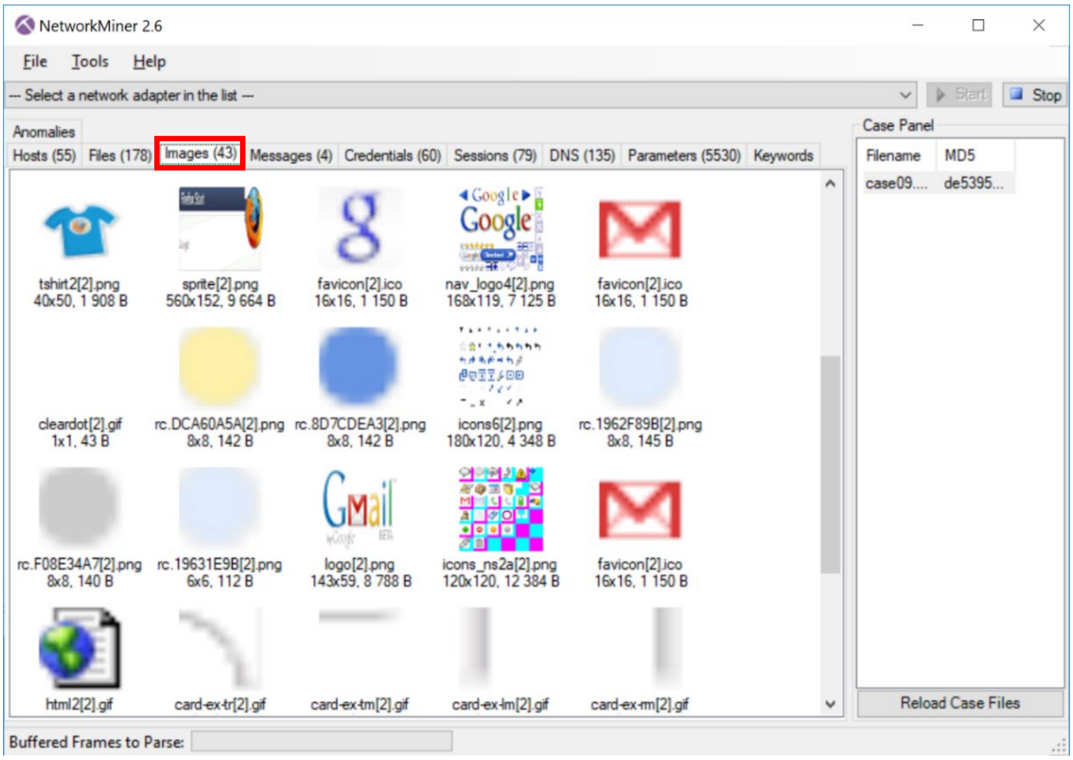
5. Now, inspect its ***Files* tab** as shown below. You can right-click on a listed file to open it (*be careful when opening an executable!*) or calculate its hash values.



Frame nr.	Filename	Extension	Size	Source host
6114	index.CE92B69D[5].js	js	3 240 B	74.125.47.18 [googlemail.l.google.com] [mai
2990	index[6].ocsp-response	ocsp-response	1 085 B	199.7.50.72 [ocsp.verisign.net] [ocsp.thawte
3030	index[7].ocsp-response	ocsp-response	1 480 B	199.7.50.72 [ocsp.verisign.net] [ocsp.thawte
3061	index[8].ocsp-response	ocsp-response	1 085 B	199.7.50.72 [ocsp.verisign.net] [ocsp.thawte
2881	nav_logo3[2].png	png	6 336 B	64.233.169.147 [www.l.google.com] [www.
4365	gradsprite[2].png	png	376 B	64.233.169.104 [www.l.google.com] [www.
4372	tshirt2[2].png			google.com] [www.
4376	sprite[2].png			google.com] [www.
4393	nav_logo4[2].png			google.com] [www.
4693	rc.DCA60A5A[2].png			l.google.com] [mai
4695	rc.8D7CDEA3[2].png			l.google.com] [mai
4707	icons6[2].png			l.google.com] [mai
4721	rc.1962F89B[2].png			l.google.com] [mai
4725	rc.F08E34A7[2].png			l.google.com] [mai
4726	rc.19631E9B[2].png			l.google.com] [mai
4727	logo[2].png	png	8 788 B	74.125.45.17 [googlemail.l.google.com] [mai
4724	icons_ns2a[2].png	png	12 384 B	74.125.45.17 [googlemail.l.google.com] [mai
3300	g[2].safebrowsing-chunk	safebrowsing-chunk	112 140 B	74.125.165.148 [static.cache.l.google.com]
5520	g[28].safebrowsing-chunk	safebrowsing-chunk	37 441 B	74.125.165.162 [static.cache.l.google.com]
5640	g[29].safebrowsing-chunk	safebrowsing-chunk	4 094 B	74.125.165.162 [static.cache.l.google.com]

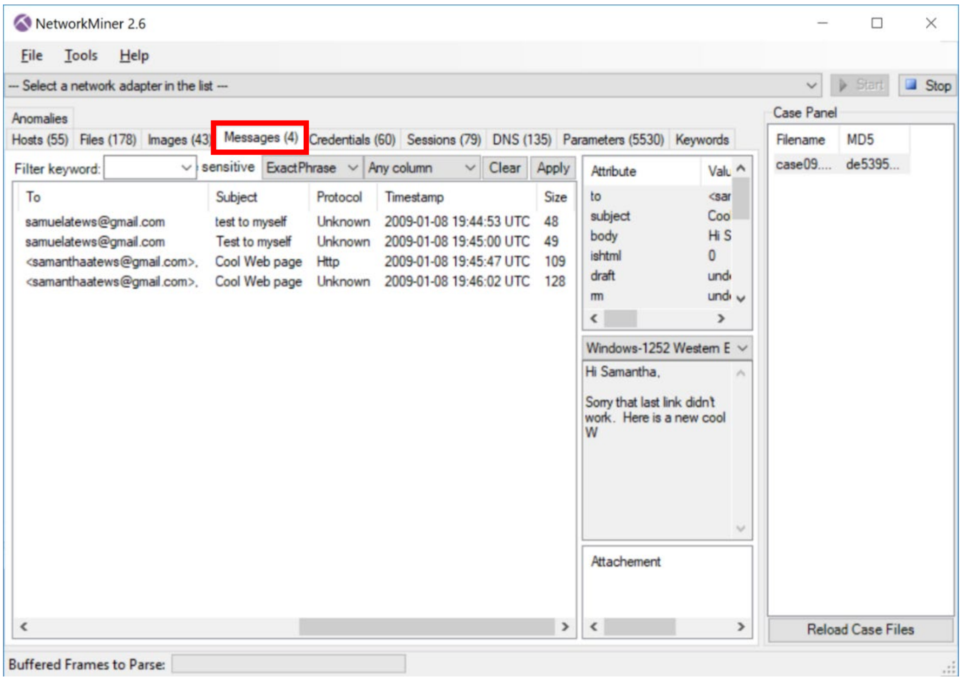
Filename	MD5
case09....	de5395...

