COURT PACK · SAMPLE

Case 2026/CY/1142

An example of the evidence bundle Invar prepares at the end of a case. Every value in it is example data, made up for this sample. No real case, agency, person, channel or file is shown.

Agency	**Example Cyber Unit (example)**
Case reference	2026/CY/1142
Case type	**Online investment fraud: a public channel, its landing page and deposit page**
Product used	**Invar Research**
Officer	**Officer 2207**
Supervisor	**Officer 1180**
Captured	**14 October 2026, 21:02 to 21:22 IST (UTC+05:30)**
Reviewed	**15 and 30 October 2026**
Pack assembled	**2 November 2026, 10:06 IST**
Items	**12 files: 10 captured, 2 exported at assembly. Each has a SHA-256 hash value and an RFC 3161 timestamp**

Contents

Hash manifest	2
RFC 3161 timestamps	3
Chain of custody	4
Section 63 BSA certificate, Part A (unsigned)	5
Section 63 BSA certificate, Part B (unsigned)	6
How to verify these hashes	7

The certificate is prepared for the officer and the expert to sign. Invar never signs.

Invar shows how each item was captured and that it has not changed since. Courts decide admissibility.

This is a sample. It is not evidence, and the files it lists are not supplied with it.

SAMPLE: example data

PAGE 2 · EVERY ITEM

Hash manifest

Every file in the pack, with its size, its source and the SHA-256 hash value Invar calculated when it was made. Items 001 to 010 were captured on 14 October 2026; items 011 and 012 were exported when the pack was assembled on 2 November 2026. Times are IST (UTC+05:30), dates are day/month.

NO.	FILE AND SOURCE	TYPE	BYTES	HASHED	SHA-256
001	001-channel-overview.warc.gz public-channel.example	WARC	1,284,331	14/10 21:02:19	db6431ad87b2d6dbf38b6ab6a7a45e41 34a3a7c56a8731932c88b60837a3ac67
002	002-post-2081.warc.gz public-channel.example/2081	WARC	412,908	14/10 21:03:40	881d491e5669610244c1a94ecb9ad584 851c6edabe1fbdd35fe6bcd4ac09156e
003	003-post-2081-image.jpg public-channel.example/2081	JPEG	248,117	14/10 21:03:52	785a5c610d48c87ca9ff5b85928f9f8b 44d0d65d8397fcd1d4e04e56b26f9197
004	004-post-2094-video.mp4 public-channel.example/2094	MP4	18,904,226	14/10 21:05:12	f900fe9cda17bdbe0e0700c208831035 3bd593d1c4d1c26045a1bed0153bb44a
005	005-post-2102.warc.gz public-channel.example/2102	WARC	388,640	14/10 21:07:03	bdba3035855b1726fab30ab5a4993b17 72bec93b621f831221a7640b6088ea6f
006	006-landing-page.warc.gz example-invest.test/join	WARC	2,031,775	14/10 21:11:26	0a29de894cb6d202101201de2c996def b5f074a37873e0e30775d87463c1a874
007	007-landing-page.har example-invest.test/join	HAR	906,412	14/10 21:11:27	efbe3636de1230361c16b403b6ca7c9d 0753d4a7e896e2b78328680d485af12c
008	008-deposit-page.warc.gz example-invest.test/deposit	WARC	744,019	14/10 21:14:48	cb4daae31c164dfe1e871cfee6c42c2b bf416ceb3958f6abaa2f94e408ca8e56
009	009-session-video.mp4 Session R-20261014-0912	MP4	96,518,330	14/10 21:22:05	9982c001c41311bda395c25495d376f3 7d1ab767aab4eeac2bb85e6b7b3e83ac
010	010-officer-notes.txt Officer 2207	Text	3,912	14/10 21:22:06	ec0fb91eaa41eefe7a839b01fe8f3bc9 8cbc33b8cf4d94914c47906eeb30f24a
011	011-audit-log.jsonl Case audit log, exported at assembly	JSON Lines	41,806	02/11 10:06:40	ec559aa8a028b16c2d24d581d8118a4b 79076326087c8cf4f0b9cc08f854ff56
012	012-case-export.jsonld Case record export, made at assembly	CASE/UCO	77,254	02/11 10:06:41	f0349d7cb76208fa76e8e19b56e2af95 47b69cf00708058f49ee9aa464972576

Hash values here are example values. In a real pack each one is the SHA-256 of the file with the same name.

SAMPLE: example data

PAGE 3 · WHEN

RFC 3161 timestamps

For each file, a timestamp authority signed the file's SHA-256 hash value together with the time. The token shows the file existed in that exact form no later than that time, independent of Invar's own clock.

