



Micro-Credentials

Version - DRAFT - WORK IN PROGRESS

Date - 2026.03.06

Editor - ECTEG (European Cybercrime Training and Education Group)

Author(s) - ECTEG - experts

Copyright - ECTEG - 2026 - Funded by the European Commission

Table of contents

1. Objectives of Micro-Credentials	7
2. Properties of Micro-Credentials	9
3. ECTEG's Approach on Micro-Credentials	10
4. Evaluation	12
5. Micro-Credentials Packages	14
5.1. Digital Forensic Examiner MC Package	14
5.1.1. Generic Knowledge and Skills (DFI)	16
5.1.1.1. 0101 - Electronic Evidence Admissibility	16
5.1.1.2. 0102 - Reporting	17
5.1.1.3. 0103 - Computer Data	18
5.1.1.4. 0104 - Forensic Copy	20
5.1.1.5. 0105 - Hashing (L1)	21
5.1.1.6. 0106 - Mounting	22
5.1.1.7. 0111 - String Encoding	23
5.1.1.8. 0112 - Date Time Stamps	24
5.1.2. File Level (DFI)	25
5.1.2.1. 0201 - File Embedded Metadata	25
5.1.2.2. 0202 - Carving (L1)	26
5.1.2.3. 0203 - Regular Expressions (L1)	27
5.1.2.4. 0204 - CSV Parsing	29
5.1.2.5. 0205 - JSON Parsing	30
5.1.2.6. 0207 - Database Fundamentals	32
5.1.2.7. 0211 - Browser History Forensics	33
5.1.3. Windows Specifics (DFI)	35
5.1.3.1. 0301 - exFAT	35
5.1.3.2. 0302 - NTFS (L1)	36
5.1.3.3. 0303 - Windows Recycle Bin	37
5.1.3.4. 0304 - Windows Event Logs	38
5.1.3.5. 0305 - Windows Prefetch	39
5.1.3.6. 0306 - Windows Registry Analysis	40
5.1.4. Forensic Environments (DFI)	42
5.1.4.1. 9901 - Linux Command Line Interface	42
5.1.4.2. 9902 - Hexadecimal Viewer	43
5.1.4.3. 9903 - GUI Forensic Software	44
5.2. Computer Networks MC Package	45
5.3. Lawful Decryption MC Package	46
6. Annexes	47
6.1. Micro-Credentials Full List	47
6.1.1. 0101 - Electronic Evidence Admissibility	47
6.1.2. 0102 - Reporting	48

6.1.3. 0103 - Computer Data	49
6.1.4. 0104 - Forensic Copy	51
6.1.5. 0105 - Hashing (L1)	52
6.1.6. 0106 - Mounting	53
6.1.7. 0111 - String Encoding	54
6.1.8. 0112 - Date Time Stamps	55
6.1.9. 0115 - Computer Memory	56
6.1.10. 0116 - Encoding	57
6.1.11. 0117 - Virtual Machines	58
6.1.12. 0201 - File Embedded Metadata	59
6.1.13. 0202 - Carving (L1)	61
6.1.14. 02A02 - Carving (L2)	62
6.1.15. 0203 - Regular Expressions (L1)	63
6.1.16. 0204 - CSV Parsing	64
6.1.17. 0205 - JSON Parsing	66
6.1.18. 0206 - XML Parsing	67
6.1.19. 0207 - Database Fundamentals	68
6.1.20. 0211 - Browser History Forensics	70
6.1.21. 0301 - exFAT	71
6.1.22. 0302 - NTFS (L1)	72
6.1.23. 03A02 - NTFS (L2)	74
6.1.24. 0303 - Windows Recycle Bin	75
6.1.25. 0304 - Windows Event Logs	76
6.1.26. 0305 - Windows Prefetch	77
6.1.27. 0306 - Windows Registry Analysis	78
6.1.28. 0307 - Windows Process Analysis (L1)	79
6.1.29. 0308 - Windows Command Line and PowerShell	81
6.1.30. 0309 - Windows Portable Executable Analysis	82
6.1.31. 0310 - Windows Critical Directories	83
6.1.32. 0311 - Windows History	85
6.1.33. 0312 - Windows Office Documents Analysis	86
6.1.34. 0313 - Windows Shadow Copies	88
6.1.35. 0314 - Windows Services	89
6.1.36. 0315 - Windows Security Model	90
6.1.37. 0316 - Windows Credentials Protection	92
6.1.38. 0317 - Windows Bootchain Startup	93
6.1.39. 0318 - Windows Virtualisation Subsystems	94
6.1.40. 0319 - Windows Memory Structure And Management	96
6.1.41. 0320 - Windows Memory Analysis	97
6.1.42. 0321 - Windows Memory Acquisition Techniques	98
6.1.43. 0401 - Cryptography Basics (L1)	99
6.1.44. 0402 - Use of Masks	100
6.1.45. 0403 - Wordlists	101
6.1.46. 0404 - Rules	102
6.1.47. 0405 - Hash Extraction	103
6.1.48. 0407 - Password Analysis	104

6.1.49.	0408 - Preprocessing	105
6.1.50.	0410 - Decryption Strategy	106
6.1.51.	0411 - Decryption Hardware Strategy	107
6.1.52.	0412 - Decryption Performance Limits	108
6.1.53.	0413 - Decentralised Decryption	109
6.1.54.	0501 - Network Fundamentals	111
6.1.55.	0502 - Network Hardware	111
6.1.56.	0503 - Network Models	112
6.1.57.	0504 - Network Protocols	113
6.1.58.	0601 - Linux Memory Structure And Management	114
6.1.59.	0602 - Linux Memory Acquisition Techniques	115
6.1.60.	0603 - Linux Memory Analysis	117
6.1.61.	0701 - macOS Architecture	118
6.1.62.	0702 - macOS GUI and Boot Options	119
6.1.63.	0703 - macOS as a Forensic Lab	120
6.1.64.	0704 - macOS Mount Images	121
6.1.65.	0705 - macOS APFS	122
6.1.66.	0706 - macOS Acquisition	123
6.1.67.	0707 - macOS File Types	124
6.1.68.	0708 - macOS Disk Images	126
6.1.69.	0709 - macOS User Accounts	127
6.1.70.	0710 - macOS Artifacts Keychain	128
6.1.71.	0711 - macOS Artifacts Browser	129
6.1.72.	0712 - macOS Artifacts Communication	130
6.1.73.	0713 - macOS Artifacts Recently Used	131
6.1.74.	0714 - macOS Artifacts Deleted Files	132
6.1.75.	0715 - macOS Artifacts Snapshots	133
6.1.76.	0716 - macOS Extended Attributes and Spotlight	134
6.1.77.	0717 - macOS Log Files	136
6.1.78.	0718 - macOS Network Connections	137
6.1.79.	0719 - macOS iOS Backups	138
6.1.80.	0720 - macOS iOS iCloud	139
6.1.81.	0721 - macOS App Activities and Device State	140
6.1.82.	0801 - Memory Acquisition (L1)	142
6.1.83.	0802 - Memory Acquisition (L2)	143
6.1.84.	0803 - Memory Analysis and Reporting	144
6.1.85.	0901 - Windows Malware Analysis Foundations and Lab Safety	145
6.1.86.	0902 - Windows Static Malware Analysis	147
6.1.87.	0903 - Windows Dynamic Malware Analysis	148
6.1.88.	1101 - Computer Architecture	150
6.1.89.	1102 - Disk Interface	151
6.1.90.	1103 - Deletion Mechanism	152
6.1.91.	1104 - Bios Access	153
6.1.92.	1105 - Bios Type	154
6.1.93.	1106 - Bios Virtualisation	155
6.1.94.	1107 - TPM Chip	156

6.1.95. 1108 - Memory Management Fundamentals	157
6.1.96. 9901 - Linux Command Line Interface	158
6.1.97. 9902 - Hexadecimal Viewer	159
6.1.98. 9903 - GUI Forensic Software	160
6.2. Taxonomy	161
6.3. Digital Forensics Stages	164

1. Objectives of Micro-Credentials

This chapter briefly describes the objectives of the Micro-Credentials (MCs) in Law Enforcement Authorities (LEA) capacity building on Cyber and Digital Forensic skills, and it is based on the [report from the High-Level expert Group on Access to Data for Law Enforcement](https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en?filename=Concluding%20Report%20of%20the%20HLG%20on%20access%20to%20data%20for%20effective%20law%20enforcement_en.pdf). [https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en?filename=Concluding%20Report%20of%20the%20HLG%20on%20access%20to%20data%20for%20effective%20law%20enforcement_en.pdf]



Evidence Admissibility and Transparent Judicial Proceedings

Assess the competences

An MC should be granted to an individual based on a sound evaluation of the capacity to accomplish the tasks related to the MC. The MC works as a micro-certification that contributes to the admissibility of evidence in Court.

Transparency

Without mentioning LEA strategies and tools, the MC provides a clear description of the competences and skills, enabling non-LEA experts to obtain the MC by following courses and training provided by the industry.



Facilitate the Development and Organisation of Training Activities

Proof of competencies to attend an intermediate or advanced course

Experience in delivering specialised courses raised the difficulty of selecting students who address all the required prerequisites, especially when organised at the EU level, where line managers or those responsible in the institutions are not able to check such prerequisites.

Monitoring tool to support capacity building strategy at national and EU levels

As of this date, there is a disparity in the levels of expertise on Cyber and Digital Forensic topics in the EU Member States and, at the Member State level, between different police entities. Several factors can explain this:

- The maturity of LEA specialised education in the entity,
- The criminal history that led some Member States to invest in some topics as priority, while others targeted different priorities because they faced other criminal phenomena,
- The rotation of the specialised staff, mainly when the private sector provides better salary conditions.

By providing a coherent MC structure, detailed at the lowest level, unit managers and political decision-makers can identify gaps and set priorities accordingly.

At the EU level, depending on the contribution of the Member State and entities, a dashboard will allow for the identification of common needs and feed into the strategy for decision-making.



Increase Trust between Investigators and Other Actors

The recognition of acquired and validated skills and competences, using a transparent set of MCs, contributes to the trust of actors in the domain.

2. Properties of Micro-Credentials

Stackable set of demonstrated skills and knowledge

The stackability of the MCs throughout a career is perceived by the practitioners as a recognition of experience and expertise, often as a result of efforts to keep their knowledge up-to-date with the evolution of technology and criminal *modus operandi*.