6. Inspect its ***Images* tab** to see all identified image files.


NetworkMiner 2.6
File Tools Help
--- Select a network adapter in the list ---
Start
Stop
Anomalies
Hosts (55)
Files (178)
Images (43)
Messages (4)
Credentials (60)
Sessions (79)
DNS (135)
Parameters (5530)
Keywords
tshirt2[2].png 40x50, 1 908 B
sprite[2].png 560x152, 9 664 B
favicon[2].ico 16x16, 1 150 B
nav_logo4[2].png 168x119, 7 125 B
favicon[2].ico 16x16, 1 150 B
cleardot[2].gif 1x1, 43 B
rc.DCA60A5A[2].png 8x8, 142 B
rc.8D7CDEA3[2].png 8x8, 142 B
icons6[2].png 180x120, 4 348 B
rc.1962F89B[2].png 8x8, 145 B
rc.F08E34A7[2].png 8x8, 140 B
rc.19631E9B[2].png 6x6, 112 B
logo[2].png 143x59, 8 788 B
icons_ns2a[2].png 120x120, 12 384 B
favicon[2].ico 16x16, 1 150 B
html2[2].gif
card-ex-tr[2].gif
card-ex-tm[2].gif
card-ex-lm[2].gif
card-ex-rm[2].gif
Case Panel
Reload Case Files
Buffered Frames to Parse:

Filename	MD5
case09....	de5395...

7. Inspect its ***Messages* tab** to see all mined messages.


NetworkMiner 2.6
File Tools Help
--- Select a network adapter in the list ---
Start
Stop
Anomalies
Hosts (55) Files (178) Images (43) Messages (4) Credentials (60) Sessions (79) DNS (135) Parameters (5530) Keywords
Filter keyword:
sensitive
ExactPhrase
Any column
Clear
Apply
Case Panel
Windows-1252 Western E
Attachement
Reload Case Files
Buffered Frames to Parse:

To	Subject	Protocol	Timestamp	Size
samuelatews@gmail.com	test to myself	Unknown	2009-01-08 19:44:53 UTC	48
samuelatews@gmail.com	Test to myself	Unknown	2009-01-08 19:45:00 UTC	49
<samanthaatews@gmail.com>,	Cool Web page	Http	2009-01-08 19:45:47 UTC	109
<samanthaatews@gmail.com>,	Cool Web page	Unknown	2009-01-08 19:46:02 UTC	128

Attribute	Valu
to	<sar
subject	Coo
body	Hi S
ishtml	0
draft	und
rm	und

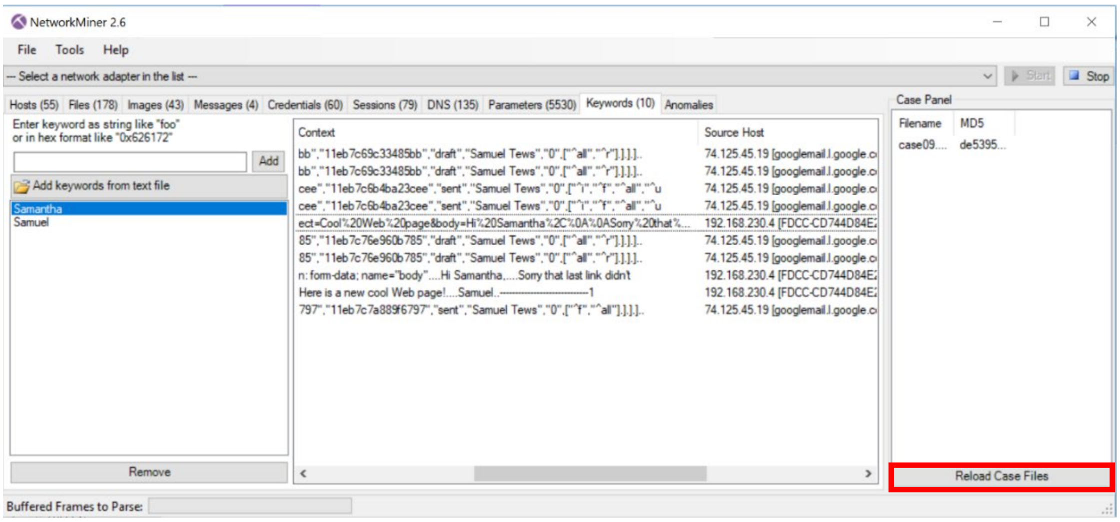
Hi Samantha,

Sorry that last link didn't work. Here is a new cool W

Filename	MD5
case09....	de5395...

8. Do inspect all ***other tabs*** for other mined object types, including **credentials**.

9. Lastly, let us perform a ***keyword matching*** on all the mined objects. Open its ***Keywords* tab**, and then add some keywords into the list of keywords to search. In the example below, two keywords "`Samantha`" and "`Samuel`" are added. (***Note***: After entering your keywords, you will need to click the "Reload Case Files" button at the bottom right of your NetworkMiner's window).
Do check the results shown to see if you can find any interesting findings.


NetworkMiner 2.6
File Tools Help
--- Select a network adapter in the list ---
Start
Stop
Hosts (55) Files (178) Images (43) Messages (4) Credentials (60) Sessions (79) DNS (135) Parameters (5530) Keywords (10) Anomalies
Add
Add keywords from text file
Remove
Case Panel
Reload Case Files
Buffered Frames to Parse:

Enter keyword as string like "foo"
or in hex format like "0x626172"

Samantha
Samuel

Context	Source Host
bb","11eb7c69c33485bb","draft","Samuel Tews","0",["^all","^r"]]]]..	74.125.45.19 [googlemail.l.google.c
bb","11eb7c69c33485bb","draft","Samuel Tews","0",["^all","^r"]]]]..	74.125.45.19 [googlemail.l.google.c
cee","11eb7c6b4ba23cee","sent","Samuel Tews","0",["^i","^f","^all","^u	74.125.45.19 [googlemail.l.google.c
cee","11eb7c6b4ba23cee","sent","Samuel Tews","0",["^i","^f","^all","^u	74.125.45.19 [googlemail.l.google.c
ect=Cool%20Web%20page&body=Hi%20Samantha%2C%0A%0ASorry%20that%...	192.168.230.4 [FDCC-CD744D84E
85","11eb7c76e960b785","draft","Samuel Tews","0",["^all","^r"]]]]..	74.125.45.19 [googlemail.l.google.c
85","11eb7c76e960b785","draft","Samuel Tews","0",["^all","^r"]]]]..	74.125.45.19 [googlemail.l.google.c
n: form-data; name="body"....Hi Samantha,....Sorry that last link didn't	192.168.230.4 [FDCC-CD744D84E
Here is a new cool Web page!....Samuel..------------------------------1	192.168.230.4 [FDCC-CD744D84E
797","11eb7c7a889f6797","sent","Samuel Tews","0",["^f","^all"]]]]..	74.125.45.19 [googlemail.l.google.c

Filename	MD5
case09....	de5395...

