

# NetAnalysis v3.1



- [Release Notes for NetAnalysis® Version 3.1](#)
- [UC Browser on Android and iOS](#)
- [Decrypting UC Login Data on Android](#)
- [Zone.Identifier Recovery](#)
- [Change Log](#)
- [Release Notes for HstEx® Version 5.1](#)

## Release Notes for NetAnalysis® Version 3.1

NetAnalysis® version 3.1 continues our quest to add further support for mobile browsers. This release adds support for **eighteen new browsers**, namely **7 Star Browser**, **Naver Whale** on desktop and mobile platforms, **Opera Mini** on mobile platforms, **Opera Touch** on Android, **Opera GX** on mobile platforms, **Dolphin Browser** on Android, **Brave** on mobile platforms, **Opera** on mobile platforms, **QQ Browser** on mobile platforms and **UC Browser** on mobile platforms.

We have also added new artefacts for existing browsers, giving us a total of **142 new artefacts** for this version. For a full list of changes, see [NetAnalysis® v3.1 Change Log](#).

## UC Browser on Android and iOS

UC Browser is a cross-platform web browser developed by mobile internet company [UCWeb](#), a subsidiary of the Alibaba Group. It is primarily targeted at mobile platforms and is extremely popular in India, Indonesia and China. It also encrypts many of the databases used to store user data.

In this release of NetAnalysis®, we have enhanced our support for UC Browser on Android and iOS. We can now decrypt History, Most Recent Visited History, Search Data and Bookmarks.

## Decrypting UC Login Data on Android

We have also added support for decrypting usernames and passwords.

NetAnalysis® v3.1 - Forensic Internet History Analysis - [UC Browser on Android]

File View Tools Search Filter Index Reports Column Window Help

(UTC+00:00) Dublin, Edinburgh, Lisbon, London

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	URL	Logon User	Logon Password	Decoded URL
→ Login Data	https		2021-09-13 13:09:19.309	2021-09-13 14:09:19.309	https://m.facebook.com/login/device-based/regular/login/	james_smith_bloggs@gmail.com	password456	https://m.facebook.com/login/device-based/regular/login/
Login Data	https		2021-09-13 13:10:03.213	2021-09-13 14:10:03.213	https://m.facebook.com/login/device-based/regular/login/	jessica_mcdonald2021@gmail.com	password123	https://m.facebook.com/login/device-based/regular/login/
Login Data	https		2021-09-13 13:12:45.704	2021-09-13 14:12:45.704	https://mega.nz/login	andrew-smith-parsley2019@gmail.com	^\$Pt1o7U~k({\$	https://mega.nz/login
Login Data	https		2021-09-14 10:24:56.872	2021-09-14 11:24:56.872	https://mega.nz/login	trawler_johnson8946@gmail.com	rI6GQyu)O%6a_~ip]5Ewz	https://mega.nz/login
Login Data	https		2021-09-14 10:26:05.741	2021-09-14 11:26:05.741	https://www.pcloud.eu	davidjasonwilliams@gmail.com	8M+[R4<23zxu9f4Ph?	https://www.pcloud.eu
Login Data	https		2021-09-14 10:26:53.951	2021-09-14 11:26:53.951	https://www.myheritage.com/	manchester78@gmail.com	PtWvcg .bu\$AHLzUjX()A	https://www.myheritage.com/
Login Data	https		2021-09-14 10:31:47.695	2021-09-14 11:31:47.695	https://m.facebook.com/login/device-based/regular/login/	stirling_mctavish223@gmail.com	Nm,RToe(CXQjU#(tez&?	https://m.facebook.com/login/device-based/regular/login/
Login Data	https		2021-09-14 10:33:56.721	2021-09-14 11:33:56.721	https://accounts.google.com/signin/v2/challenge/password/empty	jonaathan_doe_3321@gmail.com	OG,,YQ)jC[H1>)awuitd	https://accounts.google.com/signin/v2/challenge/password/empty
Login Data	https		2021-09-14 10:35:13.913	2021-09-14 11:35:13.913	https://accounts.google.com/signin/v2/challenge/password/empty	maxine-jefferson222@gmail.com	fe%k^*aNo>p?	https://accounts.google.com/signin/v2/challenge/password/empty
Login Data	https		2021-09-14 11:21:26.803	2021-09-14 12:21:26.803	https://www.digital-detective.net/cgi-bin/digitalboard/ra88.pl	abcdefghijklmnopqrstuvwxyz	~:3dQX8RvI +uIKNzu~?JE[?#xDc]	https://www.digital-detective.net/cgi-bin/digitalboard/ra88.pl
Quota Usage	https		2021-09-13 13:20:05.091	2021-09-13 14:20:05.091	https://www.digital-detective.net/			https://www.digital-detective.net/
Quota Usage	https		2021-09-14 11:22:12.636	2021-09-14 12:22:12.636	https://mega.nz/			https://mega.nz/
Quota Usage	https		2021-09-13 13:13:12.891	2021-09-13 14:13:12.891	https://news.sky.com/			https://news.sky.com/
Quota Usage	https		2021-09-14 09:28:30.094	2021-09-14 10:28:30.094	https://uk.bestdeals.today/			https://uk.bestdeals.today/
Quota Usage	https		2021-09-14 10:33:29.585	2021-09-14 11:33:29.585	https://www.myheritage.com/			https://www.myheritage.com/

