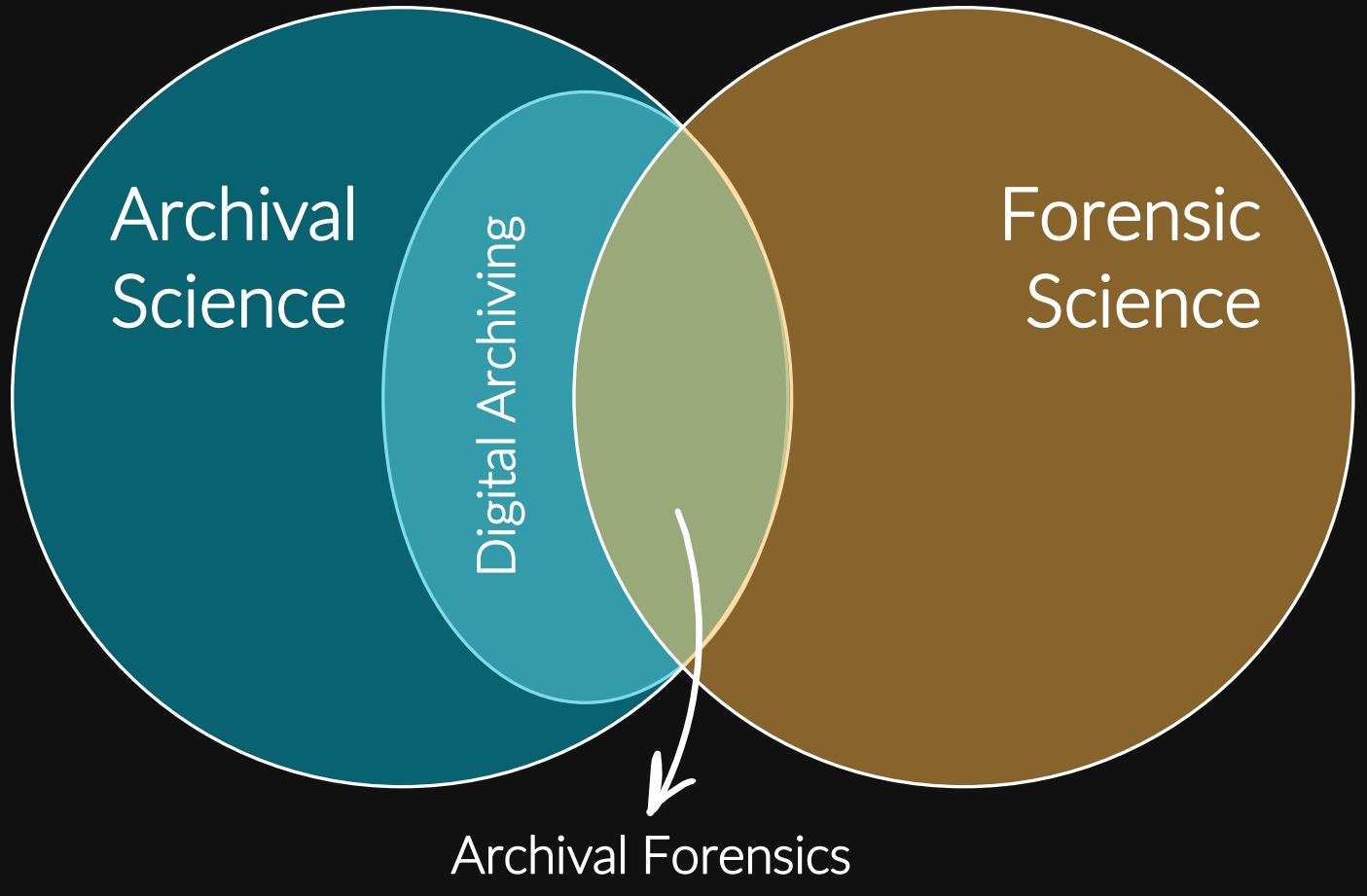

University of Glasgow
ARCHIVAL FORENSICS AT U OF GLASGOW
DIGITAL FORENSICS AND DIGITAL PRESERVATION:
INVESTIGATING GOOD PRACTICE
DPC, FEBRUARY 26TH, 2024
Leo Konstantelos
Archives & Special Collections, University of Glasgow
WORLD CHANGING GLASGOW
THE TIMES THE SUNDAY TIMES
GOOD UNIVERSITY GUIDE 2022
SCOTTISH UNIVERSITY OF THE YEAR

