CIS4203.01 **Brandon Thompson**
Dr. Ashokkumar Patel Due: 2/23//21

Lab 3: Unconvering Digital Evidence Using Bootable Forensics Utilities

In this lab we use bootable tools with write-blocking technologies to gather data from a system without compromising the original system.

2: Applied Learning

Part 1: Explore a Windows Workstation with Helix

In this section we use the Helix forensic investigation tool to identify specific data items such as disk information and image data.

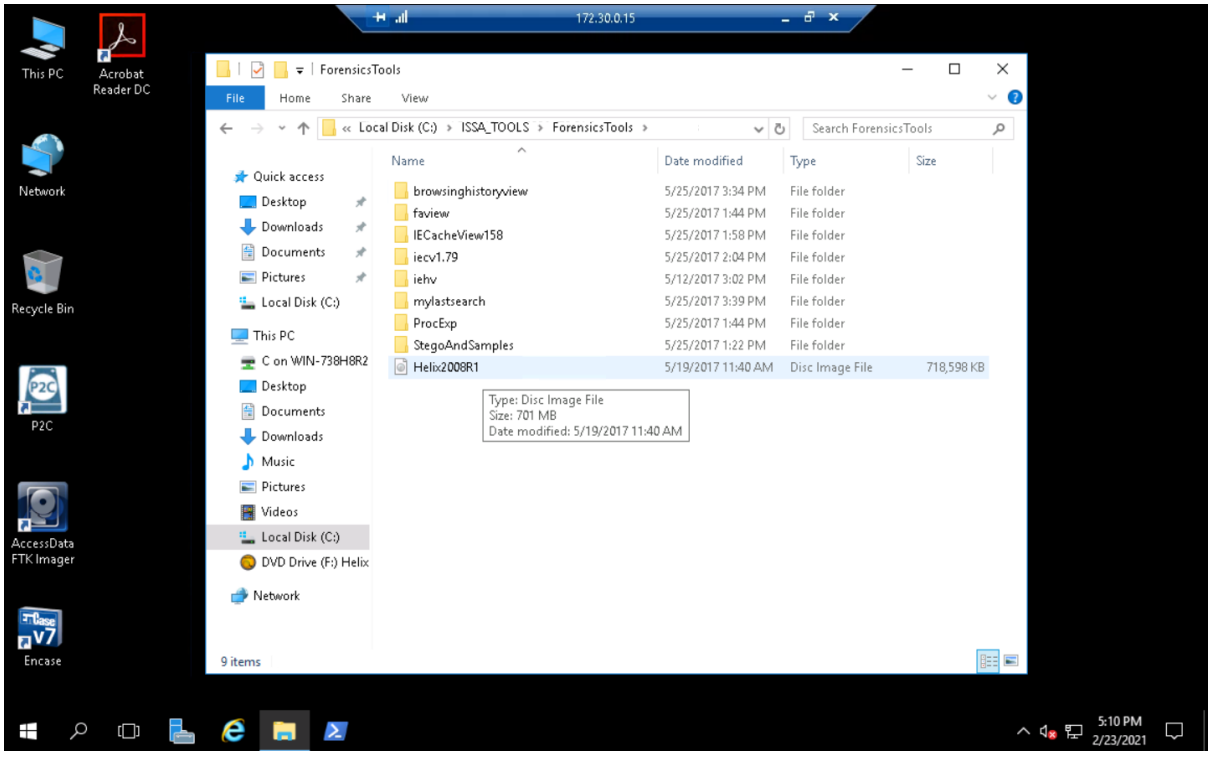


Figure 1: Helix application welcome screen.

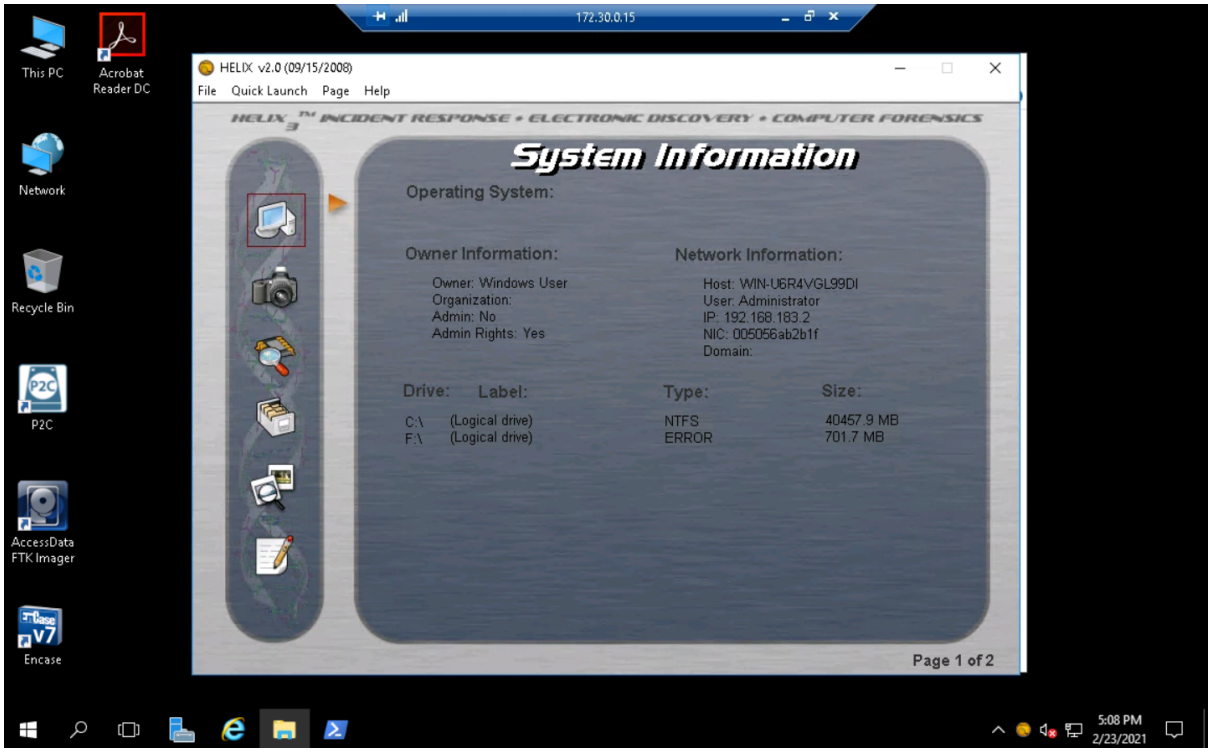


Figure 2: Network information on Preview System Information page.