Record 1 of 9372

Information

```

1  Origin URL: https://m.facebook.com/
2  Action URL: https://m.facebook.com/login/device-based/regular/login/
3  Username Element: email
4  Username Value: 22f9EBAB879CDBACEBA1A4BF988688F0B9EAB996845C...5ACF4E581819DCA
5  Decrypted Username: james_smith_bloggs@gmail.com
6  Password Element: pass
7  Password Value: D0F6E1B6B58296A0B0E0F4B6E1
8  Decrypted Password: password456
9  Signon Realm: https://m.facebook.com/
10 Preferred: False
11 Blacklisted by User: False
12 Times Used: 0
13 Date Created [UTC]: 2021-09-13 13:09:21.008
14 Skip Zero Click: False
15 Generation Upload Status: No Signal Sent
16 Date Last Used [UTC]: 2021-09-13 13:09:19.309

```

www.digital-detective.net | \\digital03\Browser Data Mobiles\Android\UC Browser\v13\2021\_09\_16 (3)\com.UCMobile.intl\app\_u4\_webview\p\_data | ID: 1 | 1

## Zone.Identifier Recovery

With the release of [HstEx® v5.1](#), we have added the ability to search and recover MFT entries containing resident Zone Identifier data. This provides us with a lot of information regarding the original file. The recovered data is easily read into NetAnalysis® for examination. The image below shows a number of recovered Zone Identifier entries. The Information panel shows the associated MFT attribute information along with the Zone Transfer data from the Zone.Identifier stream.

NetAnalysis® v3.2 - Forensic Internet History Analysis - [HstEx® Recovered Resident MFT Zone.Identifier Entries]