[Optional] Task 3-2 (Lin-FWS): Extracting and Analyzing Captured Network Traffic Logs using Xplico

Notes:

- You can use an **Ubuntu** (or any Debian-based) **machine** as your forensic workstation, and follow Step 1 below to install Xplico. Alternatively, you can create a VM by importing an OVA file as described in Step 2.
- You can reuse the three sample `.pcapng` files from Task 3. However, note that Xplico does **not** seem to accept a filename containing "–" characters. Hence, do rename the files by removing all "–" characters in the filenames. Alternatively, other sample `.pcap` files are available, such as one from https://web.archive.org/web/20160604152628/http://www.taosecurity.com/tws2_blog_sample_28feb09a.zip.

Steps:

1. **Install Xplico** using the following series of commands (see also: https://www.xplico.org/download):

```
sudo bash -c 'echo "deb http://repo.xplico.org/ $(lsb_release -s -c) main" >> /etc/apt/sources.list'
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 791C25CE
sudo apt-get update
sudo apt-get install xplico
```

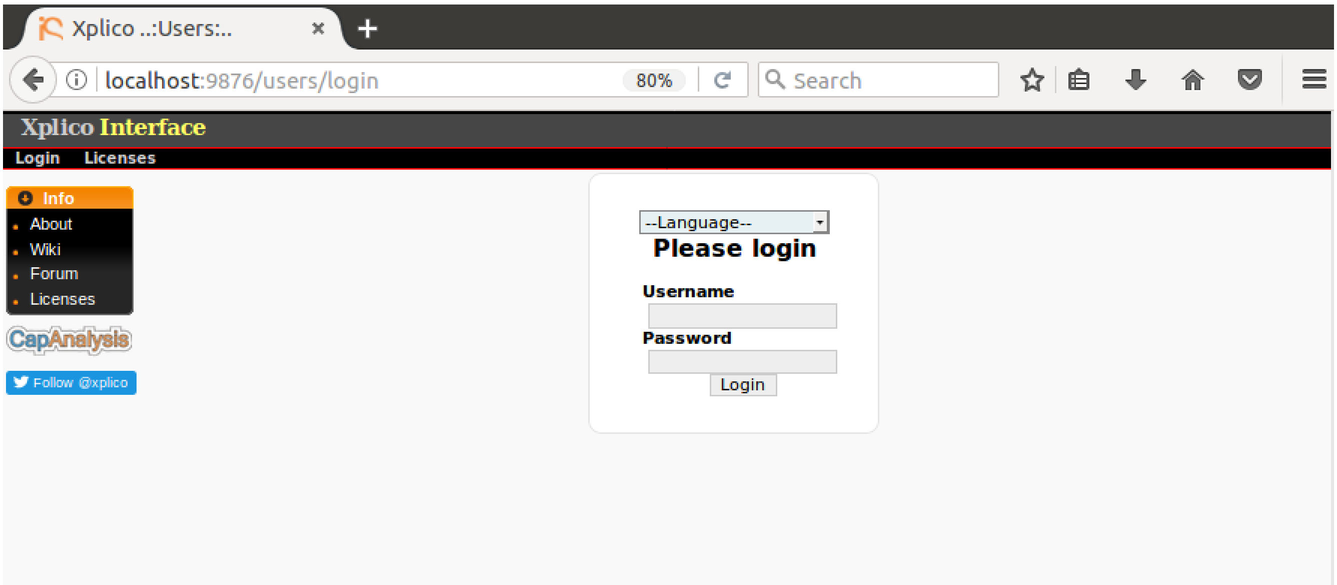
2. Alternatively, you can **download** an OVA file from: https://sourceforge.net/projects/xplico/files/VirtualBox%20images/.
   The OVA file has also been cached for our module students at: https://drive.google.com/file/d/1yCtT0ZBoQDvNzC2eomROoyz6iCoNMjai/view?usp=sharing.

Using VirtualBox, do **import** the OVA file into a VM, and then run the VM. Use the following credential to **access** the Linux host: username="`ubuntu`" and password="`reverse`".

3. **Run Xplico** by invoking the following (if still needed):

```
sudo /etc/init.d/xplico start
sudo /opt/xplico/script/sqlite_demo.sh
```

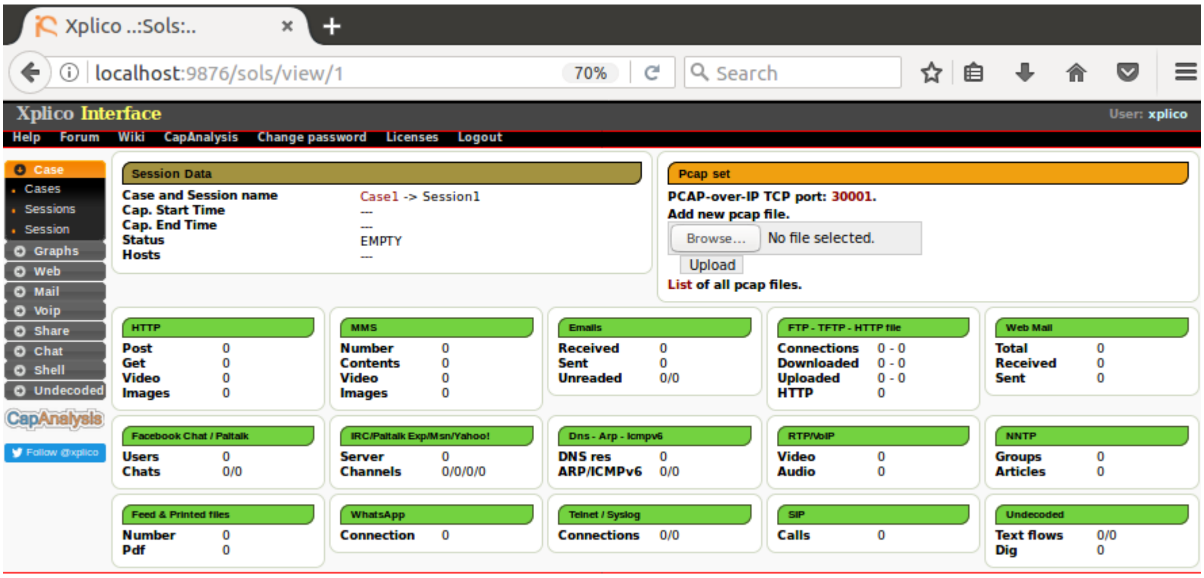
4. Launch your **browser**, and visit the following URL: localhost:9876. You should see the Xplico login page as shown below.



