

O Sistema *UserAssist* do *Windows* e Respetivo Valor Forense

Jéssica Pedrosa, IPLeiria (2180067) e Patrícia Silva IPLeiria (2180068)

Abstract— In academic terms, it was written this article, with the theme “*UserAssist* system in *Windows* and its respective forensic value”. The *UserAssist* has some information about the user of the system and that information can become important in forensic investigations. In this article, it will be presented the exploration of *UserAssist* as well as the conclusions regarding its importance in the forensics investigations.

Index Terms—Registry, *UserAssist*, Tools, Forensic

Resumo— No âmbito académico foi elaborado este artigo com o tema “O sistema *UserAssist* do *Windows* e respetivo valor forense”. O *UserAssist* apresenta algumas informações acerca dos utilizadores do sistema que podem ser relevantes em contexto de investigações forenses. Neste artigo será apresentada a exploração efetuada ao *UserAssist* bem como as conclusões obtidas relativamente à sua importância na realização de investigações forenses.

Palavras-chave—Registry, *UserAssist*, Ferramentas, Forense

I. INTRODUÇÃO

Este artigo tem como tema “O sistema *UserAssist* do *Windows* e respetivo valor forense” e foi elaborado no âmbito da unidade curricular de Administração Segura de Sistemas Informáticos do Mestrado de Cibersegurança e Informática Forense do IPLeiria. O *UserAssist* apresenta várias informações relativas aos programas executados pelo utilizador. É na *Registry* que se guarda toda esta informação. Serão usadas duas ferramentas para analisar e facilitar a compreensão dos dados do *UserAssist*, nomeadamente a *UserAssistView* e a *UserAssist* 2.6.0.0. Com a exploração efetuada aos dados do *UserAssist*, será averiguada a importância deste conjunto de dados a nível forense e o papel que os mesmos podem tomar no decorrer de uma investigação forense.

Na secção II do presente artigo, encontram-se os conceitos fundamentais inerentes ao tema abordado. Já na secção III será apresentada a análise efetuada ao *UserAssist*. Deste modo, será apresentada a exploração efetuada às duas ferramentas e a análise aos registos do *UserAssist*. A averiguação da importância desses mesmos registos a nível forense é apresentada na secção IV. Na secção V serão mencionados alguns aspetos relevantes que foram sendo descobertos ao longo da exploração do tema. Por fim, encontra-se a bibliografia, secção VI, e os autores.

II. CONCEITOS FUNDAMENTAIS

A *Registry* do *Windows* foi introduzida no *Windows 3.1*, mas a partir do *Windows 95* e do *Windows NT* o seu uso foi estendido com o intuito de substituir os ficheiros *.ini*.

A *Registry* é uma base de dados hierárquica que guarda várias informações, entre as quais o *hardware*, sistema operativo e configurações. Por exemplo, quando um programa é instalado no computador, é adicionado ao *Registry* um novo conjunto de instruções, configurações e referências a ficheiros, na localização específica para o programa. De notar, que os programas não são obrigados a usar a *Registry*, tomando como exemplo os portáteis que guardam a sua informação em um ficheiro. [1] A *Registry* é suportada por vários ficheiros de sistema, como o *Sam*, o *Software*, o *Security*, o *Default* e o *System*.

Ela é organizada em colmeias que contém chaves. As chaves podem ser apresentadas como pastas e estas contém valores que são como ficheiros ou subchaves. Os valores são como um par nome/dados. A *Registry* está organizada em 5 colmeias principais, nomeadamente, a *HKEY_CURRENT_CONFIG* (HKCC), a *HKEY_CLASSES_ROOT* (HKCR), a *HKEY_CURRENT_USER* (HKCU), a *HKEY_LOCAL_MACHINE* (HKLM) e *HKEY_USERS* (HKU). Estas 5 colmeias podem ser visualizadas na Figura 1, a partir do *regedit*.

