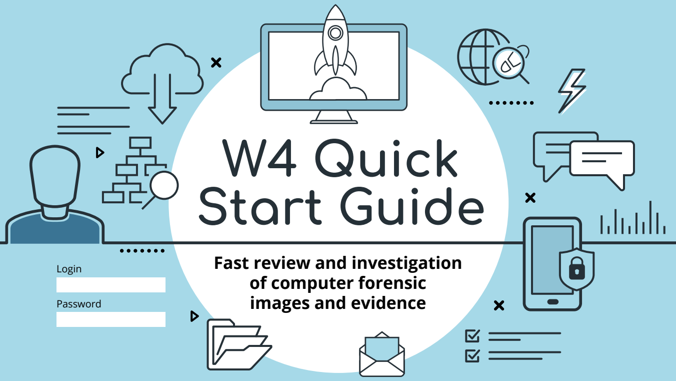
Who | What | Where | When. Simple.

Vound



W4 Quick Start Guide

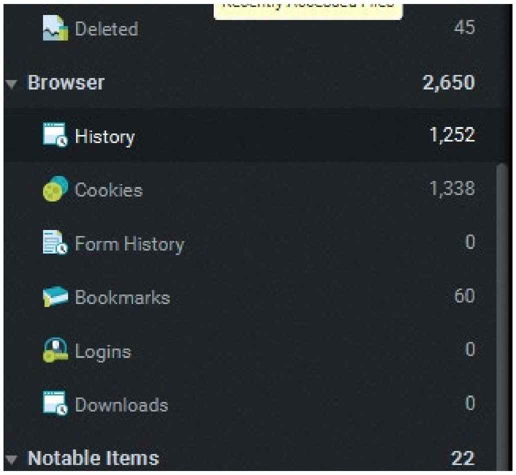
Fast review and investigation of computer forensic images and evidence

Misuse of Company Time

When discussing misuse of the company's time, we are referring to using the company's computer for personal uses during work hours. Some examples of this include the employee using the company's internet for their personal use, or the user using the company's computer to work on another business that the user has outside of his normal job. In these examples, work hours are being used for personal tasks.

There are a number of different scenarios where work time can used for personal use. Each of these scenarios include 'time theft', which is grounds for disciplinary action, and therefore an investigation may be justified. However, when investigating such events, different scenarios would require different types of analysis, and you would be likely analysing different artifacts. We cannot cover all of these scenarios in this post, so we have provide one example. In this example we have suspicion that a user is using the companies computer and internet services for his own purposes during work time. Lets presume that you have a forensic copy of the user's system, and you have indexed the forensic copy in W4.

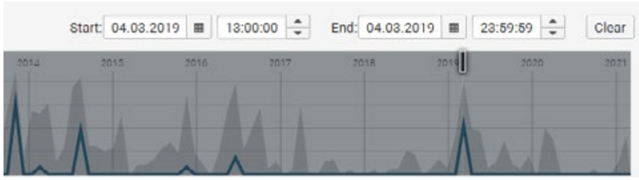
1. In this example we are investigating internet activity, so we have selected the History category on the left hand panel. This shows all internet history on the system.



Deleted	45
Browser	2,650
History	1,252
Cookies	1,338
Form History	0
Bookmarks	60
Logins	0
Downloads	0
Notable Items	22

Searching all of the internet history for every day can be overwhelming. In this type of investigation, one approach would be to break the activity down into one day at a time. There may be some other investigative information available that can help with filtering. For example, it may be known that the user only did personal browsing in the afternoon when other colleagues were out of the office. That type of information can further help you to narrow down timings, and focus of specific hours.

In this example we have been told that the user has been observed to browse the internet when he gets back from lunch at around 1pm. With that information in mind, we have set the timeline for a specific day, and started our time frame from 1pm.



