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)**

1. FIND NETWORK CONFIGURATION SETTINGS USING REGISTRY FILES **(TASK 1)**

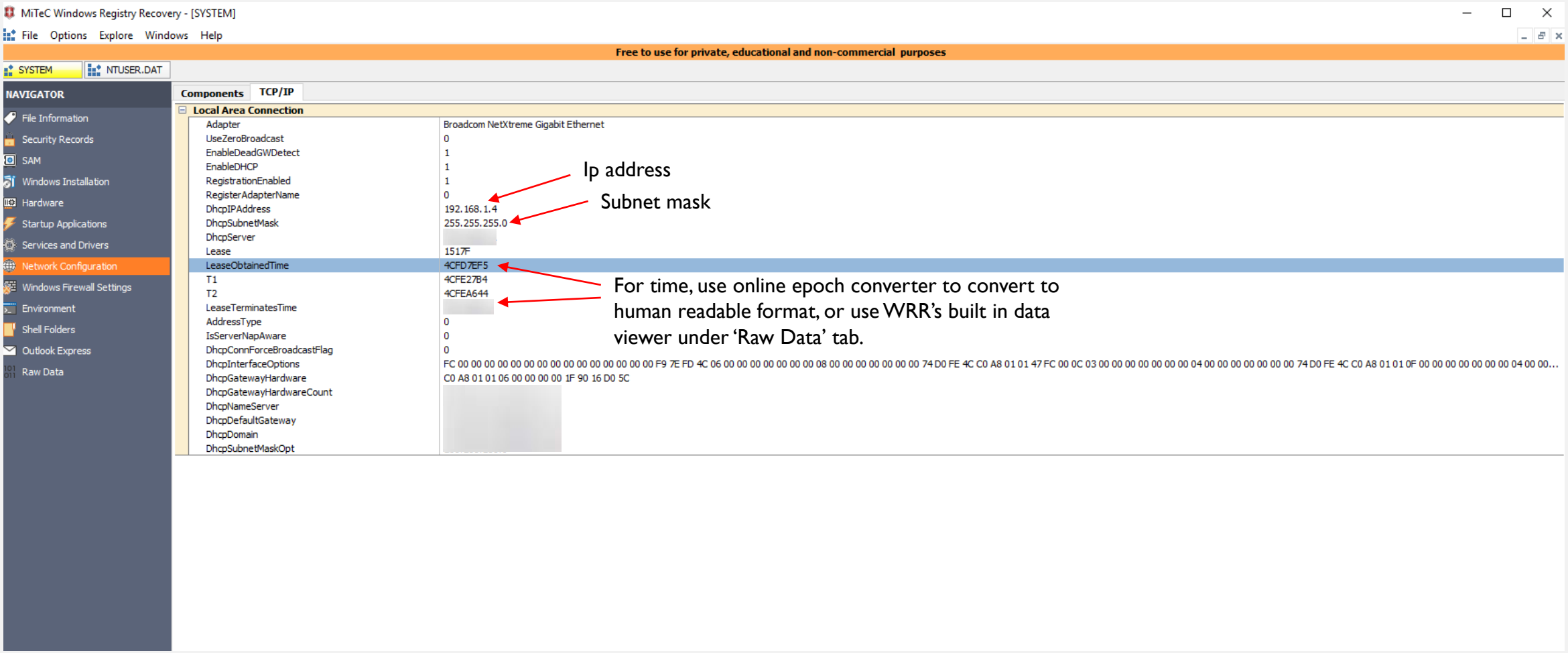
- Using Windows Registry Recovery (WRR)
  - Recall Lab 5 Task 4, we did registry analysis using Registry Editor and RegRipper
  - Similar to Registry Explorer (not introduced in lab but discussed briefly at the end of lab 5)
  - Provides automatic extraction of useful information
  - Also display the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

