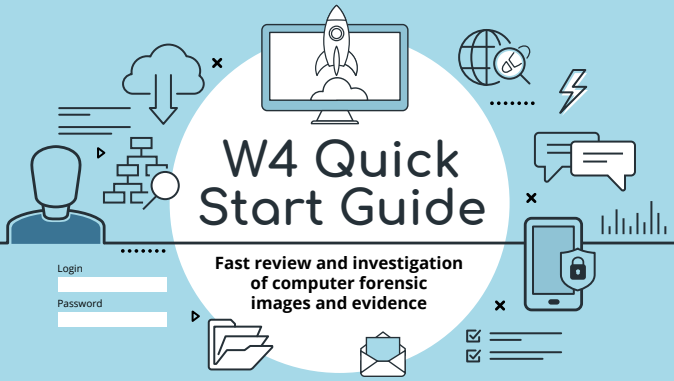
Who | What | Where | When. Simple.

Vound



Detecting IP Theft via USB Device

A common type of investigation is to determine whether any intellectual property has been taken from the company by employees who are leaving. In this guide we look at how W4 can be used to search for artifacts in relation to file access, and USB devices being used on a computer. Unfortunately there is no single log that categorically shows the actions of a file being copied from a computer to a USB drive. However, using the artifacts discovered with W4, we can form a strong presumption that files were likely copied to a USB device and taken from the company.

Below are the case details of a fabricated case that we will use as an example. Note that although the case details are fabricated, the data that you see in W4 is from actual user events.

Case details

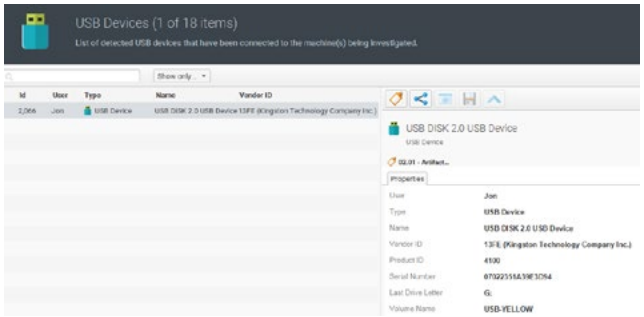
In this fabricated case, you have been notified about the following facts:

- A long time employee (Jon) left the company on 17 October 2018 at 4pm.
- He has informed the company that he is going to a competitor.
- On his last day, it was noticed that he arrived late, a little after 10am.
- On his last day, he was overheard talking about using a USB flash drive to take documents from the company. He goes on to say that he would use that information in the new company.
- On his last day, a forensic copy of his laptop was made after he left the building.
- During his employment, the user was issued with a Toshiba USB flash drive - serial number DC0686BDE247CD20ADFA89DC. This USB drive has been returned.
- There is now suspicion that he has indeed taken IP, and it needs to be investigated. You have been tasked with finding any information that indicates that the user has taken IP from the company on his last day.

Searching and analysis

1. Given that we are looking at for evidence in his last day, and we know the date and time for when the user arrived and left work, this time frame can be entered into the timeline to filter out irrelevant items based on date and time. As you can see, this dramatically reduces the overall items in the case to a very small subset for review and analysis.

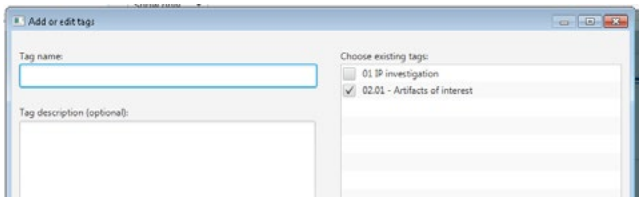
2. We also know that he was talking about using a USB flash drive to take the IP. We use the categories list on the left hand side to select the 'USB devices' category to see if any USB devices were connected within this time frame.



