

CYBR472 Lab 13: Internet Browser Forensics
greenthom – 300536064

Assessment Overview

This lab assesses your browser forensics skills through the analysis of web browser artifacts from different browsers. You will reconstruct user activities, identify visited websites, and establish timelines using metadata. This lab is worth 6% of your course grade.

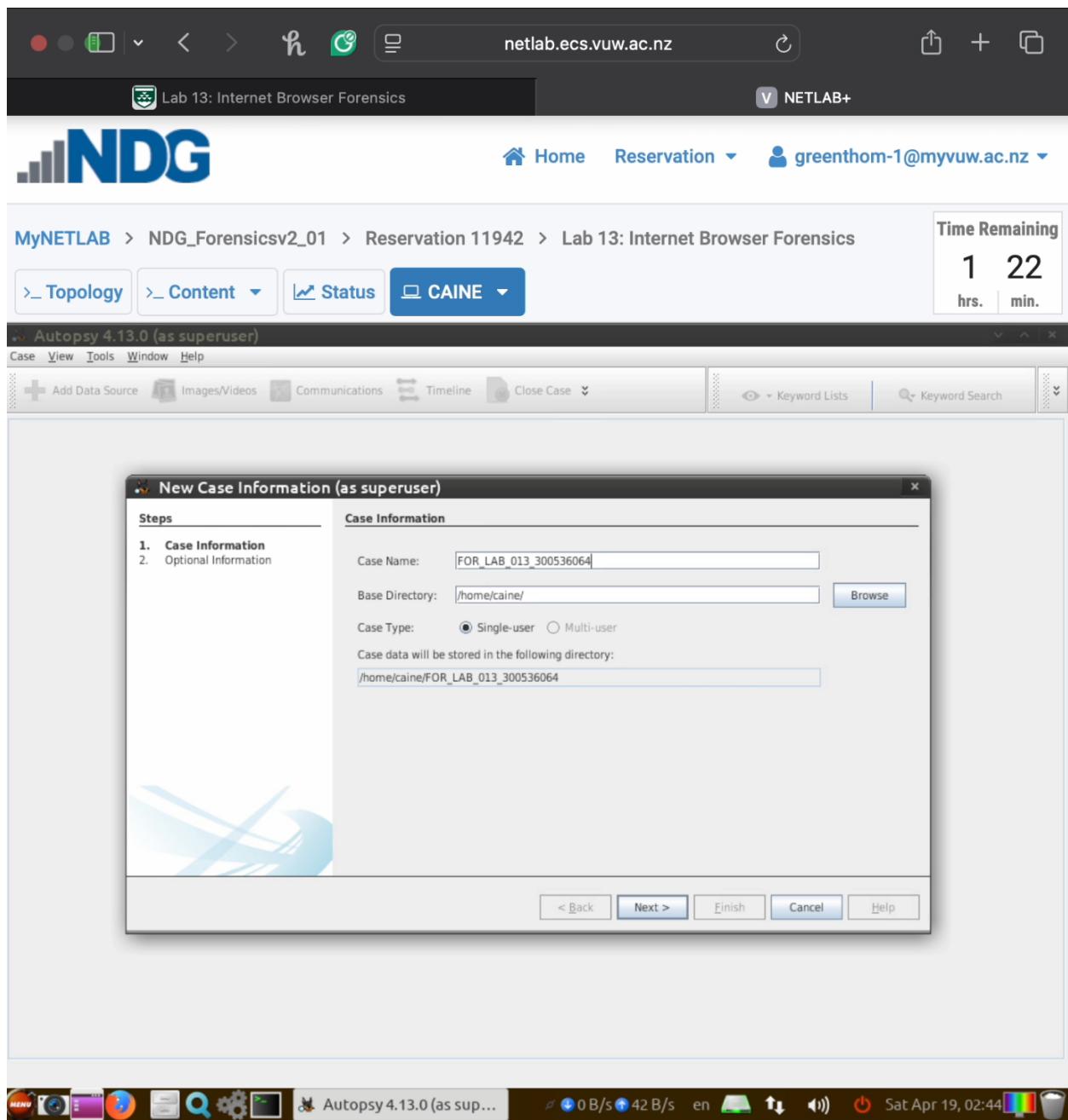
Submission Guidelines

- Include a heading with lab number, your name, and student ID
- Provide numbered screenshots as specified
- Include brief descriptions only when requested
- Submit as a single PDF document

