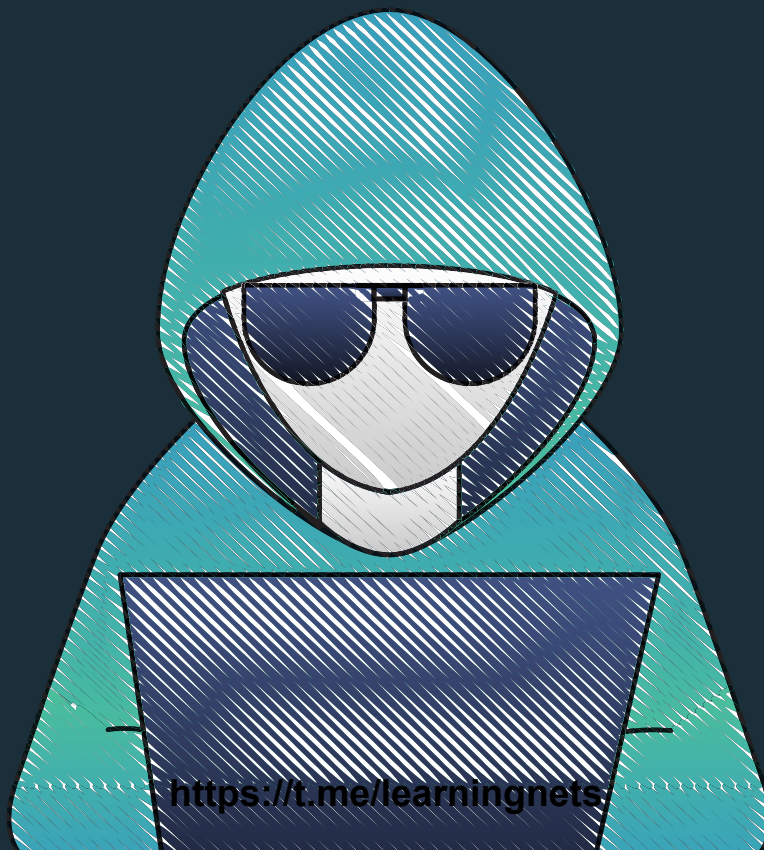




LetsDefend

THE BEST SOC ANALYST TOOLS



<https://t.me/learningnets>

TABLE OF CONTENTS

3 INVESTIGATION TOOLS

Process Hacker

BrowsingHistoryView

FullEventLogView

6 CHECKING REPUTATION

VirusTotal

AbuseIPDB

Cisco Talos

9 ONLINE SANDBOX

AnyRun

Hybrid-Analysis

urlscan

12 OTHER

MXToolBox

Koodous

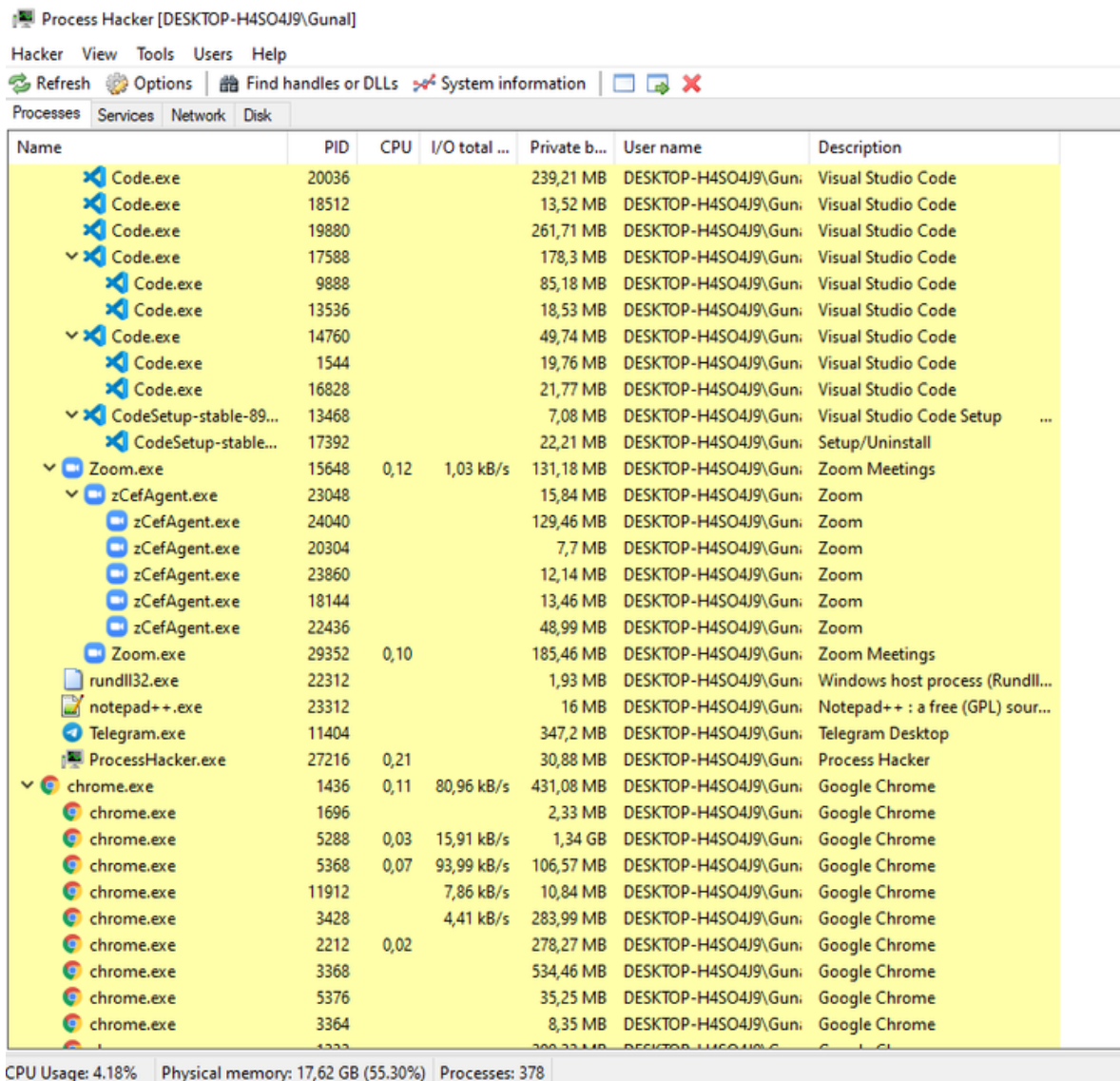
python-oletools



Investigation

Process Hacker

Great tool for monitoring the system and detecting suspicious situations. It's also free.