Adaptable to Member States LEAs profiles

The tasks allocated to practitioners' profiles may differ depending on the Member State and the entities (police, customs authorities, cyber agencies).

Accessible

The MC guidelines published at the EU level allow granting MCs using different methods. In addition to the traditional exam, demonstration of previous expertise or blended approaches may be considered.

Sustainable

Due to the evolution of the topics, some MCs may become obsolete after a few years.

3. ECTEG's Approach on Micro-Credentials

Considering the objectives defined in the [High-Level Expert Group on LEA Access to Data documentation](https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en) [https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en] and the defined properties, several criteria guided the development of the MCs by ECTEG.

Micro Level and Packs

MCs are designed as small, self-contained competence units. These units can be aggregated into larger MCs or organised into different MC packs, with individual MCs potentially forming part of multiple packs to support flexible learning pathways.

This facilitates:

- The creation of the necessary MCs for a profile that may differ between Member States and within each Member State, as well as between LEA entities. Such an approach does not prohibit the practitioner from acquiring additional MCs that are not required for their profile, facilitating internal promotions;
- When an acquired MC becomes obsolete, the robustness of the practitioner profile is not compromised; attending a few hours of an online course, for instance, may enable replacing an obsolete MC with an up-to-date one;
- The documentation of prerequisites to follow a training session, allowing attendees to address the missing MC in a smoother process.

When described, each MC is associated with a specific stage of a relevant professional process. While many MCs relate to stages of the digital forensics process, others address management, governance, operational, and broader policing functions. This classification facilitates the identification of MCs that are most relevant to existing LEA roles and tasks in EU member states.

Stackable through the EU

The stackable property can be seen as a wall made of multiple bricks. Each practitioner builds their knowledge portfolio based on an evolutionary design that may be guided by line managers or their own aspiration to acquire expertise in new domains.

The expertise is often spread throughout the EU because some countries have developed research and experience to address regional criminal phenomena. When seeking to fill gaps in specific domains, it may be necessary for practitioners to follow training delivered in the EU and have the competences acquired at the end of the training validated using MCs.

When examining the MCs stacked by a practitioner, it will then be possible that the MCs were granted by different entities, located in different Member States. A mutual recognition, across the EU, of the MC's catalogue is seen as a factor of trust and efficiency.



Equivalence

MCs or packs of MCs can be grouped to reflect existing academic degree modules, opening the path for a possible equivalence with the ECTS [<https://education.ec.europa.eu/education-levels/higher-education/inclusive-and-connected-higher-education/european-credit-transfer-and-accumulation-system>].

When described, each MC is documented with an estimation of the workload expected to be prepared to address the covered knowledge.

Similarly, when obtaining an academic degree, completing one of its volumes or the exam at the end of a course delivered by an EU institution (CEPOL, EUROPOL), National Police Academy or the industry, a practitioner may automatically be granted the associated pack of MCs.

The equivalence table has to be validated by an Authority to be defined.

4. Evaluation

Considerations

The Micro-Credentials are not graded

The MCs are acquired, or not. There are no grades delivered for the MCs.

The Micro-Credentials may address different taxonomy levels

For each MC, the listed observable objectives address different levels of  Bloom's taxonomy^[p.161]. For the validation of a professional profile, the "remember" level should be avoided, preferring at least "apply" and, whenever possible, higher levels like "evaluate" or "analyse".

The evaluation does not evaluate the English language level

In the EU, most LEA practitioners are not English speakers. At some point, they practice and use technical English related to IT. However, complex questions, especially the ones targeting the highest taxonomy level, may use grammar and sentence construction that are not easy to understand for someone who is not fluent in English.

As a consequence, a fair process requires the questions to be provided in the applicant's mother tongue.

Different ways to acquire Micro-Credentials

Some MCs, especially those related to soft skills (e.g., reporting, ethics, stress management), may be granted by demonstrating previous expertise (e.g., several case reports accepted in front of a national Court) or by providing a discussion or synthesis document.

Different sources in a homogeneous framework

Practitioners may apply for MCs at various locations, often at the conclusion of a training. In an EU-wide effort, a mutual recognition of the acquired MCs requires coordination and trust. This impacts the approach for the validation of the skills and competences.

An Authority that will validate the quality of the questions needs to be designed.

Combined with exams

Although MCs are not graded, often students are graded after completing a training. The proposed approach allows combining the MCs with the exam.

Each question is tagged with one or several MCs that are required to answer. So, a single MC may be covered by one or several questions.

A table is created to document the MC(s) covered for each question. A simple calculation will then allow to validate, or not, the MCs as a side result of the exam.

Practical evaluation requires data

For the practical questions, data (e.g., files, network traffic, encrypted volumes) are required. To avoid creating an additional workload, the data used for the practical questions may be the same as that already handled during the courses or the exam.

Validation of the acquired competences and skills process

Procedure

1. Creation of the questions

Questions are created with marks.

The exam is ready.

2. Identification of the MC(s) covered for each question

A table is created, listing all questions and, for each question, the covered MC(s). A pass mark for each MC is proposed.

3. Request for approval from the Authority

The questions and the table of MCs are provided to the Authority.

The Authority may validate the question set and the associated table or propose modifications. The modifications are only about the question's pertinence to validate the MC(s) or the expected pass-mark.

4. Applicants go through the exam

Applicants answer the question for the exam.

It is advised, for transparency purposes, to inform which MC(s) are covered for each question.

A set of answers for each applicant.

5. The exam is graded

Evaluators allocate the marks for all questions answered by the applicant.

There are marks for each question answered by an applicant.

6. The marks are counted to validate the MC(s)

Using the approved table, marks are counted to validate the MC(s).

The Applicant is granted the MC(s), equal to or over the agreed pass-mark.

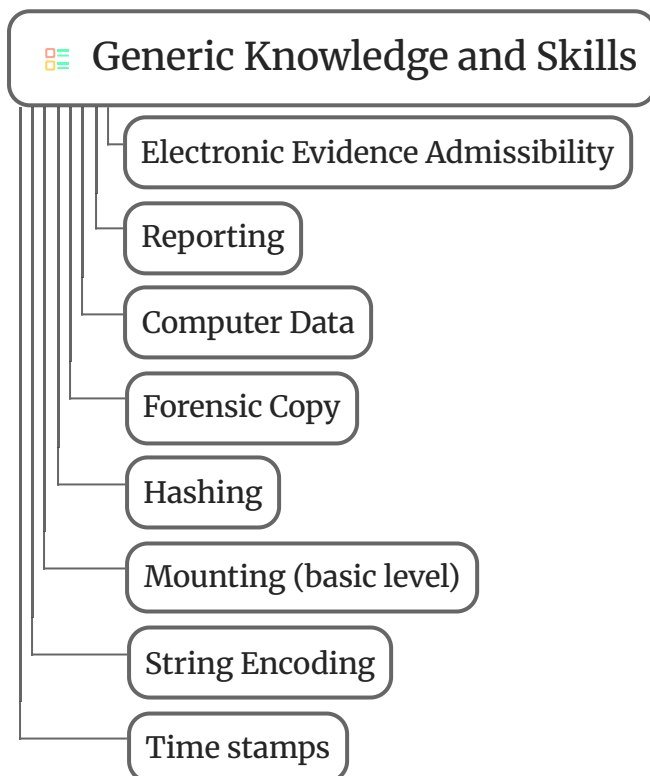
5. Micro-Credentials Packages

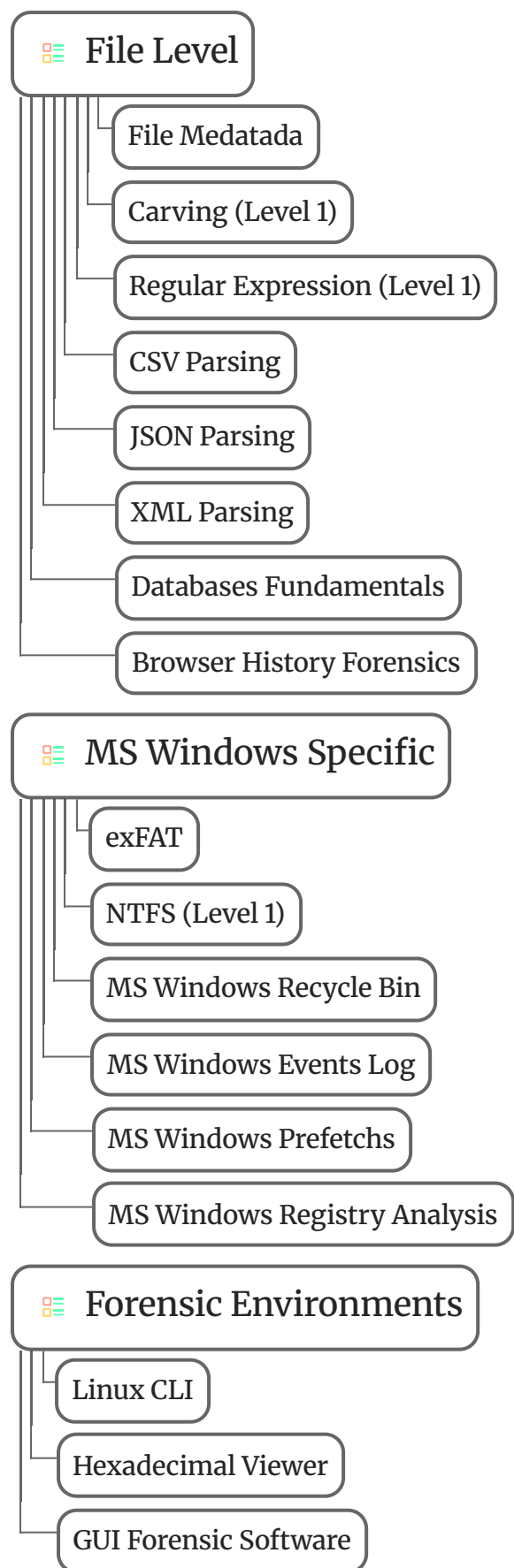
5.1. Digital Forensic Examiner MC Package

The following sets of Micro-Credentials address the basic essential knowledge and skills required to fulfil junior Digital Forensics Examiner tasks.