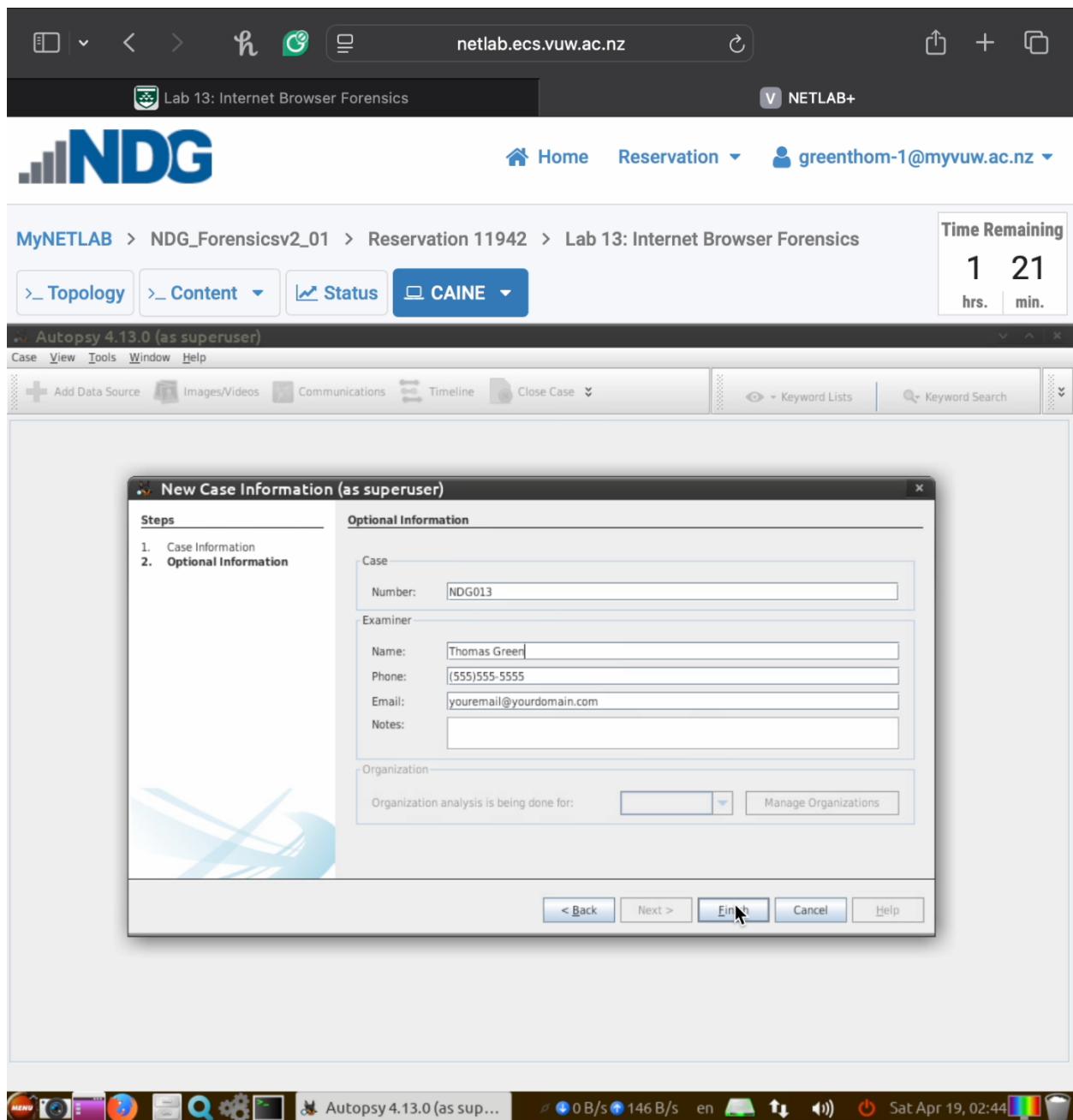
Part 1: Google Chrome Browser Forensics (30 marks)

Task 1: Autopsy Case Creation and Chrome History Database Analysis (10 marks)

- Launch Autopsy and create a new case named “FOR_LAB_013_[your student ID]”
- Enter your full name as the examiner in the Optional Information window
- Add the provided Lab13.E01 evidence file as your data source
- Enable only the Recent Activity ingest module
- Locate the Chrome History database file in the appropriate user profile folder
- Include the Autopsy title window showing case name in screenshots
- Required screenshots:
 - New Case information window with your student ID in the case name (step 1.4)