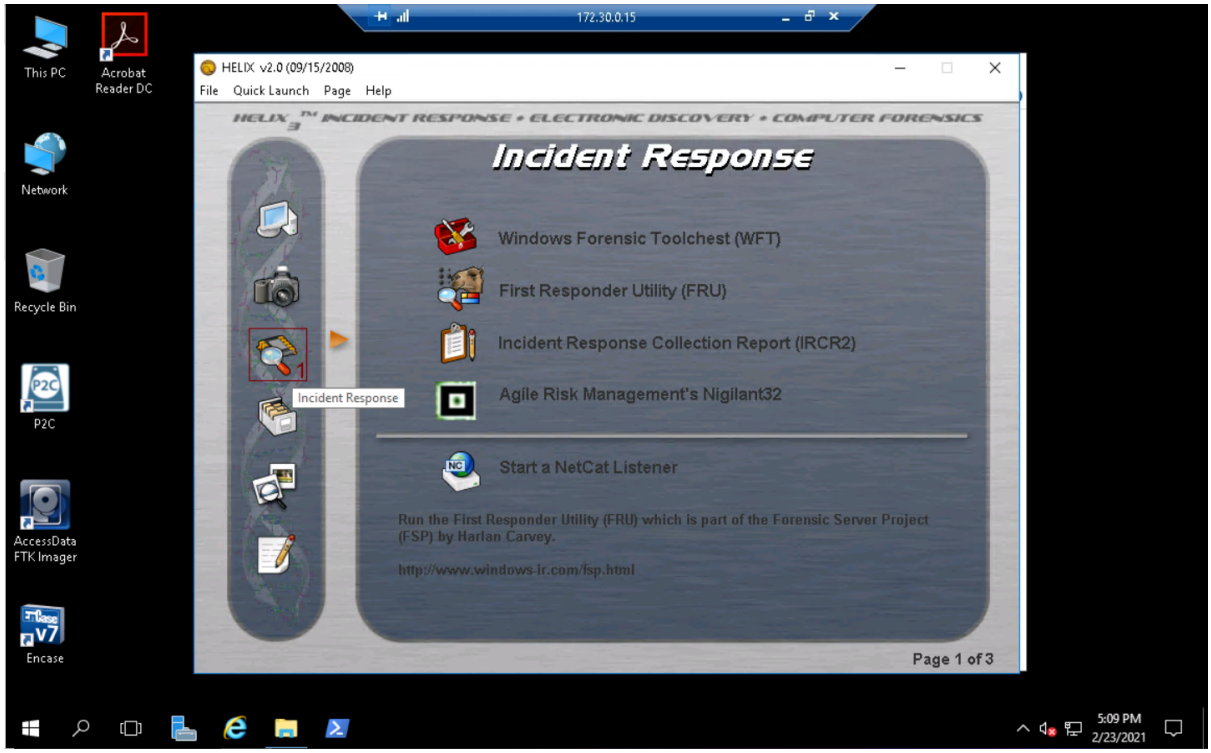


Figure 3: Incident response tools for Windows Systems.

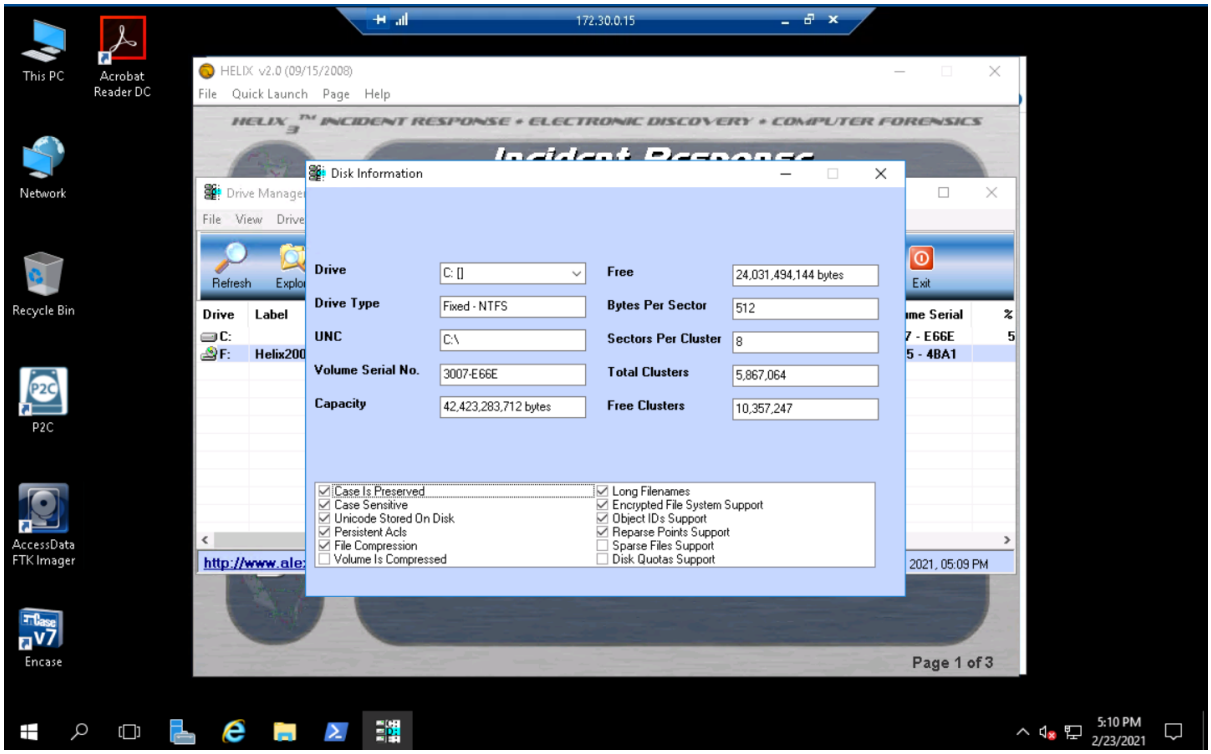


Figure 4: Disk information for the `C:` drive.

Figure 5: StegoAndSamples folder.