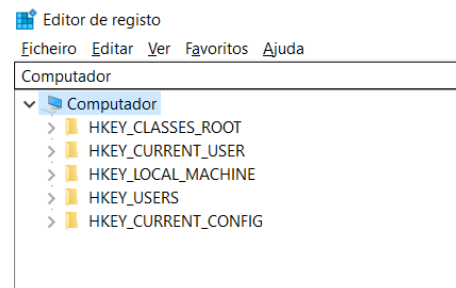


Figura 1 - As 5 colmeias principais

O *UserAssist* pode ser encontrado na *Registry*, na chave *HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist* e na *HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count*, sendo que o *GUID* é um identificador único e o *SID* é um identificador de segurança [2]. A colmeia *HKEY_CURRENT_USER* é criada

assim que o utilizador efetua login e guarda informação sobre o utilizador corrente, enquanto a *HKEY_USERS* guarda informação sobre todos os utilizadores. Os registos do *UserAssist* contêm várias informações que serão vistas com algum detalhe através de ferramentas na seção de análise. No entanto, este guarda informação sobre programas como quantas vezes foram executados, qual a data da última execução, quem o executou, entre outros. A informação do *UserAssist* é cifrada com o algoritmo *ROT13*, podendo ser decifrado pelo mesmo algoritmo. Em termos de cifragem este algoritmo é bastante fraco, no entanto impede a leitura direta da informação.

A informação do *UserAssist* pode ser manipulada, tal como a informação da *Registry*.

O *UserAssist* pode ter importância numa investigação forense. Uma investigação digital é uma investigação que se foca em dispositivos digitais que possam estar ligados a crimes. A investigação tenta responder às questões o quê, quem, como, quando e em alguns casos, porquê e onde. Deve-se tentar encontrar informação e provas que comprovem ou refutem uma hipótese. Toda a informação e provas devem ser obtidas de forma legal de forma a puder ser aceite em tribunal, pois estamos a falar de uma investigação forense.

III. ANÁLISE AO USERASSIST

Tal como já foi referido anteriormente, é na *Registry*, nas colmeias *HKEY_CURRENT_USER* e *HKEY_USERS* que se encontra a informação relativa ao *UserAssist*. Através do *regedit* disponível no sistema operativo *Windows*, é possível aceder ao *Registry* e, consequentemente, aos registos do *UserAssist* presentes em ambas as colmeias referidas. Na Figura 2 pode-se observar a localização do *UserAssist*, na colmeia *HKEY_CURRENT_USER* da *Registry*, através do *regedit*.

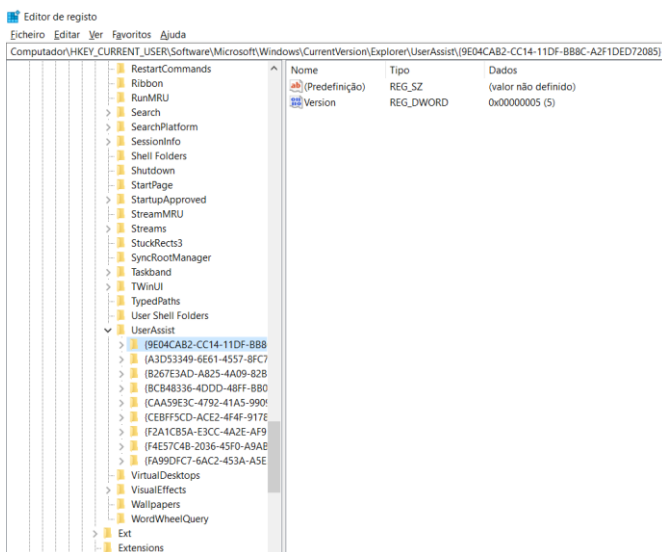


Figura 2 - Localização do *UserAssist* dentro da *Registry* na colmeia *HKEY_CURRENT_USER*

Contudo, em ambas as colmeias, os pares chave-valor

encontram-se cifrados com o algoritmo mencionado. É de referir que a cifragem dos registos por parte da *Microsoft* passa simplesmente por impedir que estes registos sejam acedidos ou até mesmo modificados por um utilizador-médio, ou seja, a *Microsoft* não pretende que esses mesmos registos sejam indecifráveis. [2] De certo modo, também é uma vantagem para o *Windows* que a decifragem dos dados seja um processo relativamente simples uma vez que, por exemplo, terá que fazer uso dos mesmos para obter a lista de programas acedidos mais frequentemente. [3]

