Blue Team Level 1 Certification (Standard)

Introduction to BTL1

- ~~Welcome to Blue Team Level 1!~~ — 4 Topics
- ~~Lab and Forum Access~~

SECURITY FUNDAMENTALS DOMAIN

- ~~Introduction to Security Fundamentals~~ — 1 Topic
- ~~Soft Skills~~ — 7 Topics
- ~~Security Controls~~ — 5 Topics | 1 Quiz
- ~~Networking 101~~ — 6 Topics | 1 Quiz
- ~~Management Principles~~ — 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

- ~~PA1) Introduction to Emails and Phishing~~ — 7 Topics | 1 Quiz
- ~~PA2) Types of Phishing Emails~~ — 10 Topics | 2 Quizzes
- ~~PA3) Tactics and Techniques Used~~ — 12 Topics | 2 Quizzes
- ~~PA4) Investigating a Phishing Email~~ — 8 Topics | 2 Quizzes
- ~~PA5) Analysing URLs, Attachments, and Artifacts~~ — 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions — 12 Topics | 1 Quiz
- PA7) Report Writing — 7 Topics | 1 Quiz
- PA8) Phishing Response Challenge — 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

- TI1) Introduction to Threat Intelligence — 7 Topics
- TI2) Threat Actors & APTs — 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence — 7 Topics | 1 Quiz
- TI4) Tactical Threat Intelligence — 7 Topics | 1 Quiz
- TI5) Strategic Threat Intelligence — 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns — 6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

- DF1) Introduction to Digital Forensics — 5 Topics
- DF2) Forensics Fundamentals — 10 Topics | 5 Quizzes

Windows Artifacts – Internet Browsers

This lesson will focus on artifacts that can be gathered from internet browsers. These can be a goldmine for information relevant to a digital forensic investigation, such as websites that have been visited, when they were last visited, what the user did on the websites, files that have been downloaded, search form strings, autofill usernames and password, and lots more. We will be looking at the three most popular web browsers on Windows: **Microsoft Edge, Google Chrome, and Mozilla Firefox.** The artifacts we will be looking at are:

- Cookies
- Favorites
- Downloaded Files
- URLs Visited
- Searches
- Cached Webpage
- Cached Images

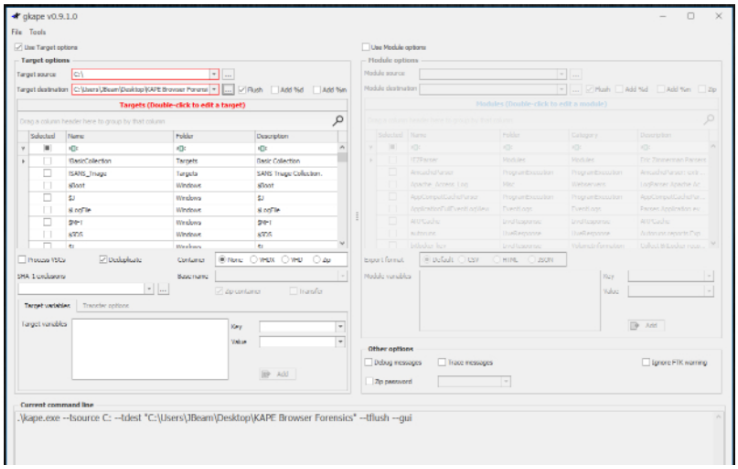
For this lesson on browser forensics, we are going to be using three main tools, and approaching this from a live acquisition view, meaning that we are investigating a powered-on system that we have access to. We will be using:

- **KAPE** – Download
- **Browser History Viewer** – Download (Choose the 100% free version)
- **Browser History Capturer** – Download

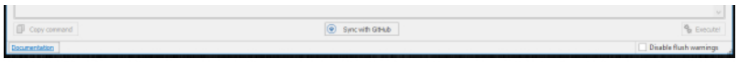
ACQUISITION VIA KAPE

We have already covered KAPE in **DF3) Digital Evidence Collection** – but for this lesson, we're going to utilize the browser-based modules to collect information from a running system, retrieving data from Chrome, Edge, and Firefox. Feel free to download KAPE and follow along, analyzing your own systems browser files!

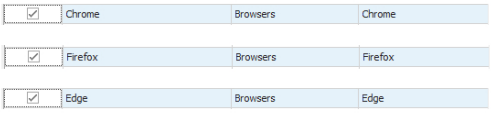
To start, let's load up KAPE and select our target directory and output directory. We'll be analyzing our host system's C drive, with an output destination as `/Desktop/KAPE Browser Forensics`.



