Forensic Equity
Safe in the knowledge

A Digital Defence:

A closer look at Computer Evidence in Criminal Cases

Forensic Equity
Safe in the knowledge

Case Study 1 – Computer Alibi

Case Study 1 – Computer Alibi

Forensic Equity
Safe in the knowledge

A crime is committed, and the defendant suggests that activity on his computer will confirm he was using it at the time of the incident.

In this case, he says he was browsing YouTube at the time of the crime.

Case Study 1 – Computer Alibi

Forensic Equity
Safe in the knowledge

1. Forensic Image of Device or the Device itself.
2. A specific time period to review.

Note

Forensic Equity
Safe in the knowledge

If the device is in the possession of the defendant, great care should be taken to not use the computer in any way from the point of their instruction (earlier if possible).

If the device is in possession of the police, we would provide the appropriate wording to send to the CPS in order for them to authorise the release of the exhibit.

ACPO Guidelines

Forensic Equity
Safe in the knowledge

https://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf

"In order to comply with the principles of digital evidence, wherever practicable, proportionate and relevant an image should be made of the device. This will ensure that the original data is preserved, enabling an independent third party to re-examine it and achieve the same result, as required by principle 3."

Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

ACPO Guidelines

Forensic Equity
Safe in the knowledge

- **Principle 1:** No action taken by law enforcement agencies, persons employed within those agencies, or their agents should change data which may subsequently be relied upon in court.
- **Principle 2:** In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- **Principle 3:** An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- **Principle 4:** The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Creating a forensic image

Forensic Equity
Safe in the knowledge

Creating a forensic image

Forensic Equity
Safe in the knowledge

Case Study 1 – Computer Alibi

Forensic Equity
Safe in the knowledge

- Can we prove that the computer was switched on at the time of the crime?
- File system timestamps assist with this:
- **Creation Time** (the time a file was created).
- **Modified Time** (the time the content of a file was last modified).
- **MFT Modified Time** (in Windows systems, the time a files metadata was last modified).
- **Accessed Time** (where recorded, the time a file was last accessed).

Case Study 1 – Computer Alibi

Forensic Equity
Safe in the knowledge

Name	Partial path	Created	Modified	Record changed	Accessed
.. = AppData (114,307)	\sidne	01/11/2020 00:01:55 +0	01/11/2020 00:01:55 +0	01/11/2020 00:01:55 +0	01/11/2020 00:02:15 +0
. = Roaming (3,205)	\sidne\AppData	01/11/2020 00:01:55 +0	17/12/2020 14:09:48 +0	17/12/2020 14:09:48 +0	17/12/2020 14:09:48 +0
zoommeeting.enc.db	Zoom\data	14/12/2020 18:57:12 +0	14/12/2020 20:31:48 +0	14/12/2020 20:31:48 +0	14/12/2020 20:31:48 +0
viper.ini	Zoom\data	14/12/2020 19:00:20 +0	14/12/2020 20:32:02 +0	14/12/2020 20:32:02 +0	14/12/2020 20:32:02 +0
conf_avatar_6910569af733...	Zoom\data\ConfAvatar	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0
conf_avatar_f9d695fbccf3adc...	Zoom\data\ConfAvatar	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0
conf_avatar_05dd8650e462c5...	Zoom\data\ConfAvatar	14/12/2020 19:00:22 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0
conf_avatar_36228b4a7895...	Zoom\data\ConfAvatar	14/12/2020 19:00:22 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0
conf_avatar_68efe30b48bde...	Zoom\data\ConfAvatar	14/12/2020 19:00:22 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0
conf_avatar_a4660cc30ba5...	Zoom\data\ConfAvatar	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0
conf_avatar_f9d695fbccf3adc...	Zoom\data\ConfAvatar	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0
conf_avatar_a4660cc30ba58...	Zoom\data\ConfAvatar	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0
conf_avatar_6910569af733b...	Zoom\data\ConfAvatar	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0	14/12/2020 19:00:22 +0
conf_avatar_36228b4a7895a...	Zoom\data\ConfAvatar	14/12/2020 19:00:22 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0
conf_avatar_05dd8650e462c5...	Zoom\data\ConfAvatar	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0
conf_avatar_68efe30b48bde0...	Zoom\data\ConfAvatar	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0
conf_avatar_db25e99a2929c...	Zoom\data\ConfAvatar	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0	14/12/2020 19:00:23 +0
conf_avatar_d68b77a4d1bf1...	Zoom\data\ConfAvatar	14/12/2020 19:00:25 +0	14/12/2020 19:00:25 +0	14/12/2020 19:00:25 +0	14/12/2020 19:00:25 +0
conf_avatar_1f96e2aeb0d49...	Zoom\data\ConfAvatar	14/12/2020 19:03:09 +0	14/12/2020 19:03:09 +0	14/12/2020 19:03:09 +0	14/12/2020 19:03:09 +0
conf_avatar_f7010ace16f0e4...	Zoom\data\ConfAvatar	14/12/2020 19:03:37 +0	14/12/2020 19:03:37 +0	14/12/2020 19:03:37 +0	14/12/2020 19:03:37 +0
conf_avatar_211c2aebaa7d9...	Zoom\data\ConfAvatar	14/12/2020 19:14:23 +0	14/12/2020 19:14:23 +0	14/12/2020 19:14:23 +0	14/12/2020 19:14:23 +0