- **Optional Information window with your name as examiner (step 1.5)**



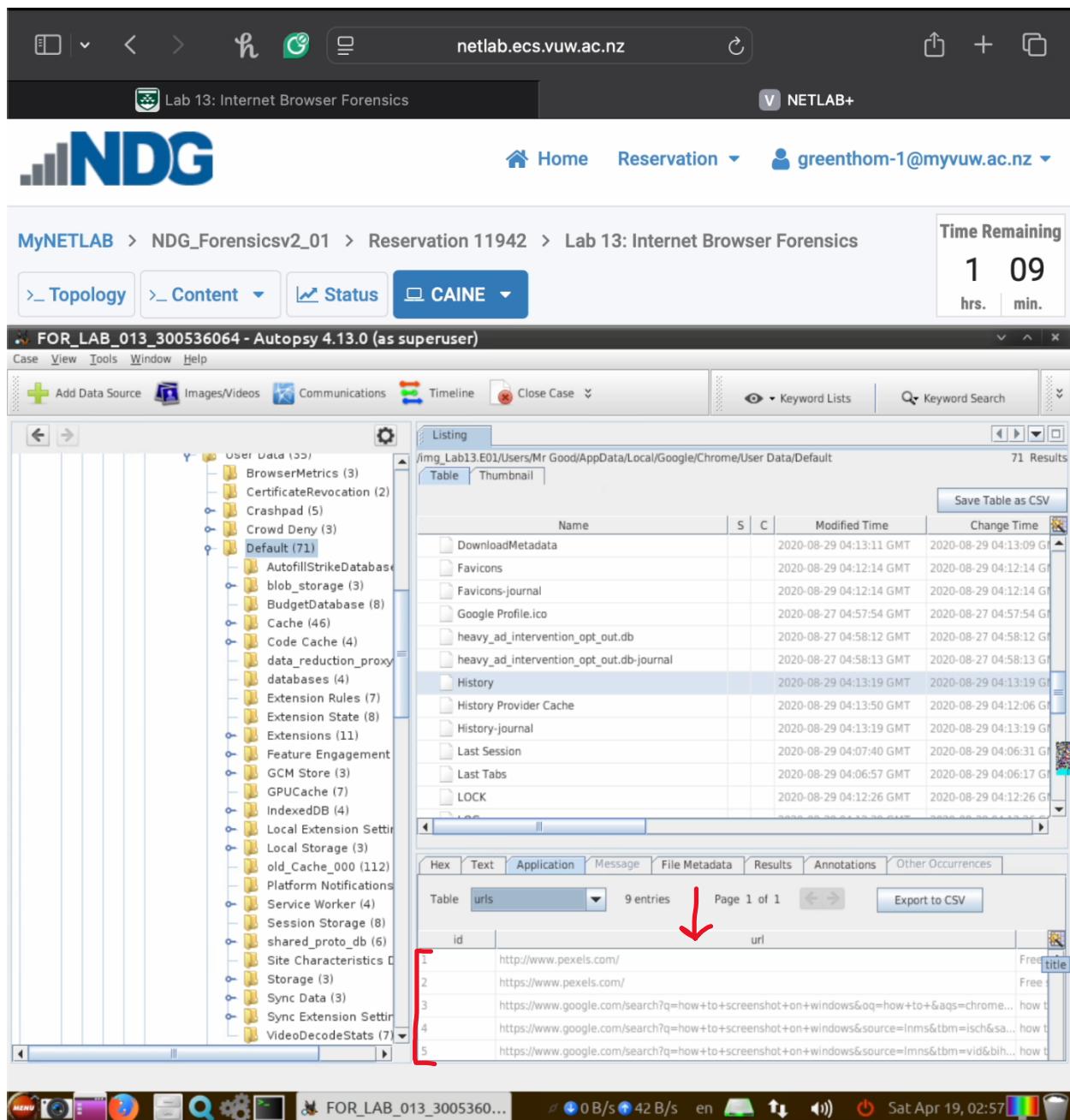
- **File path to the Chrome History database (step 1.15)**

The screenshot shows the MyNETLAB interface with the following details:

- Header:** netlab.ecs.vuw.ac.nz, Lab 13: Internet Browser Forensics, NETLAB+, Home, Reservation, greenthom-1@myvuw.ac.nz
- Breadcrumbs:** MyNETLAB > NDG_Forensicsv2_01 > Reservation 11942 > Lab 13: Internet Browser Forensics
- Time Remaining:** 1 11 hrs. min.
- Tool Tabs:** Topology, Content, Status, CAINE (selected)
- Autopsy 4.13.0 Interface:**
 - Left Panel:** Shows a tree view of database files under 'User Data' (e.g., BrowserMetrics, Crashpad, Crowd Deny, Default).
 - Center Panel:** 'Listing' tab selected, showing a table of files from the 'Default' folder. The table has columns: Name, S, C, Modified Time, Change Time. Some rows include:

DownloadMetadata			2020-08-29 04:13:11 GMT	2020-08-29 04:13:09 GMT
Favicons			2020-08-29 04:12:14 GMT	2020-08-29 04:12:14 GMT
Favicons-journal			2020-08-29 04:12:14 GMT	2020-08-29 04:12:14 GMT
Google Profile.ico			2020-08-27 04:57:54 GMT	2020-08-27 04:57:54 GMT
heavy_ad_intervention_opt_out.db			2020-08-27 04:58:12 GMT	2020-08-27 04:58:12 GMT
heavy_ad_intervention_opt_out.db-journal			2020-08-27 04:58:13 GMT	2020-08-27 04:58:13 GMT
History			2020-08-29 04:13:19 GMT	2020-08-29 04:13:19 GMT
History Provider Cache			2020-08-29 04:13:50 GMT	2020-08-29 04:12:06 GMT
History-journal			2020-08-29 04:13:19 GMT	2020-08-29 04:13:19 GMT
Last Session			2020-08-29 04:07:40 GMT	2020-08-29 04:06:31 GMT
Last Tabs			2020-08-29 04:06:57 GMT	2020-08-29 04:06:17 GMT
LOCK			2020-08-29 04:12:26 GMT	2020-08-29 04:12:26 GMT
 - Bottom Panel:** Shows system status (CPU, RAM, Network, Disk), date (Sat Apr 19, 02:55), and a trash bin icon.

