Morning Session:

Introduction to Forensics and Web Browser Forensics

Cyber Taster - Digital Forensics

14/05/2019 – 10:00-12:00

Learning Outcomes

- Morning:
- Gain a high level understanding of what Digital Forensics entails
- Develop an understanding of Web Browser Forensics

- Afternoon:
- Develop an understanding of Image and EXIF metadata forensics

Structure of Session

- Morning Session: 10:00-12:00
  - Presentation: 45 minutes
    - Introduction to Forensics
    - Web Browser Forensics
  - Workshop: 70 minutes
    - Browser Forensics

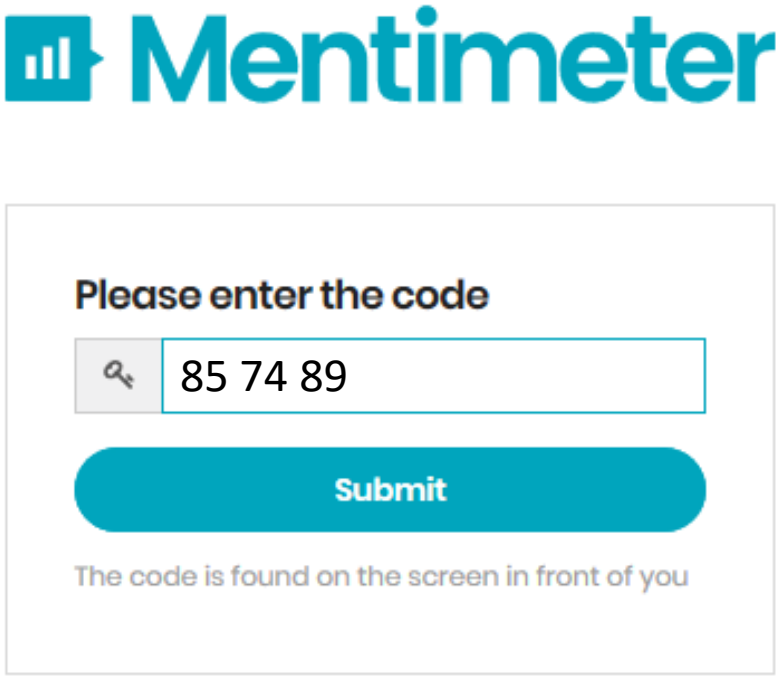
All resources for today can be found at:
https://github.com/smck1/taste_of_cyber

- Afternoon Session : 13:00-15:00
  - Presentation: 45 minutes
    - Image and EXIF Forensics
  - Workshop: 70 minutes
    - Image and EXIF Forensics

Questions

- Submit a question

- Go to: menti.com
- Code: 85 74 89



Digital Forensics - Introduction

Definitions: Digital Forensics

- There is no single standard definition
- "The process by which information is extracted from data storage media (e.g. devices, systems associated with computing, …), rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings." (UK Forensic Science Regulator, quoted in Digital Forensics and Crime - Parliament UK. http://researchbriefings.files.parliament.uk/documents/POST-PN-0520/POST-PN-0520.pdf)

Investigation Process

NIST (National Institute of Standards and Technology) 2006 - SP 800-86

Investigation Process

Collection

- Identify, label, record, acquire data from relevant sources
- e.g. devices, networks, cloud storage
- Preserve integrity
- In a timely manner

Examination

- Use Combination of automated and manual methods
- Assess and extract data of interest for the specific situation
- Preserve integrity

Investigation Process

Analysis

- Derive useful information to answer the original questions
- Use well documented methods and techniques
- Makes use of the evidence in context

Reporting

- Report the results of the analysis
- Style must be suitable for intended audience
- May include actions, tool selection, suggested additional work, recommendations for improvements to policies, tools etc