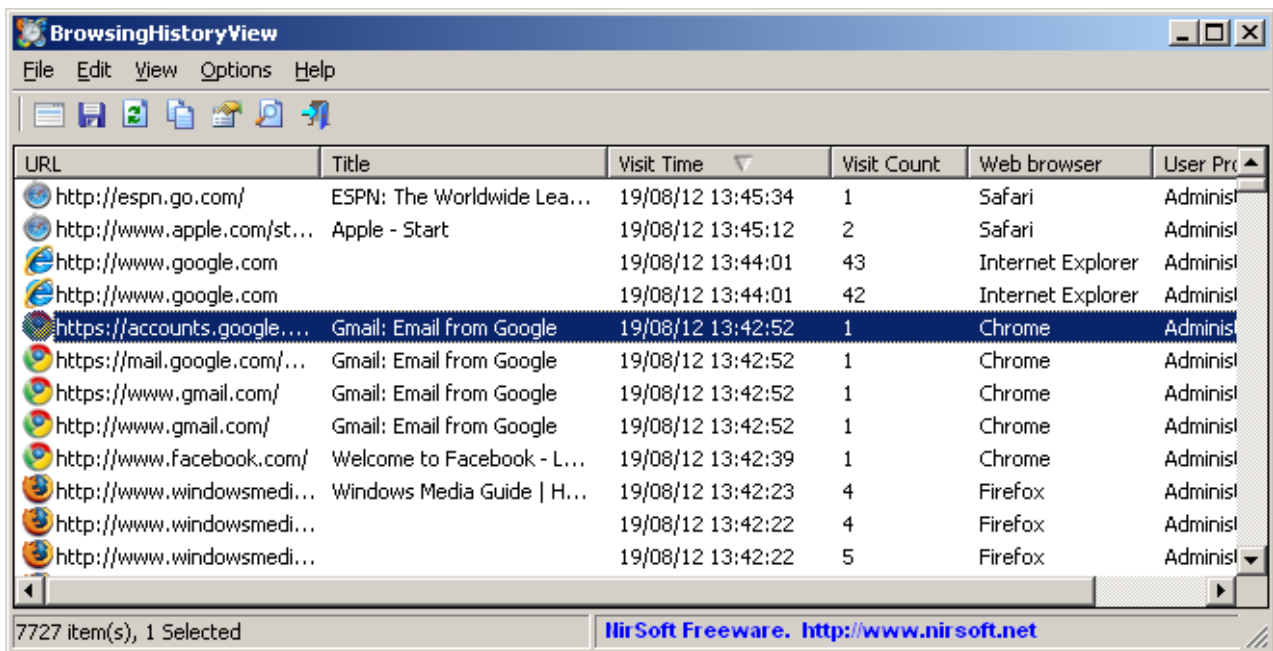
The screenshot shows the Process Hacker application window. The title bar reads "Process Hacker [DESKTOP-H4SO4J9\Gunal]". The menu bar includes "Hacker", "View", "Tools", "Users", and "Help". The toolbar contains "Refresh", "Options", "Find handles or DLLs", and "System information". The main window displays a table of processes with columns for Name, PID, CPU, I/O total, Private b..., User name, and Description. The status bar at the bottom shows "CPU Usage: 4.18%", "Physical memory: 17,62 GB (55.30%)", and "Processes: 378".

| Name | PID | CPU | I/O total ... | Private b... | User name | Description |
|------------------------|-------|------|---------------|--------------|-----------------------|----------------------------------|
| Code.exe | 20036 | | | 239,21 MB | DESKTOP-H4SO4J9\Gunal | Visual Studio Code |
| Code.exe | 18512 | | | 13,52 MB | DESKTOP-H4SO4J9\Gunal | Visual Studio Code |
| Code.exe | 19880 | | | 261,71 MB | DESKTOP-H4SO4J9\Gunal | Visual Studio Code |
| Code.exe | 17588 | | | 178,3 MB | DESKTOP-H4SO4J9\Gunal | Visual Studio Code |
| Code.exe | 9888 | | | 85,18 MB | DESKTOP-H4SO4J9\Gunal | Visual Studio Code |
| Code.exe | 13536 | | | 18,53 MB | DESKTOP-H4SO4J9\Gunal | Visual Studio Code |
| Code.exe | 14760 | | | 49,74 MB | DESKTOP-H4SO4J9\Gunal | Visual Studio Code |
| Code.exe | 1544 | | | 19,76 MB | DESKTOP-H4SO4J9\Gunal | Visual Studio Code |
| Code.exe | 16828 | | | 21,77 MB | DESKTOP-H4SO4J9\Gunal | Visual Studio Code |
| CodeSetup-stable-89... | 13468 | | | 7,08 MB | DESKTOP-H4SO4J9\Gunal | Visual Studio Code Setup ... |
| CodeSetup-stable... | 17392 | | | 22,21 MB | DESKTOP-H4SO4J9\Gunal | Setup/Uninstall |
| Zoom.exe | 15648 | 0,12 | 1,03 kB/s | 131,18 MB | DESKTOP-H4SO4J9\Gunal | Zoom Meetings |
| zCefAgent.exe | 23048 | | | 15,84 MB | DESKTOP-H4SO4J9\Gunal | Zoom |
| zCefAgent.exe | 24040 | | | 129,46 MB | DESKTOP-H4SO4J9\Gunal | Zoom |
| zCefAgent.exe | 20304 | | | 7,7 MB | DESKTOP-H4SO4J9\Gunal | Zoom |
| zCefAgent.exe | 23860 | | | 12,14 MB | DESKTOP-H4SO4J9\Gunal | Zoom |
| zCefAgent.exe | 18144 | | | 13,46 MB | DESKTOP-H4SO4J9\Gunal | Zoom |
| zCefAgent.exe | 22436 | | | 48,99 MB | DESKTOP-H4SO4J9\Gunal | Zoom |
| Zoom.exe | 29352 | 0,10 | | 185,46 MB | DESKTOP-H4SO4J9\Gunal | Zoom Meetings |
| rundll32.exe | 22312 | | | 1,93 MB | DESKTOP-H4SO4J9\Gunal | Windows host process (Rundll... |
| notepad++.exe | 23312 | | | 16 MB | DESKTOP-H4SO4J9\Gunal | Notepad++ : a free (GPL) sour... |
| Telegram.exe | 11404 | | | 347,2 MB | DESKTOP-H4SO4J9\Gunal | Telegram Desktop |
| ProcessHacker.exe | 27216 | 0,21 | | 30,88 MB | DESKTOP-H4SO4J9\Gunal | Process Hacker |
| chrome.exe | 1436 | 0,11 | 80,96 kB/s | 431,08 MB | DESKTOP-H4SO4J9\Gunal | Google Chrome |
| chrome.exe | 1696 | | | 2,33 MB | DESKTOP-H4SO4J9\Gunal | Google Chrome |
| chrome.exe | 5288 | 0,03 | 15,91 kB/s | 1,34 GB | DESKTOP-H4SO4J9\Gunal | Google Chrome |
| chrome.exe | 5368 | 0,07 | 93,99 kB/s | 106,57 MB | DESKTOP-H4SO4J9\Gunal | Google Chrome |
| chrome.exe | 11912 | | 7,86 kB/s | 10,84 MB | DESKTOP-H4SO4J9\Gunal | Google Chrome |
| chrome.exe | 3428 | | 4,41 kB/s | 283,99 MB | DESKTOP-H4SO4J9\Gunal | Google Chrome |
| chrome.exe | 2212 | 0,02 | | 278,27 MB | DESKTOP-H4SO4J9\Gunal | Google Chrome |
| chrome.exe | 3368 | | | 534,46 MB | DESKTOP-H4SO4J9\Gunal | Google Chrome |
| chrome.exe | 5376 | | | 35,25 MB | DESKTOP-H4SO4J9\Gunal | Google Chrome |
| chrome.exe | 3364 | | | 8,35 MB | DESKTOP-H4SO4J9\Gunal | Google Chrome |

