

**IFS4102 LAB**  
**WEEK 7**

REMINDER: WEEK 7 GRADED LAB TASKS #4  
SATURDAY, 18 MARCH 2023, 23:59 SGT  
**USE THE GIVEN SAMPLE FILES**

## OBJECTIVES

1. Find network configuration settings using registry files **(Task 1)**
2. Use NetworkMiner and Xplico to analyze network-traffic logs **(Task 3-1&2)**
3. Analyze web cache and history of Chrome and Firefox browsers **(Task 4-1,2,3&4)**

# I. FIND NETWORK CONFIGURATION SETTINGS USING REGISTRY FILES **(TASK I)**

- Using Windows Registry Recovery (WRR)
  - Recall Lab 5 Task 4, we did registry analysis using Registry Editor and RegRipper
  - Similar to Registry Explorer (not introduced in lab but discussed briefly at the end of lab 5)
  - Provides automatic extraction of useful information
  - Also display the entire registry in a tree format
- Demo

WRR automatically extract information from registry values and categorize them under these headers. Picture from WRR download page.

Here are described individual explorers:

- **File Information**  
In this explorer you can see basic file properties and checksums.
- **Security Record Explorer**  
Displays all security records used in registry. Usage counter, owner SID, group SID, list of affected keys and list of SACL and DACL is displayed for every record with flags and permissions enumerated. This explorer is available only for NT based system registry hives.
- **SAM**  
Displays Machine SID and part of SYSKEY. Enumerates local user and group accounts and some of their properties. This explorer is available only for NT based system registry SAM hive.
- **Windows Instalation**  
Displays Windows name, ID and key, install date and user registration info. Enumerates installed software with descriptions and install date and list of installed hotfixes with description. This explorer is available only SOFTWARE registry hive (Product ID and key are extracted in SYSTEM hive too). Last boot and shutdown datetimes are extracted only from SYSTEM hive. Also displays user and machine name and tree based Start menu for selected USER hive. This explorer is available for USER registry hive.
- **Hardware**  
Displays quick overview (CPU, Monitors, Video and Sound card and Network cards) and full device map of configured devices that worked on host machine. They are displayed in "Device Manager-like" tree with some properties. This explorer is available for SYSTEM registry hive.
- **Startup Applications**  
Enumerates applications that are registered to be run after startup. This explorer is available for SOFTWARE registry hive.
- **Services and Drivers**  
Enumerates all installed services and drivers with properties. This explorer is available only for NT based system registry SYSTEM hive.
- **Network Configuration**  
Displays all installed network clients, protocols and services. Enumerates all defined network connections with its TCP/IP configuration. This explorer is available only for NT based system registry SYSTEM hive.
- **Windows Firewall Settings**  
Displays settings (rules) for Windows Firewall. This explorer is available only for NT based system registry SYSTEM hive.
- **Environment**  
Displays all environment variables. This explorer is available only for NT based system registry SYSTEM hive.
- **Shell Folders**  
Displays shell folders (folders known to system). This explorer is available only for NT based system registry SYSTEM hive.
- **Outlook Express**  
Digs out all Outlook Express accounts and their settings. This explorer is available only for NT based system registry USER hive.
- **Raw Data**  
This explorer displays whole registry in known tree format. Contains powerful searching and data interpreter.

# Viewing Network Configuration (automatic extraction of useful information)

MiTeC Windows Registry Recovery - [SYSTEM]

FileOptionsExploreWindowsHelp

Free to use for private, educational and non-commercial purposes

SYSTEMNTUSER.DAT

NAVIGATOR

- File Information
- Security Records
- SAM
- Windows Installation
- Hardware
- Startup Applications
- Services and Drivers
- Network Configuration
- Windows Firewall Settings
- Environment
- Shell Folders
- Outlook Express
- Raw Data

ComponentsTCP/IP

Local Area Connection

- AdapterBroadcom NetXtreme Gigabit Ethernet
- UseZeroBroadcast0
- EnableDeadGWDetect1
- EnableDHCP1
- RegistrationEnabled1
- RegisterAdapterName0
- DhcpIPAddress192.168.1.4
- DhcpSubnetMask255.255.255.0
- DhcpServer
- Lease1517F
- LeaseObtainedTime4CFD7EF5
- T14CFE27B4
- T24CFA644
- LeaseTerminatesTime
- AddressType0
- IsServerNapAware0
- DhcpConnForceBroadcastFlag0
- DhcpInterfaceOptionsFC 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 08 00 00 00 00 00 74 D0 FE 4C C0 A8 01 01 47 FC 00 0C 03 00 00 00 00 00 00 04 00 00 00 00 00 74 D0 FE 4C C0 A8 01 01 0F 00 00 00 00 00 00 04 00 00...
- DhcpGatewayHardwareC0 A8 01 01 06 00 00 00 1F 90 16 D0 5C
- DhcpGatewayHardwareCount
- DhcpNameServer
- DhcpDefaultGateway
- DhcpDomain
- DhcpSubnetMaskOpt

Ip address

Subnet mask

For time, use online epoch converter to convert to human readable format, or use WRR's built in data viewer under 'Raw Data' tab.