Applicant in a team

The applicant is considered to work in a team, with access to more experienced colleagues and reports reviewed by a line manager.





5.1.1. Generic Knowledge and Skills (DFI)

MCs in this generic group are considered applicable to all forensic domains and prerequisites for understanding and handling other MC topics.

5.1.1.1. 0101 – Electronic Evidence Admissibility

The applicant is able to:

- **Explain** the criteria that are required for the admissibility of electronic evidence at court
- **Explain** the electronic evidence stages



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	1 hours
Total	4 hours



Prerequisites

The applicant should prove the knowledge of:

- National legislation on the procedural laws related to electronic evidence admissibility



Detailed Description

The applicant should be able to:

1. **List** the criteria for electronic evidence admissibility and **provide** examples and potential related risks
 - Authenticity
 - Completeness
 - Reliability
 - Believability
 - Proportionality
 - Genuine
2. **Explain** the difference between direct evidence and opinion evidence
3. **Demonstrate** the understanding of the forensic process, **provide** examples for each stage and **explain** how risks may be mitigated

4. **Explain** the evidence and the process that led to its discovery, understandably



Related Forensic Process Stages

Identification
 Extraction/Preservation
 Analysis
 Documentation
 Presentation



Observations

National laws and guidelines are considered prerequisites. They can be learnt during exercises or side sessions when attending formal training.

5.1.1.2. 0102 – Reporting

The applicant is able to:

- **Document** all forensic actions and findings to create a forensic report, **securing** the admissibility of the provided evidence in front of the court
- **Identify** non-disclosable tools, techniques, strategies, and lawful processes to address them nationally



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	4+2 hours
Total	8 hours

4 hours are embedded in other topics' exercises, where the forensic actions and findings are documented on the fly



Detailed Description

The applicant should be able to:

1. **Describe** the provided devices and other digital traces to comply with the chain of custody
2. Accurately **document** forensic tasks according to national laws and regulations
3. **Document** forensic findings, allowing, whenever possible, for the integrity and reproducibility
4. **Provide** a technical interpretation of how the trace was created and how it may provide clues, an investigation path, or evidence

5. **Segregate** the description of the traces and artefacts and the interpretation so that, when an interpretation is challenged, the finding is not compromised or rejected
6. **Document** the validation of findings by, whenever possible, cross-checking traces from multiple sources or devices
7. **Create** a graphical representation of processes, a timeline and correlation between
8. **Provide** links between traces that improve the attribution of the identified behaviour to a natural person
9. **Propose** additional forensic or investigation tasks that may lead to the validation of findings or the discovery of new traces
10. **Present** the findings to readers and listeners with either a technical or non-technical background by adopting language and explaining their tasks, findings and interpretations



Related Forensic Process Stages

 **Documentation**

 **Presentation**

Observations

This MC can be evaluated by completing tasks during exercises where partial reporting is possible, finalised by a written report, and clarity and accuracy should be considered.

Reporting and findings should be reviewed and validated by a qualified supervisor or approver.

5.1.1.3. 0103 – Computer Data

The applicant is able to:

- **Understand** the fundamental data representations encountered in digital forensic investigations, including binary and hexadecimal numbering systems, Base64 encoding, various timestamp formats, string encodings like UTF-8 and UTF-16LE, and CPU endianness and its impact on forensic analysis
- **Handle, convert** and **interpret** unsigned integer values



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	4 hours
Total	7 hours



Prerequisites

The applicant should prove the knowledge of:

- Access to raw data



Detailed Description

The applicant should be able to:

1. **Understand** and **convert** between numbering systems, particularly binary, hexadecimal and decimal
 - **Interpret** raw binary/hex data from memory dumps, or files
 - **Identify** common data structures encoded in hex (e.g., file headers)
2. **Explain** and **detect** CPU endianness (little-endian vs big-endian)
 - **Recognise** byte ordering in file system structures and memory dumps
 - **Convert** integer numbers (8, 16, 32 and 64 bits long) from raw data, considering endian byte ordering
 - **Understand** the 2's complement format used to represent negative integers
 - **Be aware** of the floating-point number format (IEEE 754 standard)
 - **Understand** implications in interpreting data structures with different sizes (groups of bytes, offsets)
3. **Encode** and **decode** Base64 and Base58
 - **Identify** hidden or obfuscated data
 - **Understand** Base64 as used in email headers, HTTP payloads, and databases
4. **Interpret** and **convert** timestamp formats
 - **Explain** the concept of EPOCH date-time values and encoded date-time values
 - **Work** with common forensic timestamp formats and **convert** between formats using command-line and GUI tools
 - DOS date and time (encoded)
 - Windows FILETIME (EPOCH)
 - UNIX timestamp (EPOCH)
5. **Recognise** and **convert** string encodings
 - **Distinguish** between ASCII, Latin1, UTF-8 and UTF-16LE in hex dumps
 - **Understand** the impact of endianness in UTF-16 encoding
 - **Convert** between encodings and **recover** readable text from raw hex
 - **Identify** forensic relevance of encodings (e.g., system language, obfuscation techniques, artefacts in memory or files)



Related Forensic Process Stages

[🔍 Analysis](#)[📄 Documentation](#)[🗣️ Presentation](#)

5.1.1.4. 0104 – Forensic Copy

The applicant is able to:

- **Understand** and **apply** the process to **create** forensic copies (bit-by-bit copies) of mass storage devices
- **Focus** on image acquisition, integrity with cryptographic hashes, with free and open-source tools
- **Make** forensic copies in standard formats like EWF (Expert Witness Format) and RAW (dd format)



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.5 hours
Labs	1.5 hours
Total	3 hours



Prerequisites

The applicant should prove the knowledge of:

- Use operating systems (intermediate knowledge)
- 0103 - Computer Data ^[p.18]
- 0105 - Hashing (L1) ^[p.21] ^[p.18]



Detailed Description

The applicant should be able to:

1. **Demonstrate** an understanding of what a forensic copy is
 - Terminology (imaging, acquisition, forensic copy, cloning, backup)
 - Software and hardware write blockers
 - Difference between logical and physical forensic images
 - Importance of cryptographic hashes to verify the integrity of forensic copies integrity
 - Standard forensic copy of usual file formats: RAW and EWF
 - Storage device technology impact on the forensic approach (SSD, Mobile Forensics)
2. **Create** forensic copies
 - Sanitisation of the storage destination device
 - Open-source and free tools (CLI and GUI)

- Identification of the best tool to make forensic copies for each case
- EWF compression and analysis performance
- Document the acquisition: case number, device details, acquisition steps, tools used, hash results and expert name



Related Forensic Process Stages

 **Extraction/Preservation**

5.1.1.5. 0105 – Hashing (L1)

The applicant is able to:

- **Validate** a forensic copy of evidential material
- Critically **appraise** different hashing algorithms and their suitability to forensic domains



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1 hours
Labs	1 hours
Total	2 hours



Prerequisites

The applicant should prove the knowledge of:

- Methods for copying digital media, such as the dd command, or similar (basic knowledge)



Detailed Description

The applicant should be able to:

1. **Explain** the fundamental hashing concepts, including (non-)cryptographic hash functions.
2. **Describe** the purpose of hashing and its relevance to digital forensics and evidential integrity
3. **Identify** and mitigate common vulnerabilities related to hashing, such as collisions and weak algorithms
4. **Compare** and contrast different hashing algorithms and their ideal use cases
5. **Validate** the integrity of a forensic copy



Related Forensic Process Stages

[Analysis](#)[Documentation](#)

5.1.1.6. 0106 – Mounting

The applicant is able to:

- Safely **mount** a forensic image acquired at the byte level and provided in the usual format
- **Access** the file system, including the encrypted ones, in order to **browse** and **process** files in a forensic way



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	4 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic OS command line skills
- 0103 - Computer Data ^[p.18]
- 0104 - Forensic Copy ^[p.20]
- 0301 - exFAT ^[p.35]
- 0302 - NTFS (L1) ^[p.36] ^[p.36] ^[p.35]



Detailed Description

The applicant should be able to:

1. **Recognise** forensic evidence formats by **identifying** images in EWF, AFF and standard raw (.dd) formats
2. **Provide** evidence integrity information by **using** tools to **verify** image hash and metadata
3. **Identify** partition scheme and related file systems by **determining** offsets and file systems within the forensic image

4. **Mount** a read-only volume from a forensic image
5. **Work** with encrypted partitions by **identifying** BitLocker-encrypted partitions and **mounting** them using the appropriate password/key
6. **Browse** the (unlocked) file system with the use of forensic tools to **explore** contents and **process** the files
7. **Document** the process to preserve the chain of custody and reproducibility for Court or audit purposes



Related Forensic Process Stages

 **Extraction/Preservation**

5.1.1.7. 0111 – String Encoding

The applicant is able to:

- **Understand** and **translate** string encodings, such as UTF-8 and UTF-16LE
- **Handle, convert** and **interpret** unsigned integer values



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	3 hours
Total	7 hours



Prerequisites

The applicant should prove the knowledge of:

- Access to raw data
-  0103 - Computer Data ^[p.18]



Detailed Description

The applicant should be able to:

1. **Distinguish** between various string encodings by **interpreting** raw binary/hex data to identify ASCII, Latin1, UTF-8 and UTF-16LE timestamps
2. **Understand** the impact of endianness in string encoding

3. **Convert** encodings and recover readable text from raw data
4. **Identify** the forensic relevance of string encodings, considering system language, obfuscation techniques, artifacts in memory or files



Related Forensic Process Stages

 **Analysis**

 **Documentation**

 **Presentation**

5.1.1.8. 0112 - Date Time Stamps

The applicant is able to:

- **Understand** and **convert** various timestamps that are commonly encountered in digital forensic examinations
- **Handle, convert** and **interpret** various timestamps from raw data



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	4 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- Access to raw data
-  0103 - Computer Data ^[p.18]



Detailed Description

The applicant should be able to:

1. **Describe** the concept of epochs, in relation to digital timestamps
2. **List** common timestamps encountered during digital investigations
3. **Demonstrate** the impact of endianness in timestamp encoding
4. **Discuss** the evidential importance of timezone accuracy when converting timestamps from raw data by **accommodating** daylight savings in evidential reports

5. **Translate** common timestamps from raw data to human-readable date-times, including main timestamps (Unix Epoch, FAT, Windows 64 (BE/LE))



Related Forensic Process Stages

 **Analysis**

 **Documentation**

 **Presentation**

5.1.2. File Level (DFI)

MCs in this file-level group address the handling of files not specific to the Operating System (OS).