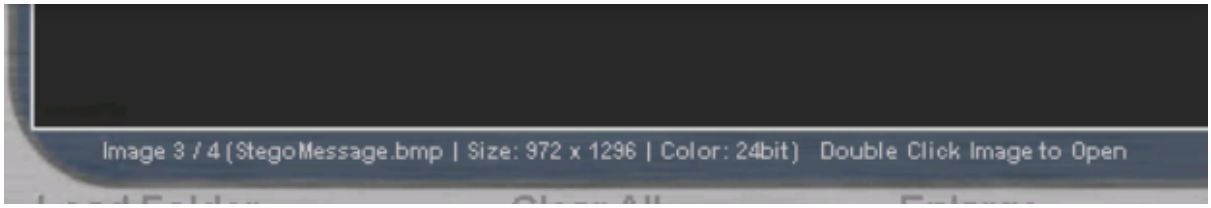


Figure 6: Data points associated with the image.

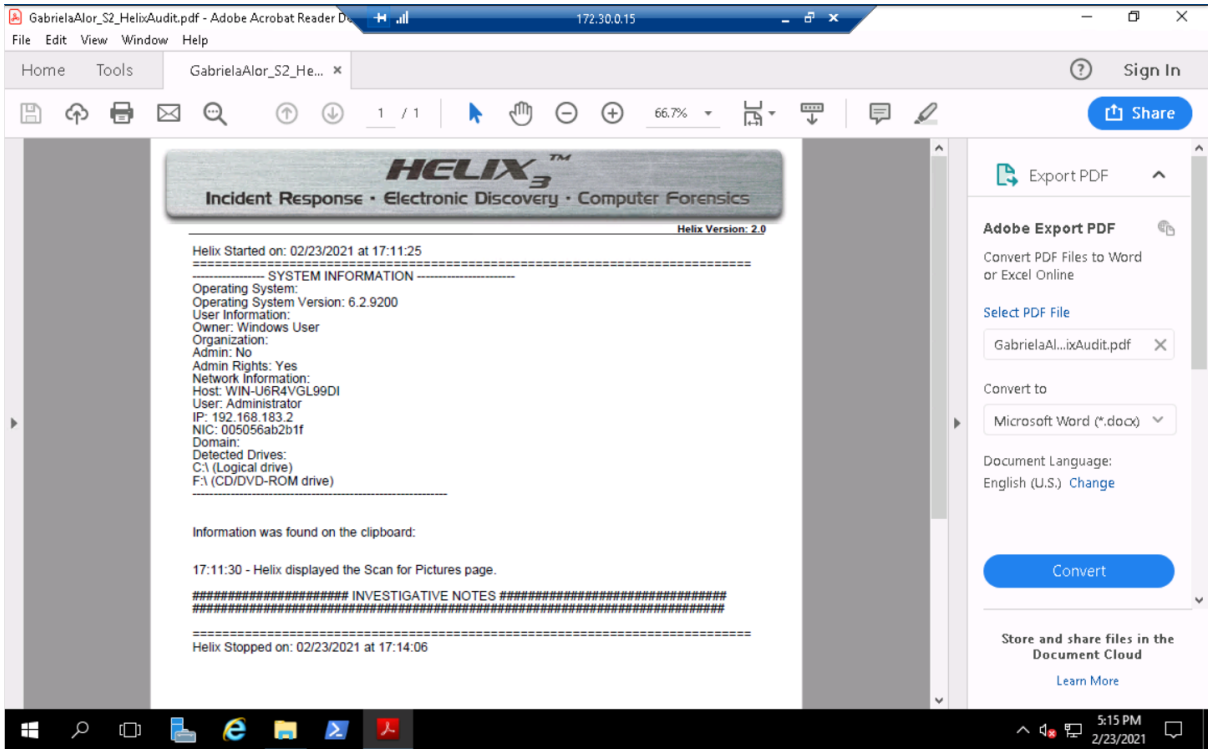


Figure 7: Helix audit log.

Part 2: Forensic Tools to Extract Data

In this section we remotely connect to a Windows machine and extract data from the Internet Explorer browser using multiple forensic tools.

The process explorer is similar to the Windows task manager, but displays much more data than