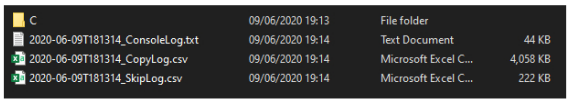
DF3) Digital Evidence Collection
8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
Section Introduction, Windows Investigations
Windows Artifacts – Programs
Lab) Windows Investigation 1
Windows Artifacts – Internet Browsers
Lab) Windows Investigation 2
Activity) End of Section Review, Windows Investigations
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 2 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes
BTL1 EXAM
Exam Preparation
Using RDP and SSH
How to Start Your Exam



Next, we need to select browser-based Targets, so we can collect the files we need to perform browser forensics. We're going to enable the Targets for Chrome, Firefox, and Edge.

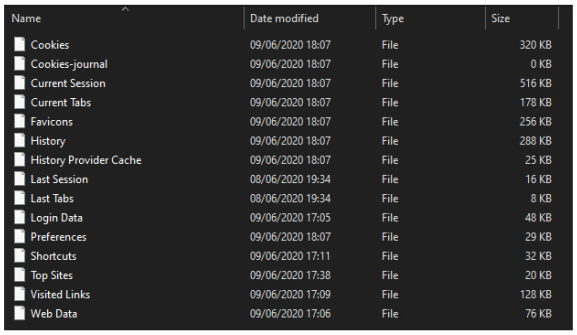


That's it – we can now run KAPE by clicking on "Execute!" in the bottom right corner. KAPE took 52 seconds to gather all the information we requested. Opening our defined output folder we can see the files we retrieved.



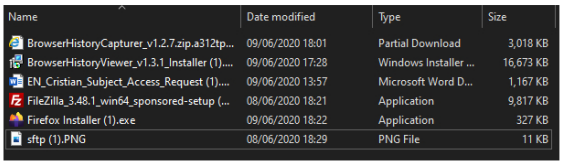
C	09/06/2020 19:13	File folder	
2020-06-09T181314_ConsoleLog.txt	09/06/2020 19:14	Text Document	44 KB
2020-06-09T181314_CopyLog.csv	09/06/2020 19:14	Microsoft Excel C...	4,058 KB
2020-06-09T181314_SkipLog.csv	09/06/2020 19:14	Microsoft Excel C...	222 KB

We can find lots of interesting Google Chrome files at the following file path: `KAPE Browser Forensics\C\Users\JBeam\AppData\Local\Google\Chrome\User Data`



Name	Date modified	Type	Size
Cookies	09/06/2020 18:07	File	320 KB
Cookies-journal	09/06/2020 18:07	File	0 KB
Current Session	09/06/2020 18:07	File	516 KB
Current Tabs	09/06/2020 18:07	File	178 KB
Favicons	09/06/2020 18:07	File	256 KB
History	09/06/2020 18:07	File	288 KB
History Provider Cache	09/06/2020 18:07	File	25 KB
Last Session	08/06/2020 19:34	File	16 KB
Last Tabs	08/06/2020 19:34	File	8 KB
Login Data	09/06/2020 17:05	File	48 KB
Preferences	09/06/2020 18:07	File	29 KB
Shortcuts	09/06/2020 17:11	File	32 KB
Top Sites	09/06/2020 17:38	File	20 KB
Visited Links	09/06/2020 17:09	File	128 KB
Web Data	09/06/2020 17:06	File	76 KB

We can also find interesting Firefox files at the following file path (please note we haven't used Firefox much on this PC, so there's limited data to display compared to Edge/Chrome): `KAPE Browser Forensics\C\Users\JBeam\AppData\Roaming\Mozilla\Firefox\Profiles`



Name	Date modified	Type	Size
BrowserHistoryCapturer_v1.2.7.zip.a312tp...	09/06/2020 18:01	Partial Download	3,018 KB
BrowserHistoryViewer_v1.3.1_Installer (1)....	09/06/2020 17:28	Windows Installer ...	16,673 KB
EN_Cristian_Subject_Access_Request (1)....	09/06/2020 13:57	Microsoft Word D...	1,167 KB
FileZilla_3.48.1_win64_sponsored-setup (...	08/06/2020 18:21	Application	9,817 KB
Firefox Installer (1).exe	09/06/2020 18:22	Application	327 KB
sftp (1).PNG	08/06/2020 18:29	PNG File	11 KB