5.1.2.1. 0201 – File Embedded Metadata

The applicant is able to:

- **Recover** file metadata embedded in the file aside the ones provided by the file system layer
- **Explain** the difference between the file system layer and embedded metadata, and how it impacts the forensic interpretation



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	3 hours
Total	5 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic command-line tools to display a file and save the resulting process to a file
-  0112 - Date Time Stamps ^[p.24]

Detailed Description

The applicant should be able to:

1. **Explain** the principle of embedded metadata, as examples:
 - Time of creation of a picture
 - Location in space
 - Software used
2. **Recover** the file's embedded metadata for, as examples:
 - Image files
 - Audio files
 - Video files
 - Document files
3. **Explain** the forensic importance of the embedded metadata (travelling with the file) and compare date-time differences

Related Forensic Process Stages

 **Analysis**

Observations

Location in time and space requires a specific methodology to check the accuracy and report, which will be covered in specific MCs.

5.1.2.2. 0202 - Carving (L1)

The applicant is able to:

- **Use** of forensic tools for automatically carving files

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	1 hours
Labs	2 hours
Total	3 hours



Prerequisites

The applicant should prove the knowledge of:

- Computer data representations and file systems (allocated/unallocated space)



Detailed Description

The applicant should be able to:

1. **Describe** what data carving is and how files can be recovered from file systems
2. **Identify** file type by recognising file signatures
3. **Explain** where file signatures can be located on the device (embedded files and issues with the sector boundaries carving process)
4. **Understand** the obstacles to and limitations of manual carving
5. **Evaluate** and critically **appraise** various carving tools



Related Forensic Process Stages

[Extraction/Preservation](#)[Analysis](#)

5.1.2.3. 0203 – Regular Expressions (L1)

The applicant is able to:

- **Understand** the structure of regular expression and their usage
- **Search / match** patterns using regex



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	4 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic command line tools to display a file and save the resulting process to a file

Detailed Description

The applicant should be able to:

1. **Explain** what a regular expression is, how it is used, and be aware of the different syntax depending on the flavour
2. **Identify** the most used regex tokens and **explain** their use
 - Quantity: zero or one, zero or more, one or more, exactly n, etc.
 - Common tokens: digit, word, whitespace, etc.
 - Character in a range
 - Negative selection
 - Anchors: start of a string, end of a string, etc.
 - General tokens: newline, tab, carriage return, etc.
3. **Identify** common errors in regex syntax
 - Wrong character
 - Wrong use of separators
 - Including unnecessary spaces
 - Missing brackets
 - Incorrect usage of anchors
 - Wrong quantifiers
 - No escape for special character
 - Unnecessary backslashes
4. **Read** and **describe** existing regex
5. **Write** a new regex to match patterns
6. **Validate** regex using scripts (e.g., Python library, etc.), GUI tools and ad-hoc testing files
7. **Filter** data to isolate the pattern of interest
8. **Explain** the importance of such filtering in a forensic context

Related Forensic Process Stages

 **Analysis**

Observations

The MC does not cover:

- Substitution with regular expression
- Grouping with regex or more advanced queries / research

5.1.2.4. 0204 – CSV Parsing

The applicant is able to:

- **Understand** the structure of CSV files and **handle** various data formats
- **Parse** a CSV file using appropriate tools to **transform** raw data logs into structured, human-readable information for an investigation



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	3 hours
Total	5 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic command line and GUI tools to display a file and save the resulting process to a file



Detailed Description

The applicant should be able to:

1. **Explain** the structure of CSV files (headers, records, fields, delimiters (e.g., ',', ';', '\t'), quotation rules)
2. **Identify** and **convert** custom encodings and **understand** encoding issues in CSV parsing
3. **Handle** non-standard formats
 - Fields containing embedded delimiters or line breaks
 - Custom timestamp formats (e.g., YYYYMMDD:HH:MM)
 - Missing or null fields
 - Anonymised or masked values
4. **Identify** common errors in CSV format
 - Distinct Separator
 - Separator inside value
 - Column number
 - Unsupported character
 - Character not escaped

- Wrong File encoding
- 5. **Parse** and **validate** CSV content using command-line utilities (e.g., awk, csvtool, Python library) and GUI tools
- 6. **Filter** or **transform** data to **isolate** transactions or records of interest (by date, amount, location, ...)
 - Filter a column on a specific criterion
 - Filter a row on a specific criterion
 - Count occurrences of certain information in a specific column (sort by column number)
 - Count occurrences of certain information in a specific column (sort by column header)
 - Filter row having a specific information in common
 - Filter row having several information in common
 - Filter row using an operator on a row with an integer format
 - Remove duplicates
- 7. **Explain** the importance of such filtering in a forensic context



Related Forensic Process Stages

 **Analysis**



Observations

The MC does not cover:

- Correlating each field with its forensic meaning (e.g., card number field partially anonymised, "type" field with forensic logic value A, O, or C)

5.1.2.5. 0205 - JSON Parsing

The applicant is able to:

- **Understand** the structure of JSON files and **handle** various data format
- **Parse** a JSON file using appropriate tools to **transform** raw data logs into structured, human-readable information for an investigation



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1 hours
Labs	4 hours
Total	5 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic command line tools to display a file and save the resulting process to a file



Detailed Description

The applicant should be able to:

1. **Explain** the structure of JSON files (key, values, delimiters, quotation rules)
2. **Identify** common errors in JSON format
 - Brackets (unclosed dictionaries/arrays, mismatched brackets/braces)
 - Trailing comma (missing or extra)
 - Unsupported character
 - Character not escaped
 - Invalid Data type
 - Improper use of quotes (simple, double)
 - Nested JSON format
3. **Parse** and **validate** JSON content using command-line utilities (e.g., jq, sed, awk, Python library) and GUI tools
4. **Filter** or **transform** data to isolate transactions or records of interest
 - Filter by key or key/value
 - Filter on several key
 - Count occurrences of a specific key or key/value
 - Reverse filter on a key/value
5. **Explain** the importance of such filtering in a forensic context



Related Forensic Process Stages

Analysis

Observations

The MC does not cover:

- Interpretation of JSON file content in forensic investigation
- Mathematical operation on JSON integer values (addition, subtraction, multiplication, selection on criteria as lower/greater than)

5.1.2.6. 0207 – Database Fundamentals

The applicant is able to:

- **Describe** the concept of relational database
- **Build** basic SQL queries
- **Use** SQLite, **open** a database of multiple tables and **join** tables to **visualise** and **export** data



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	5 hours
Total	8 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic command-line tools
- 0204 - CSV Parsing ^[p.29]



Detailed Description

The applicant should be able to:

1. **Explain** the role of rows, columns (records, fields), and keys using an example of a minimum of two joint tables
2. **Explain** the limitations of SQLite compared with SQL and other relational multi-user DB services
3. **Execute** basic SQL queries using the *select, from, where, group by*
4. **Open** a SQLite DB of multiple tables using a SQLite GUI viewer/editor
 - **Identify** the number of records in each table
 - **Identify** the keys to link tables

- **Select** the columns to display
 - **Filter** the displayed rows based on a matching string criterion
 - **Export** to CSV
5. **Use** a SQLite DB of multiple tables, a CLI viewer/editor
- **Open** an SQLite DB
 - **Display** and **export** the structure for reporting
 - **Make a simple query** to display columns from 2 different linked tables
 - **Filter** on strings
 - **Use** aggregation functions (i.e sort by, group by)
 - **Export** to CSV
6. **Convert** the date-time value to a human-readable string using the SQLite query features



Related Forensic Process Stages

 **Analysis**



Observations

The MC does not cover:

- The whole SQL language and DB services, multi-users, etc (only SQLite format)

Comments:

- Analysed DBs are usually encountered, i.e. Web history, Chat applications
- Date-Time value to convert: Webkit?

5.1.2.7. 0211 - Browser History Forensics

The applicant is able to:

- **Prove** intent and sequence (search terms → click → download/execution)
- **Trace** initial compromise and data exfiltration
- **Attribute** actions to a specific Windows user/profile and **detect** profile hopping or portable browsers
- **Corroborate** with NTFS/EVTX/SRUM/Prefetch/LNK to **raise confidence** and **spot** anti-forensics (cleared history, selective deletions, suspicious extensions)
- **Support** court-ready reporting (hashes, tool versions, TZ/DST-normalized times, scope/GDPR)



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	4 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- 0112 - Date Time Stamps ^[p.24]
- 0207 - Database Fundamentals ^[p.32]
- 0304 - Windows Event Logs ^[p.38]



Detailed Description

The applicant should be able to:

1. Safely **preserve** multi-profile browser data without altering evidence (read-only workflows)
2. **Parse** and **interpret** History (SQLite) via urls, visits, visit_source, downloads, keyword_search_terms
3. **Analyse** autofill, login data (respecting legal constraints and scope)
4. **Analyse** sessions/tab restore, local storage and indexed DB (LevelDB), cache/code cache, favicons, top sites, extensions
5. **Convert/normalise** Chromium timestamps (WebKit time μ s since 1601-01-01) and **correlate** across sources
6. **Detect** private mode traces (limitations), anti-forensics (cleanups, profile hopping, containerised browsers)



Related Forensic Process Stages

[Analysis](#)[Documentation](#)

Observations

Extended learning objectives can be:

1. **Be able to work** with Edge and Chromium profiles on Windows
2. **Retrieve** the history and downloads
 - History (SQLite -mark this as a prerequisite): tables & joins (urls ↔ visits ↔ visit_source), transition types, typed vs. link, search terms
 - Downloads: downloads, downloads_url_chains, target_path, referrers, interruptions
 - Normalisation of WebKit timestamps (mark this a **prerequisite**), time-zone/DST pitfalls
3. **Analyse** cookies, autofill, logins

- Cookies DB schema (host_key, name, encrypted_value, expires_utc)
- Autofill (Web data), login data (metadata handling when decryption is out of scope)
- Evidential value & limits

4. **Be able to retrieve** information on sessions, storage and cache

5.1.3. Windows Specifics (DFI)

MCs part of this Windows group are related to investigating MS Windows OS and File Systems.