5. Login with the default username "`xplico`" and password "`xplico`".

6. Create a new **case** by clicking "Case: New Case", and then name your case. For the new case, you also have an option on whether you want to perform a live acquisition or upload **previously captured PCAP file(s).**

7. Within the case, create a new **session** by clicking "Case: New Session". You should then see the session's interface like the one shown below:



Session Data
Case and Session name: Case1 -> Session1
Cap. Start Time: ---
Cap. End Time: ---
Status: EMPTY
Hosts: ---

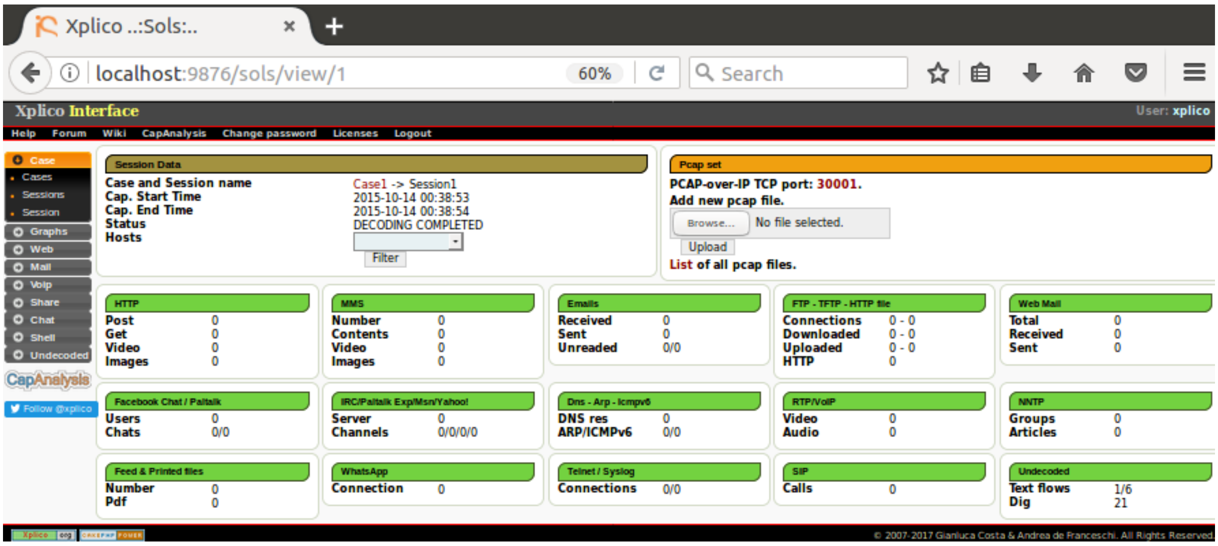
Pcap set
PCAP-over-IP TCP port: 30001.
Add new pcap file.
No file selected.
List of all pcap files.

HTTP: Post 0, Get 0, Video 0, Images 0
MMS: Number 0, Contents 0, Video 0, Images 0
Emails: Received 0, Sent 0, Unreaded 0/0
FTP - TFTP - HTTP file: Connections 0 - 0, Downloaded 0 - 0, Uploaded 0 - 0, HTTP 0
Web Mail: Total 0, Received 0, Sent 0
Facebook Chat / Paltalk: Users 0, Chats 0/0
IRC/Paltalk Exp/Msn/Yahoo!: Server 0, Channels 0/0/0/0
Dns - Arp - Icmpv6: DNS res 0, ARP/ICMPv6 0/0
RTP/VoIP: Video 0, Audio 0
NNTP: Groups 0, Articles 0
Feed & Printed files: Number 0, Pdf 0
WhatsApp: Connection 0
Telnet / Syslog: Connections 0/0
SIP: Calls 0
Undecoded: Text flows 0/0, Dig 0

8. Now, add/upload a new PCAP file.

9. Upon file uploading, Xplico will perform its decoding process on the file. Wait until the decoding process *fully completes* as indicated by Xplico.

10. Now, do check all different reported **network & web artefacts** by accessing the respective menu items, e.g. Graphs, Web & Mail, in the Case pane:



Session Data
Case and Session name: Case1 -> Session1
Cap. Start Time: 2015-10-14 00:38:53
Cap. End Time: 2015-10-14 00:38:54
Status: DECODING COMPLETED
Hosts

Pcap set
PCAP-over-IP TCP port: 30001.
Add new pcap file.
No file selected.
List of all pcap files.

HTTP: Post 0, Get 0, Video 0, Images 0
MMS: Number 0, Contents 0, Video 0, Images 0
Emails: Received 0, Sent 0, Unreaded 0/0
FTP - TFTP - HTTP file: Connections 0 - 0, Downloaded 0 - 0, Uploaded 0 - 0, HTTP 0
Web Mail: Total 0, Received 0, Sent 0
Facebook Chat / Paltalk: Users 0, Chats 0/0
IRC/Paltalk Exp/Msn/Yahoo!: Server 0, Channels 0/0/0/0
Dns - Arp - Icmpv6: DNS res 0, ARP/ICMPv6 0/0
RTP/VoIP: Video 0, Audio 0
NNTP: Groups 0, Articles 0
Feed & Printed files: Number 0, Pdf 0
WhatsApp: Connection 0
Telnet / Syslog: Connections 0/0
SIP: Calls 0
Undecoded: Text flows 1/6, Dig 21

Task 4 (Win-FWS): Analyzing Web Cache and History

Notes:

- Please download sample web cache and history files from: https://drive.google.com/file/d/1Mo8w7qpO4d3G5YoJRmMgJZu-oLlT4Cbv/view?usp=sharing.