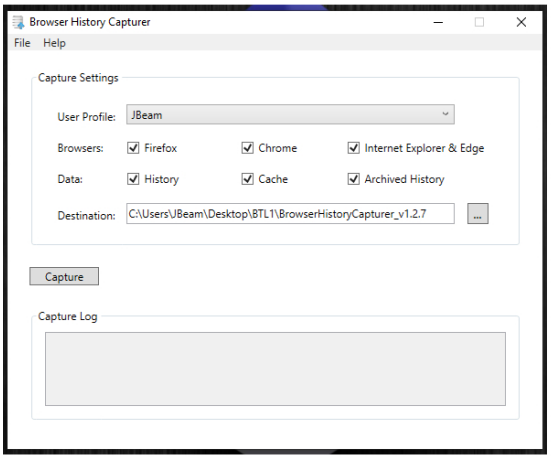
The best way for you to get a feel of browser forensics is to try it out on your own system (or if you don't run Windows as your host OS, create a Windows VM, spend a day browsing the web inside it, then complete the actions we've done above to analyze your browsing activity!). We highly suggest that students grab their own browser files via KAPE and take some time to mess around looking at what has been retrieved, and analyzing their own files.

BROWSER HISTORY VIEWER

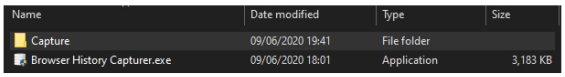
There's another way we can retrieve browser information, using two tools: Browser History Capturer (BHC) and Browser History Viewer (BHV), free tools developed by Foxton Forensics. We can run Browser History Viewer on its own, but if you're running it on the system you're investigating, it will fail at trying to retrieve Microsoft Edge files, even if it is run with elevated admin privileges. That's where Browser History Capturer comes in, we can forcefully retrieve all important files for browser forensics, and then import it into BHV. These tools allow us to view a huge amount of browsing history, when sites were accessed, visit counts, cached webpages, and cached images. If

you want to follow along, download the tools, and analyze your own system!

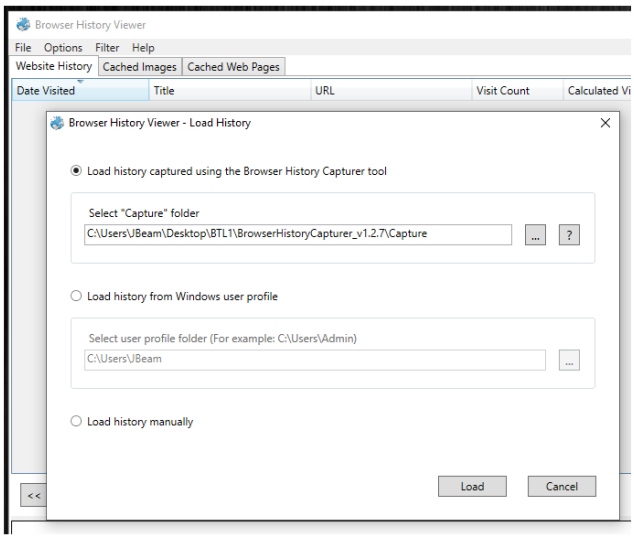
First, let's run Browser History Capturer to collect all the files we need. We need to select the User Profile we want to collect data on. The Browsers and Data tickboxes will be toggled on by default, so we can leave them as they are. The destination by default will be a new directory named "Capture" within the BHC folder. We can alter this or leave it as it is – for this example we won't alter the destination location. Now we can click on Capture.



We can now see a folder named "Capture" in our BHC directory.

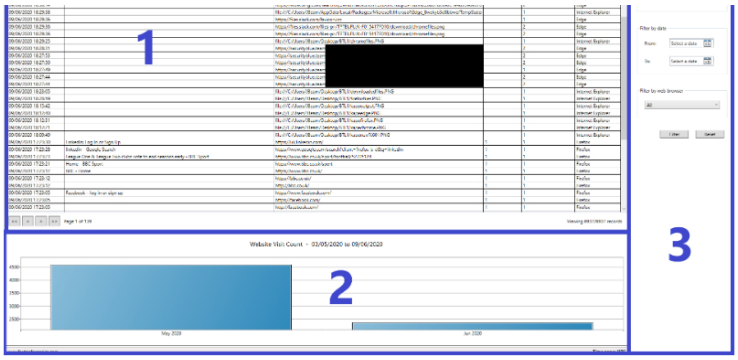


Next we need to import this directory into Browser History Viewer. Open BHV and go to **File** > **Load History**. Select "Load history captured using the Browser History Capturer tool" and navigate to the "Capture" directory we just created using BHC. Then click Load.