Also allow viewing of the whole registry in tree format (just like using regedit) in Raw Data tab

The screenshot shows the MiTeC Windows Registry Recovery application. The 'Raw Data' tab is selected in the left sidebar. A red circle highlights the tree view of the registry, and a red arrow points to the 'Raw Data' tab with the instruction: '1. Click on this tab to view whole registry in a tree format'. Another red arrow points to the tree view with the instruction: '2. Navigate registry keys here just like in regedit'. A table of registry values is displayed on the right, with a red arrow pointing to it and the instruction: '3. Value name, type and data displayed here. Double click to view and use the internal converter'. A 'Data View' dialog box is open, showing the details for the 'LeaseObtainedTime' value, including its type (REG\_DWORD) and data (12/7/2010 12:25:25 AM). The dialog also has options for 'Interpretation Format' (Hexadecimal, Decimal, Binary, UNIX 32 Timestamp, DOS 32 Timestamp) and a 'Swap Endian' checkbox. A red arrow points to the 'Key Path' at the bottom of the window, which is: 'CMI-CreateHive\F10156BE-0E87-4EFB-969E-5DA29D131144\ControlSet001\services\Tcpip\Parameters\Interfaces\{D3C29F9B-39E1-431F-B383-C1A77D72EEFF}'. A red arrow points to this path with the instruction: '3. The full path (unfortunately cannot copy and paste)'.

Value	Type	Data
UseZeroBroadcast	REG_DWORD	0x00000000
EnableDeadGWDetect	REG_DWORD	0x00000001
EnableDHCP	REG_DWORD	0x00000001
NameServer	REG_SZ	
Domain	REG_SZ	
RegistrationEnabled	REG_DWORD	0x00000001
RegisterAdapterName	REG_DWORD	0x00000000
DhcpIPAddress	REG_SZ	192.168.1.4
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpServer	REG_SZ	
Lease	REG_DWORD	0x0001517F
LeaseObtainedTime	REG_DWORD	0x4CFD7EF5
T1	REG_DWORD	0x4CFE27B4
T2	REG_DWORD	0x4CFEA644
LeaseTerminatesTime	REG_DWORD	
AddressType	REG_DWORD	0x00000000
IsServerNapAware	REG_DWORD	0x00000000
DhcpConnForceBroadcastFlag	REG_DWORD	0x00000000

# I. FIND NETWORK CONFIGURATION SETTINGS USING REGISTRY FILES **(TASK I)**

- Microsoft is weird
- Time-based information stored in a number of formats
  - 32-bit Unix Epoch Time Format
  - 64-bit FILETIME objects
  - Strings
- Example: the ShutdownTime in SYSTEM\ControlSet001\Control\Windows is stored in 64-bit windows filetime.
- But in general, no need to worry



**Forensicator\_Tom**  
(@forensicator\_tom)



New Member

It turns out that InstallDate is a unix timestamp, while InstallTime is a Windows Date/time timestamp. If you use the correct decoding they come out to the same date.

Strange of Microsoft to use the two date formats but that makes a lot more sense now.

Reply

Quote

Topic starter

Posted : 19/10/2016 5:39 pm

## Note

Time-based information is maintained in the Registry (and on Windows systems, in general) in a number of formats. There are values whose data consists of (in part or entirely) a 32-bit Unix epoch time format, while the LastWrite times of keys, as well as data of some values, consist of 64-bit FILETIME objects. Still other time-based data is maintained as 128-bit SYSTEMTIME objects (a description of the SYSTEMTIME structure can be found online at [https://msdn.microsoft.com/en-us/library/ms724950\(VA.85\).aspx](https://msdn.microsoft.com/en-us/library/ms724950(VA.85).aspx)) and others are simply maintained as strings (for example, the Skype application has a value named "LastUpdatedDate" in the user's NTUSER.DAT file with string data of "01/10/2009").