Investigation

BrowsingHistoryView

It gives you the history of different browsers in one table.



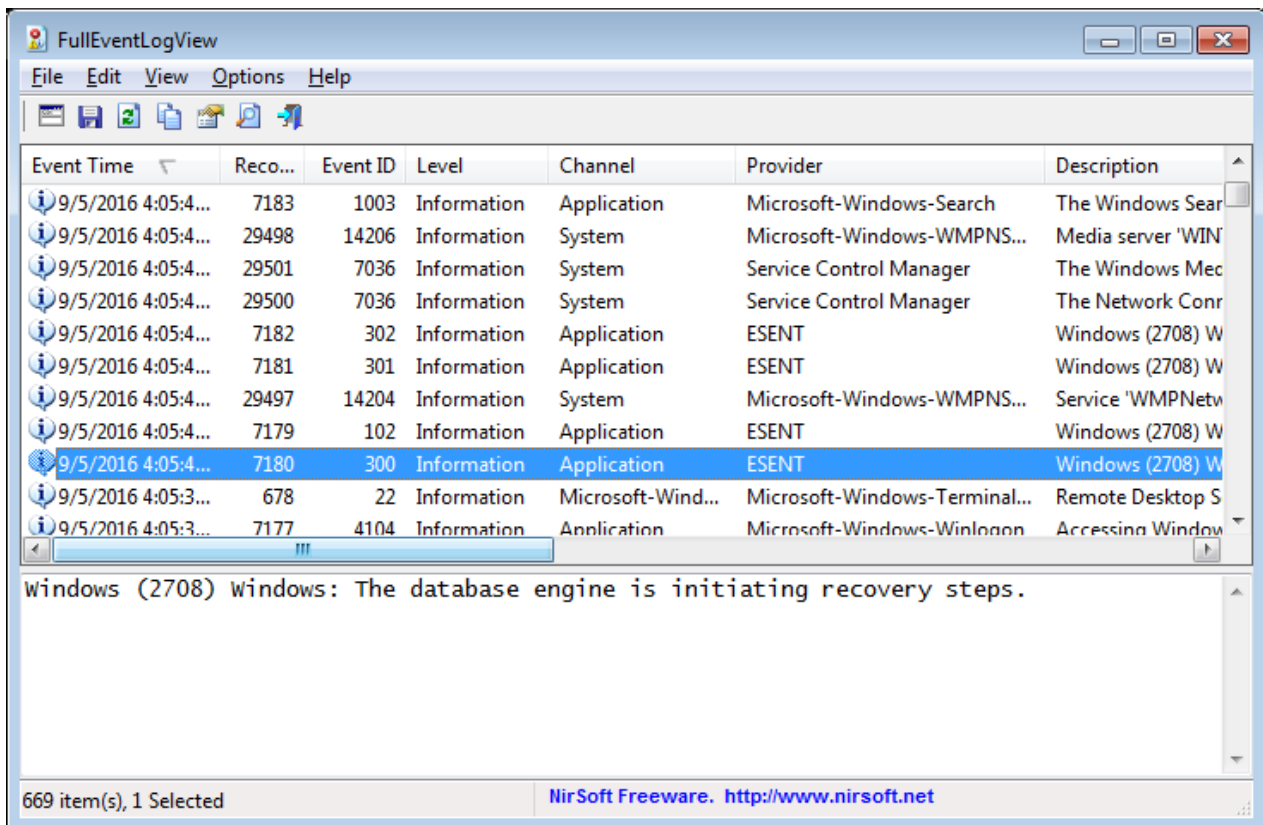
The screenshot shows the BrowsingHistoryView application window. The window title is "BrowsingHistoryView". The menu bar includes "File", "Edit", "View", "Options", and "Help". The toolbar contains icons for file operations and search. The main area displays a table with the following columns: URL, Title, Visit Time, Visit Count, Web browser, and User Profile. The table contains 11 rows of data, with the row for "https://accounts.google.com" selected. The status bar at the bottom indicates "7727 item(s), 1 Selected" and provides the NirSoft Freeware logo and website URL.