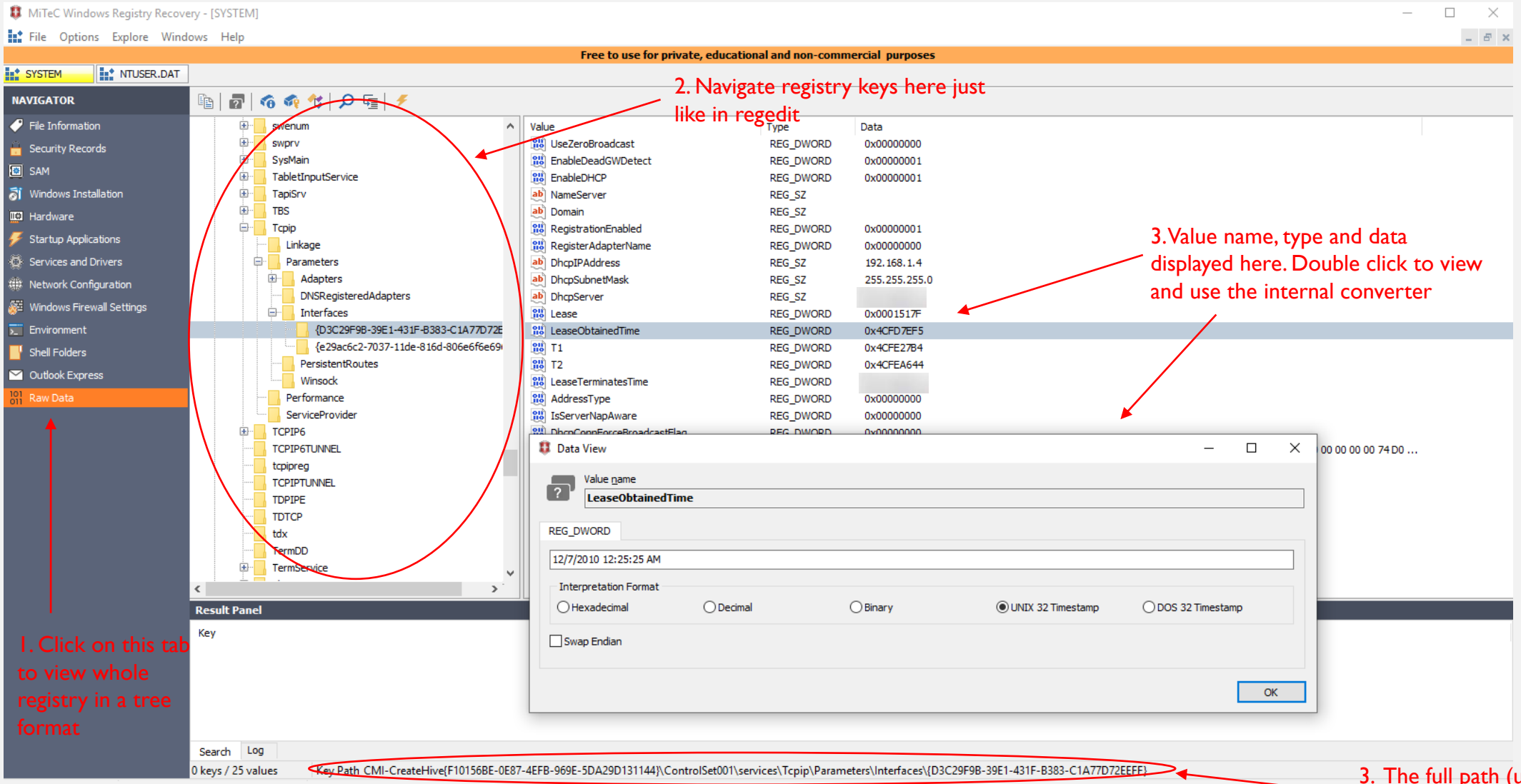
Here are described individual explorers:

- **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 wih 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)