- URLs table contents with visited websites highlighted (step 1.17)



Task 2: Chrome Cache Analysis (10 marks)

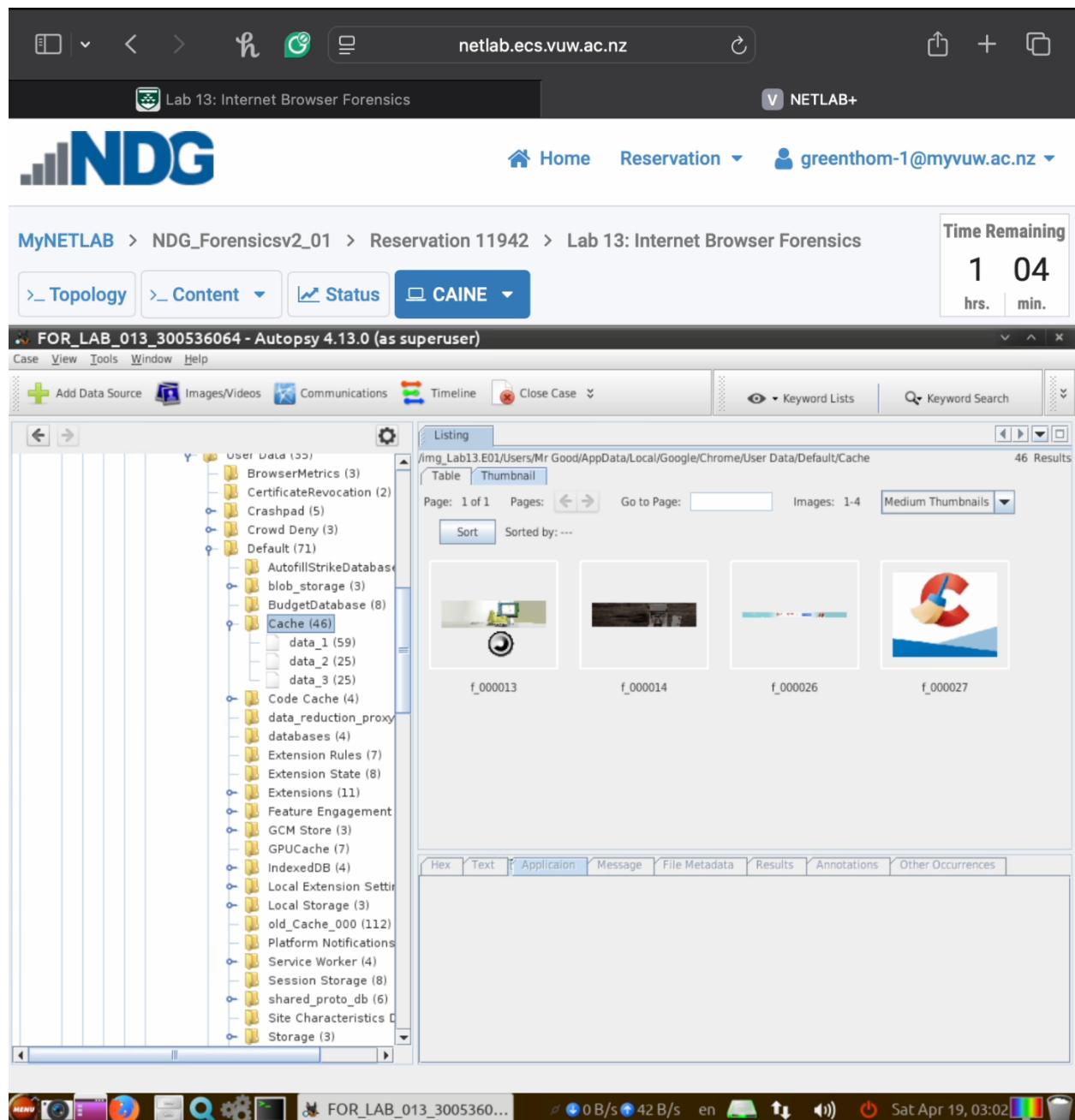
- Navigate to the Chrome Cache folder in the user's profile
- Examine cached content using thumbnail view
- Identify a cached image
- Include the Autopsy title window showing case name in screenshots
- Required screenshots:
 - Chrome Cache folder location (step 1.27)

MyNETLAB > NDG_Forensicsv2_01 > Reservation 11942 > Lab 13: Internet Browser Forensics

