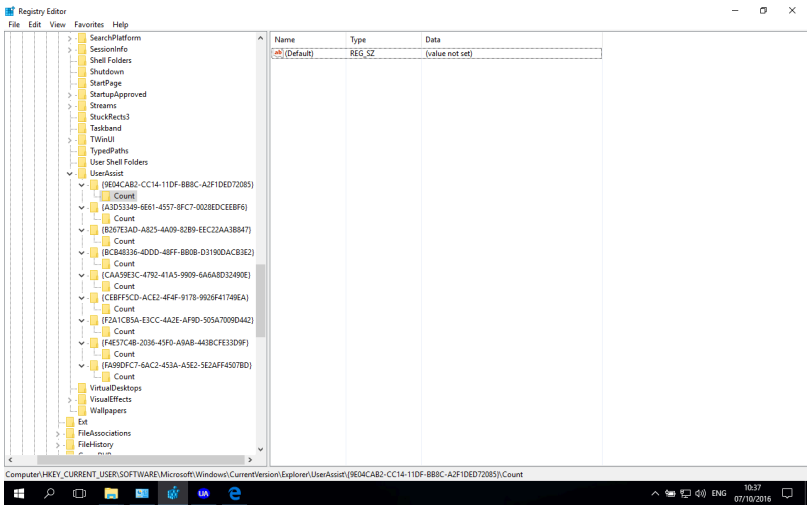
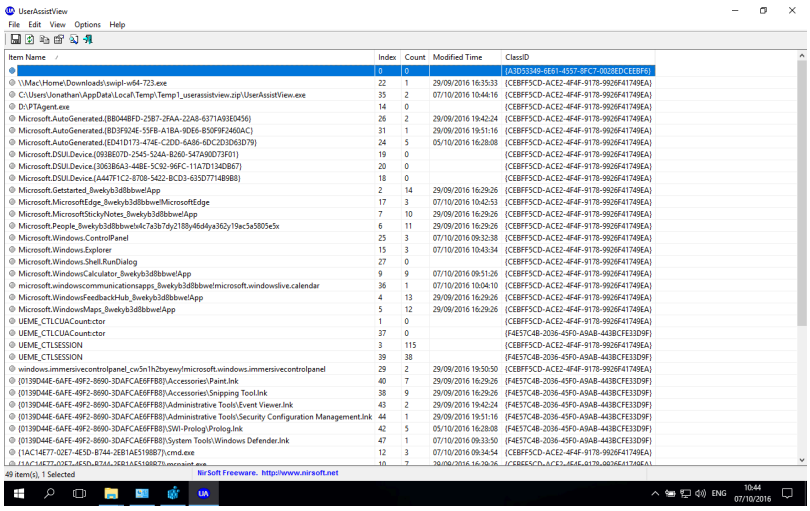
Forensic Lab 3
Student Name: Jonathan Riordan
Student ID: C13432152

In order to get to the following path. I had to click run and type the following in: %systemroot%\SysWOW64\regedit.
In the following path, the forensic evidence that can be retrieved is information such as the frequency of an application been executed. The last time the file was modified.



To view the folder, I downloaded a tool called User Assist View. It displays the application name, the index of that application. How many times that application has run. The last time the application was modified. Also the class ID can viewed.