| URL | Title | Visit Time | Visit Count | Web browser | User Profile |
|-----------------------------|----------------------------|-------------------|-------------|-------------------|--------------|
| http://espn.go.com/ | ESPN: The Worldwide Lea... | 19/08/12 13:45:34 | 1 | Safari | Administ |
| http://www.apple.com/st... | Apple - Start | 19/08/12 13:45:12 | 2 | Safari | Administ |
| http://www.google.com | | 19/08/12 13:44:01 | 43 | Internet Explorer | Administ |
| http://www.google.com | | 19/08/12 13:44:01 | 42 | Internet Explorer | Administ |
| https://accounts.google... | Gmail: Email from Google | 19/08/12 13:42:52 | 1 | Chrome | Administ |
| https://mail.google.com/... | Gmail: Email from Google | 19/08/12 13:42:52 | 1 | Chrome | Administ |
| https://www.gmail.com/ | Gmail: Email from Google | 19/08/12 13:42:52 | 1 | Chrome | Administ |
| http://www.gmail.com/ | Gmail: Email from Google | 19/08/12 13:42:52 | 1 | Chrome | Administ |
| http://www.facebook.com/ | Welcome to Facebook - L... | 19/08/12 13:42:39 | 1 | Chrome | Administ |
| http://www.windowsmedi... | Windows Media Guide H... | 19/08/12 13:42:23 | 4 | Firefox | Administ |
| http://www.windowsmedi... | | 19/08/12 13:42:22 | 4 | Firefox | Administ |
| http://www.windowsmedi... | | 19/08/12 13:42:22 | 5 | Firefox | Administ |

Investigation

FullEventLogView

It displays all event logs in a table, which helps to decrease the investigation time.



The screenshot shows the FullEventLogView application window. The window title is "FullEventLogView" and it has a menu bar with "File", "Edit", "View", "Options", and "Help". Below the menu bar is a toolbar with various icons. The main area contains a table with the following columns: "Event Time", "Reco...", "Event ID", "Level", "Channel", "Provider", and "Description". The table lists several events, with the event at 9/5/2016 4:05:4... with ID 300 selected. Below the table is a text area displaying the description of the selected event: "Windows (2708) windows: The database engine is initiating recovery steps." At the bottom of the window, it shows "669 item(s), 1 Selected" and "NirSoft Freeware. <http://www.nirsoft.net>".

| Event Time | Reco... | Event ID | Level | Channel | Provider | Description |
|--------------------|---------|----------|-------------|-------------------|-------------------------------|-------------------|
| 9/5/2016 4:05:4... | 7183 | 1003 | Information | Application | Microsoft-Windows-Search | The Windows Sear |
| 9/5/2016 4:05:4... | 29498 | 14206 | Information | System | Microsoft-Windows-WMPNS... | Media server 'WIN |
| 9/5/2016 4:05:4... | 29501 | 7036 | Information | System | Service Control Manager | The Windows Mec |
| 9/5/2016 4:05:4... | 29500 | 7036 | Information | System | Service Control Manager | The Network Conr |
| 9/5/2016 4:05:4... | 7182 | 302 | Information | Application | ESENT | Windows (2708) W |
| 9/5/2016 4:05:4... | 7181 | 301 | Information | Application | ESENT | Windows (2708) W |
| 9/5/2016 4:05:4... | 29497 | 14204 | Information | System | Microsoft-Windows-WMPNS... | Service 'WMPNetw |
| 9/5/2016 4:05:4... | 7179 | 102 | Information | Application | ESENT | Windows (2708) W |
| 9/5/2016 4:05:4... | 7180 | 300 | Information | Application | ESENT | Windows (2708) W |
| 9/5/2016 4:05:3... | 678 | 22 | Information | Microsoft-Wind... | Microsoft-Windows-Terminal... | Remote Desktop S |
| 9/5/2016 4:05:3... | 7177 | 4104 | Information | Application | Microsoft-Windows-Winlogon | Accessing Window |

Windows (2708) windows: The database engine is initiating recovery steps.

669 item(s), 1 Selected NirSoft Freeware. <http://www.nirsoft.net>


Checking Reputation

VirusTotal

You can both IP and hash search on VT database. and find relationships about suspicious IP/files