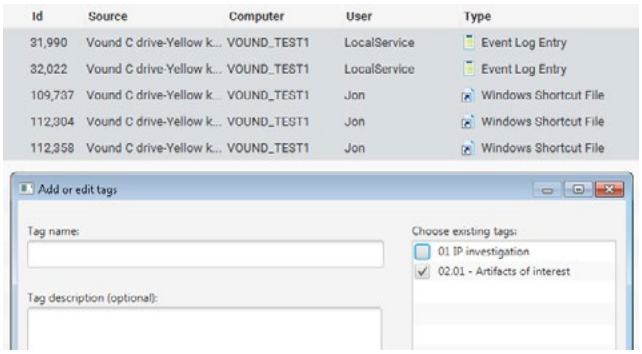
We can see that one USB device was connected to the system in this time frame. The USB flash drive is made by Kingston, and the serial number is 07022351A39E3D94. This confirms that it is not a company issued USB flash drive. Therefore, it is likely a USB flash drive that he owns.

We can also see that the mapped drive letter for this device is G:, and the volume name for the device is USB-YELLOW.

Now that we know that a USB device was used within the time frame, we can tag this item. I have tagged the item in a new tag called 'Artifacts of interest'.

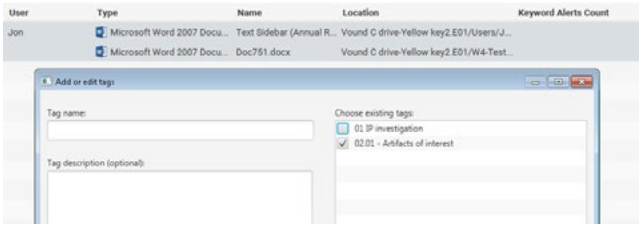


3. We know that the volume name for the USB flash drive is USB-YELLOW. Next we will look through the 'USB Device Activity' category for this name. In this case there are two items in the category that have this name. Clicking on these two categories shows us that five items are associated with the two categories. These items are shortcut files and event log entries. I have tagged these items with the same tag.



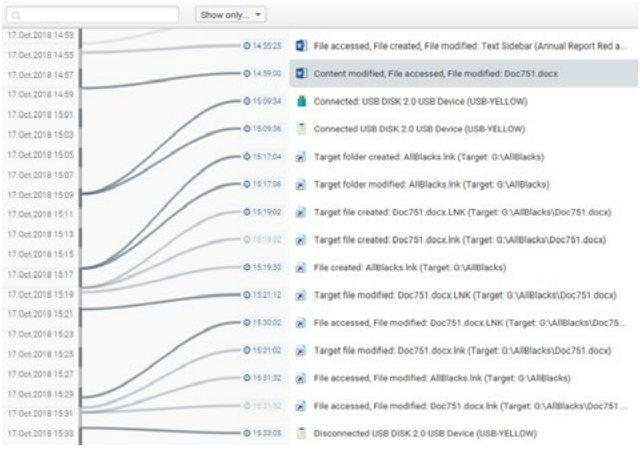
4. Documents are the most likely types to be taken from a company when an employee leaves. These can include customer lists, databases, product information, marketing information, pricing information etc.

   Next we look for access to documents. I click on the Documents category to show all documents that were accessed in this time frame. In this case there are two documents, and I have tagged them with the same tag. In total we have tagged eight artifacts of interest.



5. Now let's take a look at all of our artifacts in a sequential list of activity based on access times. In the Tags category, I clicked on the tag where I saved all of the artifacts. I then clicked on the Events button at the top right of the screen.

   With the tagged artifacts, the Events view shows us a lot of useful, and relevant information in relation to the activity which the user conducted within the time frame. In this mock example, lets imagine that the document 'Doc751.docx' is a document that contains the company's confidential information. Also, lets imagine that the user should not have been accessing this document. In the Events view, we can see that the file has been accessed by the user. In this context, this user's activity makes the document a likely candidate for IP theft.



The sample image above is from the Events view. The list of activity has been filtered to show only the activity from when the document was first accessed on that day, to when the user left the premises. This time window is a little over half an hour (just before 3:00pm to just after 3:30pm).