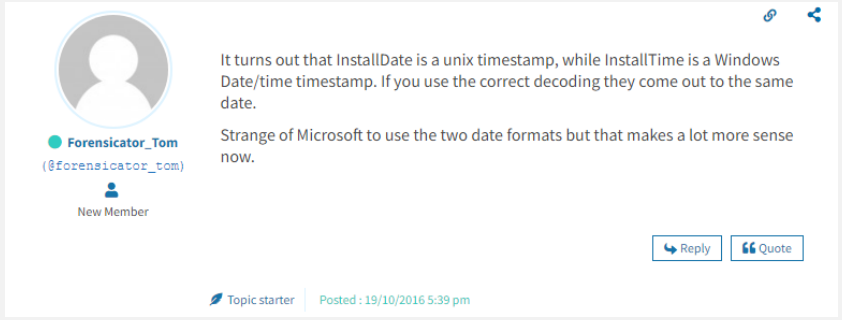


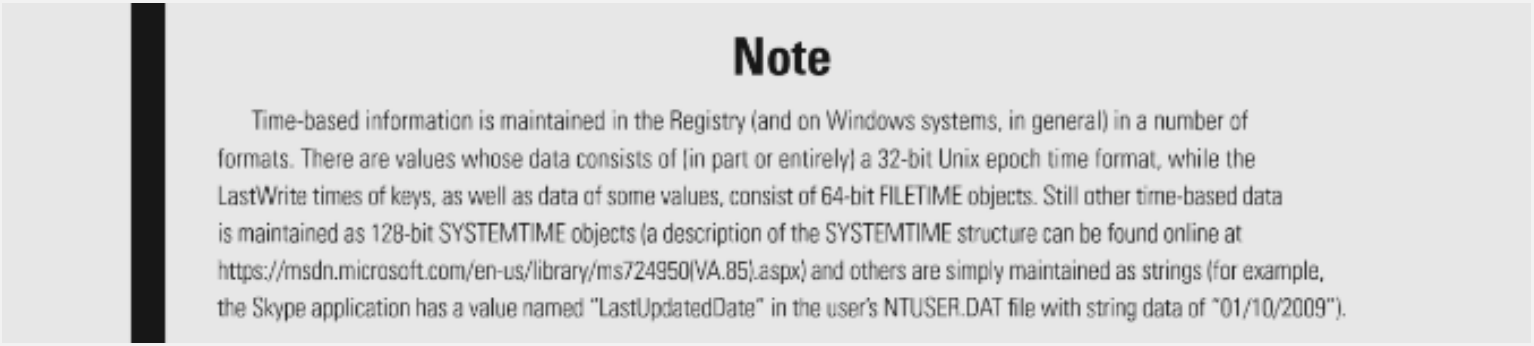
Also allow viewing of the whole registry in tree format (Just like using regedit) in Raw Data tab



1. FIND NETWORK CONFIGURATION SETTINGS USING REGISTRY FILES **(TASK 1)**

- 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





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) 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 3-1)**

- NetworkMiner free cannot parse PcapNG. How?
  - Convert PcapNG files to Pcap at 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

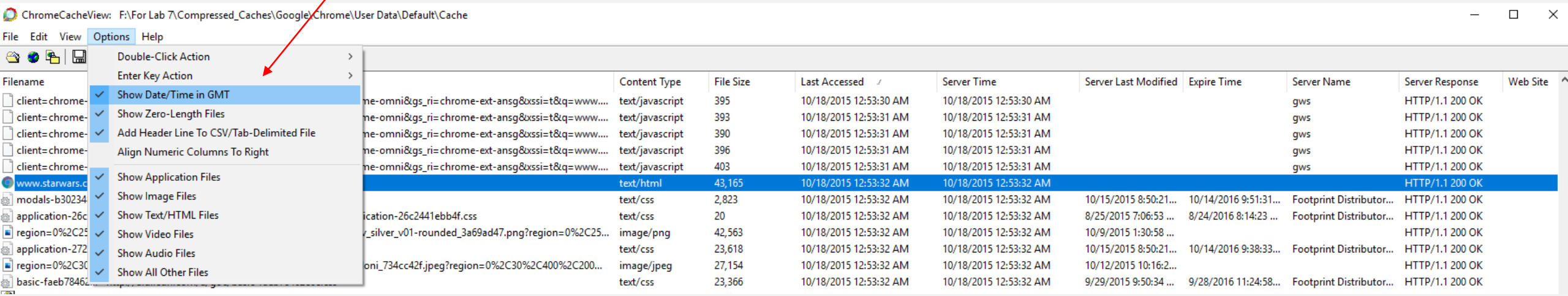
2. USE XPLICO **(TASK 3-2)**

- 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 4-1**)

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

Change timezone



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