Goals and constraints when handling evidence

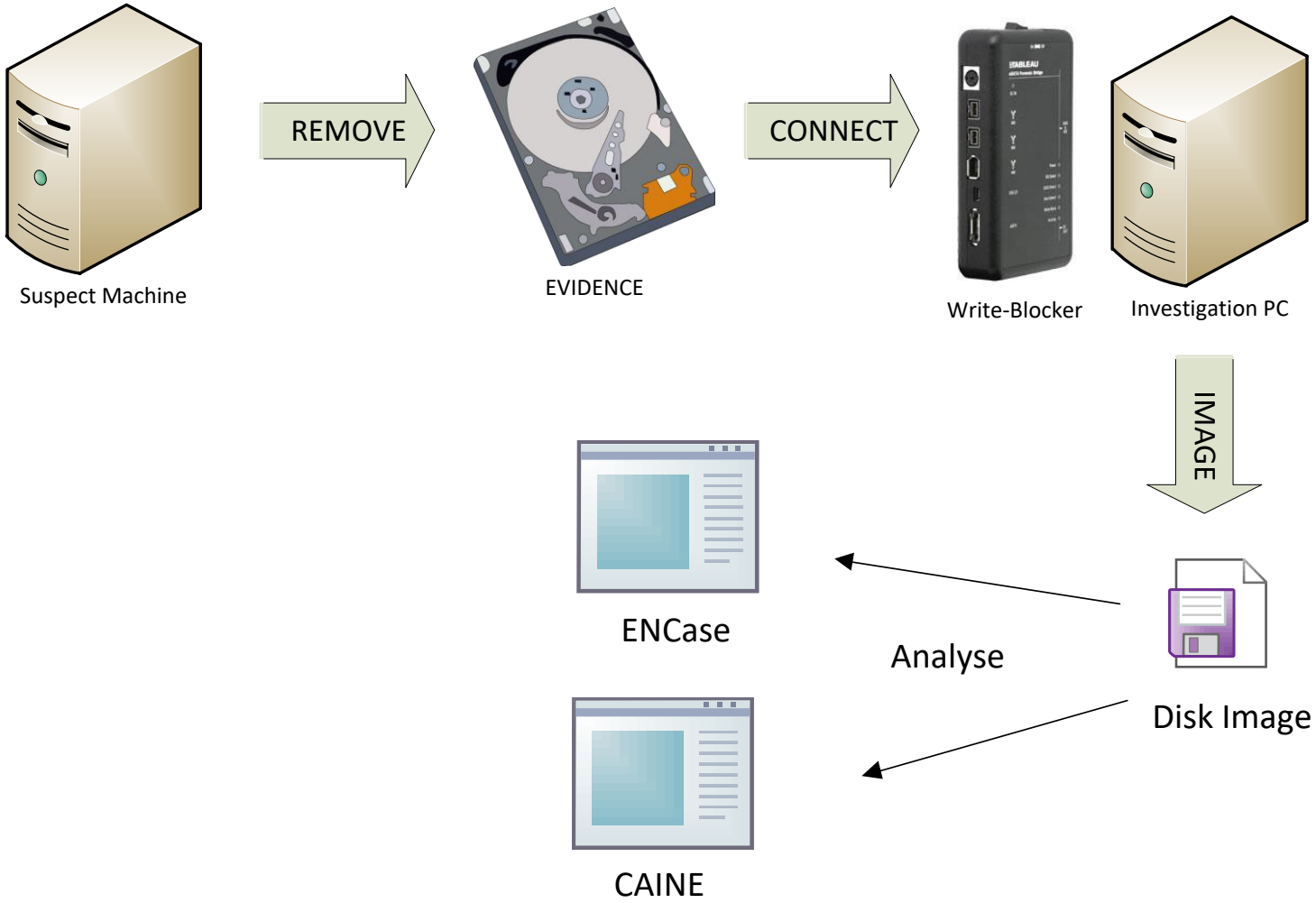
- Find and make available information of value
- Preserve evidence integrity - and show it to be preserved
  - Do not alter evidence
  - Use only tools that guarantee this
  - Chain of custody
- Methodology must be secure, controlled, repeatable, auditable
- Rules set e.g. by ACPO (Association of Chief Police Officers)

Some Challenges

- Size, number & type of storage devices - growing rapidly
  - Multi-device analysis, Embedded flash devices / SSDs
  - Cloud storage / cloud computing
- Difficult to associate with a real person
- Volatility, ease of evidence tampering / anti-forensics
- Knowledge & skills of digital forensic analysts; capability of tools
- Low technical literacy of public & judiciary - poor understanding of evidence/ reports
- Pervasive Encryption, RAM-only Malware
- Privacy laws - Legal Challenges decreasing the scope of forensic investigations

Acquisition methods: Traditional

- Remove the hard disk
  - Image elsewhere
  - Plug into investigation system as an external disk



Write Blockers

- Monitor the commands given to the Hard Disk
- Do not allow data to be written
- Do not allow the disk to be mounted with write-access
  - Read-commands only
- Hardware and Software
  - Hardware used & trusted more
  - Both equally expensive