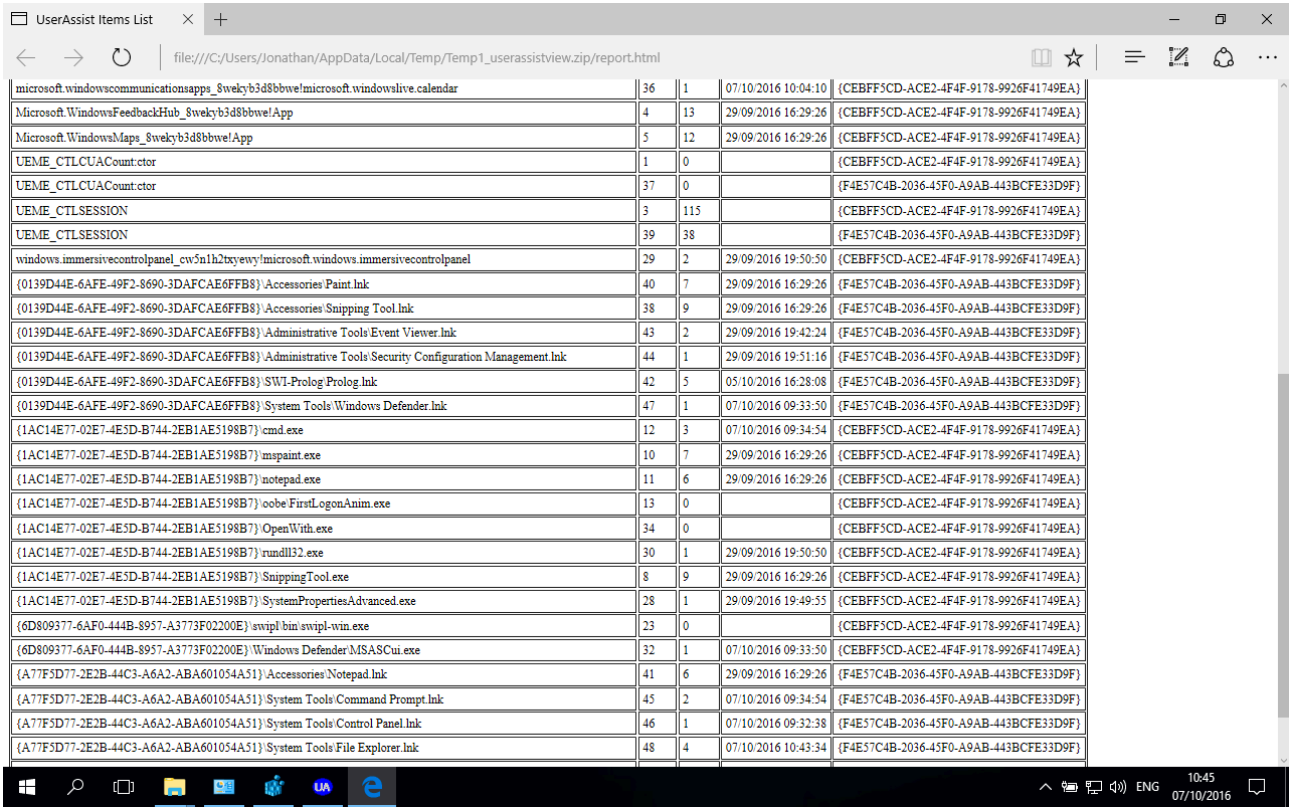


The tool also provides the ability where I am able to save the results in html, either for all the items or a selected item. eg application.

As I was running windows on a virtual machine, the amount of applications I have run are limited and the number of times that application has been run. For example to test that the software works, I ran calendar on windows. The result was saved in the top column of the screen shot. The item name, the index of the item, the number of times it was run and the last time it was modified where recorded. I have only ran calendar once since I got the Windows on a VM.

Item Name	Index	Count	Modified Time	ClassID
microsoft.windowscommunicationsapps_8wekyb3d8bbwe!microsoft.windowslive.calendar	36	1	07/10/2016 10:04:10	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}

The result of viewing all selected items in HTML.