University of Glasgow

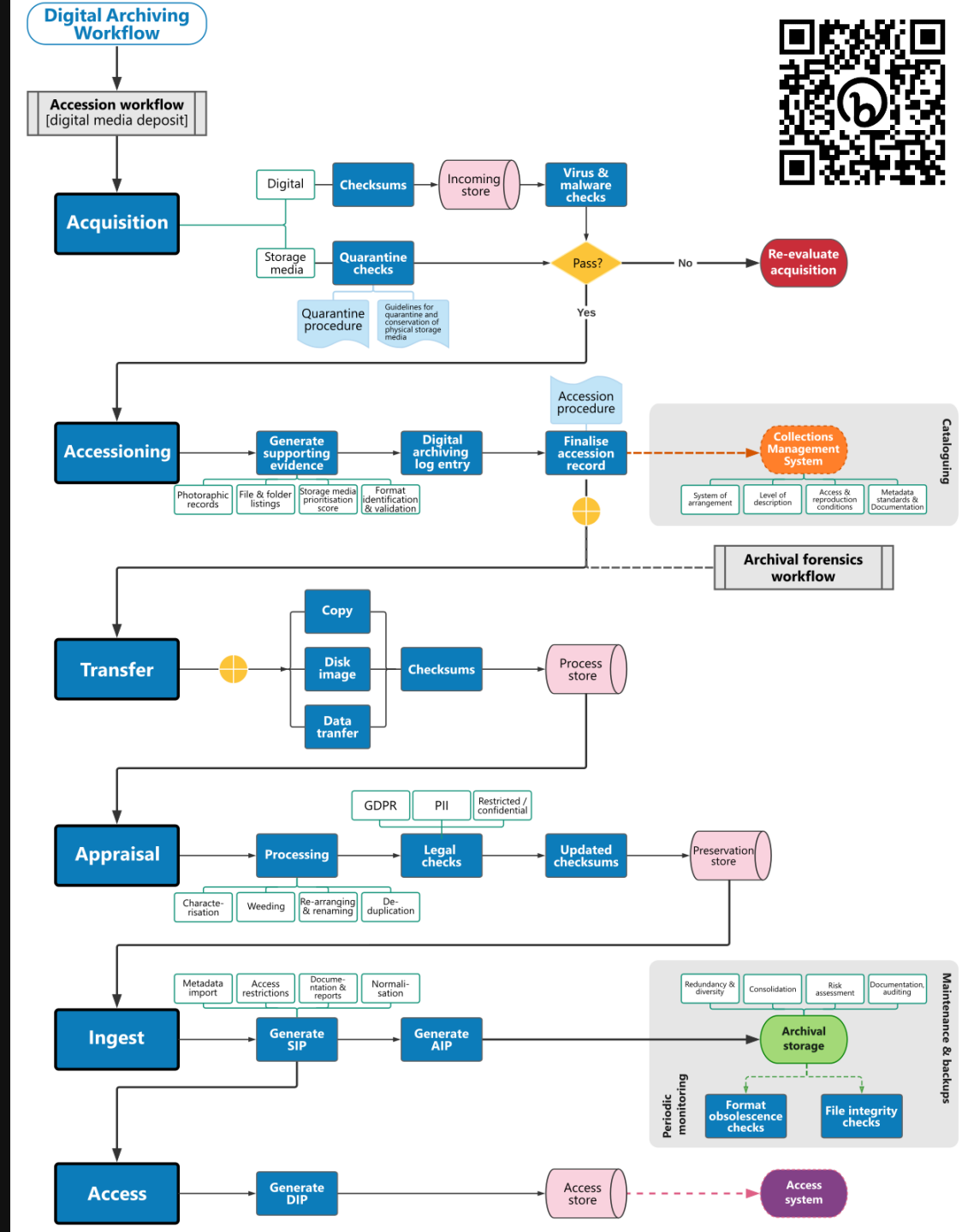
ARCHIVAL FORENSICS

The integration of Forensic Science principles, methods and tools with Archival Science principles, as part of digital archiving methodologies, workflows and practice.



University of Glasgow

Part of the UofG Digital Archiving Workflow



ARCHIVAL FORENSICS WORKFLOW

University of Glasgow

Archives & Special Collections

Use computer forensics technology to examine digital storage media

Create an exact copy of storage media, encapsulating contents and structures in a single file (a disk image)

Data carving, restoring data that was deleted.

Decrypt encrypted files and recovering passwords.

View and exporting geolocation data from files.