Reports and Courts

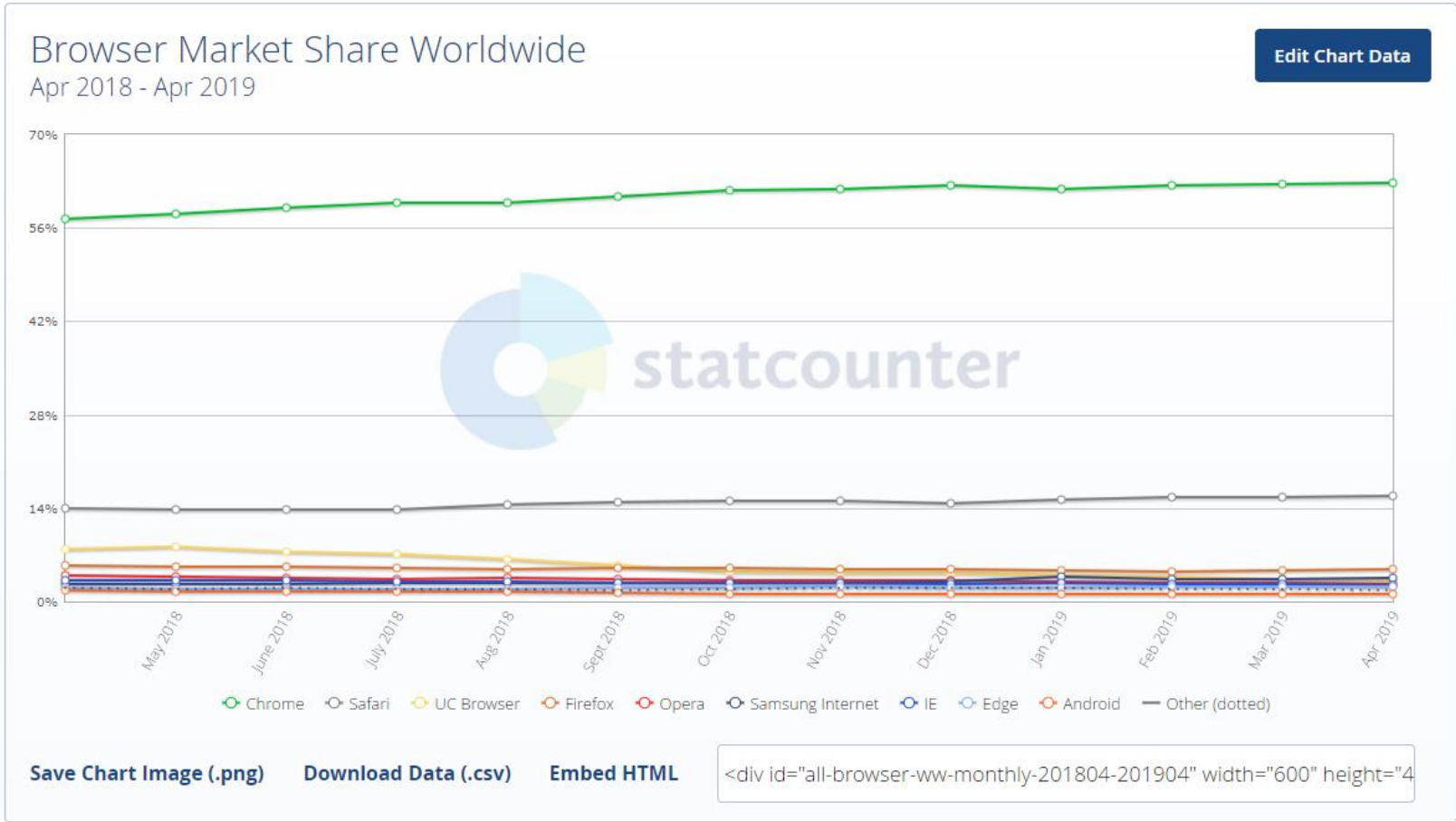
- Forensic reports
  - Contain very detailed documentation of the findings
  - What, where, when, how
  - Statement of facts with expert analysis of how the evidence came to be the way it is.
- Expert Testimony
  - Often called to court to give evidence directly to the jury
  - “Expert Witness” in a professional capacity
  - Measures statements focusing on facts and expertise, not opinion or accusation of guilt/innocence

Browser Forensics

Desktop Browser Market Share (April 2019)

Chrome	Safari	Firefox	Samsung Internet	UC Browser	IE
63.16%	15.37%	5.09%	3.17%	3.07%	2.58%

Browser Market Share Worldwide - April 2019



What does your browser know about you?

How is this information stored?

Web Browsing History

- Web browsers normally keep a record of accessed websites
- Primary purpose:
  - to allow a user to return to commonly accessed websites.
- Forensic use:
  - discover the user's activity on the internet.
- How to avoid it?
  - Use private browsing / delete your browsing history

What is stored?

- files used in displaying web pages (cache)
- pages visited (history)
- Information filled in, e.g. logins/bank cards (form history)
- automatic identification / authentication (cookies, credentials)

- Able to see a record of recently visited pages (history)
- No sign in again at sites that require it, or to specify preferences again (cookies and credentials). Also cookies are used by the visited site and other sites to track web browsing, which is a privacy discussion on its own.

Why Look at Browsers Evidence?

- Show evidence of premeditated crimes (searching for weapons, locations, how-to articles)
- Direct evidence of crimes (websites, videos)

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: urls

	id	url	title	visit_count
	Filter	Filter	flight	Filter
1	9	https://www....	flights out of scotland - Google Search	32
2	617	https://www....	Cheap Flights from Scotland to Mexico City - Cheapflights.co.uk	1

Internet Cache

- Internet Browsers keep a cache of viewed pages and other resources accessed on the internet.
- Primary purpose:
  - when the page is accessed again, the browser can retrieve stored page code and embedded files (such as graphics) from the hard drive rather than the server - speeds up access and saves bandwidth - page loads faster
- Forensic use:
  - recover information about what a user was accessing on the internet.

Cookies

- A cookie is a small piece of text that the browser can store on behalf of the web server.
- Primary purpose:
  - Allows session information to be recorded between visits to a website. (e.g. keep shopping basket contents)
- Forensic use:
  - understand how the user may have interacted with a website.
- Beware: some cookies may be spurious! (third-party cookies)
  - Useful resource: http://cookiepedia.co.uk/.

How browsers store info?

- most browsers use SQLite database files
- different files, tables and locations

Browser	Storage Format
Firefox (since v.3)	SQLite, json
Chrome	SQLite, SNSS, json
Safari	SQLite
Browser (Android Webkit)	SQLite

What is SQLite

http://www.sqlite.org/about.html

- A very "light" open source DBMS (Database Management System)
  - embedded SQL database engine
    - no separate server process; reads and writes directly to ordinary files
  - Very compact – requires little space / RAM
    - Popular for mobile devices
  - Popular as an application file format
    - Used “behind the scenes” of many apps.