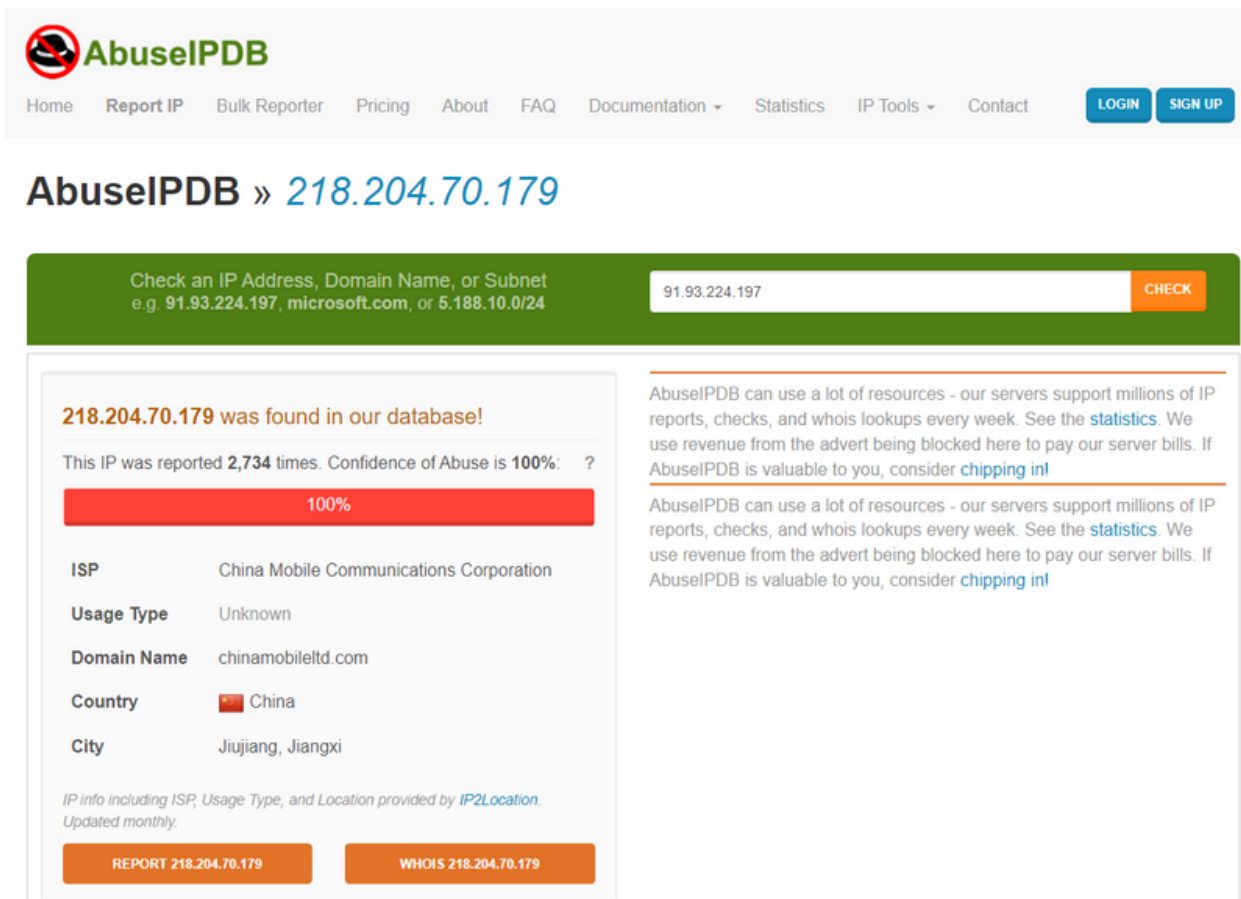
Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community

| FILE | URL | SEARCH |
|--|-----|--------|
|  Choose file | | |

Checking Reputation

Abuse IPDb

You can check if the IP address has been reported before. Let's say you found a suspicious IP address on your firewall logs and want to ensure is IP address did something bad before.



AbuseIPDB

Home Report IP Bulk Reporter Pricing About FAQ Documentation ▾ Statistics IP Tools ▾ Contact [LOGIN](#) [SIGN UP](#)

AbuseIPDB » [218.204.70.179](#)


Check an IP Address, Domain Name, or Subnet
e.g. 91.93.224.197, microsoft.com, or 5.188.10.0/24

91.93.224.197 [CHECK](#)

218.204.70.179 was found in our database!

This IP was reported **2,734** times. Confidence of Abuse is **100%**. ?

100%

| | |
|-------------|---|
| ISP | China Mobile Communications Corporation |
| Usage Type | Unknown |
| Domain Name | chinamobileltd.com |
| Country |  China |
| City | Jiujiang, Jiangxi |

IP info including ISP, Usage Type, and Location provided by [IP2Location](#).
Updated monthly.

[REPORT 218.204.70.179](#) [WHOIS 218.204.70.179](#)

AbuseIPDB can use a lot of resources - our servers support millions of IP reports, checks, and whois lookups every week. See the [statistics](#). We use revenue from the advert being blocked here to pay our server bills. If AbuseIPDB is valuable to you, consider [chipping in!](#)

AbuseIPDB can use a lot of resources - our servers support millions of IP reports, checks, and whois lookups every week. See the [statistics](#). We use revenue from the advert being blocked here to pay our server bills. If AbuseIPDB is valuable to you, consider [chipping in!](#)

Checking Reputation

Cisco Talos

You can search by IP, domain, or network owner for real-time threat data.

The screenshot displays the Cisco Talos reputation check interface, organized into several sections:

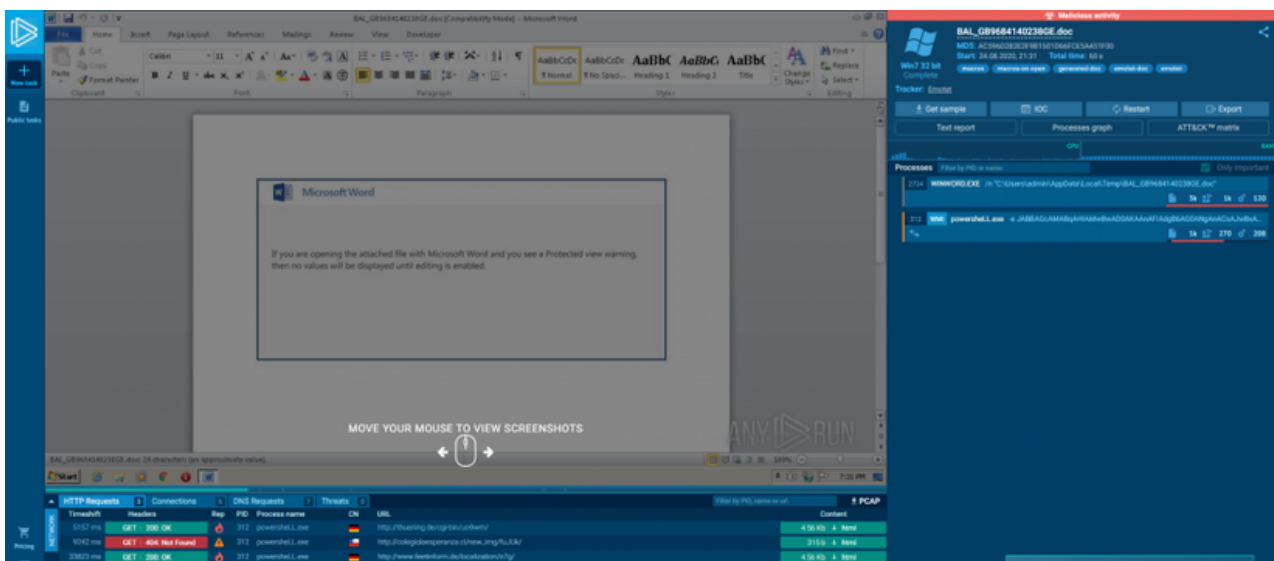
- LOCATION DATA:** Shows the location as China.
- OWNER DETAILS:** Lists IP address (218.204.70.179), FWD/REV DNS MATCH (No data), HOSTNAME (-), DOMAIN (-), and NETWORK OWNER (china mobile).
- CONTENT DETAILS:** Shows CONTENT CATEGORY (No established content categories) and a button to submit a Web Categorization Ticket.
- REPUTATION DETAILS:** Shows EMAIL REPUTATION (Neutral), WEB REPUTATION (Questionable), and a table of metrics for the last day and last month.
- BLOCK LISTS:** Shows TALOS SECURITY INTELLIGENCE BLOCK LIST with ADDED TO THE BLOCK LIST (No) and STATUS (EXPIRED).