Task 4-1: Extracting and Analyzing Chrome's Cache

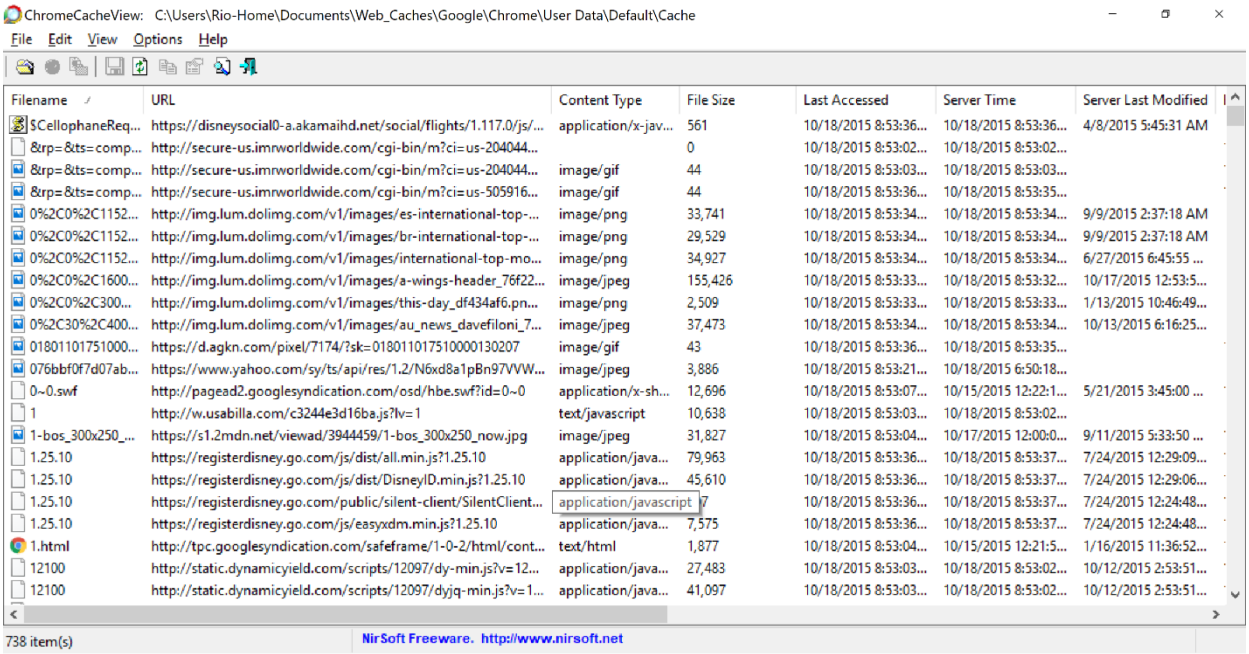
Steps:

1. Download **NirSoft's ChromeCacheView (CCV)** from https://www.nirsoft.net/utils/chrome_cache_view.html, and extract the zip file.

2. Launch CCV.

3. By default, it will point to the cache stored by the current user on the local machine: `C:\Users\`<*user-name*>`\AppData\Local\Google\Chrome\User Data\Default\Cache`.

4. To read an ***offline cache***, from the main menu, select "File", then "Select Cache Folder", and then browse to the following location of your downloaded cache file: `Web_Caches\Google\Chrome\User Data\Default\Cache`. CCV will show a window like the one below.



ChromeCacheView: C:\Users\Rio-Home\Documents\Web_Caches\Google\Chrome\User Data\Default\Cache

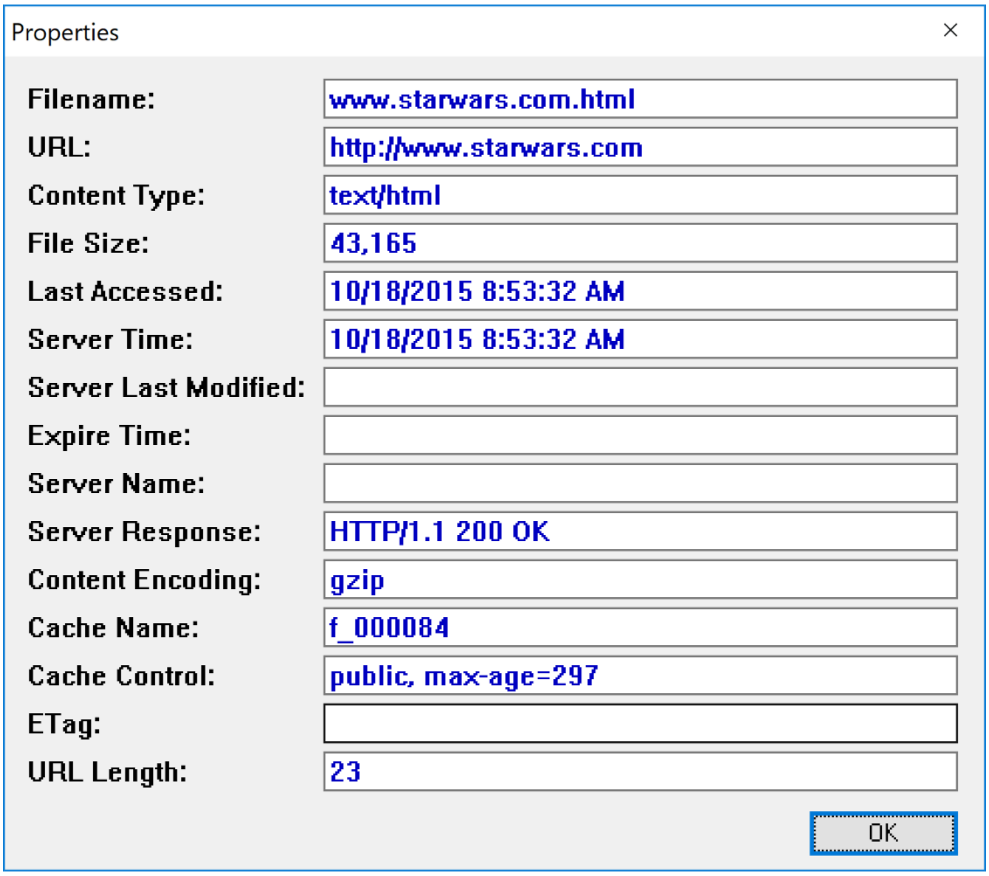
Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified
$CellophaneReq...	https://disneysocial0-a.akamaihd.net/social/flights/1.117.0/js/...	application/x-jav...	561	10/18/2015 8:53:36...	10/18/2015 8:53:36...	4/8/2015 5:45:31 AM
&rp=&ts=comp...	http://secure-us.imrworldwide.com/cgi-bin/m?ci=us-204044...		0	10/18/2015 8:53:02...	10/18/2015 8:53:02...	
&rp=&ts=comp...	http://secure-us.imrworldwide.com/cgi-bin/m?ci=us-204044...	image/gif	44	10/18/2015 8:53:03...	10/18/2015 8:53:03...	
&rp=&ts=comp...	http://secure-us.imrworldwide.com/cgi-bin/m?ci=us-505916...	image/gif	44	10/18/2015 8:53:36...	10/18/2015 8:53:35...	
0%2C0%2C1152...	http://img.lum.dolimg.com/v1/images/es-international-top-...	image/png	33,741	10/18/2015 8:53:34...	10/18/2015 8:53:34...	9/9/2015 2:37:18 AM
0%2C0%2C1152...	http://img.lum.dolimg.com/v1/images/br-international-top-...	image/png	29,529	10/18/2015 8:53:34...	10/18/2015 8:53:34...	9/9/2015 2:37:18 AM
0%2C0%2C1152...	http://img.lum.dolimg.com/v1/images/international-top-mo...	image/png	34,927	10/18/2015 8:53:34...	10/18/2015 8:53:34...	6/27/2015 6:45:55 ...
0%2C0%2C1600...	http://img.lum.dolimg.com/v1/images/a-wings-header_76f22...	image/jpeg	155,426	10/18/2015 8:53:33...	10/18/2015 8:53:32...	10/17/2015 12:53:5...
0%2C0%2C300...	http://img.lum.dolimg.com/v1/images/this-day_df434af6.pn...	image/png	2,509	10/18/2015 8:53:33...	10/18/2015 8:53:33...	1/13/2015 10:46:49...
0%2C30%2C400...	http://img.lum.dolimg.com/v1/images/au_news_davefiloni_7...	image/jpeg	37,473	10/18/2015 8:53:34...	10/18/2015 8:53:34...	10/13/2015 6:16:25...
01801101751000...	https://d.agkn.com/pixel/7174/?sk=01801101751000130207	image/gif	43	10/18/2015 8:53:36...	10/18/2015 8:53:35...	
076bbf0f7d07ab...	https://www.yahoo.com/sy/ts/api/res/1.2/N6xd8a1pBn97VVW...	image/jpeg	3,886	10/18/2015 8:53:21...	10/18/2015 6:50:18...	
0~0.swf	http://pagead2.googlesyndication.com/osd/hbe.swf?id=0~0	application/x-sh...	12,696	10/18/2015 8:53:07...	10/15/2015 12:22:1...	5/21/2015 3:45:00 ...
1	http://w.usabilla.com/c3244e3d16ba.js?lv=1	text/javascript	10,638	10/18/2015 8:53:03...	10/18/2015 8:53:02...	
1-bos_300x250_...	https://s1.2mdn.net/viewad/3944459/1-bos_300x250_now.jpg	image/jpeg	31,827	10/18/2015 8:53:04...	10/17/2015 12:00:0...	9/11/2015 5:33:50 ...
1.25.10	https://registerdisney.go.com/js/dist/all.min.js?1.25.10	application/java...	79,963	10/18/2015 8:53:36...	10/18/2015 8:53:37...	7/24/2015 12:29:09...
1.25.10	https://registerdisney.go.com/js/dist/DisneyID.min.js?1.25.10	application/java...	45,610	10/18/2015 8:53:36...	10/18/2015 8:53:37...	7/24/2015 12:29:06...
1.25.10	https://registerdisney.go.com/public/silent-client/SilentClient...	application/javascript	7	10/18/2015 8:53:36...	10/18/2015 8:53:37...	7/24/2015 12:24:48...
1.25.10	https://registerdisney.go.com/js/easyxdm.min.js?1.25.10	application/java...	7,575	10/18/2015 8:53:36...	10/18/2015 8:53:37...	7/24/2015 12:24:48...
1.html	http://tpc.googlesyndication.com/safeframe/1-0-2/html/cont...	text/html	1,877	10/18/2015 8:53:04...	10/15/2015 12:21:5...	1/16/2015 11:36:52...
12100	http://static.dynamicyield.com/scripts/12097/dy-min.js?v=12...	application/java...	27,483	10/18/2015 8:53:03...	10/18/2015 8:53:02...	10/12/2015 2:53:51...
12100	http://static.dynamicyield.com/scripts/12097/dyjq-min.js?v=1...	application/java...	41,097	10/18/2015 8:53:03...	10/18/2015 8:53:02...	10/12/2015 2:53:51...