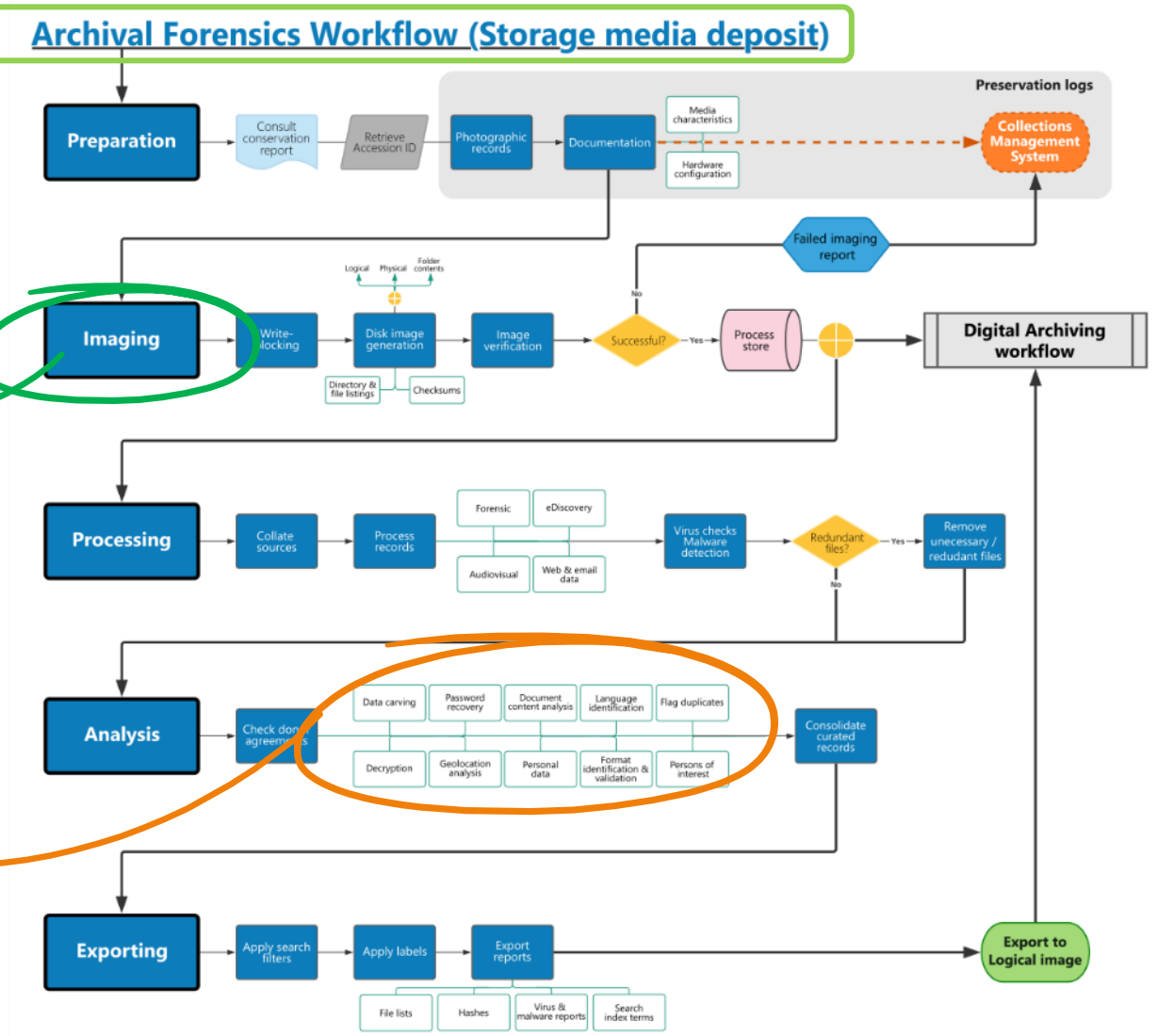
Identify personal information, such as names, phone numbers, credit card and social security numbers.

Identify the language in which documents are written.

Extract metadata from multimedia files.

Flag duplicate files.

Discover information (including documents and email communications) relating to pre-defined lists of persons of interest.