Firefox - SQLite files & locations

- **places.sqlite** is the main DB for browsing history
- Location in Windows: C:\Users\<user>\AppData\Roaming\Mozilla\Firefox\Profiles\<random characters>.default
- see http://www.forensicswiki.org/wiki/Mozilla_Firefox

Firefox (v.51, Feb 2017)

main files same for v.57 Feb 2018

addons.json	13/02/2017 09:53	JSON File	1 KB
AlternateServices.txt	13/02/2017 10:13	Text Document	0 KB
blocklist.xml	13/02/2017 09:55	XML Document	241 KB
cert8.db	13/02/2017 10:13	Data Base File	160 KB
compatibility.ini	13/02/2017 10:02	Configuration sett...	1 KB
containers.json	13/02/2017 10:02	JSON File	1 KB
content-prefs.sqlite	20/03/2016 23:10	SQLITE File	224 KB
cookies.sqlite	13/02/2017 10:13	SQLITE File	512 KB
extensions.ini	13/02/2017 10:02	Configuration sett...	1 KB
extensions.json	13/02/2017 10:02	JSON File	7 KB
formhistory.sqlite	13/02/2017 10:02	SQLITE File	192 KB
key3.db	13/02/2017 10:13	Data Base File	16 KB
logins.json	13/02/2017 10:12	JSON File	1 KB
mimeTypes.rdf	12/10/2016 14:17	RDF File	5 KB
parent.lock	13/02/2017 10:02	LOCK File	0 KB
permissions.sqlite	13/02/2017 10:02	SQLITE File	128 KB
places.sqlite	13/02/2017 10:12	SQLITE File	10,240 KB
places.sqlite-shm	13/02/2017 10:02	SQLITE-SHM File	32 KB
places.sqlite-wal	13/02/2017 10:12	SQLITE-WAL File	609 KB
pluginreg.dat	13/02/2017 09:49	DAT File	7 KB
prefs.js	13/02/2017 10:13	JavaScript File	14 KB
revocations.txt	13/02/2017 09:55	Text Document	20 KB
search.json	31/05/2016 23:59	JSON File	118 KB
search.json.mozlz4	13/02/2017 10:02	MOZLZ4 File	25 KB
secmod.db	29/09/2015 15:47	Data Base File	16 KB
sessionCheckpoints.json	13/02/2017 10:13	JSON File	1 KB
sessionstore.js	13/02/2017 10:13	JavaScript File	7 KB
SiteSecurityServiceState.txt	13/02/2017 10:13	Text Document	2 KB
storage.sqlite	13/02/2017 10:02	SQLITE File	1 KB
times.json	29/09/2015 10:46	JSON File	1 KB
webappsstore.sqlite	13/02/2017 10:13	SQLITE File	576 KB
xulstore.json	13/02/2017 10:13	JSON File	1 KB

places.sqlite example (moz_places table)

TABLE moz_places | Search | Show All | Add | Duplicate | Edit | Delete

id	url	title	rev_host	visit_count	hidden	typed	favicon_id	frecency	last_visit_date	guid
1	http://www.mozilla.com/en-US/firefox/c...		moc.allizom.w...	0	0	0		137		IEBF71z-ZB32
2	http://www.mozilla.com/en-US/firefox/...		moc.allizom.w...	0	0	0	1	137		n8nFTE7xjnJr
3	http://www.mozilla.com/en-US/firefox/c...		moc.allizom.w...	0	0	0	2	137		NXW9eWC2N...
4	http://www.mozilla.com/en-US/firefox/c...		moc.allizom.w...	0	0	0	3	137		J_Uaq29I-vWd
5	http://www.mozilla.com/en-US/about/		moc.allizom.w...	0	0	0	4	137		i7Sb_KbFLwTH
6	place:sort=8&maxResults=10			0	1	0		0		yyGGe_jP1ide
7	place:folder=BOOKMARKS_MENU&fold...			0	1	0		0		Foxui6HsO2Ib
8	place:type=6&sort=14&maxResults=10			0	1	0		0		LpSKSgX2Y6Vp
9	http://www.mozilla.com/en-US/firefox/1...		moc.allizom.w...	1	1	0		98	1360942570796...	E7rHXv43TX1z
10	http://www.mozilla.org/en-US/firefox/15...		gro.allizom.w...	1	1	0		98	1360942571109...	idBjUQPSsE0W
11	http://www.mozilla.org/en-US/firefox/u...	Mozilla Firefox Web Browser — Check for Upd...	gro.allizom.w...	1	0	0	5	-1	1360942571265...	AP4qeM6Vr3NX
12	http://www.google.co.uk/	Google	ku.oc.elgoog....	12	0	0	6	1170	1361281593...	_sArCpdOpYJ6
13	http://www.google.co.uk/#hl=en&tbo=...	mp3tag - Google Search	ku.oc.elgoog....	1	0	0	6	98	1360942586281...	htteAe-eIRWS
14	http://www.mp3tag.de/en/	Mp3tag - the universal Tag Editor (ID3v2, MP4,...	ed.gat3pm.ww...	1	0	0	7	98	1360942587734...	0S_WDpYNbyl3
15	http://www.mp3tag.de/en/download.ht...	Mp3tag - Download	ed.gat3pm.ww...	1	0	0	7	98	1360942590656...	Elg2p0hV5txd
16	http://download.mp3tag.de/mp3tagv25...		ed.gat3pm.da...	1	1	0		98	1360942592437...	Yu7QBBGJ4uuK
17	http://download.mp3tag.de/current/mp...	mp3tagv254setup.exe	ed.gat3pm.da...	0	0	0		0	1360942592828...	EMKMa1mTp...
18	http://www.google.co.uk/#hl=en&tbo=...	axcrpty - Google Search	ku.oc.elgoog....	1	0	0	6	98	1360942598656...	afUi9jOntj1Q
19	http://www.axantum.com/axcrypt/	Axantum Software AB | AxCrypt | File Encrypti...	moc.mutnaxa....	1	0	0	8	98	1360942600156...	PYsRaRXX9Be9
20	http://www.axantum.com/axcrypt/Dow...	Axantum Software AB | AxCrypt | Download	moc.mutnaxa....	1	0	0	8	98	1360942601937...	MFJWJf6STWdB
21	http://www.axantum.com/Download/Ax...	AxCrypt-1.7.2976.0-Setup.exe	moc.mutnaxa....	0	0	0		0	1360942603656...	nhuorc_cm7x9
22	http://www.google.co.uk/#hl=en&suge...	vlc - Google Search	ku.oc.elgoog....	1	0	0	6	98	1360942692125...	aYzgL94eflkA