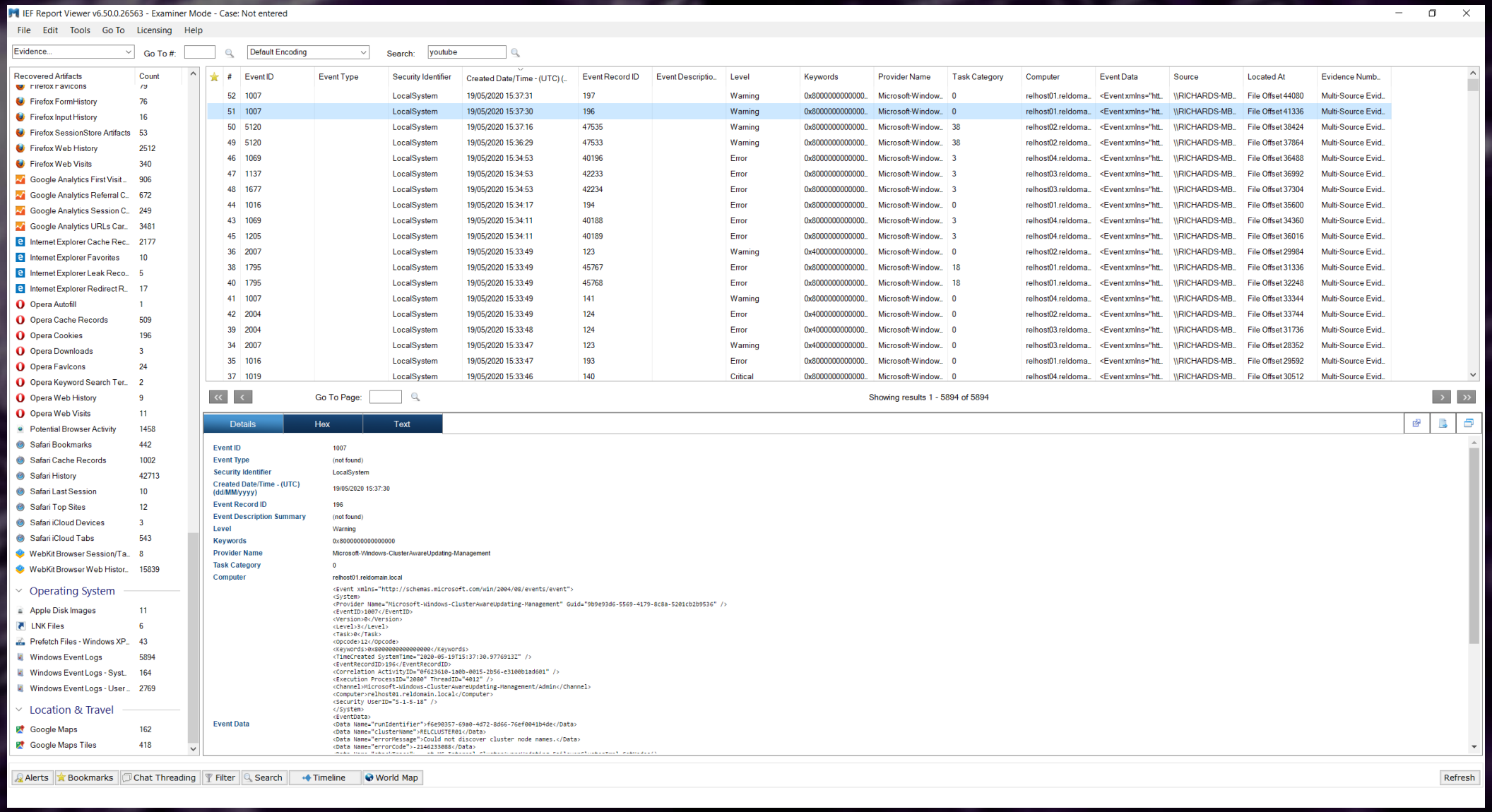
Case Study 1 – Computer Alibi

Forensic Equity
Safe in the knowledge

- Can we prove that the computer was switched on at the time of the crime?
- Various artifacts can also assist with this, such as login times, event logs and so on.

Case Study 1 – Computer Alibi

Forensic Equity
Safe in the knowledge



Case Study 1 – Computer Alibi

Forensic Equity
Safe in the knowledge

- Can we corroborate the defendant's account?
- In this case the defendant was using YouTube.
- Browsing History Records may assist.
- Browser cookies may assist.
- Browser cache records and content may assist.
- Records, including deleted records, can be retrieved and interpreted with specialist computer forensic software.

Filter Results

File Help

Evidence... Go To #: Default Encoding Search:

Filtered Artifacts

IEF Refined Results
- Cloud Services URLs
- Facebook URLs
- Google Searches
- Parsed Search Queries
- Rebuilt Webpages

Web Related
- Chrome Cache Records
- Firefox Web History
- Safari Bookmarks
- Safari History
- Safari Top Sites
- Safari iCloud Tabs
- WebKit Browser Web Histor...