5.1.3.1. 0301 – exFAT

The applicant is able to:

- **Understand** the role of exFAT in digital forensics
- **Use** open-source tools, **analyse**, **interpret**, and **investigate** digital evidence on exFAT file systems



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	3 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- 0103 - Computer Data ^[p.18]
- 0111 - String Encoding ^[p.23]
- 0112 - Date Time Stamps ^[p.24]



Detailed Description

The applicant should be able to:

1. **Understand** the fundamentals of exFAT and how it can affect digital forensics investigations
2. **Identify** the exFAT system files and **explain** their role
3. **Explain** the working of the \$Bitmap

4. **List** file records entries (active and inactive) and **extract** essential file metadata (file name, date-time values, file size, first cluster)
5. **Explain** the processes related to file move, renaming and deleting and the related impact on exFAT structures
6. **Exploit** techniques and tools for recovering deleted files on exFAT volumes
7. **Use** exFAT time stamps to allow the creation of timelines
8. **Extract** the cluster slack



Related Forensic Process Stages

 **Analysis**

5.1.3.2. 0302 – NTFS (L1)

The applicant is able to:

- **Understand** the role of NTFS in digital forensics
- **Use** open-source tools, **analyse**, **interpret**, and **investigate** digital evidence on NTFS file systems used in Windows environments



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	3 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

-  0103 - Computer Data ^[p.18]
-  0111 - String Encoding ^[p.23]
-  0112 - Date Time Stamps ^[p.24]

Detailed Description

The applicant should be able to:

1. **Explain** the fundamentals of NTFS structures and how they can affect digital forensics investigations
2. **Explain** the core system file key features and their interaction with Windows OS features (OS, Applications, file system driver)
3. **Analyse** the Master File Table (MFT) for file recovery and timeline reconstruction
4. **Explain** the difference between residential and non-residential file record attributes
5. **Identify** NTFS file attributes, security descriptors, and access control lists for evidence gathering
6. **Recover** deleted files from an NTFS partition (without mounting)
7. **Extract** file metadata for allowing timeline analysis using NTFS-specific timestamps
8. **Export** the content from identified Alternate Data Streams (ADS)
9. **Extract** the history for a file, if available, from the USN Journal \$J file
10. **Export** MFT record slack and cluster slack content
11. **Demonstrate** awareness of the detection of anti-forensics

Related Forensic Process Stages

 **Analysis**

5.1.3.3. 0303 – Windows Recycle Bin

The applicant is able to:

- **Explain** the Windows deletion process of deleted files stored in the recycle bin
- **Recover** the file and **provide** details about the deletion process

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	2 hours
Labs	3 hours
Total	5 hours



Prerequisites

The applicant should prove the knowledge of:

- 0302 - NTFS (L1) ^[p.36]



Detailed Description

The applicant should be able to:

- **Explain** how recycled files are stored in the folder structure when examining a volume during the forensic process
- **Explain** the impact on the file renaming and \$I file in the MFT and **analyse** its content
- **Explain** the process of file recovery by the user and potential traces
- **Liaise** with the \$Journal history to **provide details** about the deletion process



Related Forensic Process Stages

 **Analysis**

5.1.3.4. 0304 – Windows Event Logs

The applicant is able to:

- **Explain** the role of Windows Event Logs
- **Identify** most common Windows Channel and EventID and their usage
- **Be able to search** for specific logs in EventViewer or in .evtx files



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	2 hours
Total	4 hours



Prerequisites

The applicant should prove the knowledge of:

- 0206 - XML Parsing ^[p.67]



Detailed Description

The applicant should be able to:

- **Localise** Windows Event Logs
- **Explain** the role of Windows Event Logs
- **Identify** different Windows Provider / EventID (automatically generated by the system or generated by user activity)
- **Open** or **parse** the Event Logs with GUI or command line tools to **recover** and **export** in a human-readable form
- **Identify** the most important EventID for a forensic investigator (account manipulation, login, deletion, ...)
- **Search** for specific logs in EventViewer or in .evtx files
- **Understand** and **interpret** key/values in the most common Windows Event Logs



Related Forensic Process Stages

 **Analysis**

Observations

The MC does not cover:

- Reconstruction of user or system activity or the anti-forensics methods detection

5.1.3.5. 0305 – Windows Prefetch

The applicant is able to:

- **Enable** the identification, extraction, interpretation, and correlation of Windows artifacts in forensic investigations, focusing mainly in prefetch and log analysis
- **Reconstruct** user activity (executions, open documents, external devices used)
- **Reconstruct** system activity (software installation, services, scheduled tasks, persistence)



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	2 hours
Total	4 hours



Prerequisites

The applicant should prove the knowledge of:

- 0112 - Date Time Stamps ^[p.24]
- 0301 - exFAT ^[p.35]
- 0302 - NTFS (L1) ^[p.36]



Detailed Description

The applicant should be able to:

- **Interpret** key fields of prefetch (.pf), jump lists, and LNK to infer what was executed, when, and from where
- **Enumerate** and **analyse** scheduled tasks, their triggers, and their history (EVTX / XML on disk)
- **Detect** WMI persistence (event filters/consumers/bindings) and suspicious BITS jobs
- **Use** Windows Error Reporting (WER) artefacts and dumps to **pivot** to binaries/paths and moments of crash/execution



Related Forensic Process Stages

Analysis

5.1.3.6. 0306 – Windows Registry Analysis

The applicant is able to:

- **Explain** the role of Windows Registry Hives
- **Extract** keys and values in a human-readable form with an explanation about the forensic interest and ways to cross-check the findings



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	4 hours
Total	7 hours



Prerequisites

The applicant should prove the knowledge of:

- Access to NTFS file systems using digital forensic software
- Installation of dedicated tools (regripper, RegExplorer, ...)
- Data types (strings, integer, ...)



Detailed Description

The applicant should be able to:

1. **Localise** and **recover** the registry hives
2. **Open** or **parse** the registry hives with GUI or command line tools to **recover and export** in a human-readable form
 - Registered users and related properties, including accesses and information related to the use of a Microsoft Account (SAM)
 - USBdevices (SYSTEM)
 - USBSTOR (SYSTEM)
 - Mounted devices (SYSTEM)
 - Bluetooth devices (SYSTEM)
 - Time zone (SYSTEM)
 - Networks list (SOFTWARE)
 - Uninstalled software (SOFTWARE)
 - OneDrive (USER)
 - Typed URLs (USER)
 - Recent documents (USER)
 - User assists (USER)
 - Jump lists (USER)
3. **Explain** the forensic importance of each of the key/values exported and, if any, how it can be cross-checked with other information.



Related Forensic Process Stages

 **Analysis**

Observations

The MC does not cover:

- How to access the registry hives

Comments:

- Cross-check can be performed using FS metadata, \$J or event logs. The FiRST report is not considered a valid cross-check as it uses the registry to provide the information.

5.1.4. Forensic Environments (DFI)

MCs in this group cover using the Digital Forensic Environment as used by LEA practitioners.

5.1.4.1. 9901 – Linux Command Line Interface

The applicant is able to:

- **Understand** basic commands in Linux, for managing users, navigating the file system, managing permissions, upgrading the operating system, installing tools, using tools to gather basic session information, creating, analysing and modifying text files, using the output of one tool as the input to another, managing compressed archives, analysing raw data and metadata, manipulating files and conducting basic file system searches.



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	6 hours
Total	9 hours



Detailed Description

The applicant should be able to:

1. **Access** the terminal (command prompt) to **use** CLI commands
2. **Use** the manual pages and help files to **understand** how to use commands
3. **List** the purpose of special Linux directories (/bin, /etc, /var, /dev, /mnt)
4. **Navigate** the Linux file system (ls, cd, pwd, ~)
5. **List, modify** and **create** system users and groups
6. **Differentiate** between super users and standard users

7. **Create** files (touch) and **edit** permissions and owners
8. **Update** and **upgrade** the Linux kernel and **install** or **remove** tools
9. **Utilise** useful informational commands (date, who, whoami)
10. **Create** and **modify** files using redirection (echo) and built-in editors (e.g., nano)
11. **Chain** commands together using piping
12. **List** and **describe** the contents of text files (cat, less, more, head, tail, wc, diff)
13. **Compress** and **extract** archives (tar, gzip, zip, 7z)
14. **View** and **parse** raw data (xxd, strings)
15. **Analyse** file metadata (file, stat)
16. **Copy**, **move** and **delete** files and folders
17. **Utilise** basic file search with the locate and updatedb commands



Related Forensic Process Stages

 **Extraction/Preservation**

 **Analysis**

 **Documentation**

 **Presentation**

5.1.4.2. 9902 – Hexadecimal Viewer

The applicant is able to:

- **Open** a file or a forensic image using an hexadecimal viewer (CLI or GUI) to **navigate** in the content using absolute and relative offsets and to **search for**, **select**, **interpret** and **export** selected content for further forensic processing



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	4 hours
Total	7 hours



Prerequisites

The applicant should prove the knowledge of:

-  0101 - Electronic Evidence Admissibility ^[p.16]
-  0103 - Computer Data ^[p.18]

-  0111 - String Encoding ^[p.23]
-  0112 - Date Time Stamps ^[p.24]

Detailed Description

The applicant should be able to:

1. **Open** a file in a hexadecimal editor or viewer and **secure** the content (so it can not be tampered with)
2. **Navigate** in the file using absolute and relative offsets in bytes, sectors and multiples of it expressed in decimal and hexadecimal
3. **Select** a group of bytes
4. Using installed features, **interpret** unsigned and signed integer values, strings and date-time in different formats and endianness
5. **Export** a group of bytes to a raw file

Related Forensic Process Stages

 **Analysis**
 **Presentation**

5.1.4.3. 9903 – GUI Forensic Software

The applicant is able to:

- **Locate, recover**, and **report** digital evidence using GUI forensic software

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	5 hours
Labs	9 hours
Total	14 hours

Prerequisites

The applicant should prove the knowledge of:

-  0103 - Computer Data ^[p.18]
-  0105 - Hashing (L1) ^[p.21]
-  ^[p.21]  0111 - String Encoding ^[p.23]