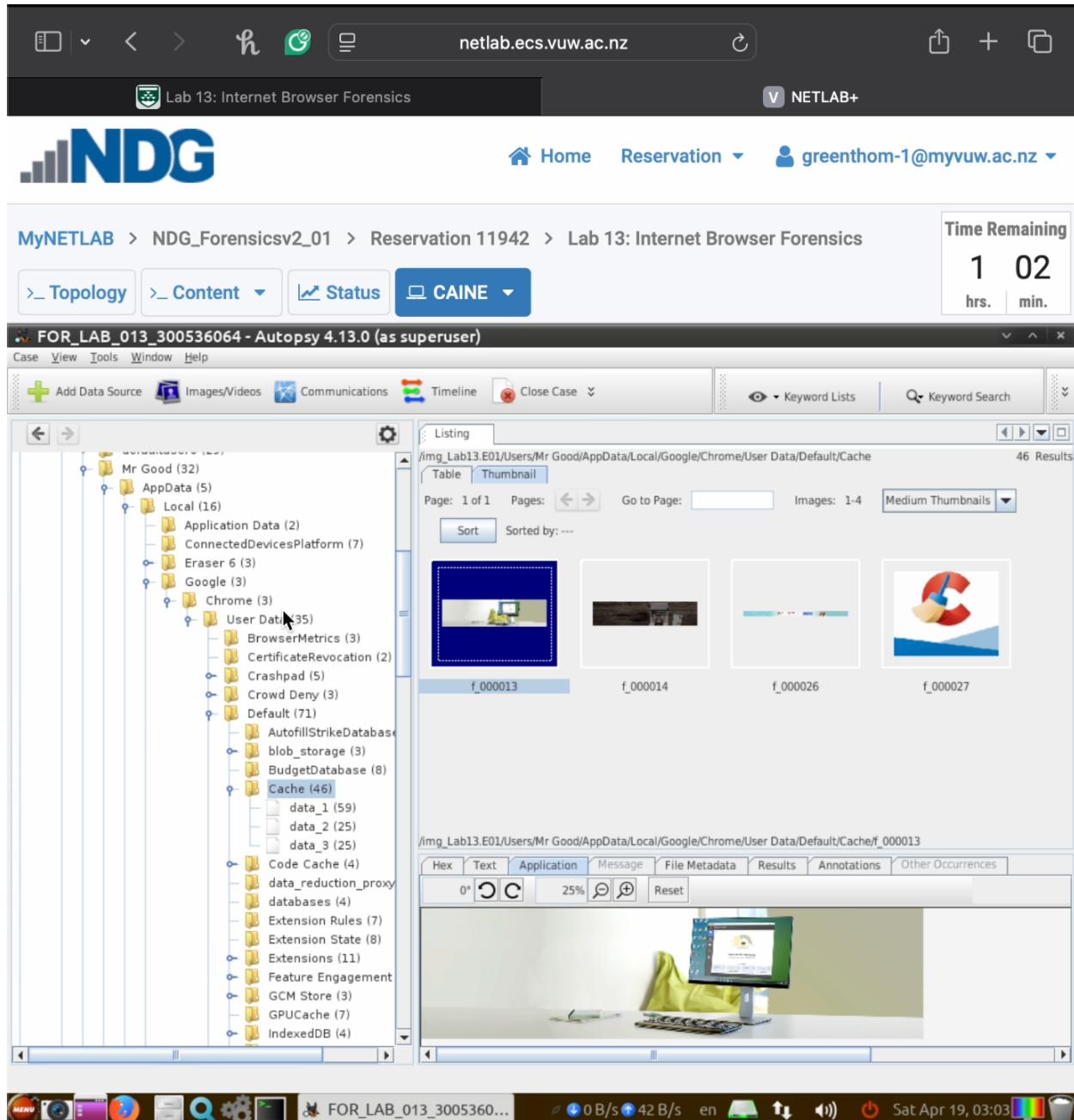
Time Remaining
1 05 hrs. min.

Name	S	C	Modified Time	Change Time	Access Time
f_000015			2020-08-29 04:12:06 GMT	2020-08-29 04:12:06 GMT	2020-08-29 04:12:06
f_000016			2020-08-29 04:12:07 GMT	2020-08-29 04:12:07 GMT	2020-08-29 04:12:07
f_000017			2020-08-29 04:12:07 GMT	2020-08-29 04:12:07 GMT	2020-08-29 04:12:07
f_000018			2020-08-29 04:12:07 GMT	2020-08-29 04:12:07 GMT	2020-08-29 04:12:07
f_000019			2020-08-29 04:12:07 GMT	2020-08-29 04:12:07 GMT	2020-08-29 04:12:07
f_00001a			2020-08-29 04:12:07 GMT	2020-08-29 04:12:07 GMT	2020-08-29 04:12:07
f_00001b			2020-08-29 04:12:07 GMT	2020-08-29 04:12:07 GMT	2020-08-29 04:12:07
f_00001c			2020-08-29 04:12:07 GMT	2020-08-29 04:12:07 GMT	2020-08-29 04:12:07
f_00001d			2020-08-29 04:12:07 GMT	2020-08-29 04:12:07 GMT	2020-08-29 04:12:07
f_00001e			2020-08-29 04:12:07 GMT	2020-08-29 04:12:07 GMT	2020-08-29 04:12:07
f_00001f			2020-08-29 04:12:08 GMT	2020-08-29 04:12:08 GMT	2020-08-29 04:12:08
f_000020			2020-08-29 04:12:08 GMT	2020-08-29 04:12:08 GMT	2020-08-29 04:12:08

- **Thumbnail view of cached content (step 1.28)**



- A selected cached image in full view (step 1.28)



Task 3: Chrome Cookies Analysis (10 marks)

- Locate the Chrome Cookies database in the user's profile
- Identify website-specific cookies and their properties
- Document cookie creation and expiration timestamps
- Include the Autopsy title window showing case name in screenshots
- Required:
 - Screenshot of Cookies database location (step 1.24)

MyNETLAB > NDG_Forensicsv2_01 > Reservation 11942 > Lab 13: Internet Browser Forensics

Time Remaining
1 06 hrs. min.