#	URL	Last Visited Date/Time ...	Title	Visit Cou...	Visit Source	Located At	Ev
2...	https://myaccount.google.com/u/1/signinoptions/recov...	11/04/2022 11:25:23	Account Recovery Options	2	Locally Browsed	Table: history_items(id: 50395), Table: history_visits(id: 97219)	Mu
8...	https://accounts.youtube.com/accounts/SetSID	11/04/2022 11:25:29		11	Locally Browsed	Table: history_items(id: 41739), Table: history_items(id: 50396), Table: ...	Mu
2...	https://www.youtube.com/watch?v=L_UX2y_or_M&t=67...	11/04/2022 14:58:29	(57) ● LIVE From Manchester Airport - SUPER SUNDAY - YouTube	2	Locally Browsed	Table: history_items(id: 50389), Table: history_visits(id: 97234)	Mu
2...	https://www.google.com/search?q=youtube&client=saf...	14/04/2022 17:43:36	youtube - Google Search	2	Locally Browsed	Table: history_items(id: 46411), Table: history_items(id: 50465), Table: ...	Mu
2...	https://www.google.com/search?q=youtube&client=saf...	14/04/2022 17:43:36	youtube - Google Search	2	Locally Browsed	Table: history_items(id: 50465), Table: history_visits(id: 97374)	Mu
1...	https://www.youtube.com/	14/04/2022 17:43:39	(57) YouTube	79	Locally Browsed	Table: history_items(id: 46411), Table: history_visits(id: 97376)	Mu
1...	https://www.youtube.com/	14/04/2022 17:44:08	(57) YouTube	79	Locally Browsed	Table: history_items(id: 46411), Table: history_visits(id: 97378)	Mu
2...	https://www.youtube.com/watch?v=2lwBU2D87ZY	14/04/2022 17:44:08	(58) LIVE From Vancouver Airport - South Terminal Viewing Area - YouTube	1	Locally Browsed	Table: history_items(id: 50466), Table: history_visits(id: 97379)	Mu
1...	https://www.youtube.com/	15/04/2022 10:37:48	(60) YouTube	79	Locally Browsed	Table: history_items(id: 46411), Table: history_visits(id: 97390)	Mu
1...	https://www.youtube.com/	15/04/2022 10:37:51	(60) YouTube	79	Locally Browsed	Table: history_items(id: 46411), Table: history_visits(id: 97392)	Mu
2...	https://www.youtube.com/watch?v=3J4ye63fVcY	15/04/2022 10:37:51	(60) ● LIVE From Manchester Airport - FRI YAY SHOW - YouTube	1	Locally Browsed	Table: history_items(id: 50474), Table: history_visits(id: 97393)	Mu
1...	https://www.youtube.com/	15/04/2022 12:33:08	(60) YouTube	79	Locally Browsed	Table: history_items(id: 46411), Table: history_visits(id: 97394)	Mu
2...	https://www.youtube.com/c/salvagerebuildsuk	15/04/2022 12:33:16	(60) salvage rebuilds uk - YouTube	6	Locally Browsed	Table: history_items(id: 49891), Table: history_visits(id: 97395)	Mu
1...	https://www.youtube.com/c/JimmysWorld1	15/04/2022 12:33:36	(60) Jimmys World - YouTube	3	Locally Browsed	Table: history_items(id: 48571), Table: history_visits(id: 97396)	Mu
1...	https://www.youtube.com/c/JimmysWorld1/videos	15/04/2022 12:33:42	(60) Jimmys World - YouTube	4	Locally Browsed	Table: history_items(id: 48124), Table: history_visits(id: 97397)	Mu
2...	https://www.youtube.com/watch?v=2thlw98Cgsc	19/04/2022 11:49:23	(63) How To Use YouCut Video Editing App on Android (2022) - YouTube	2	Locally Browsed	Table: history_items(id: 50538), Table: history_visits(id: 97505)	Mu
2...	https://www.youtube.com/watch?v=2thlw98Cgsc	19/04/2022 11:49:46	(63) How To Use YouCut Video Editing App on Android (2022) - YouTube	2	Locally Browsed	Table: history_items(id: 50538), Table: history_visits(id: 97506)	Mu
2...	https://www.youtube.com/watch?v=f2Pm4sbRCec	19/04/2022 12:06:10	How to change Storage Used for YouCut Video Editor App - YouTube	1	Locally Browsed	Table: history_items(id: 50542), Table: history_visits(id: 97513)	Mu
2...	https://www.youtube.com/attribution_link?a=dqzo7wx_7...	22/04/2022 18:04:40		1	Locally Browsed	Table: history_items(id: 50658), Table: history_items(id: 50659), Table: ...	Mu
2...	https://www.youtube.com/watch?v=Sm4hXoR_2eo&feat...	22/04/2022 18:04:40	● LIVE From CA Vancouver Airport (YVR) - YouTube	1	Locally Browsed	Table: history_items(id: 50659), Table: history_visits(id: 97778)	Mu
2...	https://www.youtube.com/watch?v=Sm4hXoR_2eo	22/04/2022 18:04:43	● LIVE From CA Vancouver Airport (YVR) - YouTube	1	Locally Browsed	Table: history_items(id: 50661), Table: history_visits(id: 97781)	Mu

Go To Page: Showing results 1 - 364 of 364

Details | Hex | Text

URL	https://www.youtube.com/watch?v=Sm4hXoR_2eo&feature=em-lbrm
Last Visited Date/Time - (UTC) (dd/MM/yyyy)	22/04/2022 18:04:40
Redirect URL	(not found)
Title	● LIVE From CA Vancouver Airport (YVR) - YouTube
Visit Count	1
Visit Source	Locally Browsed
Source	\\RICHARDS-MBP\richarddrinkwater (User Selected) - [ROOT]\Library\Safari\History.db
Located At	Table: history_items(id: 50659), Table: history_visits(id: 97778)
Evidence Number	Multi-Source Evidence 1

Timeline

Search Hits

File Help

Evidence... Go To #: Default Encoding Search:

Searched Artifacts	Count
IEF Refined Results	
Classifieds URLs	24
Cloud Services URLs	54
Facebook URLs	1
Google Analytics URLs	5
Google Searches	35
Parsed Search Queries	38
Rebuilt Webpages	1
Social Media URLs	71
Communication	
iMessage Messages	2
Documents	
CSV Documents	12
Excel Documents	36
PDF Documents	56
PowerPoint Documents	20
Text Documents	10
Word Documents	31
Email & Calendar	
EML(X) Files	5
Outlook Emails	294
Media	
Pictures	873
Videos	25
Web Related	
Chrome Bookmarks	6
Chrome Cache Records	1
Chrome Cookies	24
Chrome FavIcons	130
Chrome Keyword Search Te...	4
Chrome Shortcuts	6
Chrome Top Sites	1
Chrome Web History	65
Chrome Web Visits	115
Edge/Internet Explorer 10-11...	2
Edge/Internet Explorer 10-11...	1
Firefox FormHistory	5
Firefox Web History	19
Google Analytics URLs Car...	58