Firefox uses Unix/Epoch timestamps, convert using https://www.epochconverter.com/

Chrome SQLite files

- Google Chrome stores the browser history in SQLite databases like Firefox, however, the structure of the databases is different.
- **History** file serves a similar function to places.sqlite in Firefox.

- Windows 10/7 location: C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default
- see http://www.forensicswiki.org/wiki/Google_Chrome

Chrome (v.64, Mar 2018)

- Application Cache
- blob_storage
- Cache
- data_reduction_proxy_leveldb
- databases
- Download Service
- Extension Rules
- Extension State
- Extensions
- Feature Engagement Tracker
- File System
- GCM Store
- GPUCache
- IndexedDB
- JumpListIconsMostVisited
- JumpListIconsRecentClosed
- Local App Settings
- Local Extension Settings
- Local Storage
- Managed Extension Settings
- Media Cache
- Pepper Data
- Platform Notifications
- Service Worker
- Session Storage
- Storage
- Sync Data
- Sync Extension Settings
- Thumbnails
- VideoDecodeStats
- Web Applications

- Affiliation Database
- Affiliation Database-journal
- Bookmarks
- Bookmarks.bak
- Cookies
- Cookies-journal
- Current Session
- Current Tabs
- Custom Dictionary.txt
- Custom Dictionary.txt.backup
- DownloadMetadata
- Extension Cookies
- Extension Cookies-journal
- Favicons
- Favicons-journal
- Google Profile.ico
- History
- History-journal
- Last Session
- Last Tabs

- Login Data
- Login Data-journal
- Network Action Predictor
- Network Action Predictor-journal
- Network Persistent State
- Origin Bound Certs
- Origin Bound Certs-journal
- Preferences
- previews_opt_out.db
- previews_opt_out.db-journal
- QuotaManager
- QuotaManager-journal
- Secure Preferences
- Shortcuts
- Shortcuts-journal
- Top Sites
- Top Sites-journal
- Translate Ranker Model
- TransportSecurity
- Visited Links
- Web Data
- Web Data-journal

Sqlite yellow (no fill where not much use); JSON green; SNSS (session saver) files purple

History example (urls table)

Tables (12)

- downloads
- downloads_slices
- downloads_url_chains
- keyword_search_terms
- meta
- segment_usage
- segments
- sqlite_sequence
- typed_url_sync_metadata
- urls
- visit_source
- visits