É ainda importante mencionar a existência do ficheiro *NTUSER.DAT*. Este ficheiro guarda os valores da *Registry* de um determinado utilizador. As colmeias *HKEY_CURRENT_USER* e *HKEY_USERS* vão buscar informações a este ficheiro. Assim, é neste mesmo ficheiro que se encontram os registos relativos ao *UserAssist*. Este ficheiro encontra-se normalmente em “*C:\Users\nomeUtilizador*”, sendo o nome do utilizador, o da conta do utilizador em causa.

A. Ferramentas

Para este trabalho foram utilizados dois computadores - um *HP Spectre Notebook* e um *ASUS X556UF* - ambos com o sistema operativo *Windows 10 Home* (Figura 3 e Figura 4).

Item	Valor
Nome do SO	Microsoft Windows 10 Home
Versão	10.0.17134 Compilação 17134
Outra descrição do SO	Indisponível
Fabricante do SO	Microsoft Corporation
Nome do sistema	DESKTOP-D85TN0F
Fabricante do sistema	ASUSTeK COMPUTER INC.
Modelo do sistema	X556UF
Tipo do sistema	x64-based PC
Sistema SKU	ASUS-NotebookSKU
Processador	Intel(R) Core(TM) i7-6500U CPU @ 2.50GHz, 2592 Mhz, 2 Núcleo(s), 4 Process...
Data/versão de BIOS	American Megatrends Inc. X556UF.206, 10/09/2015
Versão SMBIOS	3.0
Versão do Controlador incorp...	255.255
Modo de BIOS	UEFI

Figura 3 – Informações do computador *ASUS*

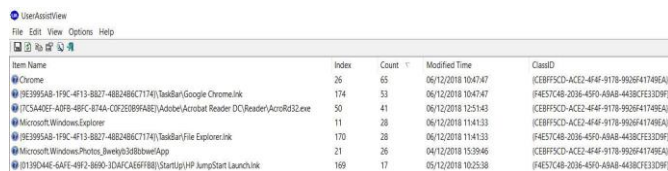
Item	Valor
Nome do SO	Microsoft Windows 10 Home
Versão	10.0.17134 Compilação 17134
Outra descrição do SO	Indisponível
Fabricante do SO	Microsoft Corporation
Nome do sistema	LAPTOP-94R08NMD
Fabricante do sistema	HP
Modelo do sistema	HP Spectre Notebook
Tipo do sistema	x64-based PC
Sistema SKU	Y7X62EA#AB9
Processador	Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz, 2904 Mhz, 2 N...
Data/versão de BIOS	Insyde F.42, 25/10/2018
Versão SMBIOS	3.0
Versão do Controlador ...	92.55
Modo de BIOS	UEFI

Figura 4 - Informações do computador *HP*

De modo a facilitar o acesso aos dados do *UserAssist*, existem disponíveis atualmente algumas ferramentas e aplicações que decifram os registos que se encontram cifrados e os apresentam de uma forma intuitiva e organizada mostrando, por exemplo, o nome do ficheiro ou até mesmo a

data/hora da última modificação desse mesmo registo.

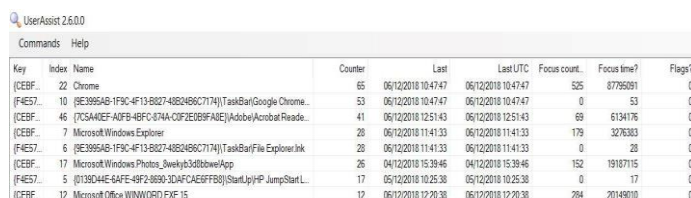
Uma das ferramentas usadas para a decifragem dos registos foi a *UserAssistView* da *Nirsoft*, um *website* que disponibiliza diversas ferramentas do sistema ou até mesmo do *browser*. Esta ferramenta encontra-se disponível em http://www.nirsoft.net/utils/userassist_view.html. A Figura 5 representa parte da informação mostrada por esta ferramenta.