ARCHIVAL FORENSICS LAB:
BUSINESS CASE

Necessity for archival forensics

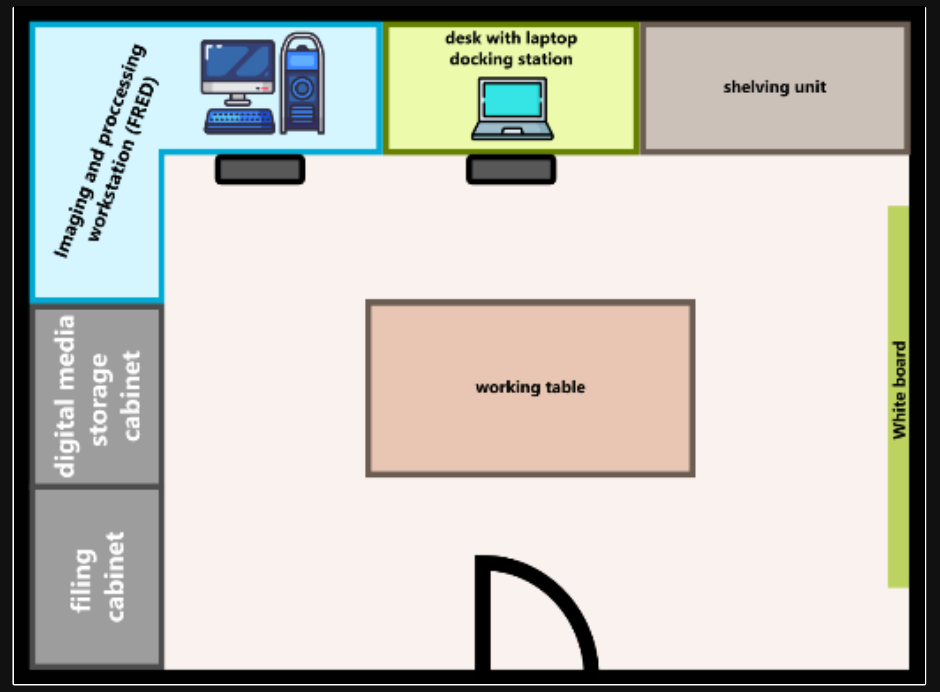
- examine digital media in a forensically sound manner
- capture contextual information
  file creation, versioning, software dependencies, user logs and IPR information
- secure sensitive data
- recover data from damaged, failed, corrupted, or otherwise inaccessible storage media
- appraise digital acquisitions and create collections suitable for preservation and access

Facility features

- Layout
- Premises
- Hardware and software
- Tools and accessories
- Health and safety
- Costs

Sources:

- Interpol Global Guidelines for Digital Forensics Laboratories
- Codes of Practice and Conduct For Forensic Science Providers and Practitioners in the Criminal Justice System



DIGITAL ARCHIVING

END-TO-END CASE STUDY

University of Glasgow

OBJECTIVES

Evidence-based approach to delivering digital preservation and digital archiving services.

Implement an end-to-end digital archiving case study using one of our collections to test workflows, explore benefits of archival forensics.