Timestamp authority	**Example Timestamp Authority (example)**
Policy	`2.999.1.1 (an example identifier)`
Hash algorithm	**SHA-256**
Token files	**One .tsr file per item, named after it**

NO.	FILE	TOKEN SERIAL	TIME (GENTIME)	MESSAGE IMPRINT (SHA-256)
001	001-channel-overview.warc.gz	0382100B546934FE	2026-10-14T15:32:20Z 21:02:20 IST	db6431ad87b2d6dbf38b6ab6a7a45e41 34a3a7c56a8731932c88b60837a3ac67
002	002-post-2081.warc.gz	EBF2831389AB4636	2026-10-14T15:33:41Z 21:03:41 IST	881d491e5669610244c1a94ecb9ad584 851c6edabe1fbdd35fe6bcd4ac09156e
003	003-post-2081-image.jpg	00C41C914F76571A	2026-10-14T15:33:53Z 21:03:53 IST	785a5c610d48c87ca9ff5b85928f9f8b 44d0d65d8397fcd1d4e04e56b26f9197
004	004-post-2094-video.mp4	04A98CDAE2A3B333	2026-10-14T15:35:13Z 21:05:13 IST	f900fe9cda17bdbe0e0700c208831035 3bd593d1c4d1c26045a1bed0153bb44a
005	005-post-2102.warc.gz	93AF020615605D8E	2026-10-14T15:37:04Z 21:07:04 IST	bdba3035855b1726fab30ab5a4993b17 72bec93b621f831221a7640b6088ea6f
006	006-landing-page.warc.gz	EC4B2066B761F233	2026-10-14T15:41:27Z 21:11:27 IST	0a29de894cb6d202101201de2c996def b5f074a37873e0e30775d87463c1a874
007	007-landing-page.har	F5BE54F74C20419E	2026-10-14T15:41:28Z 21:11:28 IST	efbe3636de1230361c16b403b6ca7c9d 0753d4a7e896e2b78328680d485af12c
008	008-deposit-page.warc.gz	5785C0CE76873972	2026-10-14T15:44:49Z 21:14:49 IST	cb4daae31c164dfe1e871cfee6c42c2b bf416ceb3958f6abaa2f94e408ca8e56
009	009-session-video.mp4	20ACF8D88AA8E63F	2026-10-14T15:52:06Z 21:22:06 IST	9982c001c41311bda395c25495d376f3 7d1ab767aab4eeac2bb85e6b7b3e83ac
010	010-officer-notes.txt	83566B3C4F94E628	2026-10-14T15:52:07Z 21:22:07 IST	ec0fb91eaa41eefe7a839b01fe8f3bc9 8cbc33b8cf4d94914c47906eeb30f24a
011	011-audit-log.jsonl	DED4694A90D7345B	2026-11-02T04:36:41Z 10:06:41 IST	ec559aa8a028b16c2d24d581d8118a4b 79076326087c8cf4f0b9cc08f854ff56
012	012-case-export.jsonld	D6F6D6DBDB81C9E3	2026-11-02T04:36:42Z 10:06:42 IST	f0349d7cb76208fa76e8e19b56e2af95 47b69cf00708058f49ee9aa464972576

SAMPLE: example data

PAGE 4 · WHO

Chain of custody

Every person who opened, captured, viewed, reviewed or exported an item, and when. Taken from the case audit log as exported with the pack (item 011); its last entry is that export. Times are IST (UTC+05:30).

DATE	TIME	WHO	WHAT	ITEMS
14/10/2026	20:58:30	Officer 1180 (Supervisor)	Research opened for the case; exit policy: India only	–
14/10/2026	21:02:11	Officer 2207	Opened Research session R-20261014-0912 · Exit Mumbai, IN · Tor off	–
14/10/2026	21:02:19	Officer 2207	Captured channel pages and media, hashed and time-stamped	001–005
14/10/2026	21:11:26	Officer 2207	Captured landing and deposit pages, hashed and time-stamped	006–008
14/10/2026	21:22:05	Officer 2207	Closed session · Session destroyed · Video and notes saved, hashed and time-stamped	009–010
15/10/2026	11:40:12	Officer 3115	Viewed items (read-only), no change	001–008
30/10/2026	16:20:37	Officer 1180 (Supervisor)	Reviewed the case record, no change	001–010
02/11/2026	10:05:44	Officer 1180 (Supervisor)	Pack assembled and exported	001–010
02/11/2026	10:06:31	Invar	Recalculated every hash at assembly: all match the values recorded at capture	001–010
02/11/2026	10:06:40	Invar	Exported the audit log and the case record for the pack, hashed and time-stamped	011–012

> No item was changed after capture. When the pack was assembled every hash value was recalculated and matched the value recorded at capture. Items 011 and 012 were made at assembly and sealed then.