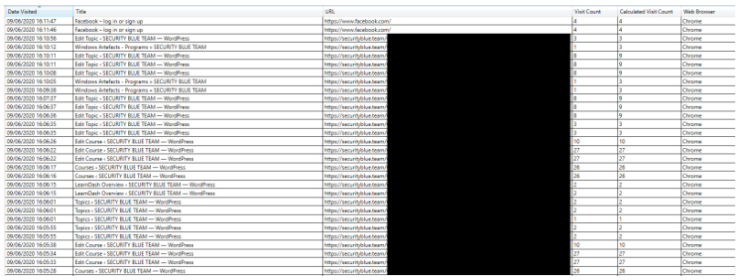


Now that we've imported the data, let's go through the different panes that Browser History Viewer has. We have split it into three regions.

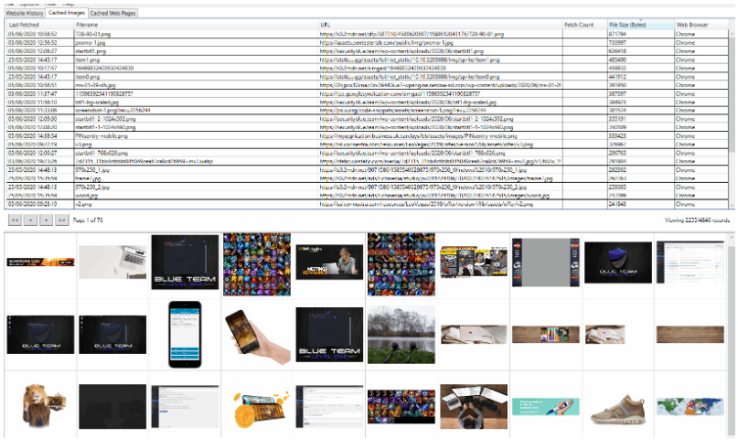
- **Pane 1 –** This is where the information imported is displayed, with three tabs: Website History, Cached Images, and Cached Web Pages. On the default tab Website History we can see the dates when sites were visited, the titles of the site if available, the full URL, visit counts, and the browser used to access the web resources.
- **Pane 2 –** Website Visit Count, showing how many resources have been accessed per month.
- **Pane 3 –** Filter Pane, allowing us to filter by keywords (such as website names), filter by date, or filter by web browser.



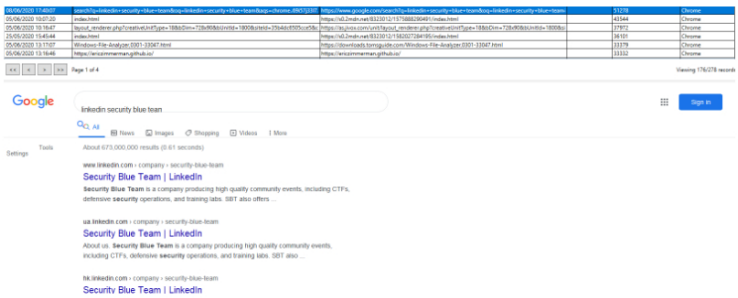
Let's filter on web resources that have been accessed via the Chrome browser by selecting Chrome from the dropdown list in Pane 3. In the below screenshot you can see it's mainly us slaving away on the Blue Team Level 1 course! We can see when we visited certain webpages, how many times we've visited them, and that this activity occurred in the Chrome browser.



Next let's take a look at the Cached Images tab of Pane 1. Below is a screenshot that shows us navigating between different pages, which shows the URLs of images, and displays them where Pane 2 was previously. These are typically downloaded from adverts, but can also indicate user browsing activity.



And finally, let's take a look at the third tab of Pane 1, Cached Web Pages. This tab allows us to view webpages that have been downloaded to the system to speed up loading time. In the below screenshot we have selected a web request on 08/06/2020 at 17:40, which is a Google search for "linkedin security blue team". In the bottom pane we can visually see the screen that the user would've viewed when performing this search.



If you haven't already, we highly suggest you play around analyzing your own system to view browsing history, cached images, and cached web pages using KAPE, and Browser History Capturer and Browser History Viewer. In the next lesson we have designed a mock scenario, where you are taking part in a digital forensics and incident response situation, analyzing a user's browsing history, as they have downloaded malware. Can you work out where it came from?

Quizzes

Lab) Windows Investigation 2

Previous Topic

Back to Lesson

Privacy & Cookies Policy

Privacy - Terms