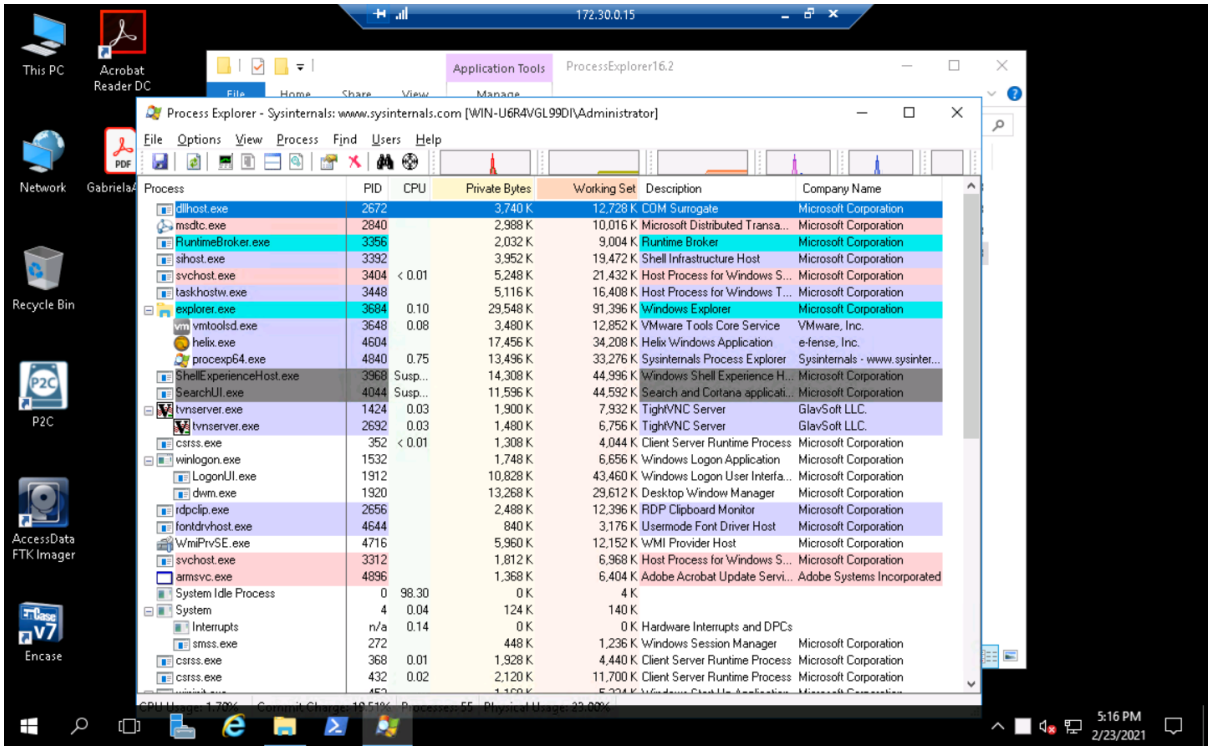


Figure 8: ProcessExplorer16.2

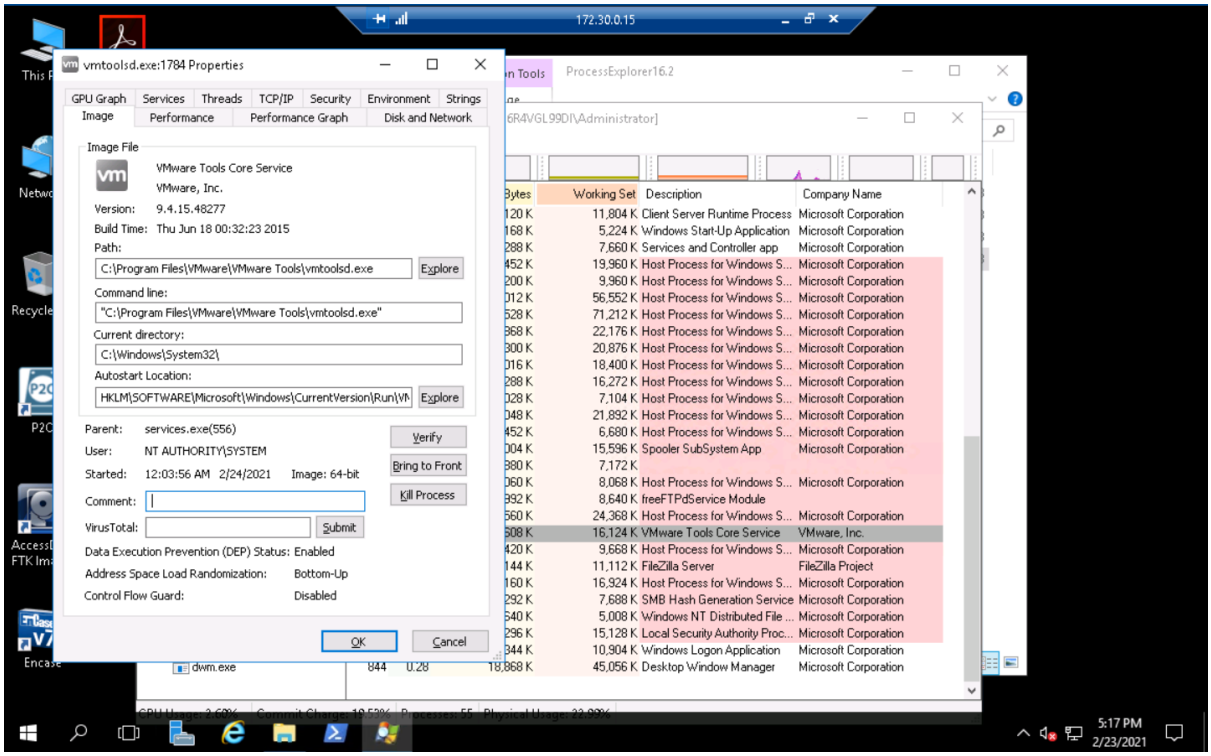


Figure 9: vmtools.exe process Image tab.

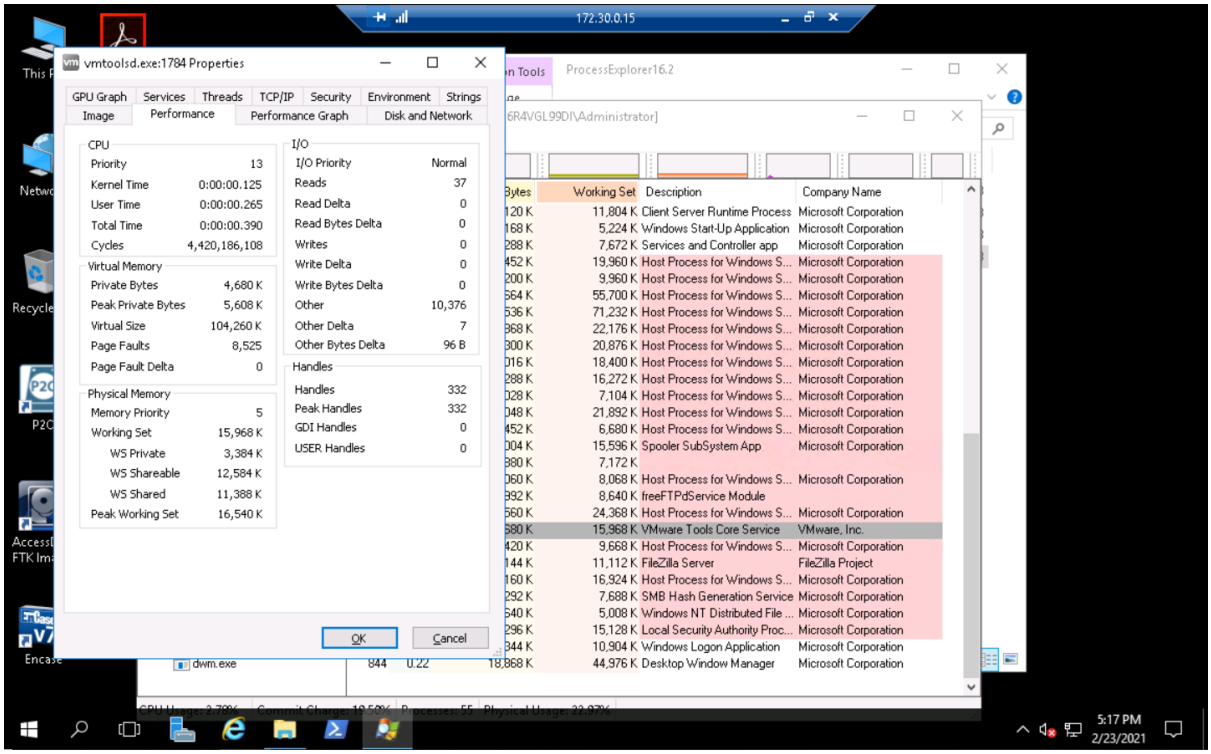


Figure 10: vmtools.exe process Performance tab.

FavoritesView summarizes all bookmarks and favorites saved from browsers, and allows you to view them in its own browser.