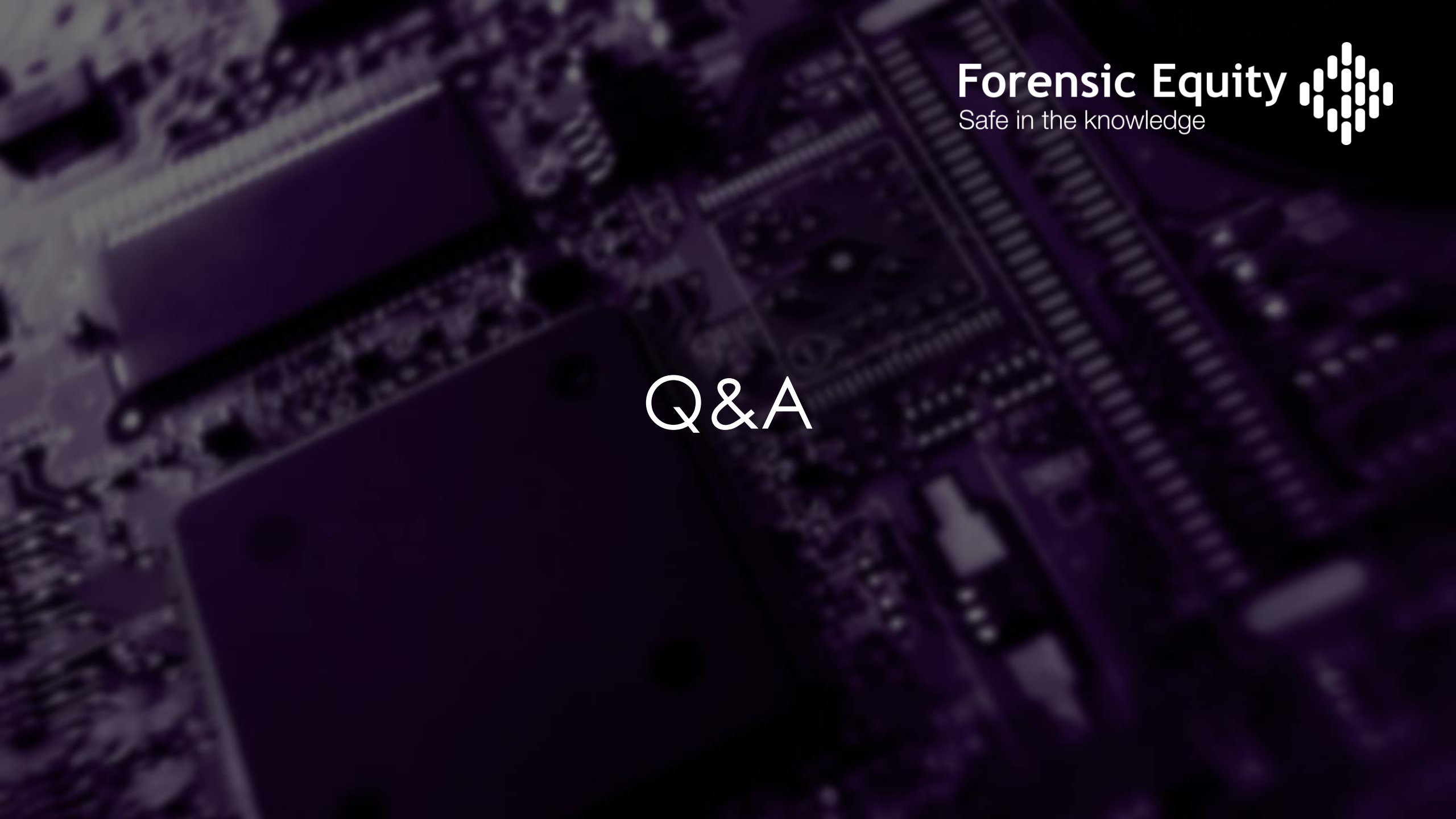
#	Host	Name	Value	Accessed Date/Tim...	Created Date/Time - (UT...	Expiration Date/...	Path	Source	Located At	Evidence Numb...
8...	.youtube.com	SID		08/01/2021 12:00:50	08/01/2021 12:00:50	08/01/2023 12:00:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 59750)	Multi-Source Evid...
8...	.youtube.com	SSID		08/01/2021 12:00:50	08/01/2021 12:00:50	08/01/2023 12:00:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 59755)	Multi-Source Evid...
9...	.youtube.com	__Secure-3PAPIS...		08/01/2021 12:00:50	08/01/2021 12:00:50	08/01/2023 12:00:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 59760)	Multi-Source Evid...
9...	.youtube.com	__Secure-3PSID		08/01/2021 12:00:50	08/01/2021 12:00:50	08/01/2023 12:00:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 59763)	Multi-Source Evid...
2...	.youtube.com	APISID		22/04/2022 21:34:55	14/04/2021 13:36:51	18/04/2024 06:44:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 6627)	Multi-Source Evid...
2...	.youtube.com	HSID		22/04/2022 21:34:55	14/04/2021 13:36:51	18/04/2024 06:44:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 6630)	Multi-Source Evid...
2...	.youtube.com	SAPISID		22/04/2022 21:34:55	14/04/2021 13:36:51	18/04/2024 06:44:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 6632)	Multi-Source Evid...
2...	.youtube.com	SSID		22/04/2022 21:34:55	14/04/2021 13:36:51	18/04/2024 06:44:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 6636)	Multi-Source Evid...
2...	.youtube.com	__Secure-3PAPIS...		22/04/2022 21:34:55	14/04/2021 13:36:51	18/04/2024 06:44:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 6639)	Multi-Source Evid...
2...	.youtube.com	VISITOR_INFO1_...		22/04/2022 21:34:55	23/11/2021 15:10:31	19/10/2022 18:05:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 12388)	Multi-Source Evid...
2...	.youtube.com	__Secure-1PAPIS...		22/04/2022 21:34:55	05/01/2022 09:45:22	18/04/2024 06:44:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 6637)	Multi-Source Evid...
2...	.youtube.com	LOGIN_INFO		22/04/2022 21:34:55	04/04/2022 11:32:20	03/04/2024 11:32:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 1431)	Multi-Source Evid...
2...	.youtube.com	YSC		22/04/2022 21:34:55	07/04/2022 18:05:12	1601-01-01 00:00:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 1484)	Multi-Source Evid...
2...	.youtube.com	SID		22/04/2022 21:34:55	19/04/2022 06:44:04	18/04/2024 06:44:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 6633)	Multi-Source Evid...
2...	.youtube.com	__Secure-1PSID		22/04/2022 21:34:55	19/04/2022 06:44:04	18/04/2024 06:44:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 6638)	Multi-Source Evid...
2...	.youtube.com	__Secure-3PSID		22/04/2022 21:34:55	19/04/2022 06:44:04	18/04/2024 06:44:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 6640)	Multi-Source Evid...
2...	.youtube.com	PREF		22/04/2022 21:34:55	20/04/2022 10:38:43	21/04/2024 18:05:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 12386)	Multi-Source Evid...
2...	.youtube.com	SIDCC		22/04/2022 21:35:44	22/04/2022 21:35:44	22/04/2023 21:35:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 13255)	Multi-Source Evid...
2...	.youtube.com	__Secure-3PSID...		22/04/2022 21:35:44	22/04/2022 21:35:44	22/04/2023 21:35:...	/	\\RICHARDS-MB...	Table: cookies(rowid: 13257)	Multi-Source Evid...