Item Name	Index	Count	Modified Time	ClassID
Chrome	26	65	06/12/2018 10:47:47	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{9E395A8-1F9C-4F13-B827-4B824B6C7174}\TaskBar\Google Chrome.lnk	174	53	06/12/2018 10:47:47	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{7C5A4EF-A0F8-48FC-074A-C0F2E89FAE2}\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	50	41	06/12/2018 12:51:43	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Microsoft Windows Explorer	11	26	06/12/2018 11:41:33	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{9E395A8-1F9C-4F13-B827-4B824B6C7174}\TaskBar\File Explorer.lnk	170	26	06/12/2018 11:41:33	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Microsoft Windows Photos, Videos\3dibbwebApp	21	26	04/12/2018 15:39:46	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{13044E-64FE-49F2-8690-10AFC4E8FFB8}\StartUp\JumpStartLaunch.lnk	169	17	05/12/2018 10:25:38	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}

Figura 5 - Ferramenta *UserAssistView*

Uma outra ferramenta existente e também utilizada é o *User Assist 2.6.0.0*, desenvolvida por Didier Stevens e que se encontra disponível em <https://blog.didierstevens.com/programs/userassist/>. A Figura 6 representa parte da lista mostrada por essa ferramenta num sistema. Esta ferramenta possibilita carregar registos de um ficheiro da *Registry* local, um ficheiro *REG* ou de um ficheiro *DAT*.



Key	Index	Name	Counter	Last	Last UTC	Focus count	Focus time?	Flags?
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\TaskBar\Google Chrome.lnk	22	Chrome	65	06/12/2018 10:47:47	06/12/2018 10:47:47	525	07795991	0
{9E395A8-1F9C-4F13-B827-4B824B6C7174}\TaskBar\Google Chrome.lnk	10	Chrome	53	06/12/2018 10:47:47	06/12/2018 10:47:47	0	53	0
{7C5A4EF-A0F8-48FC-074A-C0F2E89FAE2}\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	46	Adobe Acrobat Reader	41	06/12/2018 12:51:43	06/12/2018 12:51:43	69	6134176	0
{9E395A8-1F9C-4F13-B827-4B824B6C7174}\TaskBar\File Explorer.lnk	7	Microsoft Windows Explorer	26	06/12/2018 11:41:33	06/12/2018 11:41:33	179	3276383	0
{9E395A8-1F9C-4F13-B827-4B824B6C7174}\TaskBar\3dibbwebApp	6	Microsoft Windows Photos, Videos\3dibbwebApp	26	04/12/2018 15:39:46	04/12/2018 15:39:46	152	19187115	0
{13044E-64FE-49F2-8690-10AFC4E8FFB8}\StartUp\JumpStartLaunch.lnk	5	Microsoft Office Word\Word\15	17	05/12/2018 10:25:38	05/12/2018 10:25:38	0	17	0
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\TaskBar\Google Chrome.lnk	12	Microsoft Office Word\Word\15	12	06/12/2018 12:20:38	06/12/2018 12:20:38	204	20149010	0

Figura 6 - Ferramenta *UserAssist v.2.6.0.0*

Entre estas duas ferramentas existem algumas divergências no que diz respeito aos detalhes dos registos que apresentam. Enquanto que na ferramenta *UserAssistView* só existe uma coluna relativa à data/hora da última modificação efetuada (coluna *Modified Time*), na ferramenta *User Assist 2.6.0.0* existe a coluna *Last* e *Last UTC*. A coluna *Last* apresenta a data/hora da última vez que um dado programa foi executado ao passo que a coluna *Last UTC* contém também a data/hora da última vez que um dado programa foi executado, mas em *UTC* (*Coordinated Universal Time*). Para além disso, ambas também apresentam o número de vezes que o programa foi executado (coluna *Counter* no *UserAssist 2.6.0.0* e coluna *Count* no *UserAssistView*) e ainda o *GUID* que se encontra na coluna *Key* no *UserAssist 2.6.0.0* e na coluna *ClassID* no *UserAssistView*. [3] A ferramenta *UserAssist 2.6.0.0* apresenta três colunas que a ferramenta *UserAssistView* não contém, nomeadamente, as colunas *Focus counter*, *Focus time?* e *Flags*. Quando um utilizador executa uma aplicação, o valor do número de vezes que a aplicação é executada é incrementado em um e o sistema inicia o controlo do tempo que a aplicação fica em foco. Quando a aplicação perder o foco ou for fechada, o tempo que o sistema obteve ao efetuar o