738 item(s) NirSoft Freeware. http://www.nirsoft.net

5. Click on the “URL” column to alphabetically sort the entries by URL.

6. Can you check whether www.starwars.com was visited before? Find its entry.

7. Double-click on the entry to find out its details like the one shown below.



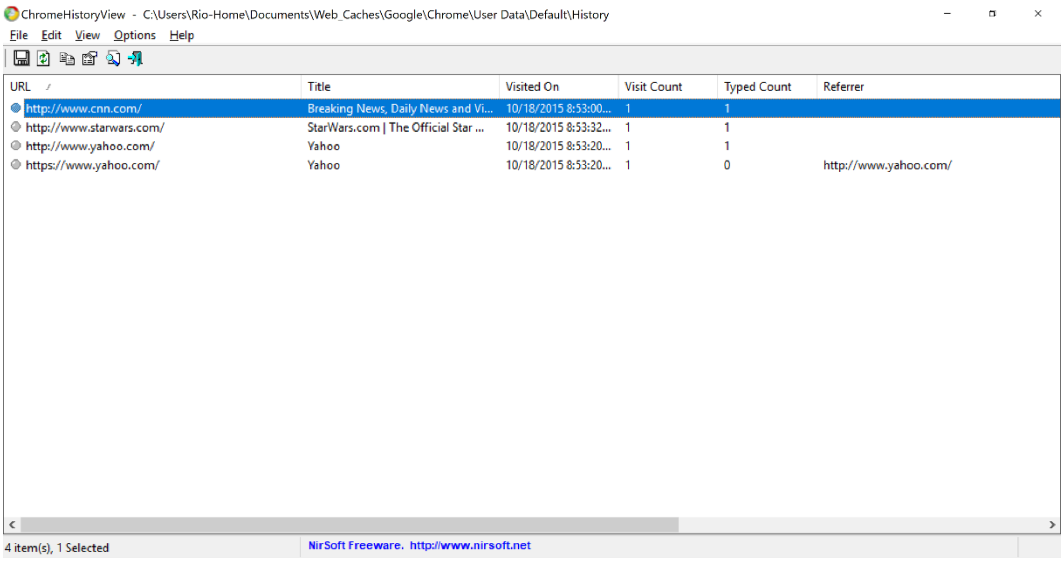
Properties

Filename:	www.starwars.com.html
URL:	http://www.starwars.com
Content Type:	text/html
File Size:	43,165
Last Accessed:	10/18/2015 8:53:32 AM
Server Time:	10/18/2015 8:53:32 AM
Server Last Modified:	
Expire Time:	
Server Name:	
Server Response:	HTTP/1.1 200 OK
Content Encoding:	gzip
Cache Name:	f_000084
Cache Control:	public, max-age=297
ETag:	
URL Length:	23

Task 4-2: Extracting and Analyzing Chrome’s History

Steps:

1. Download **NirSoft’s ChromeHistoryView (CHV)** from https://www.nirsoft.net/utils/chrome_history_view.html, and extract the zip file.
2. Launch CHV.
3. By default, it will point to the history file stored by the current user on the local machine: `C:\Users\`<*user-name*>`\AppData\Local\Google\Chrome\User Data\Default\History`.
4. To read an offline history, from the main menu, select “Options”, then “Advanced Options”, and then browse to the following location of your downloaded history file: `Web_Caches\Google\Chrome\User Data\Default\History`. CHV will show a window like the one below.