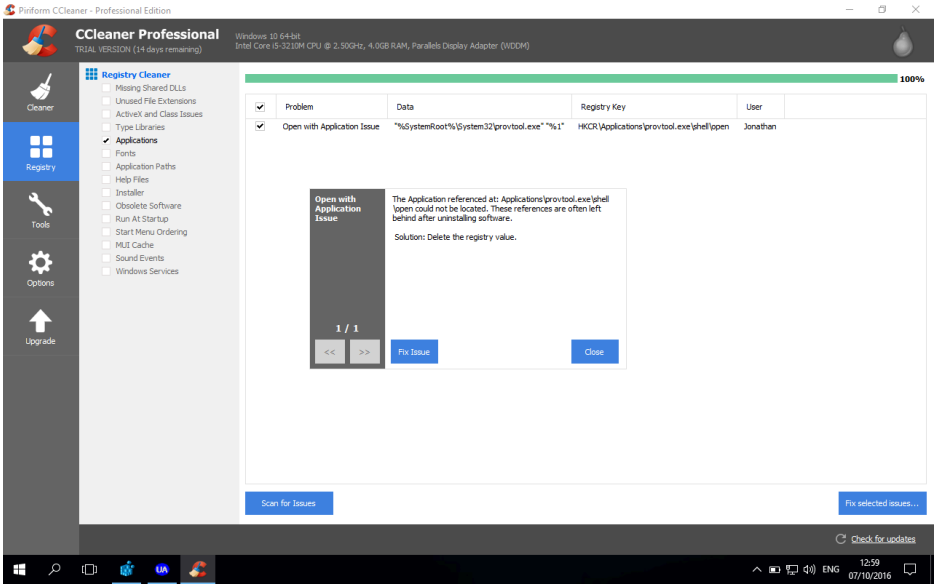


microsoft.windowscommunicationsapps_8wekyb3d8bbwe!microsoft.windowslive.calendar	36	1	07/10/2016 10:04:10	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App	4	13	29/09/2016 16:29:26	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Microsoft.WindowsMaps_8wekyb3d8bbwe!App	5	12	29/09/2016 16:29:26	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
UEME_CTLCUACount:ctor	1	0		{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
UEME_CTLCUACount:ctor	37	0		{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
UEME_CTLSESSION	3	115		{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
UEME_CTLSESSION	39	38		{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel	29	2	29/09/2016 19:50:50	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk	40	7	29/09/2016 16:29:26	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk	38	9	29/09/2016 16:29:26	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Administrative Tools\Event Viewer.lnk	43	2	29/09/2016 19:42:24	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Administrative Tools\Security Configuration Management.lnk	44	1	29/09/2016 19:51:16	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\SWI-Prolog\Prolog.lnk	42	5	05/10/2016 16:28:08	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\System Tools\Windows Defender.lnk	47	1	07/10/2016 09:33:50	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe	12	3	07/10/2016 09:34:54	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe	10	7	29/09/2016 16:29:26	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe	11	6	29/09/2016 16:29:26	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\oobe\FirstLogonAnim.exe	13	0		{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\OpenWith.exe	34	0		{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\rundll32.exe	30	1	29/09/2016 19:50:50	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe	8	9	29/09/2016 16:29:26	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SystemPropertiesAdvanced.exe	28	1	29/09/2016 19:49:55	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{6D809377-6AF0-444B-8957-A3773F02200E}\swipl\bin\swipl-win.exe	23	0		{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{6D809377-6AF0-444B-8957-A3773F02200E}\Windows Defender\MSASCui.exe	32	1	07/10/2016 09:33:50	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Notepad.lnk	41	6	29/09/2016 16:29:26	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\Command Prompt.lnk	45	2	07/10/2016 09:34:54	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\Control Panel.lnk	46	1	07/10/2016 09:32:38	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\File Explorer.lnk	48	4	07/10/2016 10:43:34	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}

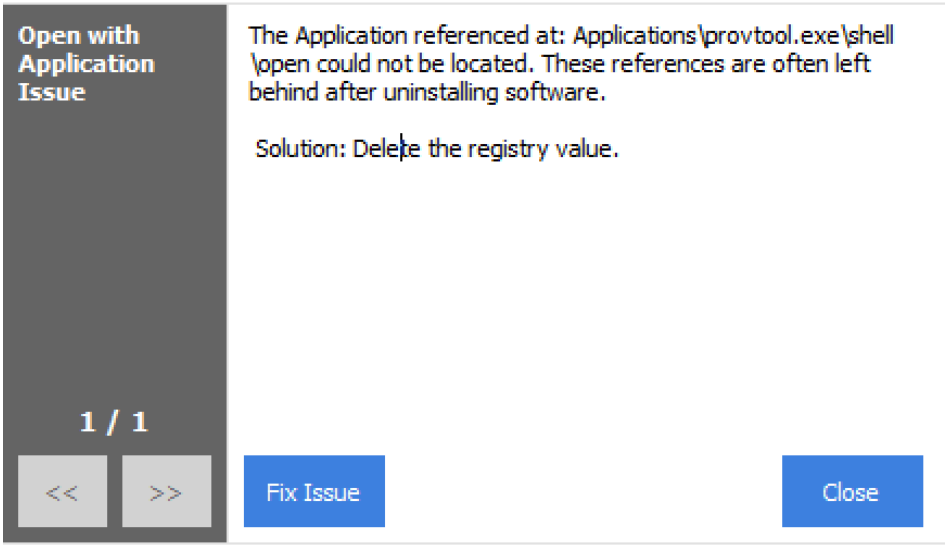
The following is steps involved in running CCleaner. The CCleaner is an utility on windows that can delete junk files left by applications on a machine. Information such as temp files or files left by application after they been deleted can be viewed by CCleaner and deleted.

The following steps are will demonstrate me deleting a registry file using CCleaner.