## 2. USE NETWORKMINER (**TASK 3-I**)

- NetworkMiner free cannot parse PcapNG. How?
  - Convert PcapNG files to Pcap at [pcapng.com](http://pcapng.com) (don't use this website if you need to convert sensitive network traces, its HTTP. But for the purpose of this lab ok to use)
  - Use wireshark's built-in function editcap
- Demo using given samples

## 2. USE XPLICO (TASK 3-2)

- Download and import  
<https://drive.google.com/file/d/1yCtT0ZBoQDvNzC2eomROoyz6iCoNMjai/view?usp=sharing>.
- Change network adapter to host only (Or if you want to use your other VM to connect to the server, use NAT Network/Bridged)
- On the vm server, login on the terminal and run
  - `ifconfig`
  - `sudo /etc/init.d/xplico start`
  - `sudo /opt/xplico/script/sqlite_demo.sh`
- On your host machine (or VM, depending on your network adapter settings that you chose just now), connect to the server using its ip + port 9876.
- Demo using given samples

### 3. ANALYZE CHROME CACHE (**TASK 4-I**)

- Using ChromeCacheView
- Offline cache:
  - `Web_Caches\Google\Chrome\User Data\Default\Cache.`
- Demo using offline cache

## Change timezone

ChromeCacheView: F:\For Lab 7\Compressed\_Caches\Google\Chrome\User Data\Default\Cache

File Edit View Options Help

Double-Click Action  
Enter Key Action

- ✓ Show Date/Time in GMT
- ✓ Show Zero-Length Files
- ✓ Add Header Line To CSV/Tab-Delimited File
- Align Numeric Columns To Right
- ✓ Show Application Files
- ✓ Show Image Files
- ✓ Show Text/HTML Files
- ✓ Show Video Files
- ✓ Show Audio Files
- ✓ Show All Other Files

Filename	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expire Time	Server Name	Server Response	Web Site
client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=www....	text/javascript	395	10/18/2015 12:53:30 AM	10/18/2015 12:53:30 AM			gws	HTTP/1.1 200 OK	
client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=www....	text/javascript	393	10/18/2015 12:53:31 AM	10/18/2015 12:53:31 AM			gws	HTTP/1.1 200 OK	
client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=www....	text/javascript	390	10/18/2015 12:53:31 AM	10/18/2015 12:53:31 AM			gws	HTTP/1.1 200 OK	
client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=www....	text/javascript	396	10/18/2015 12:53:31 AM	10/18/2015 12:53:31 AM			gws	HTTP/1.1 200 OK	
client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=www....	text/javascript	403	10/18/2015 12:53:31 AM	10/18/2015 12:53:31 AM			gws	HTTP/1.1 200 OK	
www.starwars.c	text/html	43,165	10/18/2015 12:53:32 AM	10/18/2015 12:53:32 AM				HTTP/1.1 200 OK	
modals-b30234	text/css	2,823	10/18/2015 12:53:32 AM	10/18/2015 12:53:32 AM	10/15/2015 8:50:21...	10/14/2016 9:51:31...	Footprint Distributor...	HTTP/1.1 200 OK	
application-26c	text/css	20	10/18/2015 12:53:32 AM	10/18/2015 12:53:32 AM	8/25/2015 7:06:53 ...	8/24/2016 8:14:23 ...	Footprint Distributor...	HTTP/1.1 200 OK	
region=0%2C25	image/png	42,563	10/18/2015 12:53:32 AM	10/18/2015 12:53:32 AM	10/9/2015 1:30:58 ...			HTTP/1.1 200 OK	
application-272	text/css	23,618	10/18/2015 12:53:32 AM	10/18/2015 12:53:32 AM	10/15/2015 8:50:21...	10/14/2016 9:38:33...	Footprint Distributor...	HTTP/1.1 200 OK	
region=0%2C30	image/jpeg	27,154	10/18/2015 12:53:32 AM	10/18/2015 12:53:32 AM	10/12/2015 10:16:2...			HTTP/1.1 200 OK	
basic-faeb7846	text/css	23,366	10/18/2015 12:53:32 AM	10/18/2015 12:53:32 AM	9/29/2015 9:50:34 ...	9/28/2016 11:24:58...	Footprint Distributor...	HTTP/1.1 200 OK	

### 3. ANALYZE CHROME HISTORY (TASK 4-2)

- Using ChromeHistoryView
- Column “type count” → number of times that the user typed this address
- Column “transition type” → how the browser navigated to a particular URL on a particular visit. For example, if a user visits a page by clicking a link on another page, the transition type is "link".
- Offline file:
  - `Web_Caches\Google\Chrome\User Data\Default\History.`
- Demo using offline history

## 3. ANALYZE FIREFOX CACHE (**TASK 4-3**)

- Using MozillaCacheView
- Offline cache:
  - `Web_Caches\Mozilla\AppData\Local\Mozilla\Firefox\Profiles\9asfx3h5.default\cache2.`
- Similar usage to Chrome's

## 3. ANALYZE FIREFOX HISTORY (TASK 4-4)

- Using MozillaHistoryView
- Similar to Chrome's, but don't have type count.
- Offline file:
  - `Web_Caches\Mozilla\AppData\Roaming\Mozilla\Firefox\Profiles\9asfx3h5.default\places.sqlite.`
- When opening the offline file, remember to show .sqlite files.

QUESTIONS?



REMINDER: WEEK 7 GRADED LAB TASKS #4  
SATURDAY, 18 MARCH 2023, 23:59 SGT  
**USE THE GIVEN SAMPLE FILES**