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Close Case Keyword Lists Keyword Search

User Data (55)
 BrowserMetrics (3)
 CertificateRevocation (2)
 Crashpad (5)
 Crowd Deny (3)
 Default (71)
 AutofillStrikeDatabase
 blob_storage (3)
 BudgetDatabase (8)
 Cache (46)
 Code Cache (4)
 data_reduction_proxy
 databases (4)
 Extension Rules (7)
 Extension State (8)
 Extensions (11)
 Feature Engagement
 GCM Store (3)
 GPU Cache (7)
 IndexedDB (4)
 Local Extension Settings
 Local Storage (3)
 old_Cache_000 (112)
 Platform Notifications
 Service Worker (4)
 Session Storage (8)
 shared_proto_db (6)
 Site Characteristics
 Storage (3)
 Sync Data (3)
 Sync Extension Settings
 VideoDecodeStats (7)

Listing
 /img.Lab13.E01/Users/Mr Good/AppData/Local/Google/Chrome/User Data/Default
 Table Thumbnail
 Save Table as CSV
 Change Time

Name	S	C	Modified Time
Sync Extension Settings			2020-08-27 04:58:45 GMT
VideoDecodeStats			2020-08-27 05:08:53 GMT
000003.log			2020-08-29 04:13:09 GMT
Cookies			2020-08-29 04:13:22 GMT
Cookies-journal			2020-08-29 04:13:22 GMT
CURRENT			2020-08-29 04:12:26 GMT
Current Session			2020-08-29 04:13:19 GMT
Current Tabs			2020-08-29 04:13:22 GMT
DownloadMetadata			2020-08-29 04:13:11 GMT
Favicons			2020-08-29 04:12:14 GMT
Favicons-journal			2020-08-29 04:12:14 GMT
Google Profile.ico			2020-08-27 04:57:54 GMT

Hex Text Application Message File Metadata Results Annotations Other Occurrences
 Table cookies 69 entries Page 1 of 1 Export to CSV
 creation_utc host_key name value
 1324297789... .pexels.com __cfduid /
 1324297790... .pexels.com __fp /
 1324297790... .pexels.com __ga /
 1324297790... .pexels.com __gid /
 1324297789... .pexels.com ab.storage.deviceld.5791d6db-4410-4ace-8814-12c903a548ba /

FOR_LAB_013_3005360... 0 B/s 42 B/s en Sat Apr 19, 03:00

- Screenshot of cookies table with domain information highlighted (step 1.25)

The screenshot shows the MyNETLAB interface with the NDG logo. The top navigation bar includes Home, Reservation, and a user profile. Below it, the breadcrumb path is MyNETLAB > NDG_Forensicsv2_01 > Reservation 11942 > Lab 13: Internet Browser Forensics. A timer on the right indicates 1 hour and 6 minutes remaining. The main content area is titled 'FOR_LAB_013_300536064 - Autopsy 4.13.0 (as superuser)'. The Autopsy interface shows a file tree on the left and a detailed listing of files in the center. A red arrow points to the 'cookies' table in the bottom pane, which contains the following data:

creation_utc	host_key	name	value
1324297789...	.pexels.com	ab.storage.deviceId.5791d6db-4410-4ace-8814-12c903a548ba	/
1324297789...	.pexels.com	ab.storage.sessionId.5791d6db-4410-4ace-8814-12c903a548ba	/
1324297790...	.facebook.com	fr	/
1324297790...	www.pexels.com	locale	/
1324297795...	google.com	CGIC	/comp

- Brief explanation (50 words max) of what the cookies reveal about browsing activity

The cookies show the user accessed sites like pexels.com, facebook.com, and google.com. Stored data like session IDs and user preferences indicate repeated visits, searches, or logins, revealing patterns of browsing activity. Cookies store session data, authentication tokens, or user preferences, indicating activity and login states across browsing sessions.

Part 2: Firefox and Internet Explorer Browser Forensics (20 marks)

Task 4: Firefox History Analysis (10 marks)

- Locate the Firefox places.sqlite database in the user's profile
- Extract and document browsing history from the moz_places table
- Analyze URL visit timestamps from the moz_historyvisits table
- Include the Autopsy title window showing case name in screenshots
- Required screenshots:
 - File path to the Firefox places.sqlite database (step 2.3)

The screenshot shows the MyNETLAB interface with the following details:

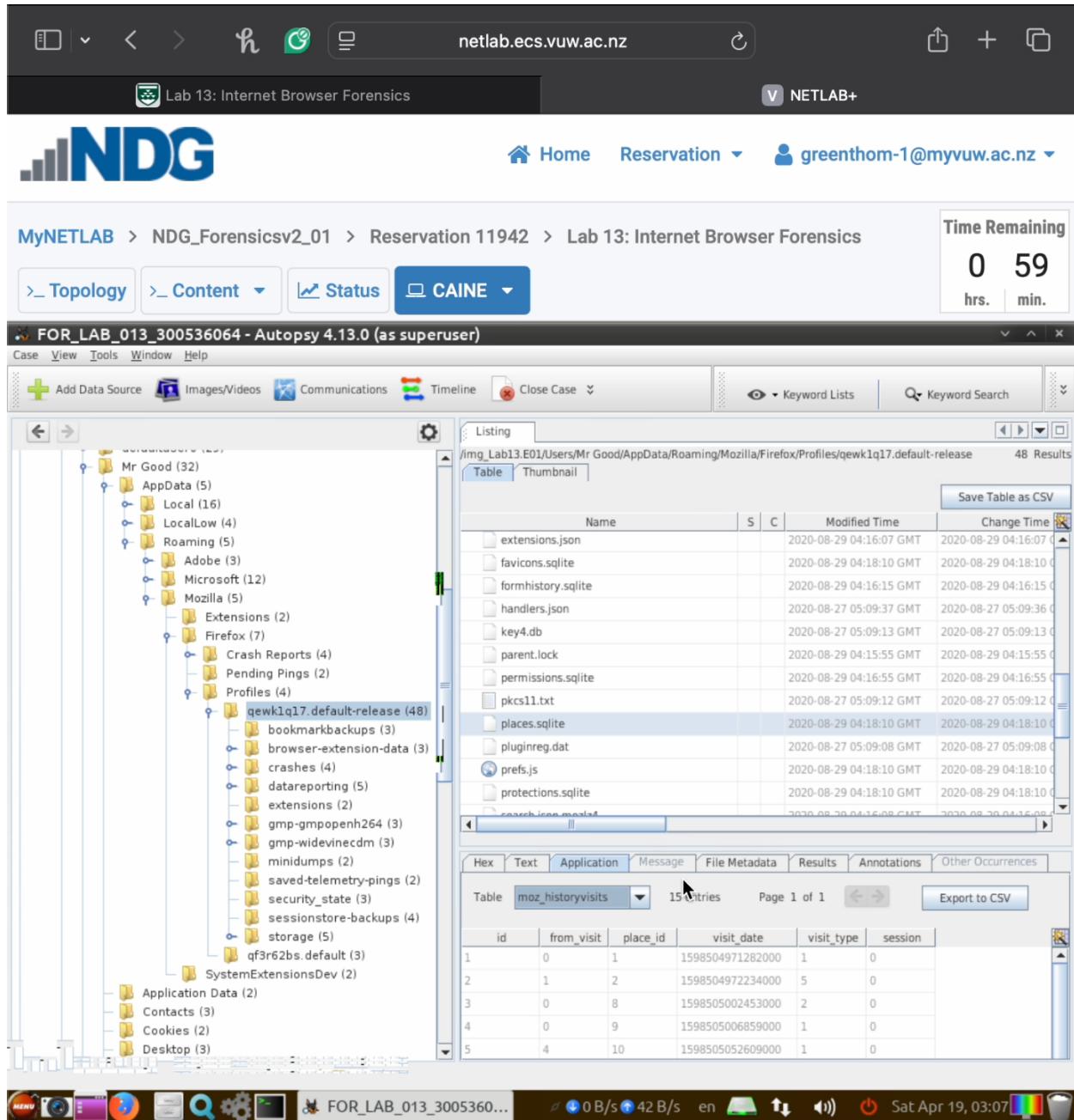
- Header:** netlab.ecs.vuw.ac.nz, NETLAB+, Lab 13: Internet Browser Forensics
- Top Navigation:** Home, Reservation, greenthom-1@myvuw.ac.nz
- Case Path:** MyNETLAB > NDG_Forensicsv2_01 > Reservation 11942 > Lab 13: Internet Browser Forensics
- Time Remaining:** 1 00 hrs. min.
- Autopsy 4.13.0 Interface:**
 - File Tree:** Shows the victim's file structure, including the Mozilla Firefox profile directory at `/img Lab13.E01/Users/Mr Good/AppData/Roaming/Mozilla/Firefox/Profiles/qewk1q17.default-release`.
 - Listing View:** Displays the contents of the `places.sqlite` database. The table has columns: Name, S, C, Modified Time, and Change Time. One row is selected: `places.sqlite` (modified on 2020-08-29 04:18:10 GMT).
 - Hex, Text, Application, Message, File Metadata, Results, Annotations, Other Occurrences:** Tabs for viewing the database content.
- Bottom Taskbar:** Shows various application icons and the system status bar indicating 0 B/s, 48 B/s, en, and the date Sat Apr 19, 03:06.

- **moz_places table content showing URLs (step 2.5)**

Screenshot of the MyNETLAB interface showing the Autopsy 4.13.0 forensic tool running on a Linux system. The browser bar shows the URL netlab.ecs.vuw.ac.nz. The main navigation bar includes Home, Reservation, and a user account for greenthom-1@myvuw.ac.nz. A "Time Remaining" timer shows 0 hours and 59 minutes.