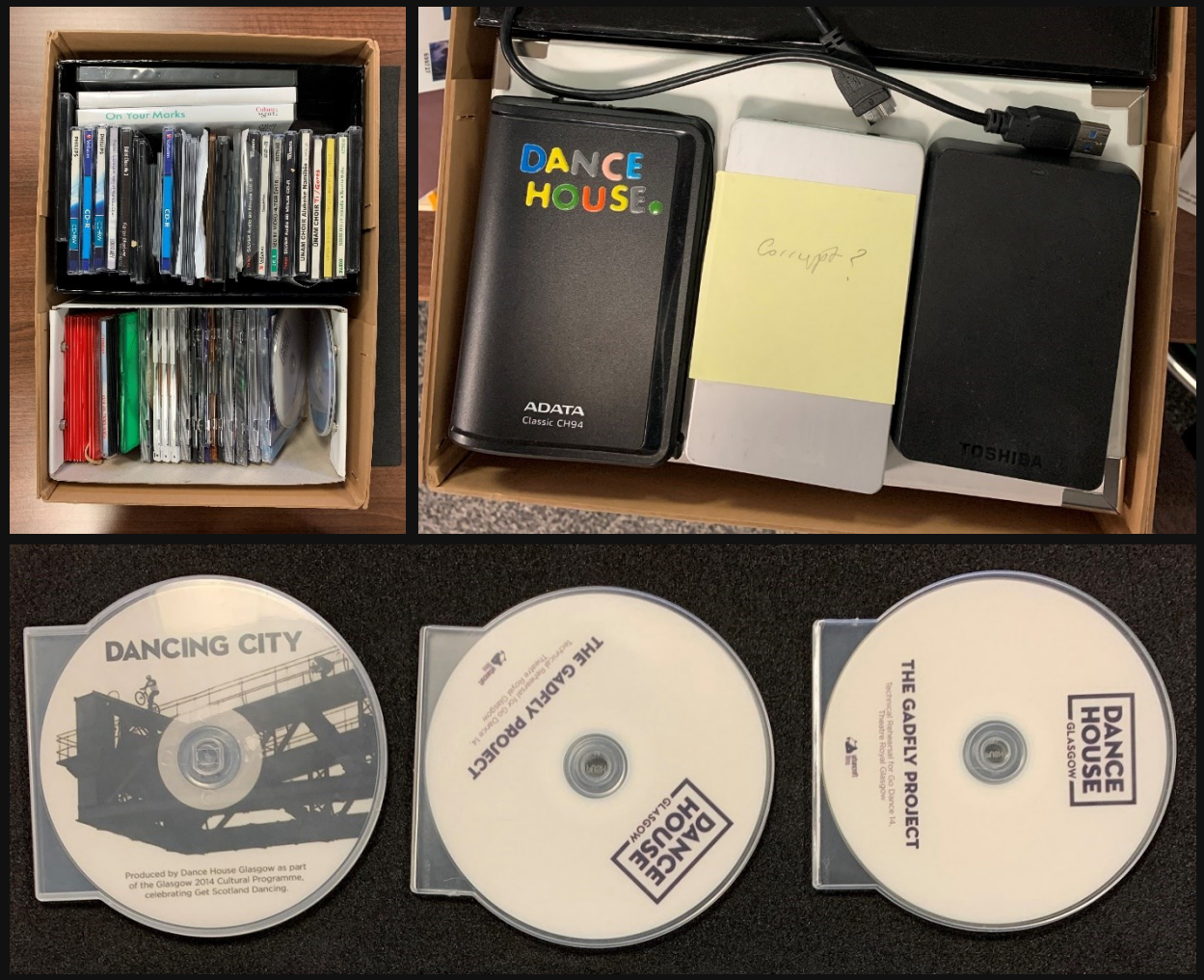
Highlight areas where improvements and further investment are required.

CASE: DANCE HOUSE GLASGOW

Description	Dance House Glasgow was a creative arts organisation involved in supporting the city's professional dance sector and offering community development programmes for over 20 years. In 2018, it lost its Creative Scotland funding and ceased operating.
Variability	The whole collection consists of records relating to Dance House Glasgow dating from c.1990 to 2018. It includes governance, financial, staff and project records, along with photographs, audio and video, press cuttings, and promotional material.
Volume (digital)	6.3TB
Representativeness	Hybrid – both born digital and paper records. Digital records across three HDDs and 90 optical media discs. At least one of the hard drives and some of the CD-ROMs not functioning, as per a survey of the material in 2021.
Legal issues	The records came to UofG ASC via the Business Archives Surveying Officer and were gifted to us in 2019. As a creative arts collection, we expected issues around IPR and rights for the music used in the collection. As a business collection, we expected issues around personal information,

University of Glasgow

CASE: DANCE HOUSE GLASGOW



University of Glasgow

CASE: DANCE HOUSE GLASGOW

CASE STUDY: METHODS & OUTCOMES

Forensic analysis – FTK and BitCurator:

- Data carving
- Decryption and password recovery
- Personal data analysis (Bulk extractor)
- Document content analysis
- Format identification and validation (FTK, Droid, JHOVE)
- Duplicate flagging
- Index search in FTK

Weeding:

- No duplicates
- No deleted files
- No free space / file slack
- No recycle bin items
- No OS / system files
- No executables
- No FTK Known File Filter (KFF) files

Files likely to be illicit (e.g. known contraband, malware) or benign (e.g. temp files) in nature from a legal forensics perspective

University of Glasgow

CASE STUDY: METHODS & OUTCOMES

	Pre-appraisal	Post appraisal	Difference	Decrease
Total volume (GB)	6363	423	-5941	93.4%
Total file size	55936	17954	-37982	68%
Selected file categories				
Archives	1572	48	-1524	97%
Databases	2	1	-1	50%
Documents	1802	219	-1583	88%
Email	2	2	0	0%
Executables	510	0	-510	100%
Graphics	24225	15278	-8947	37%
Internet	35	35	0	0%
Multimedia	1456	979	-477	33%
OS/File system	1081	0	-1081	100%
Presentations	2	2	0	0%
Slack/free space	20512	0	-20512	100%
Spreadsheets	12	11	-1	
Selected file status				
Deleted files	557	0	-557	100%
Duplicate items	14995	3607	-11388	76%
KFF Alert files	37	0	-37	100%
KFF Ignore files	1288	0	-1288	100%
From recycle bin	3060	0	-3060	100%