- 📁 0112 - Date Time Stamps [p.24]
- 📁 0203 - Regular Expressions (L1) [p.27]
- 📁 0301 - exFAT [p.35]
- 📁 0302 - NTFS (L1) [p.36]

📁 Detailed Description

The applicant should be able to:

1. **Install** and **configure** a GUI forensic tool (e.g., Autopsy)
2. **Navigate** the User Interface to **accomplish** the desired task
3. **Create** a new case and **set** its settings
4. **Add** data sources and **verify** their integrity
5. **Select** and **execute** modules or plugins, and **select** the required ones to **retrieve** the information that is being looked for
6. **Fine-tune** the keyword search module (string extraction options, lists of keywords, sub-string matches and regex)
7. **Use** the image gallery to **browse** the media files
8. **Create** timelines, including filtering based on the type of artefacts
9. **Tag, comment** and **report** artefacts

📁 Related Forensic Process Stages

📁 Extraction/Preservation

📁 Analysis

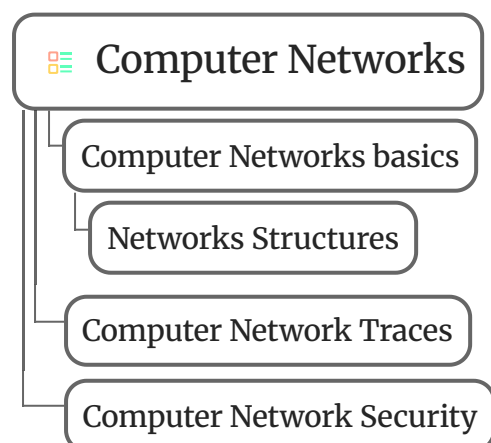
📁 Documentation

📁 Presentation

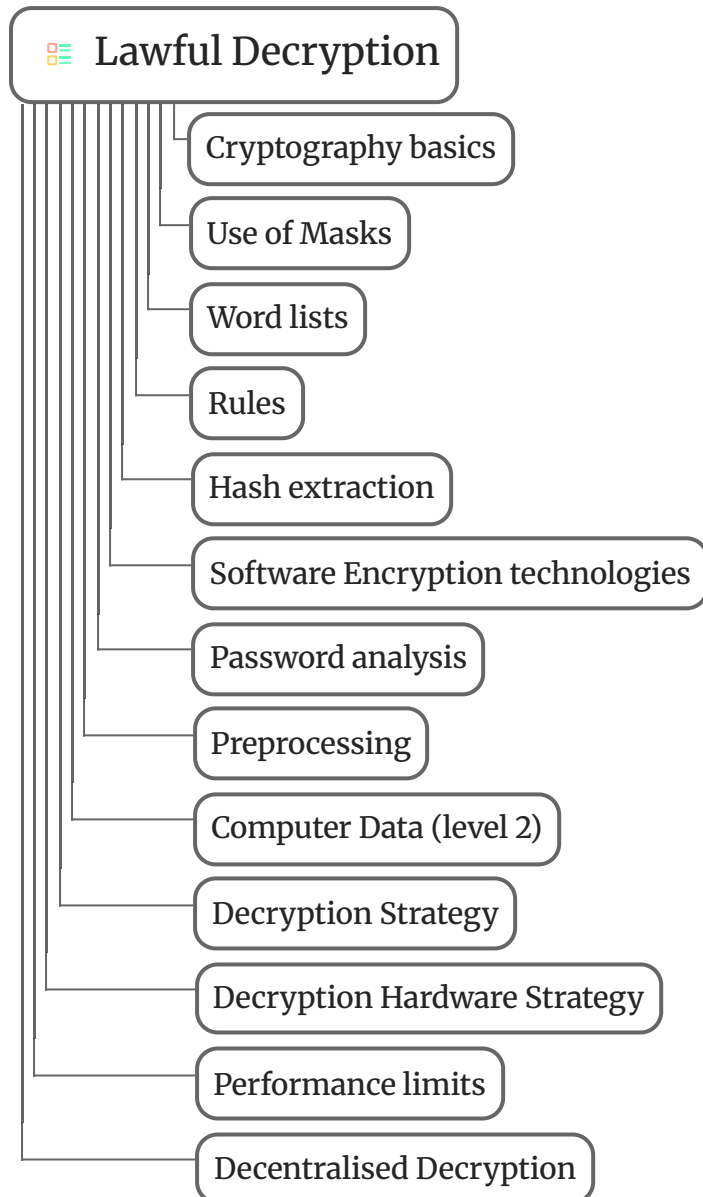
5.2. Computer Networks MC Package

Computer Networks Basic Micro Credentials cover the competencies required to understand IP network structures and areas, and to connect an investigator's computer to a simple network.

Advanced Micro Credentials address the competencies to gather and analyse traces that may be useful for criminal investigations, investigate cyber-attacks or set up lawful interception devices.



5.3. Lawful Decryption MC Package



6. Annexes

Extra

Council Recommendation of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability 2022/C 243/02 (cf. [Council Recommendation of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability 2022/C 243/02](#))

6.1. Micro-Credentials Full List

6.1.1. 0101 – Electronic Evidence Admissibility

The applicant is able to:

- **Explain** the criteria that are required for the admissibility of electronic evidence at court
- **Explain** the electronic evidence stages



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	1 hours
Total	4 hours



Prerequisites

The applicant should prove the knowledge of:

- National legislation on the procedural laws related to electronic evidence admissibility



Detailed Description

The applicant should be able to:

1. **List** the criteria for electronic evidence admissibility and **provide** examples and potential related risks
 - Authenticity
 - Completeness
 - Reliability

- Believability
 - Proportionality
 - Genuine
2. **Explain** the difference between direct evidence and opinion evidence
 3. **Demonstrate** the understanding of the forensic process, **provide** examples for each stage and **explain** how risks may be mitigated
 4. **Explain** the evidence and the process that led to its discovery, understandably

Related Forensic Process Stages

 **Identification**  **Extraction/Preservation**  **Analysis**  **Documentation**  **Presentation**

Observations

National laws and guidelines are considered prerequisites. They can be learnt during exercises or side sessions when attending formal training.

6.1.2. 0102 – Reporting

The applicant is able to:

- **Document** all forensic actions and findings to create a forensic report, **securing** the admissibility of the provided evidence in front of the court
- **Identify** non-disclosable tools, techniques, strategies, and lawful processes to address them nationally

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	2 hours
Labs	4+2 hours
Total	8 hours

4 hours are embedded in other topics' exercises, where the forensic actions and findings are documented on the fly

Detailed Description

The applicant should be able to:

1. **Describe** the provided devices and other digital traces to comply with the chain of custody
2. Accurately **document** forensic tasks according to national laws and regulations
3. **Document** forensic findings, allowing, whenever possible, for the integrity and reproducibility
4. **Provide** a technical interpretation of how the trace was created and how it may provide clues, an investigation path, or evidence
5. **Segregate** the description of the traces and artefacts and the interpretation so that, when an interpretation is challenged, the finding is not compromised or rejected
6. **Document** the validation of findings by, whenever possible, cross-checking traces from multiple sources or devices
7. **Create** a graphical representation of processes, a timeline and correlation between
8. **Provide** links between traces that improve the attribution of the identified behaviour to a natural person
9. **Propose** additional forensic or investigation tasks that may lead to the validation of findings or the discovery of new traces
10. **Present** the findings to readers and listeners with either a technical or non-technical background by adopting language and explaining their tasks, findings and interpretations

Related Forensic Process Stages

 Documentation

 Presentation

Observations

This MC can be evaluated by completing tasks during exercises where partial reporting is possible, finalised by a written report, and clarity and accuracy should be considered.

Reporting and findings should be reviewed and validated by a qualified supervisor or approver.

6.1.3. 0103 – Computer Data

The applicant is able to:

- **Understand** the fundamental data representations encountered in digital forensic investigations, including binary and hexadecimal numbering systems, Base64 encoding, various timestamp formats, string encodings like UTF-8 and UTF-16LE, and CPU endianness and its impact on forensic analysis
- **Handle, convert** and **interpret** unsigned integer values

Version

2026-06-03

**Level**

Basic

**Estimated Workload**

Lessons	3 hours
Labs	4 hours
Total	7 hours

**Prerequisites**

The applicant should prove the knowledge of:

- Access to raw data

**Detailed Description**

The applicant should be able to:

1. **Understand** and **convert** between numbering systems, particularly binary, hexadecimal and decimal
 - **Interpret** raw binary/hex data from memory dumps, or files
 - **Identify** common data structures encoded in hex (e.g., file headers)
2. **Explain** and **detect** CPU endianness (little-endian vs big-endian)
 - **Recognise** byte ordering in file system structures and memory dumps
 - **Convert** integer numbers (8, 16, 32 and 64 bits long) from raw data, considering endian byte ordering
 - **Understand** the 2's complement format used to represent negative integers
 - **Be aware** of the floating-point number format (IEEE 754 standard)
 - **Understand** implications in interpreting data structures with different sizes (groups of bytes, offsets)
3. **Encode** and **decode** Base64 and Base58
 - **Identify** hidden or obfuscated data
 - **Understand** Base64 as used in email headers, HTTP payloads, and databases
4. **Interpret** and **convert** timestamp formats
 - **Explain** the concept of EPOCH date-time values and encoded date-time values
 - **Work** with common forensic timestamp formats and **convert** between formats using command-line and GUI tools
 - DOS date and time (encoded)
 - Windows FILETIME (EPOCH)
 - UNIX timestamp (EPOCH)
5. **Recognise** and **convert** string encodings

- **Distinguish** between ASCII, Latin1, UTF-8 and UTF-16LE in hex dumps
- **Understand** the impact of endianness in UTF-16 encoding
- **Convert** between encodings and **recover** readable text from raw hex
- **Identify** forensic relevance of encodings (e.g., system language, obfuscation techniques, artefacts in memory or files)



Related Forensic Process Stages

 **Analysis**

 **Documentation**

 **Presentation**

6.1.4. 0104 – Forensic Copy

The applicant is able to:

- **Understand** and **apply** the process to **create** forensic copies (bit-by-bit copies) of mass storage devices
- **Focus** on image acquisition, integrity with cryptographic hashes, with free and open-source tools
- **Make** forensic copies in standard formats like EWF (Expert Witness Format) and RAW (dd format)