ChromeHistoryView - C:\Users\Rio-Home\Documents\Web_Caches\Google\Chrome\User Data\Default\History
File Edit View Options Help

URL	Title	Visited On	Visit Count	Typed Count	Referrer
http://www.cnn.com/	Breaking News, Daily News and Vi...	10/18/2015 8:53:00...	1	1	
http://www.starwars.com/	StarWars.com | The Official Star ...	10/18/2015 8:53:32...	1	1	
http://www.yahoo.com/	Yahoo	10/18/2015 8:53:20...	1	1	
https://www.yahoo.com/	Yahoo	10/18/2015 8:53:20...	1	0	http://www.yahoo.com/

4 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

5. Inspect the listed entries.

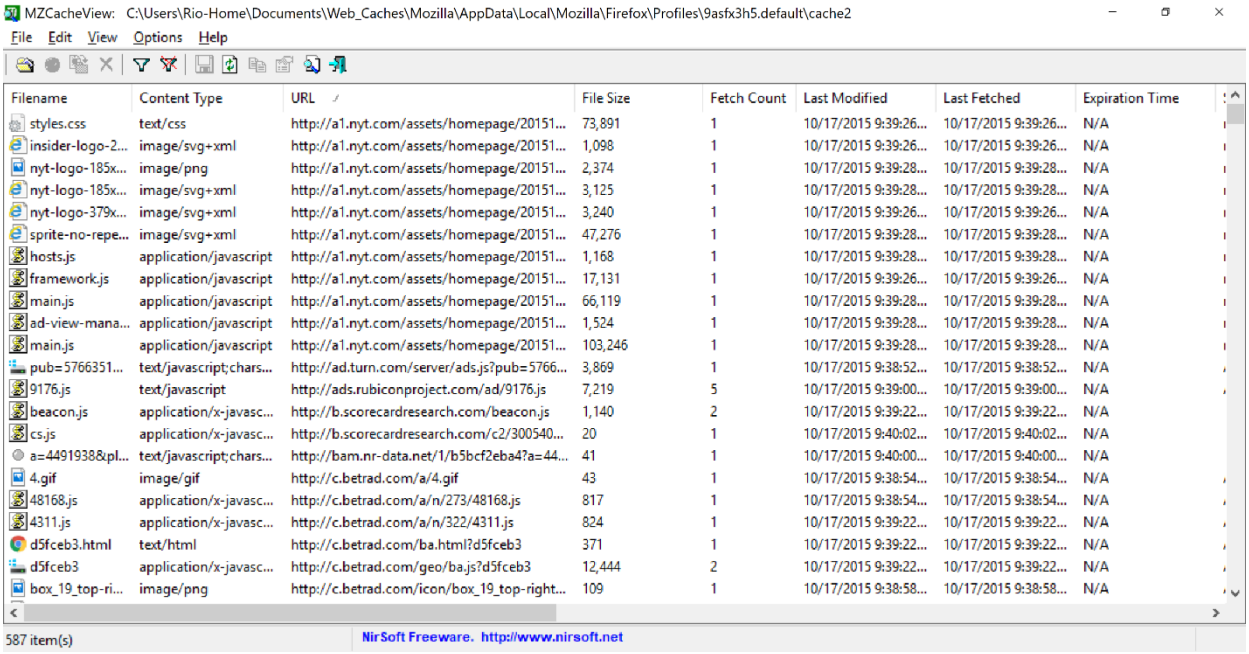
   *Why are the “Visit Count” and “Typed Count” values of the last entry (https://www.yahoo.com/) different?
6. Can you correlate the visited URLs with the cache entries in Task 4-1 before?

Task 4-3: Extracting and Analyzing Firefox's Cache

Steps:

1. Download **NirSoft's MozillaCacheView (MCV)** from https://www.nirsoft.net/utils/mozilla_cache_viewer.html, and extract the zip file.
2. Launch MCV.
3. By default, it will point to the cache stored by the current user on the local machine: `C:\Users\`*<user-name>*`\AppData\Local\Mozilla\Firefox\Profiles\profile.default\Cache`.
4. To read an **offline cache**, access the following location of your downloaded Mozilla cache file: `Web_Caches\Mozilla\AppData\Local\Mozilla\Firefox\Profiles\9asfx3h5.default\cache2`.

   MCV will show a window like the one below.


MZCacheView: C:\Users\Rio-Home\Documents\Web_Caches\Mozilla\AppData\Local\Mozilla\Firefox\Profiles\9asfx3h5.default\cache2
File
Edit
View
Options
Help

Filename	Content Type	URL	File Size	Fetch Count	Last Modified	Last Fetched	Expiration Time
styles.css	text/css	http://a1.nyt.com/assets/homepage/20151...	73,891	1	10/17/2015 9:39:26...	10/17/2015 9:39:26...	N/A
insider-logo-2...	image/svg+xml	http://a1.nyt.com/assets/homepage/20151...	1,098	1	10/17/2015 9:39:26...	10/17/2015 9:39:26...	N/A
nyt-logo-185x...	image/png	http://a1.nyt.com/assets/homepage/20151...	2,374	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
nyt-logo-185x...	image/svg+xml	http://a1.nyt.com/assets/homepage/20151...	3,125	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
nyt-logo-379x...	image/svg+xml	http://a1.nyt.com/assets/homepage/20151...	3,240	1	10/17/2015 9:39:26...	10/17/2015 9:39:26...	N/A
sprite-no-repe...	image/svg+xml	http://a1.nyt.com/assets/homepage/20151...	47,276	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
hosts.js	application/javascript	http://a1.nyt.com/assets/homepage/20151...	1,168	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
framework.js	application/javascript	http://a1.nyt.com/assets/homepage/20151...	17,131	1	10/17/2015 9:39:26...	10/17/2015 9:39:26...	N/A
main.js	application/javascript	http://a1.nyt.com/assets/homepage/20151...	66,119	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
ad-view-mana...	application/javascript	http://a1.nyt.com/assets/homepage/20151...	1,524	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
main.js	application/javascript	http://a1.nyt.com/assets/homepage/20151...	103,246	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
pub=5766351...	text/javascript;chars...	http://ad.turn.com/server/ads.js?pub=5766...	3,869	1	10/17/2015 9:38:52...	10/17/2015 9:38:52...	N/A
9176.js	text/javascript	http://ads.rubiconproject.com/ad/9176.js	7,219	5	10/17/2015 9:39:00...	10/17/2015 9:39:00...	N/A
beacon.js	application/x-javasc...	http://b.scorecardresearch.com/beacon.js	1,140	2	10/17/2015 9:39:22...	10/17/2015 9:39:22...	N/A
cs.js	application/x-javasc...	http://b.scorecardresearch.com/c2/300540...	20	1	10/17/2015 9:40:02...	10/17/2015 9:40:02...	N/A
a=4491938&pl...	text/javascript;chars...	http://bam.nr-data.net/1/b5bcf2eba4?a=44...	41	1	10/17/2015 9:40:00...	10/17/2015 9:40:00...	N/A
4.gif	image/gif	http://c.betrad.com/a/4.gif	43	1	10/17/2015 9:38:54...	10/17/2015 9:38:54...	N/A
48168.js	application/x-javasc...	http://c.betrad.com/a/n/273/48168.js	817	1	10/17/2015 9:38:54...	10/17/2015 9:38:54...	N/A
4311.js	application/x-javasc...	http://c.betrad.com/a/n/322/4311.js	824	1	10/17/2015 9:39:22...	10/17/2015 9:39:22...	N/A
d5fceb3.html	text/html	http://c.betrad.com/ba.html?d5fceb3	371	1	10/17/2015 9:39:22...	10/17/2015 9:39:22...	N/A
d5fceb3	application/x-javasc...	http://c.betrad.com/geo/ba.js?d5fceb3	12,444	2	10/17/2015 9:39:22...	10/17/2015 9:39:22...	N/A
box_19_top-ri...	image/png	http://c.betrad.com/icon/box_19_top-right...	109	1	10/17/2015 9:38:58...	10/17/2015 9:38:58...	N/A

