Cyber&DigitalForensics
21st Century Investigations

INVESTIGATION PACKAGE
BREAK-DOWN

	BRONZE	SILVER	GOLD	GOLD PLUS
Exhibit specifications and details	✓	✓	✓	✓
Exhibit content summary	✓	✓	✓	✓
ADVANCED ANALYSIS				
Hash matches		✓	✓	✓
Keywords matches		✓	✓	✓
RECENT ACTIVITY				
Applications used	7 DAYS	30 DAYS	90 DAYS	ALL
Files used, downloaded and saved	7 DAYS	30 DAYS	90 DAYS	ALL
Unique websites visited	7 DAYS	30 DAYS	90 DAYS	ALL
Search engine searches	7 DAYS	30 DAYS	90 DAYS	ALL
External devices connected	7 DAYS	30 DAYS	90 DAYS	ALL
All usernames and passwords recovered			✓	✓
Password protected containers identified			✓	✓
All contacts listed			✓	✓
Deleted files recovered			✓	✓
Recycle Bin items recovered			✓	✓
RECENT MESSAGES				
Most emailed contact	7 DAYS	30 DAYS	90 DAYS	ALL
Emails sent and received	7 DAYS	30 DAYS	90 DAYS	ALL
WhatsApp messages	7 DAYS	30 DAYS	90 DAYS	ALL
Skype messages	7 DAYS	30 DAYS	90 DAYS	ALL
ADVANCED SOFTWARE/HARDWARE DETAILS				
Hardware	✓	✓	✓	✓
Disk partitions	✓	✓	✓	✓
Network adaptors	✓	✓	✓	✓
Network connections	✓	✓	✓	✓
Application-file associations	✓	✓	✓	✓
Installed programs	✓	✓	✓	✓
OS information	✓	✓	✓	✓
OS users	✓	✓	✓	✓

ADDITIONAL DETAILS

+ FORENSIC IMAGING

Imaging is the process of taking a like-for-like copy (including both live and deleted files) of a hard drive, SSD, USB or other storage media. It allows the investigator to obtain and examine digital data without effecting the devices evidential integrity. Cyber & Digital Forensics produce and verify this image using the Detego® Unified Forensics Platform, an industry-leading digital forensics tool.

+ HASH MATCHES

Every digital file (document, picture, audio, video etc.) has a unique combination of numbers and letters assigned to it called a HASH. Similar to a fingerprint, it's incredibly unlikely that two files containing different content would ever generate the same HASH. When a file is transferred from one device to another its 'fingerprint' goes with it and can be found on both the sending and receiving devices.

Cyber & Digital Forensics are able to search hundreds of thousands of files in minutes using HASH searching, rapidly identifying any files that you are particularly interested in, even if they are hidden or deleted.

+ KEYWORD MATCHES

An examination technique used to identify relevant evidence on a digital device by searching the acquired content using a pre-determined list of keywords imported into the forensic tool, even if the word or phrase occurs in an unallocated space or deleted file.

+ RECOVERY OF DELETED DATA

Deletion doesn't destroy a file, it continues to exist on your hard drive even after you empty it from your Recycle Bin. These files are recovered by conducting file carving, a process that scans the raw bytes of a disk drive and reassembles them. However, a deleted file becomes unrecoverable if it's overwritten by the operating system deciding to use the space to store another file.

SPEAK TO AN EXPERT

T: (0)333 358 3680

E: support@cyberdigitalforensics.com