Go To Page: Showing results 1 - 24 of 24

Details Hex Text

Host	.youtube.com
Name	__Secure-3PSID
Value	(not found)
Accessed Date/Time - (UTC) (dd/MM/yyyy)	22/04/2022 21:34:55
Created Date/Time - (UTC) (dd/MM/yyyy)	19/04/2022 06:44:04
Expiration Date/Time - (UTC) (dd/MM/yyyy)	18/04/2024 06:44:04
Path	/
Source	\\RICHARDS-MBP\richarddrinkwater (User Selected) - [ROOT]\Library\Application Support\Google\Chrome\Profile 1\Cookies
Located At	Table: cookies(rowid: 6640)
Evidence Number	Multi-Source Evidence 1

Timeline



Forensic Equity
Safe in the knowledge

Q&A

Case Study 2 – IIoC

Case Study 2 – IIoC

Forensic Equity
Safe in the knowledge

Your client is charged with possession of indecent material, and the defendant's instructions are that he was hacked and that the images located on his computer were not due to his actions.

Counsel also wants the categorisation of the images checked.

Disclosure Request

Forensic Equity
Safe in the knowledge

1. Forensic Images of the entire hard drive or storage of all media where evidence was found (copied in line with ACPO guidelines).

We obtain a complete bit for bit copy of all media subject of the prosecution case which allows us to comply with defendant's instructions.

For example, a defendant may instruct they were hacked, only a full complete bit for bit copy would allow us to properly investigate this.

Disclosure Request

Forensic Equity
Safe in the knowledge

2. A copy of the case files produced by any forensic tool used by the police examiner or other police staff. This includes, for example, Encase case files, X-Ways case files, Axiom case files and Internet Evidence Finder case files (the fully processed IEF case). [In cases where Axiom has been used we would ask for a copy of the Axiom Case in Portable Case format].

These case files often contain bookmarks to the evidence, images and videos relied upon in the prosecution case and referred to in their SFDRs and MG11s. The Police are generally very reluctant to disclose these case files and would prefer a defence examiner spend their time *rediscovering* their evidence as opposed to locating information that may help the defendant. By reviewing case files we can also find that the police knew about certain aspects to the case that they had not illuminated in their evidence e.g. defendant accessing IIoC when their intention was to access hard core adult pornography or clear evidence that the examined computer had been used by someone other than the defendant.

Disclosure Request

Forensic Equity
Safe in the knowledge

3. A copy of ALL exhibits (e.g. html report stored on CD) referred to within witness statements or reports or SFDRs produced by the prosecution analyst or any other officer or analyst involved.

We are generally instructed to scrutinise the prosecution evidence along with other requirements. We are of the view that we cannot do this adequately unless we actually review all exhibits. Surprisingly, the police are often reluctant to disclose the exhibits the prosecution case relies upon.

Disclosure Request

Forensic Equity
Safe in the knowledge

4. A copy of any other reports relied on such as an IEF (Internet Evidence Finder) or Axiom Report.

In many cases a police forensic examiner has used forensic software such as IEF or Axiom to retrieve a myriad of technical artifacts from an examined computer. Bizarrely in my view, rather than assess the recovered material they simply use IEF or Axiom to create a report and give it to a nontechnical officer such as the OIC to review. We then see references to the report's contents in Case Summaries, Records of Interviews and the OIC's MG11 but on occasions, possibly due to the reviewing officers lack of technical training, the relevance of artifacts can be misrepresented.