Table: urls

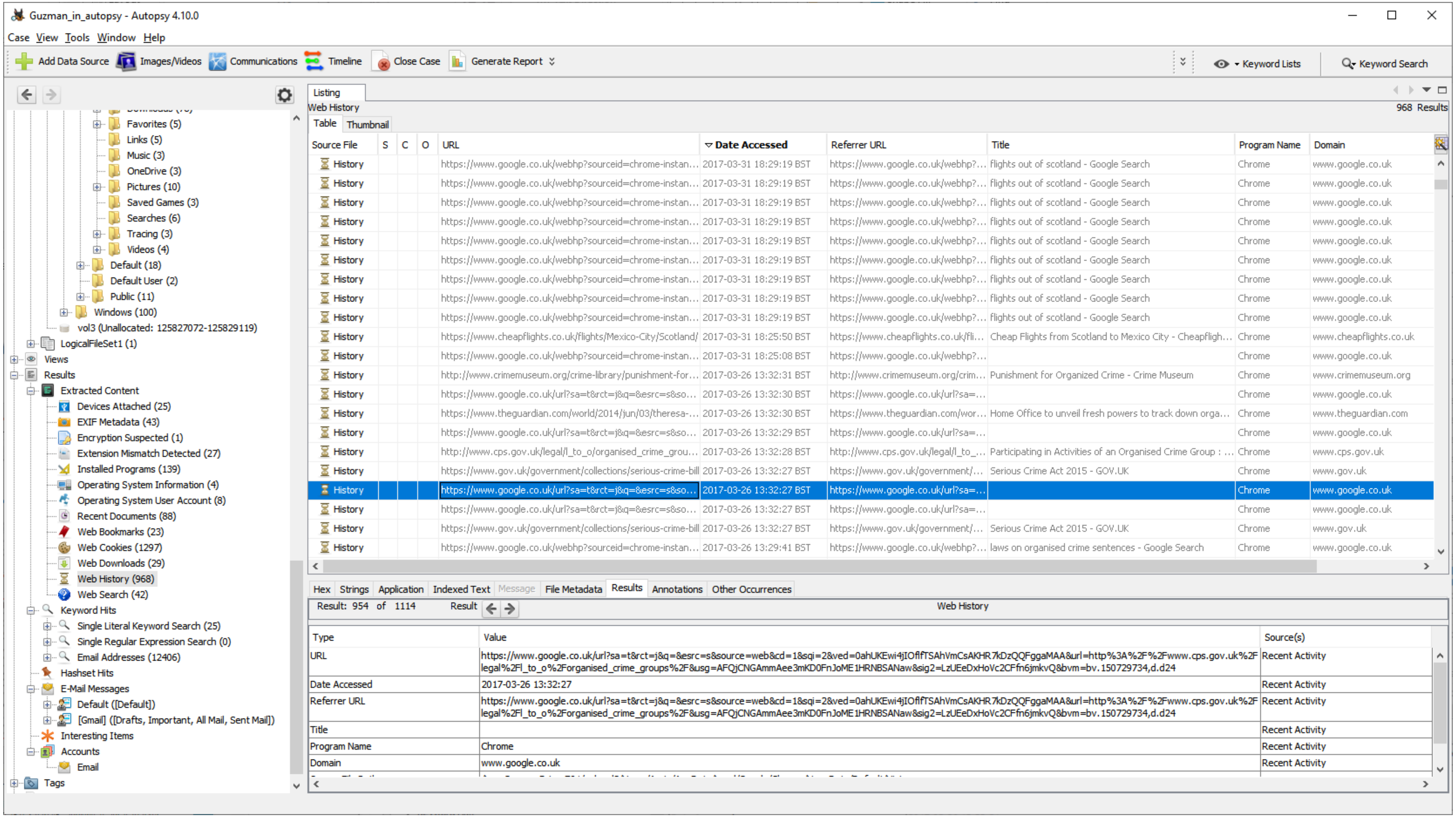
New Record | Delete Reco

	id	url	title	visit_count	typed_count	last_visit_time	hidden	favicon_id
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	109	http://www.modules.napier.ac.uk/	Modules Information	2	0	13114003955629840	0	0
2	116	https://tracker.napier.ac.uk/	Tracker: Student Management	5	0	13116947102185278	0	0
3	191	https://hrconnect.napier.ac.uk/mthrpr...		10	0	13114606794322029	1	0
4	192	https://hrconnect.napier.ac.uk/mthrpr...		10	0	13114606794322029	1	0
5	273	http://www.ee.surrey.ac.uk/Teaching...	UNIX / Linux Tutorial for Beginners	0	0	0	0	0
6	286	http://archive.oreilly.com/linux/cmd/	Linux Command Directory: Index	0	0	0	0	0
7	299	http://www.nationwide.co.uk/	Nationwide Building Society | On your side	6	5	13116760498332133	0	0
8	315	https://www.facebook.com/	Facebook	67	0	13116369720369144	0	0
9	316	https://www.linkedin.com/	Welcome! | LinkedIn	6	2	13114632954214338	0	0
10	327	http://www.facebook.com/	(13) Facebook	23	0	13116354070834011	0	0
11	330	https://www.evernote.com/Home.action	Evernote Web	5	0	13114708051321772	0	0
12	341	https://evernote.com/	The note-taking space for your life's work | Ev...	3	0	13114708042925936	0	0
13	342	https://www.evernote.com/	The note-taking space for your life's work | Ev...	3	0	13114708042925936	0	0
14	344	http://k2b-bulk.ebay.co.uk/ws/eBayIS...	Sign in or Register | eBay	0	0	0	0	0
15	345	http://www.davidlloyd.co.uk/home	Gym Membership, Racquets, Classes & Swimm...	0	0	0	0	0

(Chrome uses WebKit timestamps – convert using https://www.epochconverter.com/webkit

Forensic Tool View

Chrome History in Autopsy (Forensics Tool)