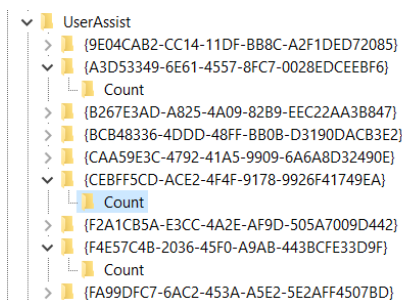
controlo referido vai ser incrementado ao valor presente em *Focus time?* (em milissegundos). Quando a aplicação voltar a ter o foco, o sistema reinicia a contagem do tempo em que a aplicação está em foco e incrementa em um o valor presente em *Focus counter?*, coluna esta que se refere ao número de vezes que uma aplicação está em foco.

Para testar os valores destas duas colunas, foi efetuado um teste com as entradas relativas ao *browser Google Chrome*. Assim, começou-se por abrir uma janela deste *browser* e identificou-se que o *Counter* do registo relativo a esta aplicação foi incrementado em um. De seguida, retirou-se de foco a janela do *browser* minimizando-se a mesma e, logo de seguida, verificou-se que o valor de *Focus time?* foi incrementado. De seguida, voltou-se a colocar a janela do *browser* em foco, maximizando-a. Com esta ação foi possível verificar que o valor de *Focus counter?* foi incrementado em um.

B. Análise dos Registos do UserAssist

Para a análise dos registos presentes no *UserAssist* foram utilizadas ambas as ferramentas apresentadas no ponto anterior de modo a conseguir perceber melhor que dados o *UserAssist* regista.

O *GUID* é um valor de 128 *bits* que identifica informações diversas do sistema operativo comum em algumas plataformas e que na *Registry* está representado em formato hexadecimal. De um modo geral, existem *GUID* referentes a aplicações, a ficheiros ou até mesmo a utilizadores. Por exemplo, o *GUID* {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} refere-se, por exemplo, à lista de aplicações que foram acedidas. Numa análise aos registos presentes no *UserAssist*, verificou-se que a entrada relativa ao executável do *browser Google Chrome* ou e o executável do *Adobe Acrobat View*, encontrava-se dentro desta chave. Já a chave {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F} possui as entradas relativas a atalhos de aplicações, como por exemplo os atalhos dos executáveis ditos acima. [4] A Figura 7 mostra algumas *GUIDs* que podem estar presentes no *UserAssist*.



GUID	Count	Focus time?
{9E04CAB2-CC14-11D1-B88C-A2F1DED72085}		
{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}		
{B267E3AD-A825-4A09-82B9-EEC22AA3B847}		
{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}		
{CAA59E3C-4792-41A5-9909-6A6A8D32490E}		
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}		
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}		
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}		
{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}		

Figura 7 - Algumas *GUIDs* presentes no *UserAssist*

Ao se efetuar uma análise à lista de registos do *UserAssist*, verificou-se a existência de algumas entradas com o nome *UEME_CTLSESSION* ou com o nome