587 item(s)

NirSoft Freeware. http://www.nirsoft.net

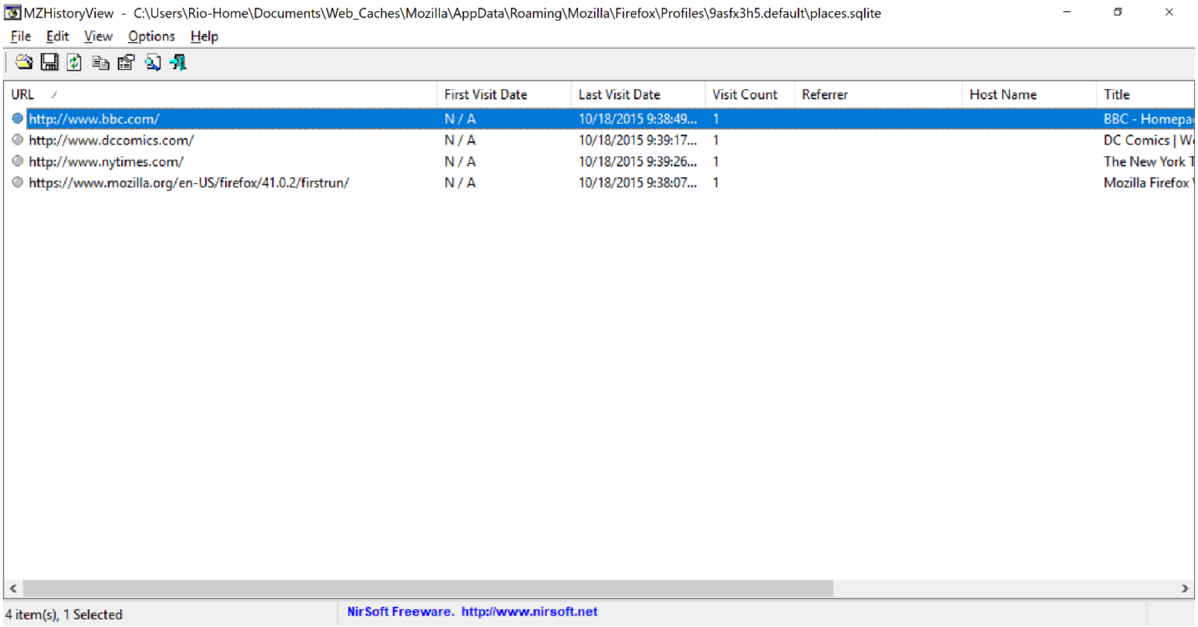
5. Inspect the shown entries.

Task 4-4: Extracting and Analyzing Firefox's History

Steps:

1. Download NirSoft's **MozillaHistoryView (MHV)** from https://www.nirsoft.net/utils/mozilla_history_view.html, and extract the zip file.
2. Launch MHV.
3. By default, it will point to the history file stored by the current user on the local machine: `C:\Users\`*<user-name>*`\AppData\Roaming\Mozilla\Firefox\Profiles\profile.default\places.sqlite`.
4. To read an offline history, access the following location of your downloaded Mozilla history file: `Web_Caches\Mozilla\AppData\Roaming\Mozilla\Firefox\Profiles\9asfx3h5.default\places.sqlite`.

   MHV will show a window like the one below.



MZHistoryView - C:\Users\Rio-Home\Documents\Web_Caches\Mozilla\AppData\Roaming\Mozilla\Firefox\Profiles\9asfx3h5.default\places.sqlite

URL	First Visit Date	Last Visit Date	Visit Count	Referrer	Host Name	Title
http://www.bbc.com/	N / A	10/18/2015 9:38:49...	1			BBC - Homepa
http://www.dccomics.com/	N / A	10/18/2015 9:39:17...	1			DC Comics | W
http://www.nytimes.com/	N / A	10/18/2015 9:39:26...	1			The New York T
https://www.mozilla.org/en-US/firefox/41.0.2/firstrun/	N / A	10/18/2015 9:38:07...	1			Mozilla Firefox

4 item(s), 1 Selected

5. Inspect the listed entries. How many entries were visited by the user? Notice that a newly installed Firefox will automatically visit Mozilla homepage.

Graded Lab Tasks #4 (2 Marks)

From your Lab 7, you will need to submit **your 3 answers** according to the following instructions:

- The selected **3 questions** in this lab are:
    - (0.5 marks) **Task 1, Step 5-c (page 3)**: When would the IP address lease expire/terminate (in human-readable time format)?
    - (0.75 marks) **Task 1, Step 5-d (page 3)**: What were the IP addresses of the DHCP server and default gateway?
    - (0.75 marks) **Task 4-2, Step 5 (page 21)**: Why are the “Visit Count” and “Typed Count” values of the last entry (https://www.yahoo.com/) different?
- From your correct 3 answers, you will earn a total of **2 marks**.
- This graded lab task assignment is an **individual** assignment.
  Hence, you MUST finish the assignment and report **independently**.
- Please prepare your answers in a self-contained **PDF file** by using your name and matric number as part of your file name. For example, Jack Lee with Matric No A001 should submit the filename JackLee-A001-**GLT4**.pdf. Your report should also contain your name, matric number, and email address on its first page.
- Upload your PDF file using **`Graded-Lab-Tasks-4`** Canvas Assignment by **Saturday, 18 March 2023, 23:59 SGT**. Note that this deadline is a ***firm & final*** **deadline**. There will be ***no*** deadline extensions.
  As such, you are advised to submit **well before** the cut-off time
  so as to avoid any technical issues with Canvas or your uploading!
- *Have fun with your assigned lab tasks!* :)