Source File	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name	Domain
History				https://www.google.co.uk/webhp?sourceid=chrome-instan…	2017-03-31 18:29:19 BST	https://www.google.co.uk/webhp?…	flights out of scotland - Google Search	Chrome	www.google.co.uk
History				https://www.google.co.uk/webhp?sourceid=chrome-instan…	2017-03-31 18:29:19 BST	https://www.google.co.uk/webhp?…	flights out of scotland - Google Search	Chrome	www.google.co.uk
History				https://www.google.co.uk/webhp?sourceid=chrome-instan…	2017-03-31 18:29:19 BST	https://www.google.co.uk/webhp?…	flights out of scotland - Google Search	Chrome	www.google.co.uk
History				https://www.google.co.uk/webhp?sourceid=chrome-instan…	2017-03-31 18:29:19 BST	https://www.google.co.uk/webhp?…	flights out of scotland - Google Search	Chrome	www.google.co.uk
History				https://www.google.co.uk/webhp?sourceid=chrome-instan…	2017-03-31 18:29:19 BST	https://www.google.co.uk/webhp?…	flights out of scotland - Google Search	Chrome	www.google.co.uk
History				https://www.google.co.uk/webhp?sourceid=chrome-instan…	2017-03-31 18:29:19 BST	https://www.google.co.uk/webhp?…	flights out of scotland - Google Search	Chrome	www.google.co.uk
History				https://www.google.co.uk/webhp?sourceid=chrome-instan…	2017-03-31 18:29:19 BST	https://www.google.co.uk/webhp?…	flights out of scotland - Google Search	Chrome	www.google.co.uk
History				https://www.google.co.uk/webhp?sourceid=chrome-instan…	2017-03-31 18:29:19 BST	https://www.google.co.uk/webhp?…	flights out of scotland - Google Search	Chrome	www.google.co.uk
History				https://www.google.co.uk/webhp?sourceid=chrome-instan…	2017-03-31 18:29:19 BST	https://www.google.co.uk/webhp?…	flights out of scotland - Google Search	Chrome	www.google.co.uk
History				https://www.cheapflights.co.uk/flights/Mexico-City/Scotland/	2017-03-31 18:25:50 BST	https://www.cheapflights.co.uk/fli…	Cheap Flights from Scotland to Mexico City - Cheapfligh…	Chrome	www.cheapflights.co.uk
History				https://www.google.co.uk/webhp?sourceid=chrome-instan…	2017-03-31 18:25:08 BST	https://www.google.co.uk/webhp?…		Chrome	www.google.co.uk
History				http://www.crimemuseum.org/crime-library/punishment-for…	2017-03-26 13:32:31 BST	http://www.crimemuseum.org/crim…	Punishment for Organized Crime - Crime Museum	Chrome	www.crimemuseum.org
History				https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&so…	2017-03-26 13:32:30 BST	https://www.google.co.uk/url?sa=…		Chrome	www.google.co.uk
History				https://www.theguardian.com/world/2014/jun/03/theresa-…	2017-03-26 13:32:30 BST	https://www.theguardian.com/wor…	Home Office to unveil fresh powers to track down orga…	Chrome	www.theguardian.com
History				https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&so…	2017-03-26 13:32:29 BST	https://www.google.co.uk/url?sa=…		Chrome	www.google.co.uk
History				http://www.cps.gov.uk/legal/l_to_o/organised_crime_grou…	2017-03-26 13:32:28 BST	http://www.cps.gov.uk/legal/l_to_…	Participating in Activities of an Organised Crime Group : …	Chrome	www.cps.gov.uk
History				https://www.gov.uk/government/collections/serious-crime-bill	2017-03-26 13:32:27 BST	https://www.gov.uk/government/…	Serious Crime Act 2015 - GOV.UK	Chrome	www.gov.uk
History				https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&so…	2017-03-26 13:32:27 BST	https://www.google.co.uk/url?sa=…		Chrome	www.google.co.uk
History				https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&so…	2017-03-26 13:32:27 BST	https://www.google.co.uk/url?sa=…		Chrome	www.google.co.uk
History				https://www.gov.uk/government/collections/serious-crime-bill	2017-03-26 13:32:27 BST	https://www.gov.uk/government/…	Serious Crime Act 2015 - GOV.UK	Chrome	www.gov.uk
History				https://www.google.co.uk/webhp?sourceid=chrome-instan…	2017-03-26 13:29:41 BST	https://www.google.co.uk/webhp?…	laws on organised crime sentences - Google Search	Chrome	www.google.co.uk

Result: 954 of 1114 Result

Web History

Type	Value	Source(s)
URL	https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&sqi=2&ved=0ahUKEwi4jIOflfTSAhVmCsAKHR7kDzQQFggaMAA&url=http%3A%2F%2Fwww.cps.gov.uk%2Flegal%2Fl_to_o%2Forganised_crime_groups%2F&usg=AFQjCNGAmmAee3mKD0FnJoME1HRNBSANaw&sig2=LzUEeDxHoVc2CFfn6jmkvQ&bvm=bv.150729734,d.d24	Recent Activity
Date Accessed	2017-03-26 13:32:27	Recent Activity
Referrer URL	https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&sqi=2&ved=0ahUKEwi4jIOflfTSAhVmCsAKHR7kDzQQFggaMAA&url=http%3A%2F%2Fwww.cps.gov.uk%2Flegal%2Fl_to_o%2Forganised_crime_groups%2F&usg=AFQjCNGAmmAee3mKD0FnJoME1HRNBSANaw&sig2=LzUEeDxHoVc2CFfn6jmkvQ&bvm=bv.150729734,d.d24	Recent Activity
Title		Recent Activity
Program Name	Chrome	Recent Activity
Domain	www.google.co.uk	Recent Activity

Private Browsing

How private browsing works

When you browse privately, other people who use the device won't see your activity.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you close Incognito mode.