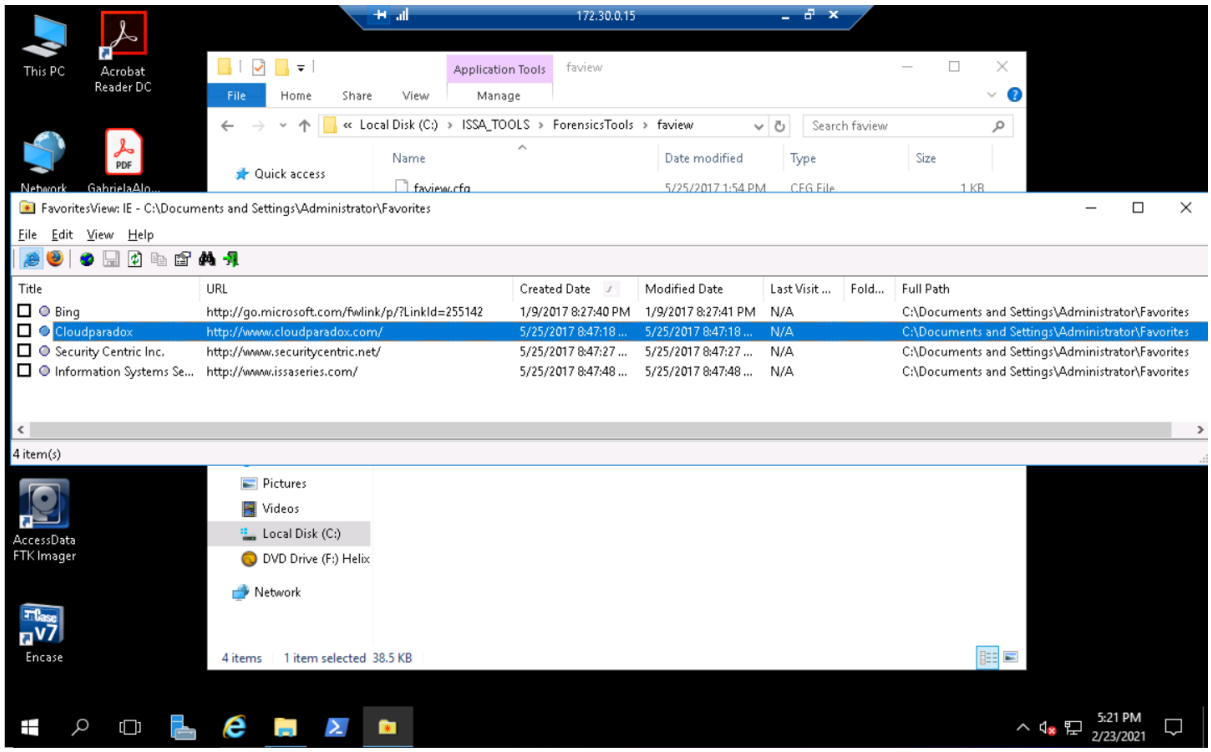


Figure 11: Faview application.

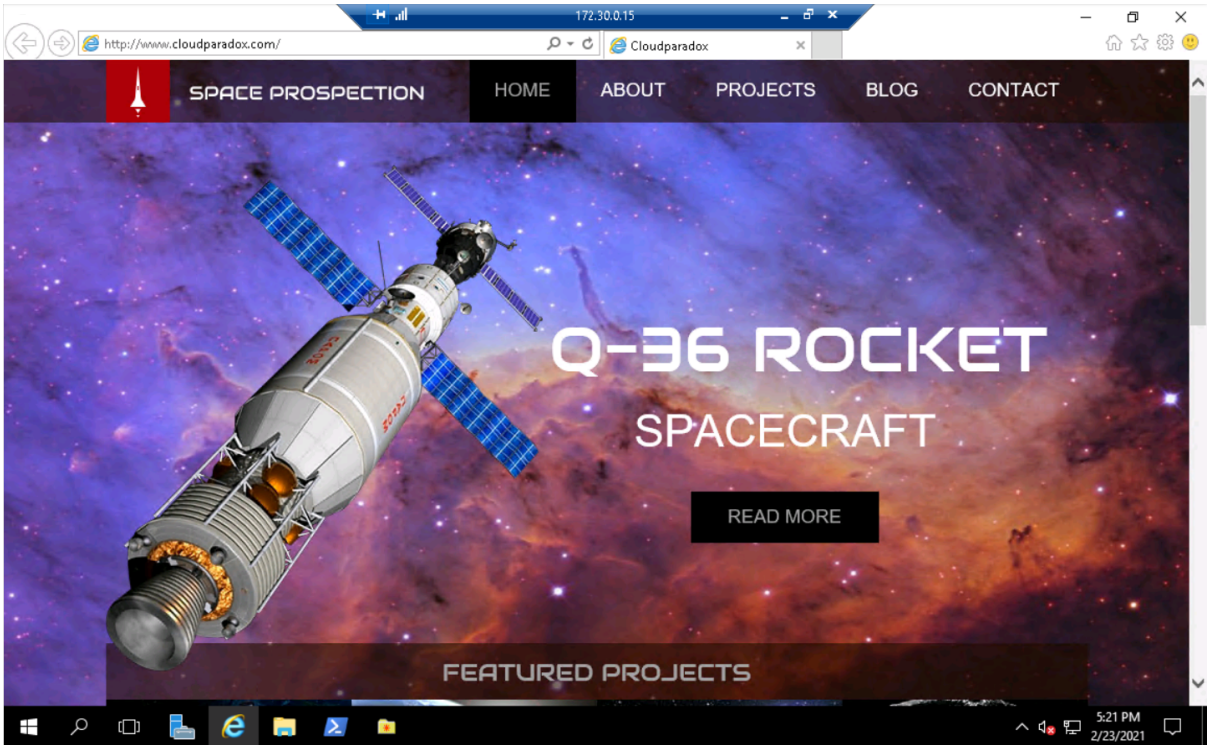


Figure 12: Cloudparadox web site.

IECacheView displays Internet Explorer's cache folder for any user logged onto the local machine and lists all currently stored file types without looking at cookies.