| | LAST DAY | LAST MONTH |
|---------------|----------|------------|
| EMAIL VOLUME | 0.0 | 0.5 |
| VOLUME CHANGE | 0% | |
| SPAM LEVEL | Medium | |

Online Sandbox

AnyRun

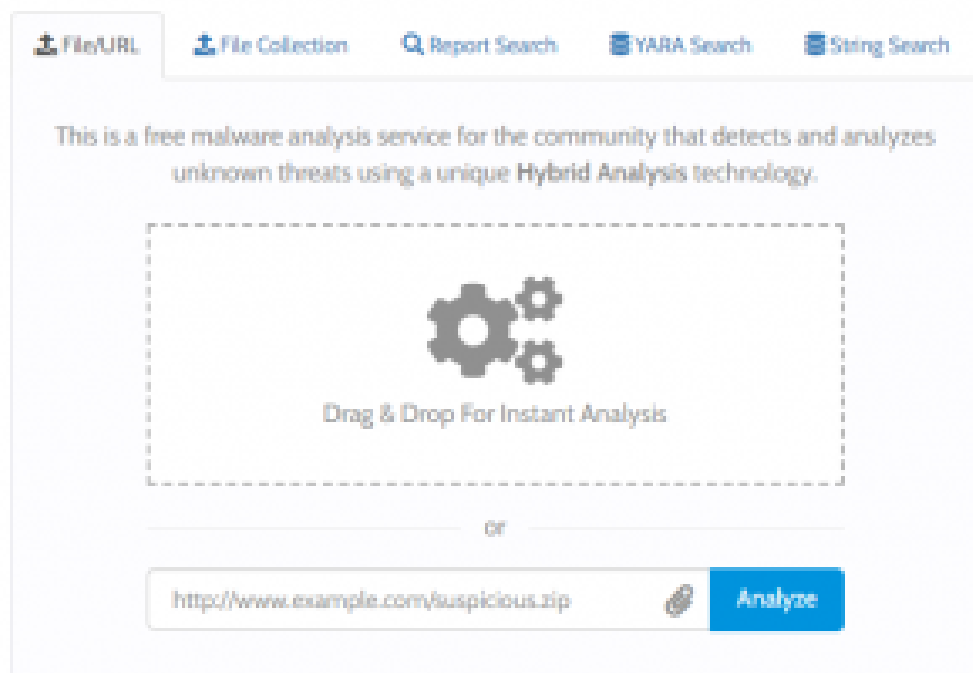
This is an interactive malware analysis platform. Very useful for finding command and control addresses of malware and understanding the purpose. You can use it with the free version.



Online Sandbox

Hybrid-Analysis

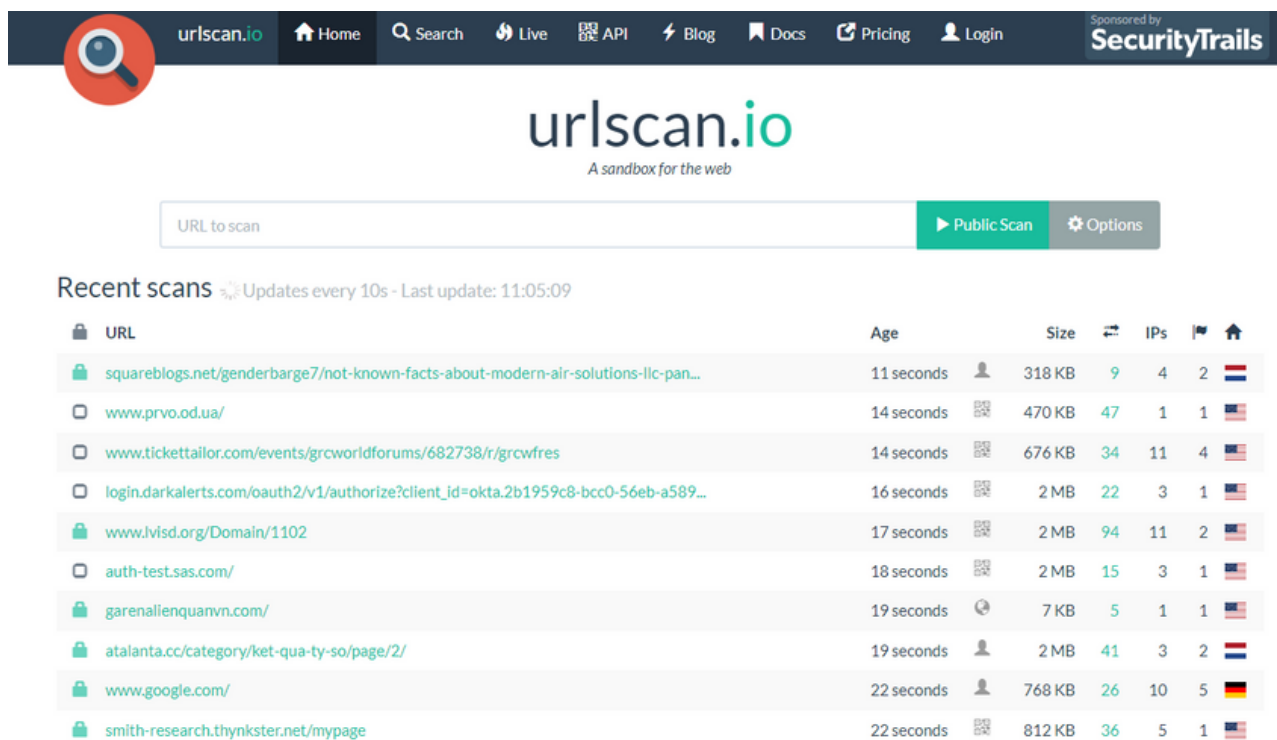
It provides an analysis report with Falcon Sandbox and Hybrid Analysis technology.