SAMPLE: example data

THE SCHEDULE

[See section 63(4)(c)]

CERTIFICATE

PART A

(To be filled by the Party)

I, Inspector A. Sample (Name), Son/daughter/spouse of B. Sample residing/employed at Example Cyber Unit, Example City do hereby solemnly affirm and sincerely state and submit as follows:—

I have produced electronic record/output of the digital record taken from the following device/digital record source (tick mark):—

☐ Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐ CD/DVD ☐ Server ☑ Cloud ☑ Other

Other: Invar Research investigation browser, cloud deployment (example)

Make & Model: Invar Research (example release) Color: Not applicable

Serial Number: Not applicable (cloud service)

IMEI/UIN/UID/MAC/Cloud ID: Tenant EXAMPLE-01 · Session R-20261014-0912 (as applicable)

and any other relevant information, if any, about the device/digital record: items 001–008 are page captures; 009–010 are session records; 011–012 are case records (specify).

The digital device or the digital record source was under the lawful control for regularly creating, storing or processing information for the purposes of carrying out regular activities and during this period, the computer or the communication device was working properly and the relevant information was regularly fed into the computer during the ordinary course of business. If the computer/digital device at any point of time was not working properly or out of operation, then it has not affected the electronic/digital record or its accuracy. The digital device or the source of the digital record is:—

☐ Owned ☐ Maintained ☐ Managed ☑ Operated

by me (select as applicable).

I state that the HASH value/s of the electronic/digital record/s is listed for each file in the enclosed hash manifest (items 001 to 012), obtained through the following algorithm:—

SHA1: _____

SHA256: Yes: see the hash manifest

MD5: _____

Other _____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

NOT SIGNED · SAMPLE

(Name and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____ hours (In 24 hours format)

Place: _____

Laid out as in the Schedule to the Bharatiya Sakshya Adhiniyam, 2023. Example entries are shown in teal. Part A is completed by the party producing the record. The signature, date, time and place are left blank: they are for the person who signs. Invar never signs.

SAMPLE · example data

PART B

(To be filled by the Expert)

I, C. Example, Examiner (Name), Son/daughter/spouse of D. Example residing/employed at Example Digital Forensics Laboratory, Example City do hereby solemnly affirm and sincerely state and submit as follows:—

The produced electronic record/output of the digital record are obtained from the following device/digital record source (tick mark):—

☐ Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐ CD/DVD ☐ Server ☑ Cloud ☑ Other

Other: Invar Research investigation browser, cloud deployment (example)

Make & Model: Invar Research (example release) Color: Not applicable

Serial Number: Not applicable (cloud service)

IMEI/UIN/UID/MAC/Cloud ID: Tenant EXAMPLE-01 · Session R-20261014-0912 (as applicable)

and any other relevant information, if any, about the device/digital record: items 001–008 are page captures; 009–010 are session records; 011–012 are case records (specify).

I state that the HASH value/s of the electronic/digital record/s is listed for each file in the enclosed hash manifest (items 001 to 012), obtained through the following algorithm:—

SHA1: _____

SHA256: Yes: see the hash manifest

MD5: _____

Other _____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

NOT SIGNED · SAMPLE

(Name, designation and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____ hours (In 24 hours format)

Place: _____

Laid out as in the Schedule to the Bharatiya Sakshya Adhiniyam, 2023. Example entries are shown in teal. Part B is completed by an expert, who recalculates the hash values independently. The signature, date, time and place are left blank: they are for the person who signs. Invar never signs.

SAMPLE: example data

PAGE 7 · CHECK IT YOURSELF

How to verify these hashes

Anyone with the files can check them with free tools, without Invar. In a real pack, every file named in the manifest and every .tsr token is supplied with it.

1. **Recalculate each file's SHA-256 hash value.** On macOS or Linux:

   ```
   shasum -a 256 002-post-2081.warc.gz
   ```

   On Windows (PowerShell or Command Prompt):

   ```
   Get-FileHash -Algorithm SHA256 .\002-post-2081.warc.gz
   certutil -hashfile 002-post-2081.warc.gz SHA256
   ```

   Compare the result with the manifest. If one character differs, the file is not the one listed in the manifest.

2. **Check the RFC 3161 timestamp.** With OpenSSL and the timestamp authority's certificate chain:

   ```
   openssl ts -verify -data 002-post-2081.warc.gz -in 002-post-2081.tsr -CAfile tsa-chain.pem
   openssl ts -reply -in 002-post-2081.tsr -text
   ```

   "Verification: OK" means the token was issued for exactly this file. The second command shows the time.

3. **Replay the page archives.** Open each .warc.gz in any WARC replay tool to see the page as it was served. Open the .har network log in a browser's developer tools or a HAR viewer.

4. **Read the chain of custody against the audit log.** Every entry on page 4 appears in item 011 with the same officer, time and items.

5. **Check copies you hand over.** Recalculate the hash of every copy, such as a DVD or a pen drive. Re-saving, converting or re-exporting a file changes its hash value.

> **This sample has no files with it,** so these values cannot be checked against anything. They show the layout of a real pack only.

SAMPLE: example data