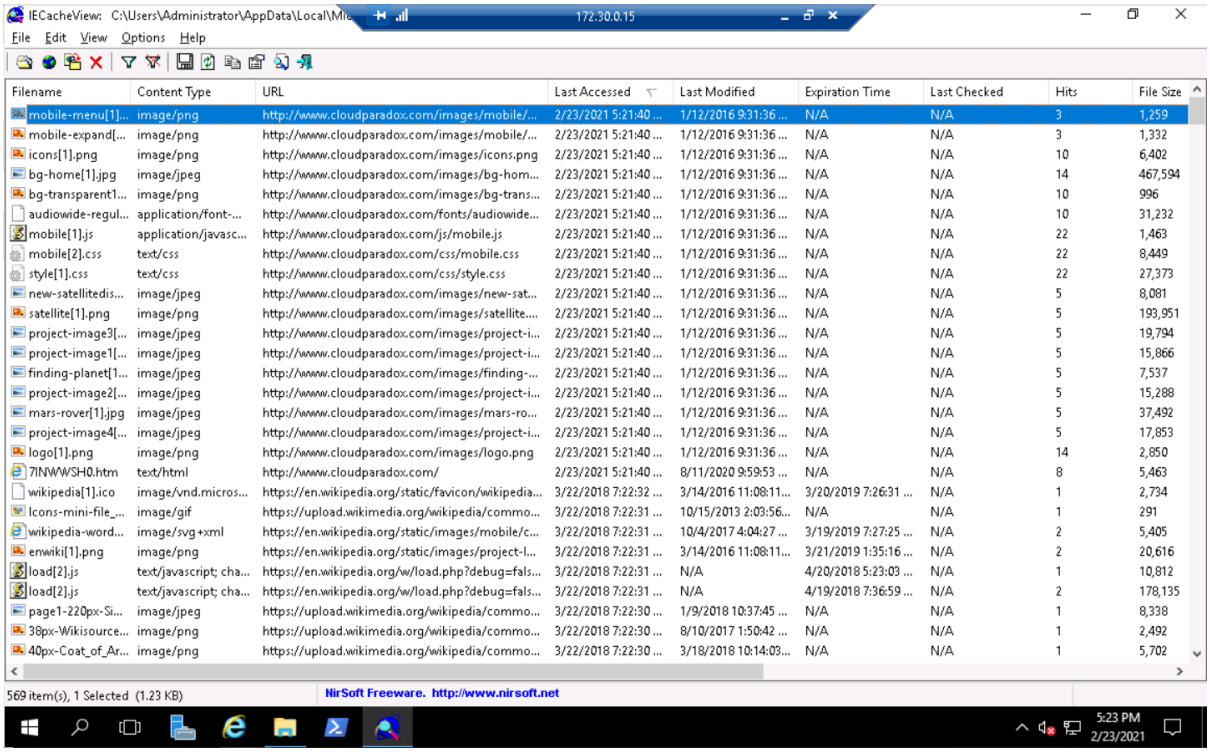


Figure 13: Most recently accessed item.

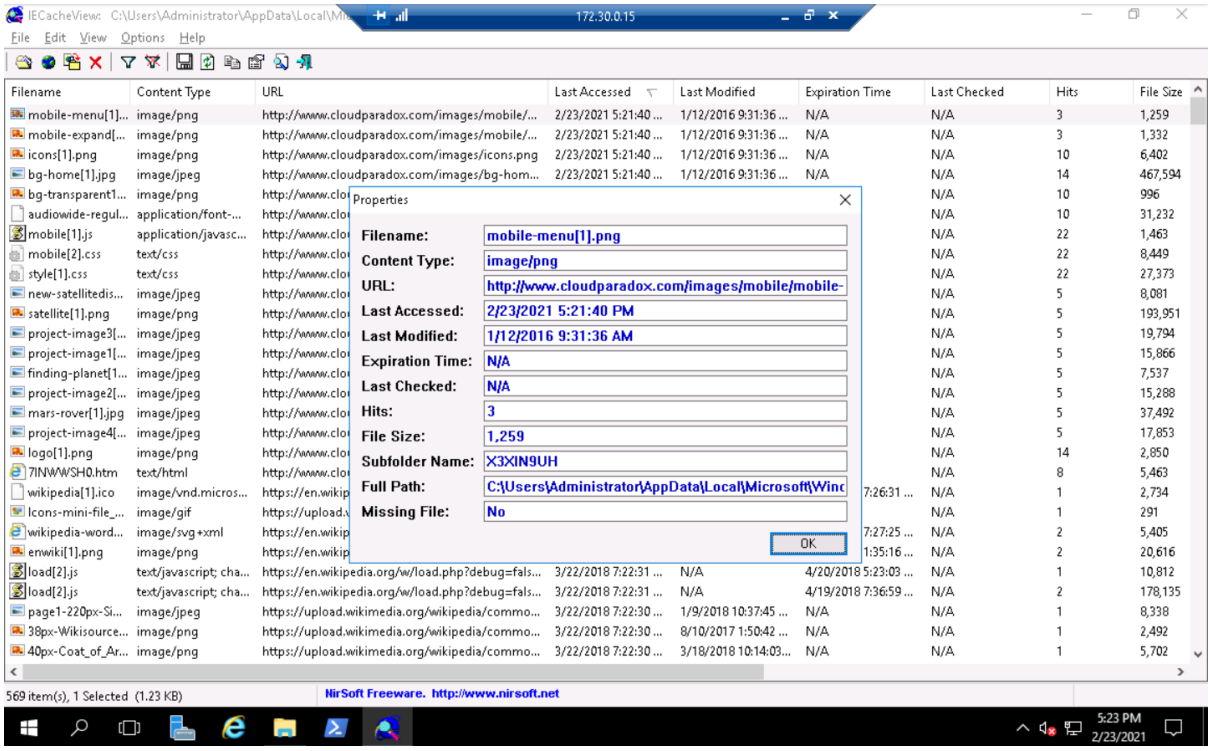


Figure 14: Properties dialog of the most recently accessed item.