Axiom's documentation contains a 1,716-page pdf listing recoverable artifact:
https://www.magnetforensics.com/docs/artifacts/html-axiom/Content/Resources/PDFs/Artifact%20Reference.pdf

We believe that any mentions made of report contents by OICs should be properly cross referenced.

Disclosure Request

Forensic Equity
Safe in the knowledge

5. If Griffeye was used to grade the indecent images, we require an export of the graded case (illegal files only) in Project VIC (JSON) format including the illegal files.

In most IIoC cases the Police use Griffeye software to locate and categorise the indecent images. The counts of images alluded to within indictments are likely to have been sourced from a Griffeye case. If Count 1 specifies 50 Category A images, we check that 50 Category A images can be located upon the defendant's media. Obtaining information from the Police Griffeye case is the most expeditious way for us to locate the images relied upon. It also allows a quick assessment of duplication which is a recurring problem in this arena.

Disclosure Request

Forensic Equity
Safe in the knowledge

6. A schedule in a spreadsheet (CSV or XLSX) of all images and movies specified within the indictment. So, for example, if Count 1 upon the relevant indictment specifies that our client made 50 indecent images of children, we wish to know the path, filename and hash value of all 50 images and a file offset for images within a container file (e.g., thumbs cache, volume shadow copy). If images or movies have been recovered from unallocated clusters, we need the Physical Sector number (not a file offset) where the start of the recovered file can be located. If the examiner responding to our request was not involved in the preparing of charges or the indictment, please liaise with the officers that were in order to fulfil this request.

Reconciling the number of images specified upon an indictment with those we can locate upon the defendant's media can be difficult, particularly when the police won't tell you where they are!

Disclosure Request

Forensic Equity
Safe in the knowledge

7. Anything else the examiner thinks appropriate.

Lack of Police disclosure is a constant problem. Often the Police view is that the defence should repeat the Prosecution processes and examinations despite the fact that it would not be funded. They regularly refuse to disclose any of their created material beyond a forensic image, in those cases I wonder if they appreciate that this question is asked slightly tongue-in-cheek.

Quantity and Categorisation

Forensic Equity
Safe in the knowledge

- As alluded to in our disclosure requests locating and reviewing all images and videos specified within the indictment is a key task undertaken in most cases.
- We have observed that the police often double or treble count making no allowances for visual duplicates or the same recovered deleted file that has been identified by overlapping forensic data recovery processes.
- Categorisation can be an issue in some cases where photographs of young adults have been assessed by the police as children or the level of indecency has been exaggerated.

Quantity and Categorisation

Forensic Equity
Safe in the knowledge

- Initial identification of IIoC is normally achieved via hash analysis.
- Hashes are the output of a hashing algorithm like MD5 (Message Digest 5) or SHA (Secure Hash Algorithm). These algorithms essentially aim to produce a unique, fixed-length string – the hash value, or "message digest" – for any given piece of data or "message". As every file on a computer is, ultimately, just data that can be represented in binary form, a hashing algorithm can take that data and run a complex calculation on it and output a fixed-length string as the result of the calculation. The result is the file's hash value or message digest.
- In IIoC cases the police usually provide a schedule of the images subject of the indictment which includes the images hash value. Using Forensic Software, we can load the Forensic Image supplied and calculate a hash value for every file stored therein. These hash values are compared with the schedule allowing identification of IIoC.