UEME_CTLCUACount:ctor. Estas entradas correspondem a *UEME-strings* cuja a sua utilização tem como objetivo classificar o tipo de valor do *UserAssist*. Fora os dois exemplos já mencionados, existem outras *UEME-strings*, como por exemplo, *UEME_RUNPATH* que é um registo que guarda dados sobre os programas executados, *UEME_UITOOLBAR* que corresponde a uma entrada que guarda informações sobre os cliques efetuados nos botões da barra de ferramentas do *Windows Explorer*, ou ainda também a *UEME_UISCUT* que é uma entrada que conta os programas executados através de um atalho do *Desktop*. Os registos com o nome *UEME_CTLSESSION* é para o *session ID* e não têm qualquer tipo de dados relativos a aplicações que tenham sido executadas. Fora as *UEME-strings* já mencionadas também poderá surgir na lista de entradas do *UserAssist* a *UEME_UIQCUT* que corresponde a uma entrada que guarda o total de programa executados através de um atalho existente no *Quick Launch* menu, a *UEME_RUNCPL* que é um registo do *UserAssist* que guarda dados sobre *control applets* (.cpl) que tenham sido executados e ainda a *UEME_RUNPIDL* que é uma entrada que guarda dados sobre os *PIDLs* executados. [5]

Estes registos do *UserAssist* podem ser eliminados de diversas formas. Tal como se verificou através da realização de um teste, após ser efetuada uma limpeza do disco com o *software CCleaner*, com a opção “Historial de assistência ao utilizador” na secção “Avançado”, Figura 8, constatou-se que os registos do *UserAssist* eram eliminados. Para além disto, os registos do *UserAssist* também podem ser eliminados (tanto da lista de entradas das ferramentas como também do próprio *Registry*) através das ferramentas anteriormente mencionadas. Na ferramenta *UserAssistView* é possível eliminar os registos através da opção *Delete Selected Items* e na ferramenta *UserAssist 2.6.0.0* através da opção *Clear All*. Para além desses métodos, o próprio *regedit* do *Windows* também permite eliminar os registos presentes no *UserAssist*.

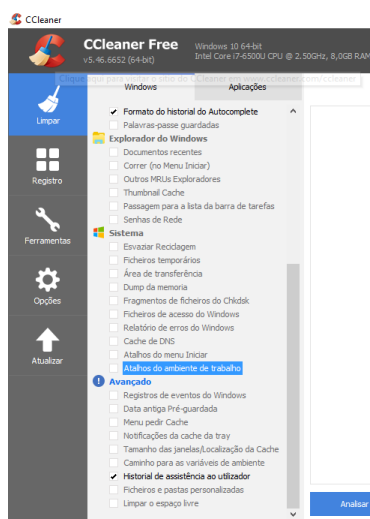


Figura 8 - Opção de limpeza do *UserAssist* no *CCleaner*

Após uma pesquisa foram encontrados alguns métodos que permitem efetuar essa mesma desativação. Os dois primeiros métodos que serão apresentados foram encontrados em respostas num fórum a uma dúvida similar.

Um dos métodos testados consistiu em criar duas novas chaves na *Registry* em *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced*, sendo que uma chave foi designada de *Start_TrackProgs* e a outra por *Start_TrackEnabled*. A ambas as chaves foi atribuído o valor zero de modo a indicar que se pretende que o *UserAssist* esteja desativo. De seguida, foram apagadas as subchaves da *Registry* que se encontram em *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist*. Por fim, desligou-se o dispositivo tendo-se voltado a ligar o mesmo logo de seguida. Assim, para verificar se o método de desativação aplicado funcionou, foram abertas algumas aplicações no dispositivo e, passado algum tempo, foi-se ao *regedit* verificar o estado da chave *UserAssist* e constatou-se que esta já possui subchaves com as respetivas *GUIDs*; no entanto, nenhuma dessas subchaves apresentava informação referente às aplicações executadas. Para além disto, recorreu-se ainda às ferramentas utilizadas neste trabalho de modo a verificar se as mesmas apresentavam algum registo tendo-se constatado que as mesmas se encontram sem qualquer registo. Todo este processo foi repetido através do *logout* da sessão do utilizador com posterior *login*, sendo que os resultados foram os mesmos. Deste modo, conclui-se que este método de desativação resultou. [6]