Online Sandbox

urlscan

If you specifically want to scan URL addresses, it's useful tool for you.



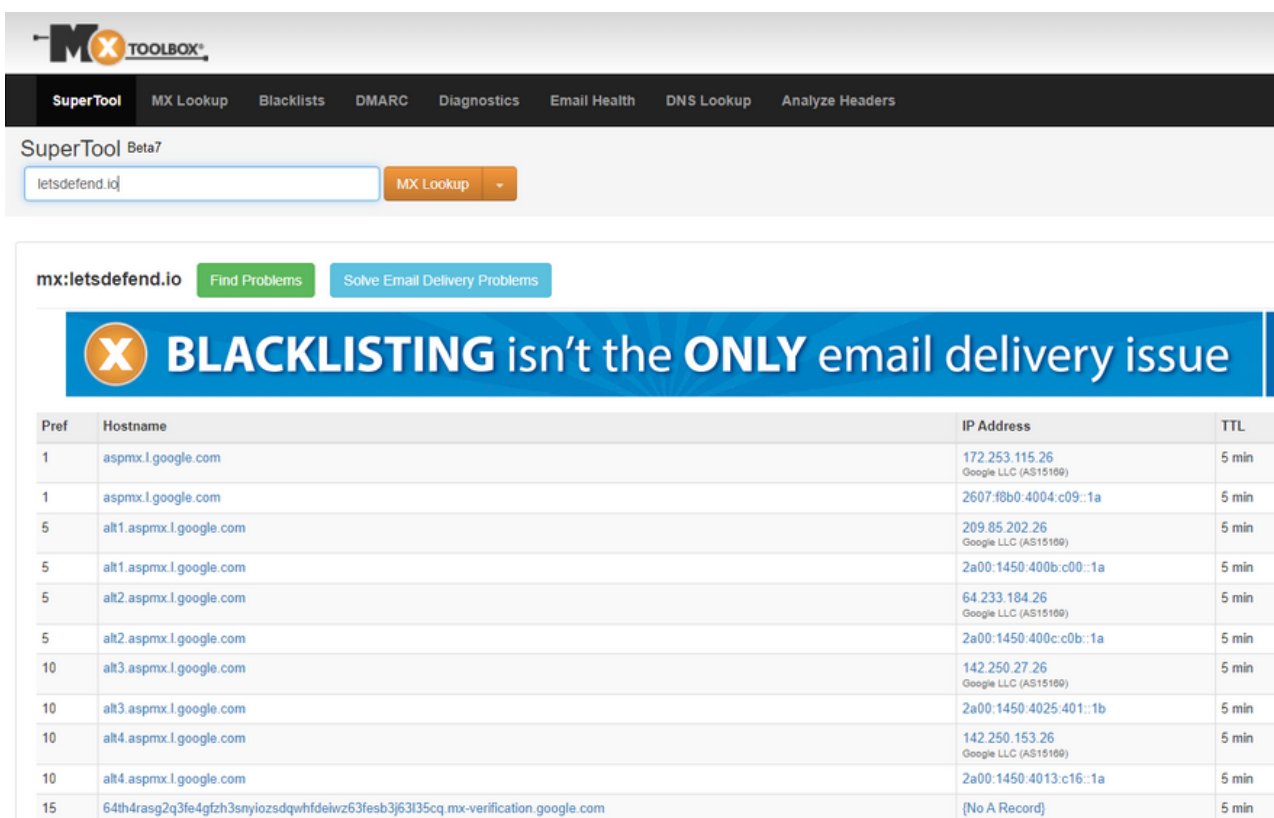
The screenshot shows the urlscan.io website interface. At the top, there is a navigation bar with links for Home, Search, Live, API, Blog, Docs, Pricing, and Login. A search bar is located in the center of the page, with a "Public Scan" button and an "Options" button to its right. Below the search bar, there is a section titled "Recent scans" with a sub-header "Updates every 10s - Last update: 11:05:09". A table lists the recent scans with columns for URL, Age, Size, and IPs.

| URL | Age | Size | IPs |
|---|------------|--------|-----|
| squareblogs.net/genderbarg7/not-known-facts-about-modern-air-solutions-llc-pan... | 11 seconds | 318 KB | 9 |
| www.prvo.od.ua/ | 14 seconds | 470 KB | 47 |
| www.tickettailor.com/events/grcworldforums/682738/r/grcwfres | 14 seconds | 676 KB | 34 |
| login.darkalerts.com/oauth2/v1/authorize?client_id=okta.2b1959c8-bcc0-56eb-a589... | 16 seconds | 2 MB | 22 |
| www.lvisd.org/Domain/1102 | 17 seconds | 2 MB | 94 |
| auth-test.sas.com/ | 18 seconds | 2 MB | 15 |
| garenalienquanvn.com/ | 19 seconds | 7 KB | 5 |
| atalanta.cc/category/ket-qua-ty-so/page/2/ | 19 seconds | 2 MB | 41 |
| www.google.com/ | 22 seconds | 768 KB | 26 |
| smith-research.thynkster.net/mypage | 22 seconds | 812 KB | 36 |

Other

MXToolBox

During the phishing campaign analysis, it would be helpful for spoofing analysis. You can compare the SMTP addresses.