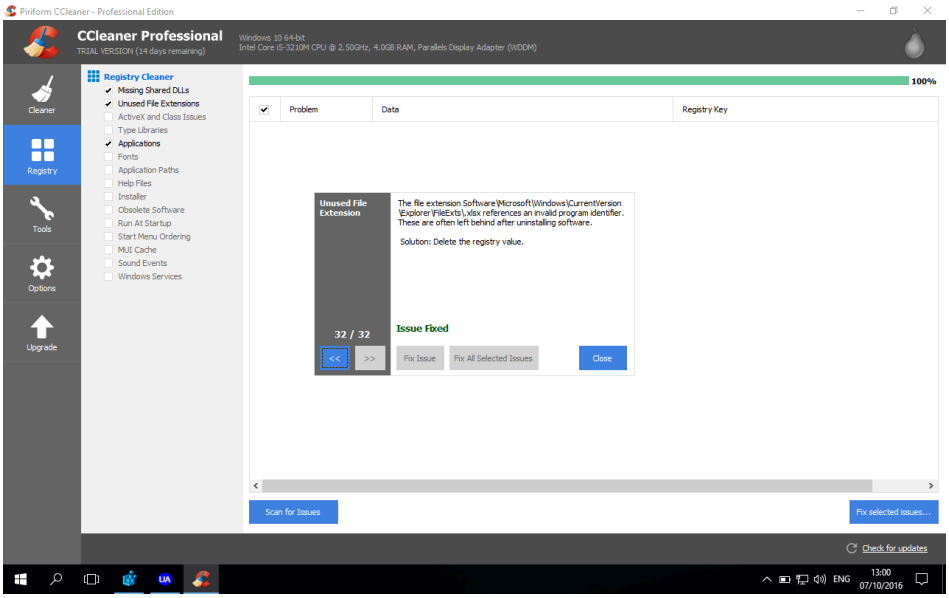
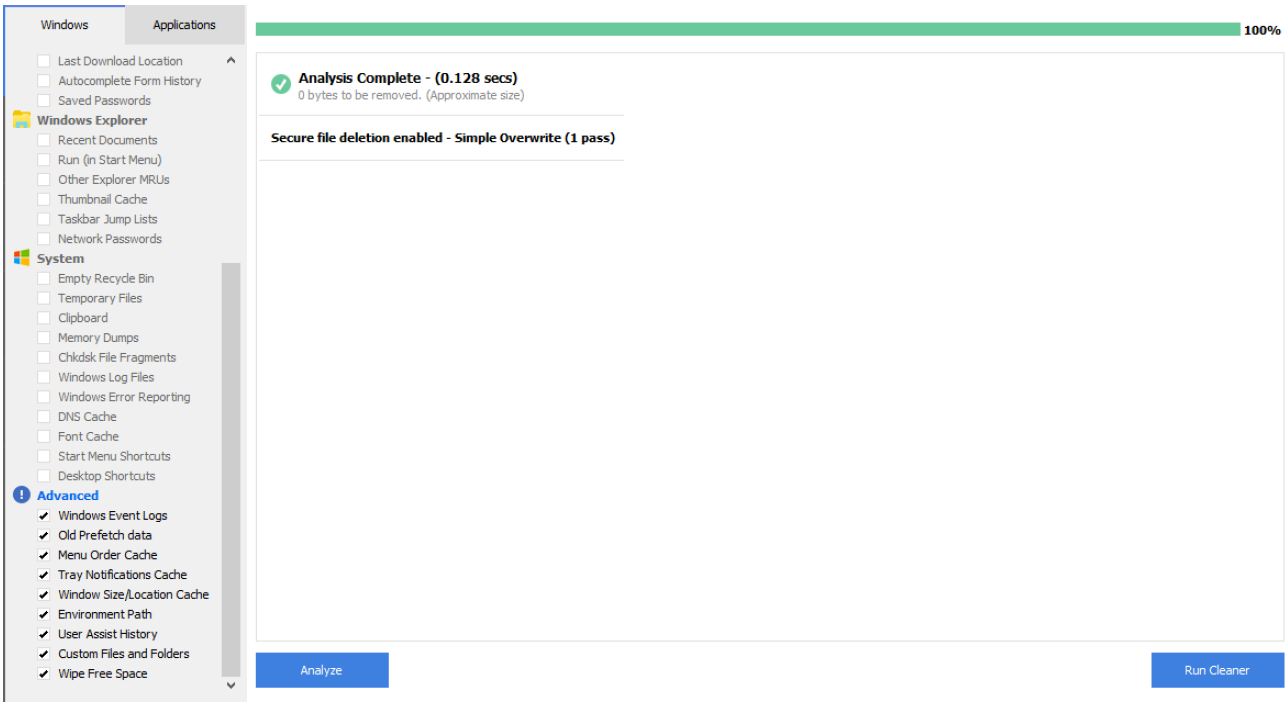
I clicked on the registry on the side bar and performed a search for just applications log. Only one results showed up called: Application\protocol.exe\shell\open.



To delete the file, just click fix issue. As a result of clicking “Fix Issue”, the registry entry is deleted.



The following screenshot displays that the issue was deleted.



I went to the cleaner section and in the advanced section tab. I ticked user assist history and custom files. The custom file because I included the path to the directory for the user assist. The path was HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}\,
When I ran the “analysis”, no results turned back up.
As a result, no user assist was deleted.