You can switch between Incognito windows and regular Chrome windows. You'll only browse in private when you're using an Incognito window.

Your activity might still be visible

Incognito mode stops Chrome from saving your browsing activity. But your activity might still be visible to:

Your activity might still be visible to:

- **Websites you visit**, including the ads and resources used on those sites
- **Your employer, school**, or whoever runs the network you're using
- **Your internet service provider**

For more information about what's saved, visit the Chrome Privacy Policy.

Downloads and bookmarks are saved

Chrome won't remember the files you download while browsing in private. But, they're still saved to your Downloads folder, even after you exit Incognito. You and anyone who uses your device can see and open the files.

All bookmarks you create are saved to Chrome.

For more information about what's saved in Incognito mode, visit the Chrome Privacy Policy.

So how "good" are the different browsers' private modes?

- Montasari and Peltola (2015) compared Chrome v26, Firefox v20, IE 9, Safari v5 – looking at "local attacker" security.

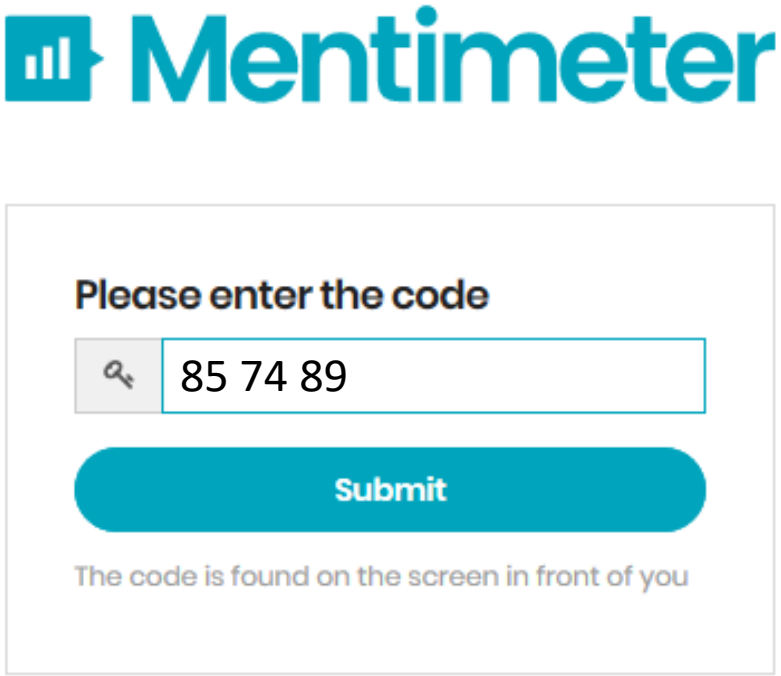
	Artefacts found in Hard Drive				Found in RAM (while browser running)			
activity	Chrome	Firefox	IE	Safari	Chrome	Firefox	IE	Safari
Visited URL www.youtube.com	None	46	74	63	1,180	204	504	4,038
Visited URL www.google.com	None	22	322	21	1,611	210	1,053	2,142
Visited URL www.facbook.com	None	7	259	47	1,764	396	5,757	7,077
Visited URL www.amazon.co.uk	None	3	514	19	1,719	760	3,292	11,744
Search term "Jessie ware …"	None	None	191	22	412	412	488	1,416
Search term "Pirate Bay Proxy"	None	1	161	46	906	330	2,697	1,281
Search term "Ubuntu"	None	3	182	25	197	164	330	665
Search term "Casio F-91W"	None	None	151	10	268	216	780	8,253
Search term "Doppelganger: …"	None	None	13	4	2,586	2,232	264	12,552
Downloaded profile picture	None	1	2	1	None	None	None	3

Tables 8 & 9 combined from Montasari &Peltola

Questions

- Submit a question

- Go to: menti.com
- Code: 85 74 89



Appendix

Reading and references

References - web

All browsers

- http://kb.digital-detective.net/display/BF/Browser+Forensics+and+Analysis

Firefox

- http://www.forensicswiki.org/wiki/Mozilla_Firefox - updated fairly recently
- Firefox Forensics and SQLite Tables for Computer Forensics Analysis http://resources.infosecinstitute.com/firefox-and-sqlite-forensics/ (from 2011, now out of date in places)

Chrome

- http://www.forensicswiki.org/wiki/Google_Chrome
- https://digital-forensics.sans.org/blog/2010/01/21/google-chrome-forensics/ (from 2010!)
- https://www.academia.edu/16383095/Forensic_Investigation_of_User_s_Web_Activity_on_Google_Chrome_using_Open-source_Forensic_Tools
- SSNS files (session, tabs) http://www.cclgroupltd.com/chrome-session-and-tabs-files-and-the-puzzle-of-the-pickle/

More about SQLite

- Homepage: http://www.sqlite.org/sqlite.html
- Detailed Documentation: http://www.sqlite.org/docs.html
- Tutorial: http://www.tutorialspoint.com/sqlite/sqlite_overview.htm

Workshop Resources

- https://github.com/smck1/taste_of_cyber