Total volume reduced by 5.94TB (93.4% decrease)

University of Glasgow

CASE STUDY: METHODS & OUTCOMES

	Pre-appraisal	Post appraisal	Difference	Decrease
Total volume (GB)	6363	423	-5941	93.4%
Total file size	55936	17954	-37982	68%
Selected file categories				
Archives	1572	48	-1524	97%
Databases	2	1	-1	50%
Documents	1802	219	-1583	88%
Email	2	2	0	0%
Executables	510	0	-510	100%
Graphics	24225	15278	-8947	37%
Internet	35	35	0	0%
Multimedia	1456	979	-477	33%
OS/File system	1081	0	-1081	100%
Presentations	2	2	0	0%
Slack/free space	20512	0	-20512	100%
Spreadsheets	12	11	-1	
Selected file status				
Deleted files	557	0	-557	100%
Duplicate items	14995	3607	-11388	76%
KFF Alert files	37	0	-37	100%
KFF Ignore files	1288	0	-1288	100%
From recycle bin	3060	0	-3060	100%

Total volume reduced by 5.94TB (93.4% decrease)

Post-appraisal differences include duplicate, deleted and/or temporary files

University of Glasgow

CASE STUDY: METHODS & OUTCOMES

	Pre-appraisal	Post appraisal	Difference	Decrease
Total volume (GB)	6363	423	-5941	93.4%
Total file size	55936	17954	-37982	68%

Selected file categories

Archives	1572	48	-1524	97%
Databases	2	1	-1	50%
Documents	1802	219	-1583	88%
Email	2	2	0	0%
Executables	510	0	-510	100%
Graphics	24225	15278	-8947	37%
Internet	35	35	0	0%
Multimedia	1456	979	-477	33%
OS/File system	1081	0	-1081	100%
Presentations	2	2	0	0%
Slack/free space	20512	0	-20512	100%
Spreadsheets	12	11	-1	

Selected file status

Deleted files	557	0	-557	100%
Duplicate items	14995	3607	-11388	76%
KFF Alert files	37	0	-37	100%
KFF Ignore files	1288	0	-1288	100%
From recycle bin	3060	0	-3060	100%

Selection and appraisal

Only post-appraisal records retained

↓

Arrangement

Original order - maintain the original folder structure for the exported files. The root location is the disk image of each storage medium included in the FTK case. This means that we can trace files back to the storage medium that they originated.

↓

Submission Documentation

- Pre- and post-appraisal file listings and checksums
- Malware and virus scan reports
- FTK report

  information and metadata about an FTK case – including thumbnails of all or a selection of images; a list of all file paths and all file properties organised by both file type (e.g. documents, databases, graphics) and file extension
- Bulk Extractor results
- DFXML metadata

↓

Digital Preservation

SIP generated with RODA-In → Archivematica

ARCHIVAL FORENSICS:

OPPORTUNITIES & CHALLENGES

ARCHIVAL FORENSICS :
BUSINESS BENEFITS

Dedicated facility

A dedicated space for archival forensic processing with procedures and policy around access – a parallel to the conservation studio.

Policies and procedures

Expand existing policies and procedures to include actions specific to digital materials.

Economies of scale

Ability to process very large volumes of digital information by utilising forensic software capabilities, which would have been otherwise prohibitive.

ARCHIVAL FORENSICS : CHALLENGING ESTABLISHED ARCHIVAL PROCESSES

Dealing with change

Change to established practices can be scary!

Obsolete media & file systems

Modern computer forensics systems are designed to work with contemporary technology. The necessary interfaces to connect legacy hardware are either not present or difficult to acquire and set up without relevant expertise.

Complexity of forensic data

Large and complex disk image files produced by forensic software require relevant expertise. A range of tools is required to access and process these files, while arrangements need to be made for storage and preservation.

CONTACTS

ARCHIVES & SPECIAL COLLECTIONS

Dr. Leo Konstantelos, Senior Assistant Archivist (Digital):

leo.konstantelos@glasgow.ac.uk

@lkonstantelos

Emma Yan, Assistant Archivist (Accessions):

emma.yan@glasgow.ac.uk

@eswyan


University of Glasgow
THANK YOU!
#UofGWorldChangers
@UofGlasgowASC