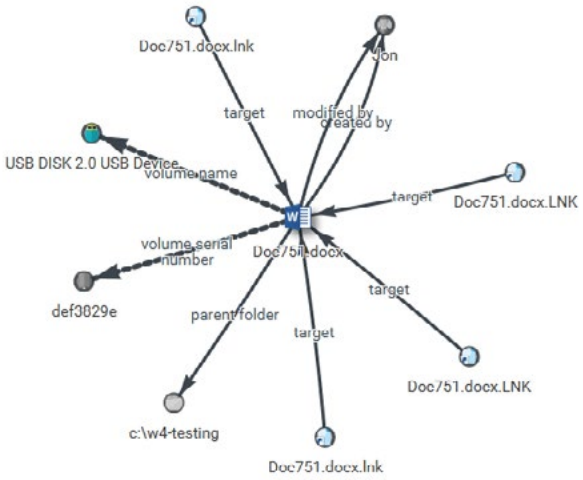
Stepping through the events shown in the Events view.

- At 14:59 we see that the document was accessed and modified.
- Around 10 minutes later, a USB drive was connected to the system.
- At 15:17, approximately 8 minutes after the USB drive was connected, a folder named 'AllBlacks' was created on the USB drive. Note that the USB drive is mapped as the G: drive.
- Approximately 2 minutes later, a link file with the same name as the document (Doc751.docx) was created on the USB drive. The link file contains information about the target file (the document in question). We can see that the link file tells us that the document was created in the AllBlacks folder

(on the USB drive) at this time. This suggests that the document was copied from the system to the USB drive.

- Further down the list we can see several times where the document (stored on the USB drive) has been accessed and modified. This activity could be related to the user opening the file on the USB drive and inspecting the content to make sure that it is accessible.
- Finally, the USB device is removed from the system.

6. W4 has a nice feature where we can see links and relationships between artifacts. The document can be shown in the Links tab by first selecting the Word document in question from the Events view, then clicking on the Links button. The Links tab shows a view of all of the artefacts which are related to this document.



From the Links view, you can immediately see the following associated artifacts:

- Which user has accessed the document.
- The location of the document.
- That the document is linked to a USB device.
- There are several shortcut files for the document.
- The mapped drive letter for the USB drive is G:

This alone is useful information regarding artifacts linked to the document. But, we can find out more information by diving deeper into the metadata of these linked artifacts. For example, all of the metadata and information regarding the associated USB drive can be viewed when you click on that artifact. We can see information such as: the user associated with the USB drive, what make the USB device is, the serial number, and the volume name. This is all useful information in regards to what to look out for if a search warrant is subsequently issued.

User	**Jon**
Type	**USB Device**
Name	**USB DISK 2.0 USB Device**
Vendor ID	**13FE (Kingston Technology Company Inc.)**
Product ID	**4100**
Serial Number	**07022351A39E3D94**
Last Drive Letter	**G:**
Volume Name	**USB-YELLOW**
Volume Serial Number	-

In addition, the links for the shortcut files also provide useful information. For example, in the properties view for one shortcut file, we can see that the location of the document is shown to be on the C: drive.

Doc751.docx.LNK
Windows Shortcut File
01 IP investigat...

Properties

User	**Jon**
Type	**Windows Shortcut File**
Name	**Doc751.docx.LNK**
App ID	-
Potential App Name	-
Target Path	**C:\W4-Testing\Doc751.docx**

However, another shortcut file shows that the document is stored in the 'AllBlacks' folder on the G: drive. From that information, along with the created dates for the shortcut files, we can infer that the document was copied from the C: drive to the USB drive.

Doc751.docx.LNK
Windows Shortcut File
02.01 - Artifact...

Properties

User	**Jon**
Type	**Windows Shortcut File**
Name	**Doc751.docx.LNK**
App ID	-
Potential App Name	-
Target Path	**G:\AllBlacks\Doc751.docx**

Note that this is an example of how W4 can be used to investigate IP theft. There may be other useful information located in other artifacts, or, other workflows used by investigators that are not mentioned here. Although following the workflow in this guide may help locate evidence of IP theft, you should follow your own standard operating procedures for investigating IP theft.