The screenshot shows the MXToolBox website interface. At the top, there is a navigation bar with the following links: SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, and Analyze Headers. Below the navigation bar, the page title is "SuperTool Beta7". A search input field contains "letsdefend.io" and a button labeled "MX Lookup" is next to it. Below the search bar, there are two buttons: "Find Problems" and "Solve Email Delivery Problems". A prominent blue banner with a white 'X' icon contains the text "BLACKLISTING isn't the ONLY email delivery issue". Below the banner is a table with the following columns: Pref, Hostname, IP Address, and TTL.

| Pref | Hostname | IP Address | TTL |
|------|---|---|-------|
| 1 | aspmx.l.google.com | 172.253.115.26 <small>Google LLC (AS15100)</small> | 5 min |
| 1 | aspmx.l.google.com | 2607:f8b0:4004:c09::1a | 5 min |
| 5 | alt1.aspmx.l.google.com | 209.85.202.26 <small>Google LLC (AS15100)</small> | 5 min |
| 5 | alt1.aspmx.l.google.com | 2a00:1450:400b:c00::1a | 5 min |
| 5 | alt2.aspmx.l.google.com | 64.233.184.26 <small>Google LLC (AS15100)</small> | 5 min |
| 5 | alt2.aspmx.l.google.com | 2a00:1450:400c:c0b::1a | 5 min |
| 10 | alt3.aspmx.l.google.com | 142.250.27.26 <small>Google LLC (AS15100)</small> | 5 min |
| 10 | alt3.aspmx.l.google.com | 2a00:1450:4025:401::1b | 5 min |
| 10 | alt4.aspmx.l.google.com | 142.250.153.26 <small>Google LLC (AS15100)</small> | 5 min |
| 10 | alt4.aspmx.l.google.com | 2a00:1450:4013:c16::1a | 5 min |
| 15 | 64th4rasg2q3fe4gfzh3snyiozsdqwhfdeiwz63fesb3j63l35cq.mx-verification.google.com | [No A Record] | 5 min |

Other

Koodous

Provides malicious APK data

The screenshot shows the Koodous dashboard interface. The top navigation bar includes the Koodous logo, a menu icon, and a 'Send us your feedback' link. The main content area is titled 'Dashboard' and features four large colored boxes with icons and numbers: a purple box with a document icon and '4,757,503', a blue box with a cloud icon and '14,188', a green box with a bug icon and '1,083,931', and a light blue box with a trophy icon and '0'. Below these are two tabs: 'Timeline' and 'Global Activity'. The 'Latest APKs' section lists several items with their respective icons and timestamps:

| APK Name | Platform | Timestamp |
|------------------|------------|-------------------------|
| 中国移动端 | Android | Oct 21, 2015 8:21:26 AM |
| 中国移动 | Android | Oct 21, 2015 8:21:18 AM |
| Music WapCash | WapCash | Oct 21, 2015 8:21:00 AM |
| Flashlight Ultra | smartgame0 | Oct 21, 2015 8:20:46 AM |

Other

python-oletools

It helps to analyze the Microsoft OLE2 files (Office documents, Outlook messages, etc.)

```
$ oledir 41a84ee951ec7efa36dc16c70aaaf6b8e6d1bce8bd9002d0ab5236197eb3b32a.bin
oledir 0.02 - http://decalage.info/python/oletools
OLE directory entries in file 41a84ee951ec7efa36dc16c70aaaf6b8e6d1bce8bd9002d0ab5236197eb3b32a.bin:
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
id |Status|Type  |Name                                     |Left|Right|Child|1st Sect|Size
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
0  |<Used>|Root  |Root Entry                             |-   |-   |3    |2A     |2496
1  |unused|Empty |                                         |-   |-   |-    |0      |0
2  |<Used>|Stream|WordDocument                           |5   |-   |-    |0      |4096
3  |<Used>|Stream|\x05SummaryInformation                 |2   |4   |-    |16     |4096
4  |<Used>|Stream|\x05DocumentSummaryInformation      |-   |-   |-    |1E     |4096
5  |<Used>|Stream|1Table                                 |-   |13  |-    |8      |7094
6  |unused|Empty |                                         |-   |-   |-    |0      |0
7  |unused|Empty |                                         |-   |-   |-    |0      |0
8  |unused|Empty |                                         |-   |-   |-    |0      |0
9  |unused|Empty |                                         |-   |-   |-    |0      |0
10 |unused|Empty |                                         |-   |-   |-    |0      |0
11 |unused|Empty |                                         |-   |-   |-    |0      |0
12 |unused|Empty |                                         |-   |-   |-    |0      |0
13 |<Used>|Stream|\x01CompObj                       |-   |-   |-    |25     |114
14 |unused|Empty |                                         |-   |-   |-    |0      |0
15 |unused|Empty |                                         |-   |-   |-    |0      |0
$
$ oledir 6780af202bf7534fd7fcfc37aa57e5a998e188ca7d65e22c0ea658c73fad36a2.bin
oledir 0.02 - http://decalage.info/python/oletools
OLE directory entries in file 6780af202bf7534fd7fcfc37aa57e5a998e188ca7d65e22c0ea658c73fad36a2.bin:
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
id |Status|Type  |Name                                     |Left|Right|Child|1st Sect|Size
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
0  |<Used>|Root  |Root Entry                             |-   |-   |3    |2A     |2496
1  |<Used>|Stream|1Table                                 |-   |-   |-    |8      |7094
2  |<Used>|Stream|WordDocument                           |5   |-   |-    |0      |4096
3  |<Used>|Stream|\x05SummaryInformation                 |2   |4   |-    |16     |4096
4  |<Used>|Stream|\x05DocumentSummaryInformation      |-   |-   |-    |1E     |4096
5  |<Used>|Storage|Macros                                 |1   |13  |12   |0      |0
6  |<Used>|Storage|VBA                                   |-   |-   |7    |0      |0
7  |<Used>|Stream|ThisDocument                           |8   |9   |-    |0      |1214
8  |<Used>|Stream|Module1                               |10  |-   |-    |32     |42488
9  |<Used>|Stream|_VBA_PROJECT                          |-   |-   |-    |88     |10014
10 |<Used>|Stream|dir                                    |-   |-   |-    |13     |571
11 |<Used>|Stream|PROJECTwm                             |-   |-   |-    |1C     |65
12 |<Used>|Stream|PROJECT                              |6   |11  |-    |1E     |419
13 |<Used>|Stream|\x01CompObj                       |-   |-   |-    |25     |114
14 |unused|Empty |                                         |-   |-   |-    |0      |0
15 |unused|Empty |                                         |-   |-   |-    |0      |0
```