Start: 04.03.2019 13:00:00 End: 04.03.2019 23:59:59

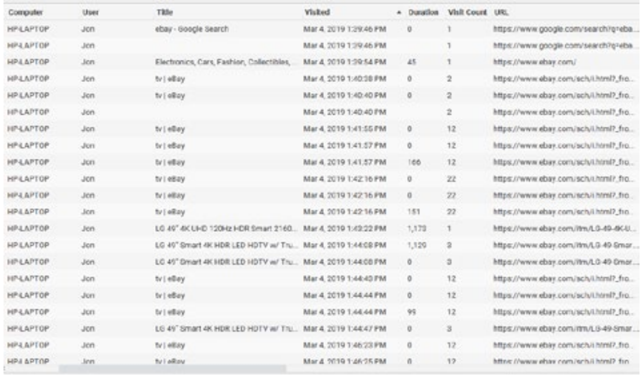
2. The settings above provides us with all of the internet history for this time period. An important aspect to check, is that this data belongs to the user under investigation. If a system is shared by different users, you should tag only the activity by the user in question. That way you can search on that tag to only show their activity.

   We have some great information about the user's internet activity in the table view. Immediately we can see the following:

   - That the user ran a Google search for the term ebay.
   - From there, they entered the ebay site and looked in specific categories.
   - The information in the **Title** field shows us that the user was looking at TVs, specifically 49" LG TVs.
   - The Visited column shows that the user browsed for TVs from around 1:40pm to around 2:10pm.

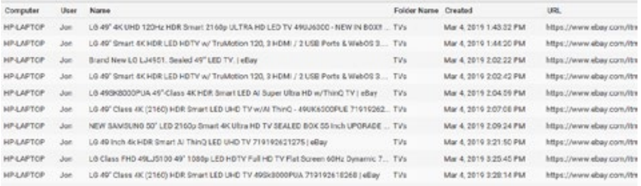
Then there was a break, and more browsing for TVs commenced from around 3:22pm.

- We can see the duration of how long the webpage was open on the system. Note that this does not mean the user was actively browsing the page. For example, the page could have been opened, then the user may have gone out for some time.
- We can see the visit count. This represents how many times that particular page, or items on that page were clicked on.
- We can also see the URL for the visited page. This allows us to copy the link and us a browser to view the page that the user was viewing.



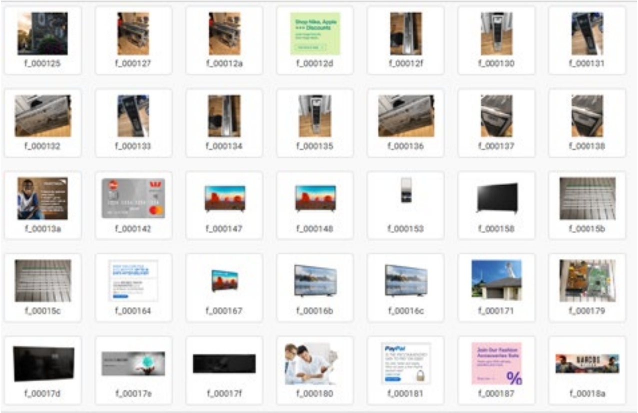
Computer	User	Title	Visited	Duration	Visit Count	URL
HP-LAPTOP	Jon	ebay - Google Search	Mar 4, 2019 1:39:46 PM	0	1	https://www.google.com/search?q=eba...
HP-LAPTOP	Jon		Mar 4, 2019 1:39:46 PM		1	https://www.google.com/search?q=eba...
HP-LAPTOP	Jon	Electronics, Cars, Fashion, Collectibles, ...	Mar 4, 2019 1:39:54 PM	45	1	https://www.ebay.com/
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:40:38 PM	0	2	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:40:40 PM	0	2	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon		Mar 4, 2019 1:40:40 PM		2	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:41:55 PM	0	12	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:41:57 PM	0	12	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:41:57 PM	166	12	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:42:16 PM	0	22	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:42:16 PM	0	22	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:42:16 PM	151	22	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	LG 49" 4K UHD 120Hz HDR Smart 2160...	Mar 4, 2019 1:43:22 PM	1,173	1	https://www.ebay.com/itm/LG-49-4K-U...
HP-LAPTOP	Jon	LG 49" Smart 4K HDR LED HDTV w/ Tru...	Mar 4, 2019 1:44:08 PM	1,120	3	https://www.ebay.com/itm/LG-49-Smar...
HP-LAPTOP	Jon	LG 49" Smart 4K HDR LED HDTV w/ Tru...	Mar 4, 2019 1:44:08 PM	0	3	https://www.ebay.com/itm/LG-49-Smar...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:44:40 PM	0	12	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:44:44 PM	0	12	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:44:44 PM	99	12	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	LG 49" Smart 4K HDR LED HDTV w/ Tru...	Mar 4, 2019 1:44:47 PM	0	3	https://www.ebay.com/itm/LG-49-Smar...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:46:23 PM	0	12	https://www.ebay.com/sch/i.html?_fro...
HP-LAPTOP	Jon	tv | eBay	Mar 4, 2019 1:46:25 PM	0	12	https://www.ebay.com/sch/i.html?_fro...