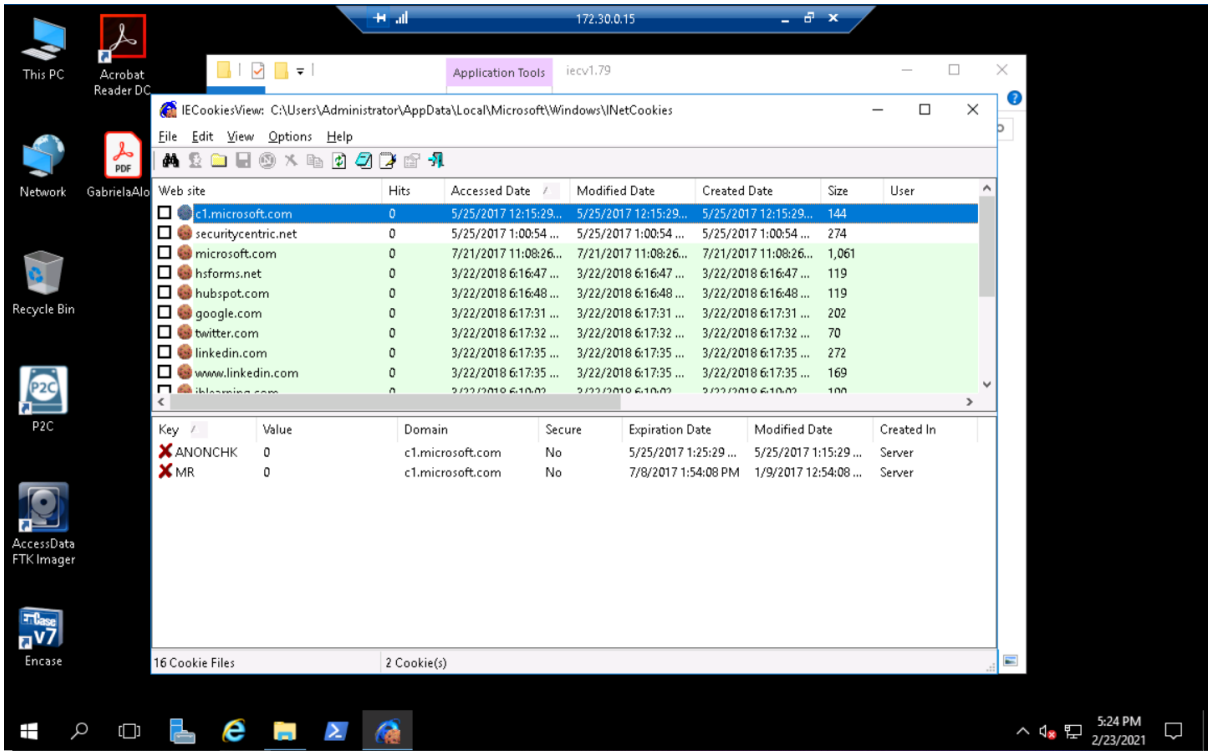


Figure 15: IECookiesView window and details.

BrowsingHistoryView displays a collection of all the internet sites visited from all browsers in one window.

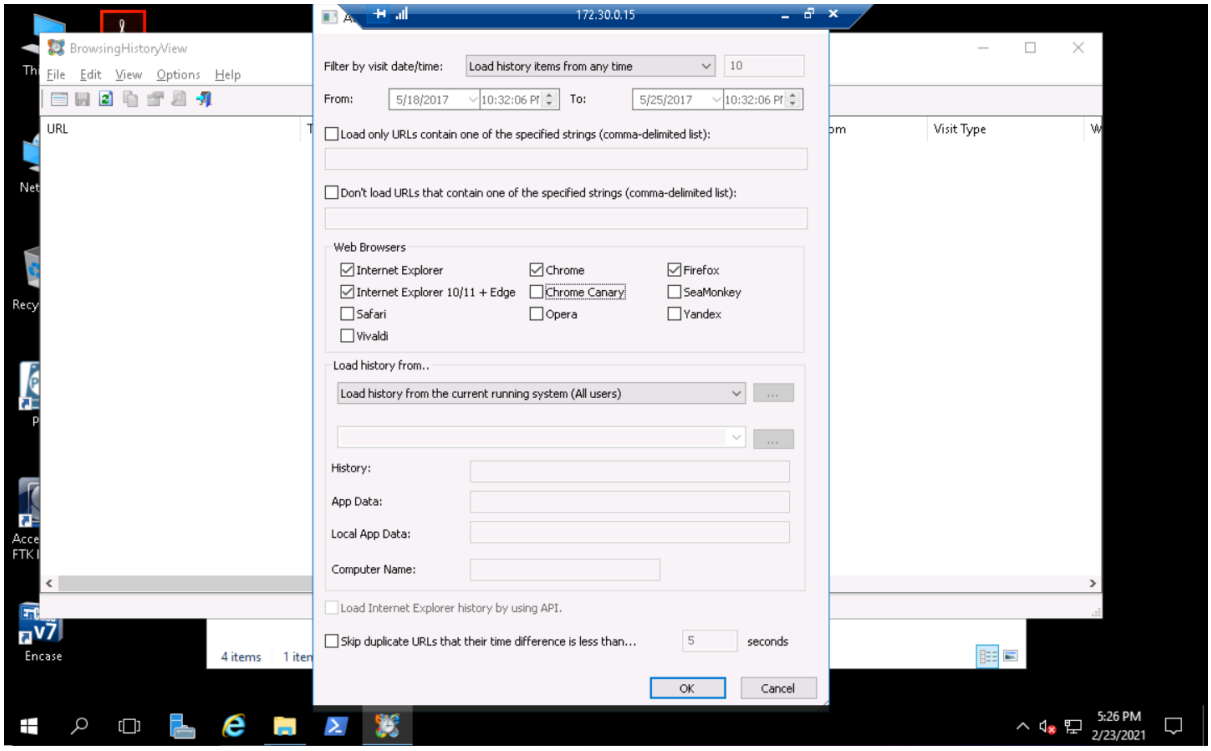


Figure 16: BrowsingHistoryView list of browsers.