Um outro método testado para desativar o *UserAssist* consistiu em nas Definições do dispositivo, em Privacidade, no separador “Histórico de Atividade”, desseleccionar a opção “Permitir que o Windows recolha as minhas atividades deste PC”. Após isto, foi ainda eliminada a chave *UserAssist* da *Registry*. Antes de se desligar o computador, foram abertas várias aplicações e verificou-se que não foi efetuado nenhum registo destas ações nas ferramentas. Contudo, após se desligar e voltar a ligar o computador, ao abrir aplicações no mesmo, o sistema voltou a registar essas mesmas ações, surgindo valores no *UserAssist*. Assim, pelo apurado neste cenário de teste, este método de desativação só funciona enquanto a sessão se mantiver. [6]

Também foi ainda testado um método que consistiu em ir a *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist* e eliminar as pastas *Count* que se encontram dentro das pastas com as *GUIDs* *CEBFF5CD-ACE2-4F4F-9178-9926F41749EA* e *F4E57C4B-2036-45F0-A9AB-443BCFE33D9F*. Depois, cria-se uma nova chave designada de *Settings create* e, dentro dessa chave cria-se um valor *DWORD* com o nome *NoLog*, sendo que esse valor está a um. Voltou-se a executar o mesmo processo dos outros métodos, relativamente ao encerrar, iniciar e às aplicações e confirmou-se que as ferramentas voltam a mostrar os registos das ações tomadas durante o teste, sendo o resultado exatamente o mesmo que o método descrito anteriormente. [7]

O armazenamento destes registos pode ainda ser desativado.

IV. VALOR FORENSE DO *UserAssist*

Uma investigação forense digital consiste na obtenção da informação e provas através da investigação de dispositivos digitais que possam ter alguma ligação a crimes que foram praticados, mas sendo esse mesmo processo de obtenção efetuado de forma legal de modo a ser aceite em tribunal.

Os registos do *UserAssist* apresentam um conjunto de informação detalhada, como por exemplo, o nome do programa, a data/hora da última execução e até mesmo quantas vezes uma aplicação foi executada. Por vezes, pode ocorrer que este conjunto de dados seja relevante para clarificar certos aspetos de uma investigação. Supondo-se que existe a suspeita de o utilizador ter usado um programa de *hacking*, através dos registos existentes no *UserAssist* consegue-se perceber, caso exista alguma entrada relativa a esse programa, quantas vezes o mesmo foi executado. Por exemplo, se o *UserAssist* indicar que esse programa de *hacking* só foi executado algumas vezes, poderá ser possível provar que o programa em causa foi executado no dispositivo.

A informação presente na *Registry* para além de manipulável também pode ser eliminada. Deste modo, não se pode considerar que exista um nível elevado de fiabilidade dos registos presentes na *Registry*. Além do mais, com uma simples limpeza do disco com o recurso a um *software*, ou simplesmente eliminando as entradas da *Registry*, é possível apagar a informação presente na *Registry* e, consequentemente, os registos existentes do *UserAssist*. No entanto, perante este cenário, é importante mencionar que existem *software* que permitem recuperar dados que tenham sido eliminados. Também de referir que o *UserAssist* pode ser desativado, contudo, pode ser verificado se o mesmo foi desativado através dos rastros deixados pelo método de desativação aplicado.

Já no que diz respeito às *UEME-strings*, do *Windows XP* para o *Windows Vista*, verificou-se uma redução do número de *UEME-strings* existentes. Assim, do *Windows XP* para o *Windows Vista* ocorreu uma redução dos dados recolhidos pelas chaves do *UserAssist*.

Um outro aspeto que também é interessante no contexto forense é a possibilidade de através do *UserAssist* conseguir-se perceber se a aplicação foi executada através, por exemplo, de um atalho ou através do próprio executável.

V. CONCLUSÃO

Após ser efetuada a exploração e análise do *UserAssist*, foi possível obter um conjunto de inferências importantes.

Em primeiro lugar, o *UserAssist* é uma chave da *Registry* presente em duas colmeias – *HKEY_CURRENT_USER* e *HKEY_USERS*. A informação que o *UserAssist* apresenta corresponde a dados sobre a execução de programas pelo utilizador.