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.5 hours
Labs	1.5 hours
Total	3 hours



Prerequisites

The applicant should prove the knowledge of:

- Use operating systems (intermediate knowledge)
-  0103 - Computer Data ^[p.18]
-  0105 - Hashing (L1) ^[p.21]  ^[p.18]

Detailed Description

The applicant should be able to:

1. **Demonstrate** an understanding of what a forensic copy is
 - Terminology (imaging, acquisition, forensic copy, cloning, backup)
 - Software and hardware write blockers
 - Difference between logical and physical forensic images
 - Importance of cryptographic hashes to verify the integrity of forensic copies integrity
 - Standard forensic copy of usual file formats: RAW and EWF
 - Storage device technology impact on the forensic approach (SSD, Mobile Forensics)
2. **Create** forensic copies
 - Sanitisation of the storage destination device
 - Open-source and free tools (CLI and GUI)
 - Identification of the best tool to make forensic copies for each case
 - EWF compression and analysis performance
 - Document the acquisition: case number, device details, acquisition steps, tools used, hash results and expert name

Related Forensic Process Stages

 **Extraction/Preservation**

6.1.5. 0105 – Hashing (L1)

The applicant is able to:

- **Validate** a forensic copy of evidential material
- Critically **appraise** different hashing algorithms and their suitability to forensic domains

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	1 hours
Labs	1 hours
Total	2 hours



Prerequisites

The applicant should prove the knowledge of:

- Methods for copying digital media, such as the dd command, or similar (basic knowledge)



Detailed Description

The applicant should be able to:

1. **Explain** the fundamental hashing concepts, including (non-)cryptographic hash functions.
2. **Describe** the purpose of hashing and its relevance to digital forensics and evidential integrity
3. **Identify** and mitigate common vulnerabilities related to hashing, such as collisions and weak algorithms
4. **Compare** and contrast different hashing algorithms and their ideal use cases
5. **Validate** the integrity of a forensic copy



Related Forensic Process Stages

[Analysis](#)[Documentation](#)

6.1.6. 0106 – Mounting

The applicant is able to:

- Safely **mount** a forensic image acquired at the byte level and provided in the usual format
- **Access** the file system, including the encrypted ones, in order to **browse** and **process** files in a forensic way



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	4 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic OS command line skills

-  0103 - Computer Data ^[p.18]
-  0104 - Forensic Copy ^[p.20]
-  0301 - exFAT ^[p.35]
-  0302 - NTFS (L1) ^[p.36]  ^[p.36]  ^[p.35]

Detailed Description

The applicant should be able to:

1. **Recognise** forensic evidence formats by **identifying** images in EWF, AFF and standard raw (.dd) formats
2. **Provide** evidence integrity information by **using** tools to **verify** image hash and metadata
3. **Identify** partition scheme and related file systems by **determining** offsets and file systems within the forensic image
4. **Mount** a read-only volume from a forensic image
5. **Work** with encrypted partitions by **identifying** BitLocker-encrypted partitions and **mounting** them using the appropriate password/key
6. **Browse** the (unlocked) file system with the use of forensic tools to **explore** contents and **process** the files
7. **Document** the process to preserve the chain of custody and reproducibility for Court or audit purposes

Related Forensic Process Stages

 **Extraction/Preservation**

6.1.7. 0111 – String Encoding

The applicant is able to:

- **Understand** and **translate** string encodings, such as UTF-8 and UTF-16LE
- **Handle, convert** and **interpret** unsigned integer values

Version

2026-06-03

Level

Basic



Estimated Workload

Lessons	2 hours
Labs	3 hours
Total	7 hours



Prerequisites

The applicant should prove the knowledge of:

- Access to raw data
- 0103 - Computer Data ^[p.18]



Detailed Description

The applicant should be able to:

1. **Distinguish** between various string encodings by **interpreting** raw binary/hex data to identify ASCII, Latin1, UTF-8 and UTF-16LE timestamps
2. **Understand** the impact of endianness in string encoding
3. **Convert** encodings and recover readable text from raw data
4. **Identify** the forensic relevance of string encodings, considering system language, obfuscation techniques, artifacts in memory or files



Related Forensic Process Stages

Analysis

Documentation

Presentation

6.1.8. 0112 – Date Time Stamps

The applicant is able to:

- **Understand** and **convert** various timestamps that are commonly encountered in digital forensic examinations
- **Handle, convert** and **interpret** various timestamps from raw data



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	4 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- Access to raw data
- 0103 - Computer Data ^[p.18]



Detailed Description

The applicant should be able to:

1. **Describe** the concept of epochs, in relation to digital timestamps
2. **List** common timestamps encountered during digital investigations
3. **Demonstrate** the impact of endianness in timestamp encoding
4. **Discuss** the evidential importance of timezone accuracy when converting timestamps from raw data by **accommodating** daylight savings in evidential reports
5. **Translate** common timestamps from raw data to human-readable date-times, including main timestamps (Unix Epoch, FAT, Windows 64 (BE/LE))



Related Forensic Process Stages

 **Analysis**

 **Documentation**

 **Presentation**

6.1.9. 0115 – Computer Memory

The applicant is able to explain the role of computer memory, distinguish common memory types, and describe why volatile memory can contain high-value forensic evidence.



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	1 hours
Total	4 hours



Prerequisites

The applicant should prove the knowledge of:

- 1101 - Computer Architecture ^[p.150]



Detailed Description

The applicant will be able to:

- **Describe** the purpose of memory in computer systems and why it matters to investigations.
- **Define** common terminology: RAM, ROM, cache, registers, virtual memory, pages, frames, stack, heap, kernel space, user space.
- **Distinguish** volatile and non-volatile memory and explain what changes when a system is powered off, suspended, hibernated, or crashed.
- **Explain** common RAM and storage-backed memory artefacts such as hibernation files, crash dumps, pagefiles, swap files, and compressed memory.
- **Compare** high-level memory behavior across physical systems, virtual machines, and cloud/hosted environments.
- **Identify** the types of evidence commonly found in memory: processes, network connections, loaded modules, credentials, encryption material, command history, malware traces, and recently accessed data.



Related Forensic Process Stages

Identification



Observations

This credential should remain conceptual and **should not duplicate acquisition or analysis tool workflows.**

6.1.10. 0116 – Encoding

The applicant is able to:

- **Do** this thing
- **Do** this other thing
- ...

**Version**

2026-06-03

**Level**

Basic / Intermediate / Advanced

**Estimated Workload**

Lessons	X hours
Labs	X hours
Total	X hours

**Prerequisites**

The applicant should prove the knowledge of:

- ...
- ...

**Detailed Description**

The applicant should be able to:

- ...
- ...

**Related Forensic Process Stages** **Identification** **Extraction/Preservation** **Analysis** **Documentation** **Presentation**

6.1.11. 0117 – Virtual Machines

The applicant is able to explain virtualisation concepts, identify common virtual-machine artefacts, and preserve VM state relevant to memory forensics.

**Version**

2026-06-03

**Level**

Intermediate



Estimated Workload

Lessons	2 hours
Labs	2 hours
Total	4 hours



Prerequisites

The applicant should prove the knowledge of:

- 1101 - Computer Architecture ^[p.150]
- 0115 - Computer Memory ^[p.56]



Detailed Description

The applicant should be able to:

- **Discuss** the purpose of virtualisation and **list** the scenarios where virtual machines may be encountered
- **Differentiate** Type 1 and Type 2 hypervisors and identify common platforms such as VMware, VirtualBox, Hyper-V, KVM/QEMU, and cloud hypervisors.
- **Discuss** the features of virtual machines (e.g., snapshots, portability, resource sharing, security)
- **Demonstrate** how to build a virtual machine and **create** and restore a snapshot
- **Preserve** VM artifacts without accidentally resuming, modifying, consolidating, or deleting snapshots.



Related Forensic Process Stages

Identification

Extraction/Preservation



Observations

Avoiding making this a general virtualisation administration course; keep the emphasis on evidence preservation and memory state.

6.1.12. 0201 – File Embedded Metadata

The applicant is able to:

- **Recover** file metadata embedded in the file aside the ones provided by the file system layer
- **Explain** the difference between the file system layer and embedded metadata, and how it impacts the forensic interpretation



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	3 hours
Total	5 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic command-line tools to display a file and save the resulting process to a file
- 0112 - Date Time Stamps ^[p.24]



Detailed Description

The applicant should be able to:

1. **Explain** the principle of embedded metadata, as examples:
 - Time of creation of a picture
 - Location in space
 - Software used
2. **Recover** the file's embedded metadata for, as examples:
 - Image files
 - Audio files
 - Video files
 - Document files
3. **Explain** the forensic importance of the embedded metadata (travelling with the file) and compare date-time differences



Related Forensic Process Stages

 **Analysis**



Observations

Location in time and space requires a specific methodology to check the accuracy and report, which will be covered in specific MCs.