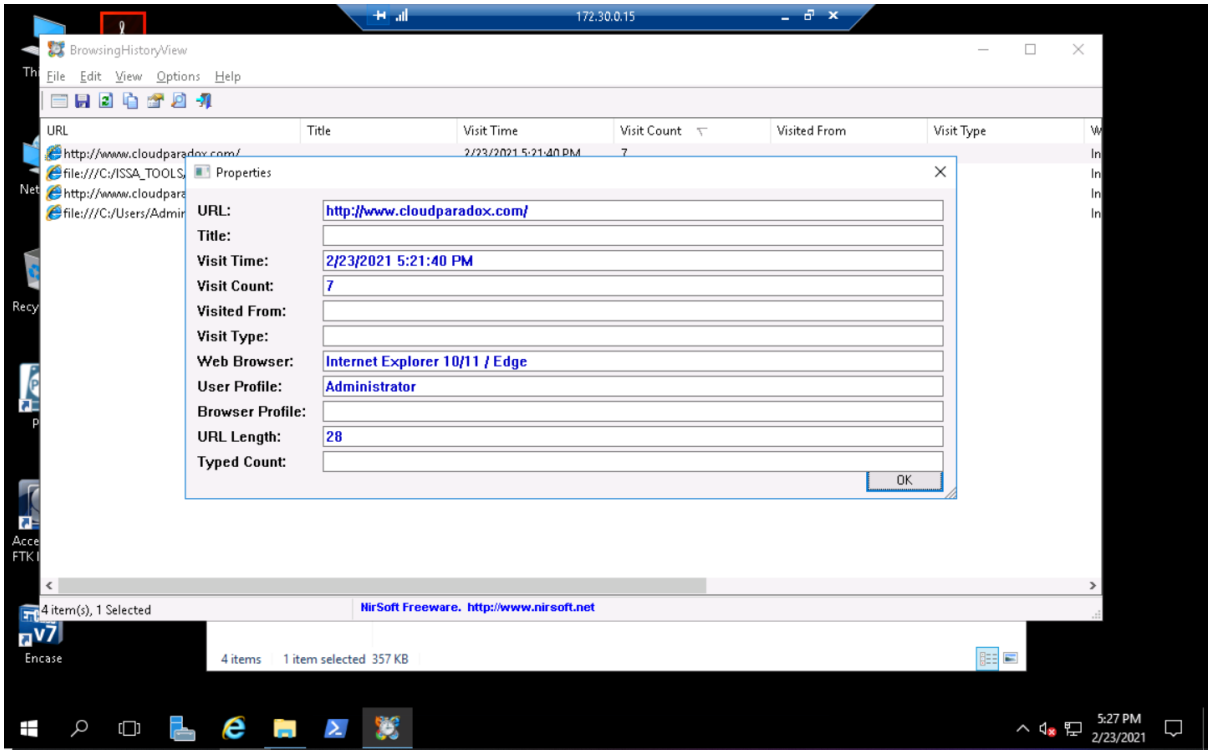


Figure 17: Properties dialog for CloudParadox Blog.

MyLastSearch collects internet search queries made by users using different search engines.

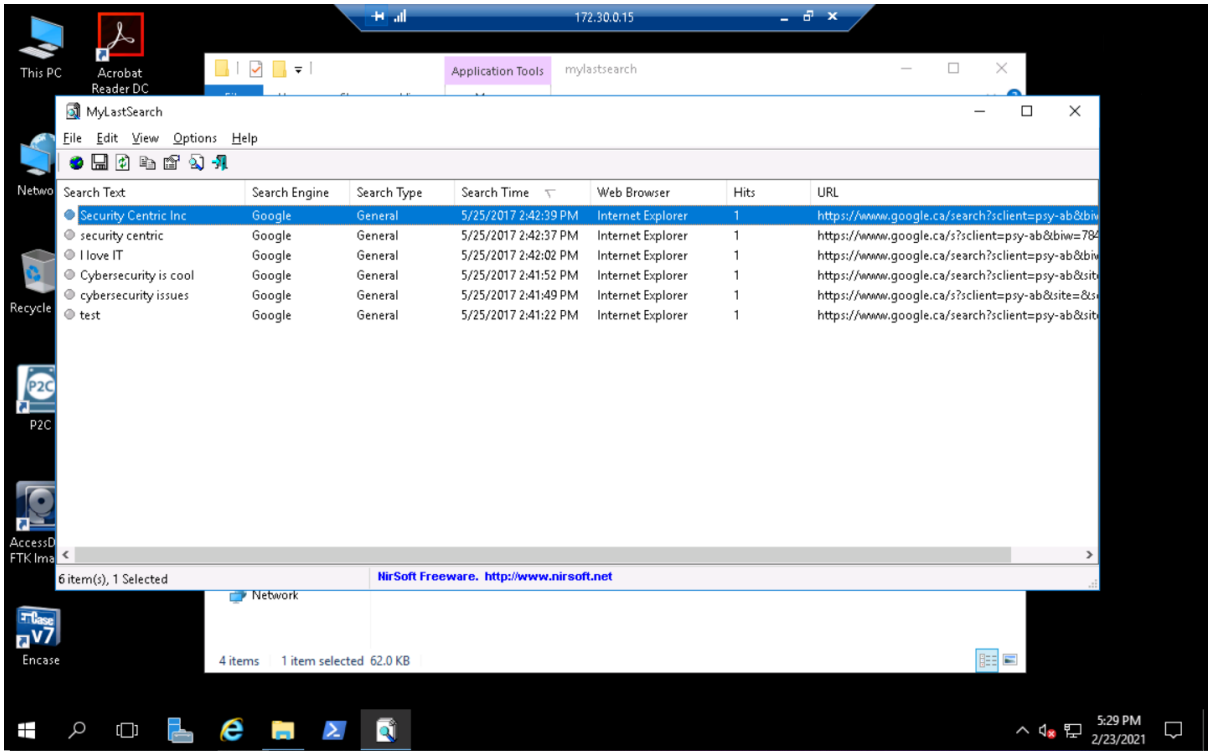
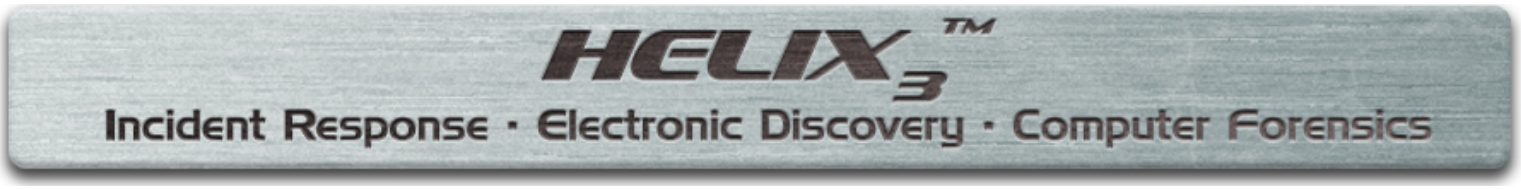


Figure 18: List of searches with the most recent highlighted.



Helix Version: 2.0

Helix Started on: 02/23/2021 at 17:11:25
==========
---------- SYSTEM INFORMATION ----------
Operating System:
Operating System Version: 6.2.9200
User Information:
Owner: Windows User
Organization:
Admin: No
Admin Rights: Yes
Network Information:
Host: WIN-U6R4VGL99DI
User: Administrator
IP: 192.168.183.2
NIC: 005056ab2b1f
Domain:
Detected Drives:
C:\ (Logical drive)
F:\ (CD/DVD-ROM drive)

Information was found on the clipboard:

17:11:30 - Helix displayed the Scan for Pictures page.

########## INVESTIGATIVE NOTES ##########
##########

==========
Helix Stopped on: 02/23/2021 at 17:14:06

Forensic analysts face challenges of retrieving data from a system without altering evidence in the process. Using bootable tools means that the host OS is not altered by running these tools. The tools we used were designed without write capabilities to remove the risk of altering data during retrieval. During the lab we used the Helix tool to gather in depth information about data on a machine. Multiple tools were used to gather internet browsing activity such as search history, bookmarks and favorites.