3. Another area of interest is the Bookmarks category. We can look at this category for more user activity within the time frame. This category shows if any bookmarks were created by the user. In this case, we can see that 10 bookmarks were created by the user. The Name column shows us a descriptive name for the bookmark, along with the site that was being viewed. We can also see that the bookmarks were placed into a folder named TVs. This indicates that the user created a custom folder to capture the pages which he was viewing, so that he could quickly reference them later.



Computer	User	Name	Folder Name	Created	URL
HP-LAPTOP	Jon	LG 49" 4K UHD 120Hz HDR Smart 2160p ULTRA HD LED TV 49UJ6300 - NEW IN BOX!! ...	TVs	Mar 4, 2019 1:43:32 PM	https://www.ebay.com/itm
HP-LAPTOP	Jon	LG 49" Smart 4K HDR LED HDTV w/ TruMotion 120, 3 HDMI / 2 USB Ports & WebOS 3....	TVs	Mar 4, 2019 1:44:20 PM	https://www.ebay.com/itm
HP-LAPTOP	Jon	Brand New LG LJ4951. Sealed 49" LED TV. | eBay	TVs	Mar 4, 2019 2:02:22 PM	https://www.ebay.com/itm
HP-LAPTOP	Jon	LG 49" Smart 4K HDR LED HDTV w/ TruMotion 120, 3 HDMI / 2 USB Ports & WebOS 3....	TVs	Mar 4, 2019 2:02:42 PM	https://www.ebay.com/itm
HP-LAPTOP	Jon	LG 49SK8000PUA 49"-Class 4K HDR Smart LED AI Super Ultra HD w/ThinQ TV | eBay	TVs	Mar 4, 2019 2:04:59 PM	https://www.ebay.com/itm
HP-LAPTOP	Jon	LG 49" Class 4K (2160) HDR Smart LED UHD TV w/AI ThinQ - 49UK6300PUE 71919262...	TVs	Mar 4, 2019 2:07:08 PM	https://www.ebay.com/itm
HP-LAPTOP	Jon	NEW SAMSUNG 50" LED 2160p Smart 4K Ultra HD TV SEALED BOX 55 Inch UPGRADE ...	TVs	Mar 4, 2019 2:09:24 PM	https://www.ebay.com/itm
HP-LAPTOP	Jon	LG 49 Inch 4k HDR Smart AI ThinQ LED UHD TV 719192621275 | eBay	TVs	Mar 4, 2019 3:21:50 PM	https://www.ebay.com/itm
HP-LAPTOP	Jon	LG Class FHD 49LJ5100 49" 1080p LED HDTV Full HD TV Flat Screen 60Hz Dynamic 7...	TVs	Mar 4, 2019 3:25:45 PM	https://www.ebay.com/itm
HP-LAPTOP	Jon	LG 49" Class 4K (2160) HDR Smart LED UHD TV 49SK8000PUA 719192618268 | eBay	TVs	Mar 4, 2019 3:28:14 PM	https://www.ebay.com/itm

4. Another artefact that you could look at is what images were downloaded to the system when the user was browsing the internet. The images from the internet cache below show a number of TVs. This is more evidence to show what the user was browsing at that time.



In summary, with W4 you can investigate a specific user's internet activity with little effort. W4 categorises the different artefacts so that they can be searched, filtered and displayed to highlight the most pertinent evidence to support the allegations of the case.