Quantity and Categorisation

Forensic Equity
Safe in the knowledge

Name	Path	Description	MD5	Hash set	Report tab
-6985825886392782866.0 ★	\data\com.sec.android.gallery3d\cache\micro	existing	7299817DAD955E755CEFA9D0E6DA6D90	05 DF 1262 20 - Extreme	Count 5 [Me]
-213693297484649607.0 ★	\data\com.sec.android.gallery3d\cache\micro	existing	DC1BC3A58D3C1A4F32BAA1669FA485B2	05 DF 1262 20 - Extreme	Count 5 [Me]
-1937472085725855200.0 ★	\data\com.sec.android.gallery3d\cache\micro	existing	176F9E5AE8E344CB77E8F3E37CB9EECE	05 DF 1262 20 - Extreme	Count 5 [Me]
6134564584926812091.0 ★	\data\com.sec.android.gallery3d\cache\micro	existing	4A84ED6FA665322C288BAE9873614ED7	05 DF 1262 20 - Extreme	Count 5 [Me]
dfd9936e8c41a1de5899361943629989805cloud ★	\media\0\youcut\.diskCache	existing, already viewed	CF8602CCE4B041D2A1DEA3C9856D023D	05 DF 1262 20 - Extreme	Count 5 [Me]
ab7612dc8772c7af2633528574805622038cloud ★	\media\0\youcut\.diskCache	existing, already viewed	5925C61AC527418BBC4CBF7B08354329	05 DF 1262 20 - Extreme	Count 5 [Me]
858466ed7a23c50e5264737130486711769cloud ★	\media\0\youcut\.diskCache	existing, already viewed	97B7FF15FDA7D6566B4AEA5352004F68	05 DF 1262 20 - Extreme	Count 5 [Me]
3f8d8e41ba78e88279986971317239257 58cloud ★	\media\0\youcut\.diskCache	existing, already viewed	4966942080A8D08802779EFB664D0823	05 DF 1262 20 - Extreme	Count 5 [Me]
75a861e7aab6d3dd15103728466725536 68cloud ★	\media\0\youcut\.diskCache	existing, already viewed	C56C0812D2A5F4EFC7DEB37F30716758	05 DF 1262 20 - SC Cat A	Count 1 [Me]
38dc6b1368fc3a1088847498965158160 9cloud ★	\media\0\youcut\.diskCache	existing, already viewed	24497034A999E3A62372B15159165A4B	05 DF 1262 20 - SC Cat A	Count 1 [Me]
0dd2345ac1474aa4918860663954692932 0cloud ★	\media\0\youcut\.diskCache	existing, already viewed	8D8E2FAB528D703A7764D619C9895B20	05 DF 1262 20 - SC Cat A	Count 1 [Me]
24b78ab7e30ad78236249663325687201 40cloud ★	\media\0\youcut\.diskCache	existing, already viewed	6ADAC7FAF2677F50E73811D89211DDA7	05 DF 1262 20 - SC Cat A	Count 1 [Me]
b2f40883e413742480076947946957247 41cloud ★	\media\0\youcut\.diskCache	existing, already viewed	B441FE31B172D06563A0FB352794D25C	05 DF 1262 20 - SC Cat A	Count 1 [Me]
24b78ab7e30ad7825954633279651533512cloud ★	\media\0\youcut\.diskCache	existing	6ADAC7FAF2677F50E73811D89211DDA7	05 DF 1262 20 - SC Cat A	
b2f40883e413742410348273739653914 86cloud ★	\media\0\youcut\.diskCache	existing	B441FE31B172D06563A0FB352794D25C	05 DF 1262 20 - SC Cat A	
fabcdc07dc7fad3770714130319495879 54cloud ★	\media\0\youcut\.diskCache	existing, already viewed	3320BF4233952C838D48A5360D5DAB42	05 DF 1262 20 - SC Cat A	Count 1 [Me]
3b93b68858761bb2685913502327244759 7cloud ★	\media\0\youcut\.diskCache	existing, already viewed	8060A0F1E4D3F527A6A0F726693D8F14	05 DF 1262 20 - SC Cat A	Count 1 [Me]
f70c8361f2060267419896389816514351 2cloud ★	\media\0\youcut\.diskCache	existing, already viewed	275D034E8820EA4A6A7FC7350F81BA8A	05 DF 1262 20 - SC Cat A	Count 1 [Me]
38dc6b1368fc3a1027136036201785977 47cloud ★	\media\0\youcut\.diskCache	existing, already viewed	24497034A999E3A62372B15159165A4B	05 DF 1262 20 - SC Cat A	
6424018697964091697.0 ★	\data\com.sec.android.gallery3d\cache\micro	existing, already viewed	47478A90CE35C602F79A7D11F505BDF1	05 DF 1262 20 - SC Cat B	Count 2 [Me]
8545387210997735788.0 ★	\data\com.sec.android.gallery3d\cache\micro	existing, already viewed	4248F073E0E968E2B9C3676C0BE1BF0B	05 DF 1262 20 - SC Cat B	Count 2 [Me]
1397690669028903206.0 ★	\data\com.sec.android.gallery3d\cache\large	existing	47478A90CE35C602F79A7D11F505BDF1	05 DF 1262 20 - SC Cat B	
4383263434602107259.0 ★	\data\com.sec.android.gallery3d\cache\large	existing	4248F073E0E968E2B9C3676C0BE1BF0B	05 DF 1262 20 - SC Cat B	
461727806182fdf0496329244687901 5913cloud ★	\media\0\youcut\.diskCache	existing	E4052CEBD7EA5E2CE744912F7CD9C26A	05 DF 1262 20 - SC Cat B	Count 2 [Me]
b9cb608021ea5b7262193563983437567 48cloud ★	\media\0\youcut\.diskCache	existing	69D157AA54A6EC5440AEA9351D20062E	05 DF 1262 20 - SC Cat B	Count 2 [Me]
b9cb608021ea5b7263946217283612507 66cloud ★	\media\0\youcut\.diskCache	existing	69D157AA54A6EC5440AEA9351D20062E	05 DF 1262 20 - SC Cat B	
461727806182fdf0457047202167161934 7cloud ★	\media\0\youcut\.diskCache	existing	E4052CEBD7EA5E2CE744912F7CD9C26A	05 DF 1262 20 - SC Cat B	
3a37067590459c4e4380693644011198701cloud ★	\media\0\youcut\.diskCache	existing	4533A1002E9324BC945F83E342A22093	05 DF 1262 20 - SC Cat B	Count 2 [Me]
7e968c643128260e7898415840749798378cloud ★	\media\0\youcut\.diskCache	existing	19F63A1A006B6312EC55EC37A365C25A	05 DF 1262 20 - SC Cat B	Count 2 [Me]
7e968c643128260e5620846756636126913cloud ★	\media\0\youcut\.diskCache	existing	19F63A1A006B6312EC55EC37A365C25A	05 DF 1262 20 - SC Cat B	
2787972d5e10d6d7248620734035735366 0cloud ★	\media\0\youcut\.diskCache	existing	2E5A1EBC79670762727AE48DA3836D17	05 DF 1262 20 - SC Cat B	Count 2 [Me]
0c60573e25a4cdc0861205756015396870 5cloud ★	\media\0\youcut\.diskCache	existing, already viewed	A165D92D52A044623B16F205FFD95C90	05 DF 1262 20 - SC Cat B	Animated GIF
70e8af7a296b89be1032916794625765136cloud ★	\media\0\youcut\.diskCache	existing, already viewed	155371F955BB2B51D7CB33A7FCE2C55A	05 DF 1262 20 - SC Cat C	Count 3 [Me]

Quantity and Categorisation

Forensic Equity
Safe in the knowledge

- Generally, the initial hash analysis fails to locate all the IIoC subject of the indictment.
- In the main this is because the missing images are deleted images recovered from unallocated clusters.
- A cluster is a portion of hard disk drive space used to store files. Unallocated clusters are areas of the hard drive currently unused by the file system and, therefore, not allocated to store files, as opposed to allocated clusters, which are being used to store live files.
- Forensic data recovery software use a number of different processes to recover deleted files from unallocated clusters (a process known as file carving). Most software tools successfully identify the start of a deleted file (via something known as its file header) but many tools can not accurately establish the precise end of a file which results in hash values not matching. This is why we seek such detailed disclosure.
- The alternative would be to manually *carve* out deleted files by locating the file header within a scheduled Physical Sector, carving out the scheduled number of bytes then hashing and comparing the carved file – a very time-consuming process when hundreds of files are involved.