Em segundo lugar, de modo a facilitar a tarefa de análise desses mesmos dados, existem disponíveis algumas

ferramentas. No decorrer da exploração efetuada foram utilizadas duas dessas ferramentas que apresentam algumas diferenças no que diz respeito à informação contida nas entradas do *UserAssist*. Assim, o caminho mais viável passa por recorrer a diferentes ferramentas para análise do *UserAssist* de modo a se obter uma visão mais alargada do conteúdo dos registos.

Em terceiro lugar, numa investigação forense, por vezes, quando existirem certos aspetos que não estejam muito claros, o *UserAssist* poderá ser utilizado, em certos cenários, de modo a se obter um contexto mais alargado das ações do utilizador no sistema, no que diz respeito à execução de programas. Assim, o *UserAssist* pode providenciar algumas provas digitais adicionais. Contudo, há que ter em consideração que a *Registry* pode ser manipulada e os seus dados podem até mesmo ser eliminados como se verificou ao longo da exploração realizada. Dos testes efetuados para a desativação do *UserAssist*, verificou-se que um deles funcionou com sucesso, não registando nenhuma ação antes e depois da sessão terminar. Assim, em termos forenses, por vezes, se o utilizador tiver os conhecimentos necessários para desativar os serviços do *UserAssist*, não será possível por parte da equipa de investigação obter informação acerca do mesmo. No entanto, pode ser verificado se foi aplicado algum método para esse fim visto que o mesmo deixa registos.

VI. BIBLIOGRAFIA

- [1] T. Fisher, “What Is the Windows Registry?,” 6 Setembro 2018. [Online]. Available: <https://www.lifewire.com/windows-registry-2625992>. [Acedido em 6 Dezembro 2018].
- [2] ALDEID, “Windows-userassist-keys,” [Online]. Available: <https://www.aldeid.com/wiki/Windows-userassist-keys>. [Acedido em 6 Dezembro 2018].
- [3] D. Stevens, “Didier Stevens,” [Online]. Available: <https://blog.didierstevens.com/>. [Acedido em 6 Dezembro 2018].
- [4] W. Diaz, “A Quick Glance At The UserAssist Key in Windows,” Windows Explored, 6 Fevereiro 2012. [Online]. Available: <https://windowsexplored.com/2012/02/06/a-quick-glance-at-the-userassist-key-in-windows/>. [Acedido em 6 Dezembro 2018].
- [5] D. Stevens, “Windows 7 UserAssist Registry Keys,” Welcome To Into The Boxes, 1 Janeiro 2010. [Online]. Available: https://intotheboxes.files.wordpress.com/2010/04/intotheboxes_s_2010_q1.pdf. [Acedido em 6 Dezembro 2018].
- [6] superuser, “How do I disable UserAssist on Windows 10?,” 18 fevereiro 2018. [Online]. Available: <https://superuser.com/questions/1209496/how-do-i-disable-userassist-on-windows-10>. [Acedido em 22 janeiro 2019].
- [7] R. A. Kazmi, “Remove Windows 10 Activity, Achieve Faster Performance,” 21 agosto 2017. [Online]. Available: <https://www.stcleaner.com/blog/2017/08/21/remove->

windows-10-activity-achieve-faster-performance/. [Acedido em 22 janeiro 2019].



Pedrosa, Jéssica tem 21 anos e vive em Leiria, Portugal. Acabou em 2018 a licenciatura em Engenharia Informática, no ramo de Sistemas de Informação, no Instituto Politécnico de Leiria, na Escola Superior de Tecnologia e Gestão, estando agora no 1º ano do Mestrado de Cibersegurança e Informática Forense, lecionado na mesma escola.



Silva, Patrícia tem 21 anos e vive em Boavista, Leiria, Portugal. Acabou em 2018 a Licenciatura em Engenharia Informática, no ramo de Sistemas de Informação, no Instituto Politécnico de Leiria, na Escola Superior de Tecnologia e Gestão, estando agora no 1º ano do Mestrado de Cibersegurança e Informática Forense, lecionado na mesma escola.