File View Tools Search Filter Index Reports Column Window Help

(UTC+00:00) Dublin, Edinburgh, Lisbon, London

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	URL	Local Path	Host Name
Zone Identifier	https		2021-09-21 15:42:05.097	2021-09-21 16:42:05.097	https://www.digital-detective.net/download/downloadbac.php?downcode=sv0by94fhzy9z9lg...	Blade-x86-EN-1.17.21169.57.zip	www.digital-detective.net
Zone Identifier	https		2021-06-03 08:34:23.145	2021-06-03 09:34:23.145	https://ftp.mozilla.org/pub/firefox/releases/88.0b9/win64/en-GB/Firefox%20Setup%2088.0b...	Firefox Setup 88.0b9.exe	ftp.mozilla.org
Zone Identifier	https		2021-05-27 09:03:04.223	2021-05-27 10:03:04.223	https://dl.teamviewer.com/download/version_15x/TeamViewer_Setup_x64.exe	TeamViewer_Setup_x64.exe	dl.teamviewer.com
Zone Identifier	https		2021-06-08 10:43:29.530	2021-06-08 11:43:29.530	https://phoenixnap.dl.sourceforge.net/project/wincache/development/wincache-2.0.0.8-dev-...	wincache-2.0.0.8-dev-7.2.beta2-nts-vc15-x64.exe	phoenixnap.dl.sourceforge.net
Zone Identifier	https		2021-06-08 10:11:35.635	2021-06-08 11:11:35.635	https://deac-ans.dl.sourceforge.net/project/wincache/development/wincache-2.0.0.8-dev-7-...	wincache-2.0.0.8-dev-7.3-nts-vc15-x64.exe	deac-ans.dl.sourceforge.net
Zone Identifier	https		2021-06-08 10:35:00.756	2021-06-08 11:35:00.756	https://deac-fra.dl.sourceforge.net/project/wincache/wincache-2.0.0/wincachewpi-2.0.0.8-7-...	wincachewpi-2.0.0.8-7.2-nts-vc15-x64(1).exe	deac-fra.dl.sourceforge.net
Zone Identifier	https		2021-06-08 10:19:38.719	2021-06-08 11:19:38.719	https://netcologne.dl.sourceforge.net/project/wincache/wincache-2.0.0/wincachewpi-2.0.0.8-...	wincachewpi-2.0.0.8-7.2-nts-vc15-x64.exe	netcologne.dl.sourceforge.net
Zone Identifier	https		2021-06-08 10:34:18.444	2021-06-08 11:34:18.444	https://netcologne.dl.sourceforge.net/project/wincache/wincache-2.0.0/wincachewpi-2.0.0.8-...	wincachewpi-2.0.0.8-7.2-nts-vc15-x86.exe	netcologne.dl.sourceforge.net
Zone Identifier	https		2021-06-08 10:09:23.851	2021-06-08 11:09:23.851	https://altushost-swe.dl.sourceforge.net/project/wincache/development/wincache-2.0.0.8-de...	wincache-2.0.0.8-dev-7.1-nts-vc14-x64.exe	altushost-swe.dl.sourceforge.net

Record 3 of 11

Information

```
1 MFT Record Information
2   Entry Index: 41
3   Entry Flags: InUse
4
5 File Information ($FILE_NAME 0x30)
6   Name: Blade-x86-EN-1.17.21169.57.zip
7   Parent Entry Index: 5
8   Allocated Size: 25,231,360 (24.06 MB)
9   Real Size: 0 (0.00 KB)
10  File Attributes: Archive
11    Date Created [UTC]: 2021-10-06 11:49:46.302
12    Date Modified [UTC]: 2021-10-06 11:49:46.302
13    Date Accessed [UTC]: 2021-10-06 11:49:46.302
14    Entry Modified [UTC]: 2021-10-06 11:49:46.302
15
16 Standard Information ($STANDARD_INFORMATION 0x10)
17   File Flags: Archive
18     Date Created [UTC]: 2021-09-21 15:42:05.097
19     Date Modified [UTC]: 2021-09-21 15:42:18.753
20     Date Accessed [UTC]: 2021-10-06 11:49:46.443
21     Entry Modified [UTC]: 2021-10-06 11:49:46.490
22
23 Object ID Information ($OBJECT_ID 0x40)
24   Object ID: 7823cb48-2670-11ec-92d4-fcaal4290f80
25   Version: 1
26   Timestamp [UTC]: 2021-10-06 06:41:43.544
27   Clock Sequence: 4020
28   Node: FC-AA-14-29-0F-80
29
30 Zone Transfer
31   Zone ID: 3 (Internet)
32   Stream Length: 196 (0.19 KB)
```

www.digital-detective.net D:\Desktop\downloads.img PS: 2097234 SO: 000 3

## Change Log

The full list of changes can be found here: [NetAnalysis® v3.1 Change Log](#).

## Release Notes for HstEx® Version 5.1

Don't forget to review the release notes for HstEx® which can be found here: [HstEx v5.1 Release Notes](#).