Hacking

Forensic Equity
Safe in the knowledge

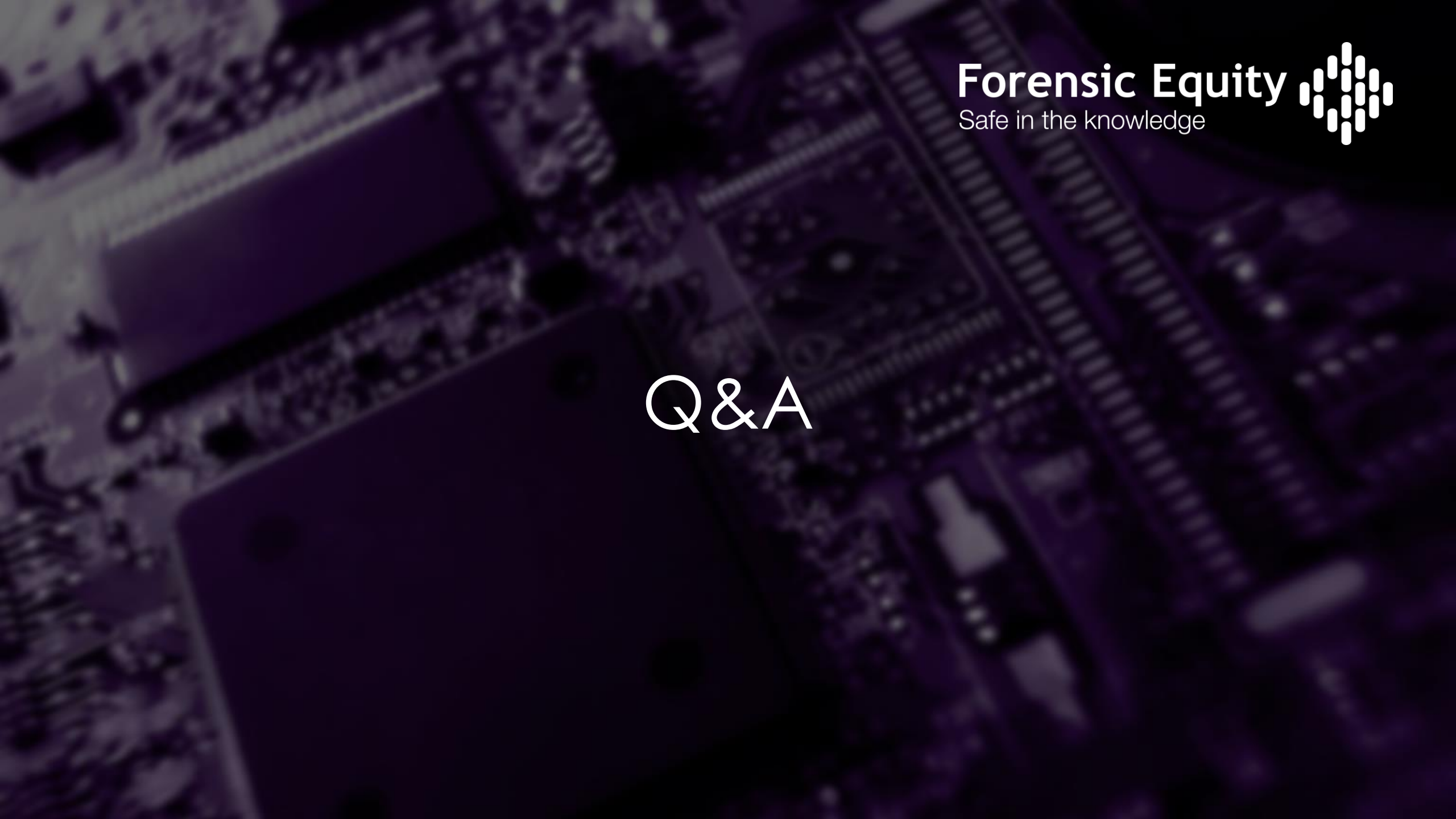
- The possibility of a home-based PC being the subject of a targeted attack is probably quite low.
- It is a reasonable premise that for a computer to have acquired IIoC via the actions of a hacker it is likely to have been targeted.
- More common, are malware attacks with a financial motive such as spyware, spam bots and so on. This type of malware can be acquired by drive by malware attacks, opening malformed files, downloading and executing pirated software.
- For a hacker to create IIoC on a computer they must have control of it and be able to access it remotely. An important part of any hacking investigation is to establish if the target was compromised with malware that would facilitate remote access. Specialist tools such as FireEye Redline, Netstat and Sysinternals Autoruns can be utilised along with virtualisation to investigate this. Standard AV tools are also useful.

Hacking

Forensic Equity
Safe in the knowledge

Other considerations where hacking is alleged:

- Has the IIoC been created by utilising the computer's graphical user interface (thumbcache images)?
- Is the IIoC stored on removable media (e.g. USB stick)?
- Is there evidence of the defendant's interaction with the computer at the time IIoC was created (e.g. logging in an checking webmail, signing into the government gateway etc etc)?
- Is there a clear timeline of events leading to the IIoC creation (e.g. Google Search leading to website visit causing cached IIoC)?
- Is the computer protected with AV, Firewalls and Anti Malware?



Forensic Equity
Safe in the knowledge

Q&A