The current view is under the "Content" tab, specifically for the "FOR_LAB_013_300536064 - Autopsy 4.13.0 (as superuser)" case. The left sidebar displays a file tree of the victim's file system, including AppData, Local, LocalLow, Roaming, Adobe, Microsoft, Mozilla (with sub-folders like Extensions, Firefox, and Profiles), and SystemExtensionsDev. The right panel shows a "Listing" table for the "/img_Lab13.E01/Users/Mr Good/AppData/Roaming/Mozilla/Firefox/Profiles/qewk1q17.default-release" directory, containing 48 results. The table includes columns for Name, S, C, Modified Time, and Change Time. Below the table are tabs for Hex, Text, Application, Message, File Metadata, Results, Annotations, and Other Occurrences, with the "Table" tab selected. The bottom status bar shows network activity (0 B/s, 42 B/s), system status (en), and the date/time (Sat Apr 19, 03:06).

- **moz_historyvisits table with timestamps (step 2.7)**



Task 5: Internet Explorer Cache and History Analysis (10 marks)

- Locate Internet Explorer's WebCache database and cache folders
- Examine the structure of IE's browsing artifacts
- View Autopsy's extracted web history results from all three browsers
- Include the Autopsy title window showing case name in screenshots
- Required screenshots:
 - WebCacheV01.dat file location (step 3.3)

MyNETLAB > NDG_Forensicsv2_01 > Reservation 11942 > Lab 13: Internet Browser Forensics

Time Remaining
0 55 hrs. min.

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Close Case Keyword Lists Keyword Search

FOR_LAB_013_300536064 - Autopsy 4.13.0 (as superuser)

Listing /img_Lab13.E01/Users/Mr Good/AppData/Local/Microsoft/Windows/WebCache 12 Results

Name	S	C	Modified Time	Change Time	Acc
[current folder]			2020-08-29 04:34:55 GMT	2020-08-29 04:34:55 GMT	2020-08-29 0
[parent folder]			2020-08-29 19:29:07 GMT	2020-08-29 19:29:07 GMT	2020-08-29 1
V01.chk			2020-08-29 19:29:04 GMT	2020-08-29 19:29:04 GMT	2020-08-27 0
V01.log			2020-08-29 19:29:04 GMT	2020-08-29 19:29:04 GMT	2020-08-27 0
V0100015.log			2020-08-29 04:30:54 GMT	2020-08-29 04:30:54 GMT	2020-08-27 0
V0100016.log			2020-08-29 04:33:31 GMT	2020-08-29 04:33:31 GMT	2020-08-27 0
V0100017.log			2020-08-29 04:34:55 GMT	2020-08-29 04:34:55 GMT	2020-08-27 0
V01res00001.jrs			2020-08-27 04:39:18 GMT	2020-08-27 04:39:18 GMT	2020-08-27 0
V01res00002.jrs			2020-08-27 04:39:18 GMT	2020-08-27 04:39:18 GMT	2020-08-27 0
V01tmp.log			2020-08-29 04:29:39 GMT	2020-08-29 04:29:39 GMT	2020-08-27 0
WebCacheV01.dat			2020-08-29 19:29:04 GMT	2020-08-29 19:29:04 GMT	2020-08-27 0
WebCacheV01.jfm			2020-08-29 19:29:04 GMT	2020-08-29 19:29:04 GMT	2020-08-27 0

Hex Text Application Message File Metadata Results Annotations Other Occurrences

FOR_LAB_013_3005360... 0 B/s 42 B/s en ↑ ↓ Sat Apr 19, 03:10

- o **IE cache folder structure (step 3.6)**

The screenshot shows the Autopsy 4.13.0 interface running on a Linux system. The title bar indicates the case name is "FOR_LAB_013_300536064 - Autopsy 4.13.0 (as superuser)". The left sidebar displays a file tree with various folders like Media Player, OneDrive, PenWorkspace, PlayReady, Vault, and Windows. A red arrow points to the "IE" folder under the Windows section. The main pane shows a "Listing" table with 7 results from the path "/img_Lab13.E01/Users/Mr Good/AppData/Local/Microsoft/Windows/INetCache/IE/75UO5CND". The table includes columns for Name, S, C, and Modified Time. The results include various files and folders, such as "[current folder]", "[parent folder]", "a5ea21[1].png", "a5ea21[2].ico", and "microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg". Below the table are tabs for Hex, Text, Application, Message, File Metadata, Results, Annotations, and Other Occurrences, with the Strings tab selected.

Name	S	C	Modified Time
[current folder]			2020-08-29 18:52:09 GMT
[parent folder]			2020-08-27 04:41:11 GMT
a5ea21[1].png			2020-08-27 04:42:15 GMT
a5ea21[2].ico			2020-08-29 04:27:28 GMT
ConvergedLoginPaginatedStrings.en_gZsc0Qued7WFkvXXfirs			2020-08-29 04:12:02 GMT
logo-180x180[1].png			2020-08-29 04:35:10 GMT
microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg			2020-08-29 18:52:09 GMT

- Autopsy extracted web history results pane (step 4.3 from Part 4)