6.1.13. 0202 – Carving (L1)

The applicant is able to:

- **Use** of forensic tools for automatically carving files



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1 hours
Labs	2 hours
Total	3 hours



Prerequisites

The applicant should prove the knowledge of:

- Computer data representations and file systems (allocated/unallocated space)



Detailed Description

The applicant should be able to:

1. **Describe** what data carving is and how files can be recovered from file systems
2. **Identify** file type by recognising file signatures
3. **Explain** where file signatures can be located on the device (embedded files and issues with the sector boundaries carving process)
4. **Understand** the obstacles to and limitations of manual carving
5. **Evaluate** and critically **appraise** various carving tools



Related Forensic Process Stages

 **Extraction/Preservation**

 **Analysis**

6.1.14. 02A02 – Carving (L2)

The applicant is able to:

- **Use** advanced carving techniques to **address** the limitations of the basic carving process by **rebuilding** fragmented files, **recovering** potential file system metadata, **carving** items that are notfiles and **rebuilding** partition structures



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	2 hours
Labs	4 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- 0202 - Carving - Level 1 ^[p.26]
- 0302 - NTFS (L1) ^[p.36]
- 0103 - Computer Data ^[p.18]



Detailed Description

The applicant should be able to:

1. **Identify** when to utilise manual carving instead of automated carving techniques
2. **Explain** the file system management for the usual file systems (boot record, cluster size, file catalogue, allocation and chaining of clusters)
3. **Differentiate** between different file signatures and recognise their importance for carving
4. **Identify** and **locate** fragmented files on a storage device
5. **Identify** and **locate** non-file items on storage devices (boot record, MFT records, ...)
6. **Analyse** and **rebuild** the partitions configuration
7. Manually **carve** and **reconstruct** various types of fragmented files by using file system properties
8. **Validate** the successful reconstruction of files
9. **Report** and **explain**
10. **Appreciate** the obstacles and challenges to successful file carving



Related Forensic Process Stages

[Extraction/Preservation](#)[Analysis](#)[Documentation](#)[Presentation](#)

6.1.15. 0203 – Regular Expressions (L1)

The applicant is able to:

- **Understand** the structure of regular expression and their usage
- **Search** / **match** patterns using regex



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	4 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic command line tools to display a file and save the resulting process to a file



Detailed Description

The applicant should be able to:

1. **Explain** what a regular expression is, how it is used, and be aware of the different syntax depending on the flavour
2. **Identify** the most used regex tokens and **explain** their use
 - Quantity: zero or one, zero or more, one or more, exactly n, etc.
 - Common tokens: digit, word, whitespace, etc.
 - Character in a range
 - Negative selection
 - Anchors: start of a string, end of a string, etc.
 - General tokens: newline, tab, carriage return, etc.
3. **Identify** common errors in regex syntax

- Wrong character
- Wrong use of separators
- Including unnecessary spaces
- Missing brackets
- Incorrect usage of anchors
- Wrong quantifiers
- No escape for special character
- Unnecessary backslashes

4. **Read** and **describe** existing regex

5. **Write** a new regex to match patterns

6. **Validate** regex using scripts (e.g., Python library, etc.), GUI tools and ad-hoc testing files

7. **Filter** data to isolate the pattern of interest

8. **Explain** the importance of such filtering in a forensic context



Related Forensic Process Stages

 **Analysis**

Observations

The MC does not cover:

- Substitution with regular expression
- Grouping with regex or more advanced queries / research

6.1.16. 0204 – CSV Parsing

The applicant is able to:

- **Understand** the structure of CSV files and **handle** various data formats
- **Parse** a CSV file using appropriate tools to **transform** raw data logs into structured, human-readable information for an investigation



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	3 hours
Total	5 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic command line and GUI tools to display a file and save the resulting process to a file



Detailed Description

The applicant should be able to:

1. **Explain** the structure of CSV files (headers, records, fields, delimiters (e.g., ',', ';', '\t'), quotation rules)
2. **Identify** and **convert** custom encodings and **understand** encoding issues in CSV parsing
3. **Handle** non-standard formats
 - Fields containing embedded delimiters or line breaks
 - Custom timestamp formats (e.g., YYMMDD:HH:MM)
 - Missing or null fields
 - Anonymised or masked values
4. **Identify** common errors in CSV format
 - Distinct Separator
 - Separator inside value
 - Column number
 - Unsupported character
 - Character not escaped
 - Wrong File encoding
5. **Parse** and **validate** CSV content using command-line utilities (e.g., awk, csvtool, Python library) and GUI tools
6. **Filter** or **transform** data to **isolate** transactions or records of interest (by date, amount, location, ...)
 - Filter a column on a specific criterion
 - Filter a row on a specific criterion
 - Count occurrences of certain information in a specific column (sort by column number)
 - Count occurrences of certain information in a specific column (sort by column header)
 - Filter row having a specific information in common
 - Filter row having several information in common
 - Filter row using an operator on a row with an integer format
 - Remove duplicates

7. **Explain** the importance of such filtering in a forensic context

Related Forensic Process Stages

 **Analysis**

Observations

The MC does not cover:

- Correlating each field with its forensic meaning (e.g., card number field partially anonymised, "type" field with forensic logic value A, O, or C)

6.1.17. 0205 – JSON Parsing

The applicant is able to:

- **Understand** the structure of JSON files and **handle** various data format
- **Parse** a JSON file using appropriate tools to **transform** raw data logs into structured, human-readable information for an investigation

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	1 hours
Labs	4 hours
Total	5 hours

Prerequisites

The applicant should prove the knowledge of:

- Basic command line tools to display a file and save the resulting process to a file

Detailed Description

The applicant should be able to:

1. **Explain** the structure of JSON files (key, values, delimiters, quotation rules)
2. **Identify** common errors in JSON format

- Brackets (unclosed dictionaries/arrays, mismatched brackets/braces)
 - Trailing comma (missing or extra)
 - Unsupported character
 - Character not escaped
 - Invalid Data type
 - Improper use of quotes (simple, double)
 - Nested JSON format
3. **Parse** and **validate** JSON content using command-line utilities (e.g., jq, sed, awk, Python library) and GUI tools
 4. **Filter** or **transform** data to isolate transactions or records of interest
 - Filter by key or key/value
 - Filter on several key
 - Count occurrences of a specific key or key/value
 - Reverse filter on a key/value
 5. **Explain** the importance of such filtering in a forensic context



Related Forensic Process Stages

 **Analysis**

Observations

The MC does not cover:

- Interpretation of JSON file content in forensic investigation
- Mathematical operation on JSON integer values (addition, subtraction, multiplication, selection on criteria as lower/greater than)

6.1.18. 0206 – XML Parsing

The applicant is able to:

- **Understand** the structure of XML files and **handle** various data formats
- **Parse** a XML file using appropriate tools to **transform** raw data logs into structured, human-readable information for an investigation



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1 hours
Labs	2 hours
Total	3 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic command line and GUI tools to display a file and save the resulting process to a file



Detailed Description

The applicant should be able to:

1. **Explain** the structure of XML files (headers, records, fields)
2. **Identify** common errors in XML format
3. **Parse** and **validate** XML content using command-line utilities and GUI tools
4. **Filter** or **transform** data to isolate transactions or records of interest
5. **Explain** the importance of such filtering in a forensic context



Related Forensic Process Stages

 **Analysis**



Observations

The MC does not cover:

- Correlating each field with its forensic meaning

6.1.19. 0207 – Database Fundamentals

The applicant is able to:

- **Describe** the concept of relational database
- **Build** basic SQL queries
- **Use** SQLite, **open** a database of multiple tables and **join** tables to **visualise** and **export** data



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	5 hours
Total	8 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic command-line tools
- 0204 - CSV Parsing ^[p.29]



Detailed Description

The applicant should be able to:

1. **Explain** the role of rows, columns (records, fields), and keys using an example of a minimum of two joint tables
2. **Explain** the limitations of SQLite compared with SQL and other relational multi-user DB services
3. **Execute** basic SQL queries using the *select, from, where, group by*
4. **Open** a SQLite DB of multiple tables using a SQLite GUI viewer/editor
 - **Identify** the number of records in each table
 - **Identify** the keys to link tables
 - **Select** the columns to display
 - **Filter** the displayed rows based on a matching string criterion
 - **Export** to CSV
5. **Use** a SQLite DB of multiple tables, a CLI viewer/editor
 - **Open** an SQLite DB
 - **Display** and **export** the structure for reporting
 - **Make a simple query** to display columns from 2 different linked tables
 - **Filter** on strings
 - **Use** aggregation functions (i.e sort by, group by)
 - **Export** to CSV
6. **Convert** the date-time value to a human-readable string using the SQLite query features



Related Forensic Process Stages

Analysis

Observations

The MC does not cover:

- The whole SQL language and DB services, multi-users, etc (only SQLite format)

Comments:

- Analysed DBs are usually encountered, i.e. Web history, Chat applications
- Date-Time value to convert: Webkit?

6.1.20. 0211 – Browser History Forensics

The applicant is able to:

- **Prove** intent and sequence (search terms → click → download/execution)
- **Trace** initial compromise and data exfiltration
- **Attribute** actions to a specific Windows user/profile and **detect** profile hopping or portable browsers
- **Corroborate** with NTFS/EVTX/SRUM/Prefetch/LNK to **raise confidence** and **spot** anti-forensics (cleared history, selective deletions, suspicious extensions)
- **Support** court-ready reporting (hashes, tool versions, TZ/DST-normalized times, scope/GDPR)



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	4 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

-  0112 - Date Time Stamps ^[p.24]
-  0207 - Database Fundamentals ^[p.32]
-  0304 - Windows Event Logs ^[p.38]

Detailed Description

The applicant should be able to:

1. Safely **preserve** multi-profile browser data without altering evidence (read-only workflows)
2. **Parse** and **interpret** History (SQLite) via urls, visits, visit_source, downloads, keyword_search_terms
3. **Analyse** autofill, login data (respecting legal constraints and scope)
4. **Analyse** sessions/tab restore, local storage and indexed DB (LevelDB), cache/code cache, favicons, top sites, extensions
5. **Convert/normalise** Chromium timestamps (WebKit time μ s since 1601-01-01) and **correlate** across sources
6. **Detect** private mode traces (limitations), anti-forensics (cleanups, profile hopping, containerised browsers)

Related Forensic Process Stages

[📄 Analysis](#)
[📄 Documentation](#)

Observations

Extended learning objectives can be:

1. **Be able to work** with Edge and Chromium profiles on Windows
2. **Retrieve** the history and downloads
 - History (SQLite -mark this as a prerequisite): tables & joins (urls $\leftrightarrow$ visits $\leftrightarrow$ visit_source), transition types, typed vs. link, search terms
 - Downloads: downloads, downloads_url_chains, target_path, referrers, interruptions
 - Normalisation of WebKit timestamps (mark this a **prerequisite**), time-zone/DST pitfalls
3. **Analyse** cookies, autofill, logins
 - Cookies DB schema (host_key, name, encrypted_value, expires_utc)
 - Autofill (Web data), login data (metadata handling when decryption is out of scope)
 - Evidential value & limits
4. **Be able to retrieve** information on sessions, storage and cache

6.1.21. 0301 – exFAT

The applicant is able to:

- **Understand** the role of exFAT in digital forensics
- **Use** open-source tools, **analyse**, **interpret**, and **investigate** digital evidence on exFAT file systems

Version

2026-06-03

**Level**

Basic

**Estimated Workload**

Lessons	3 hours
Labs	3 hours
Total	6 hours

**Prerequisites**

The applicant should prove the knowledge of:

- 0103 - Computer Data ^[p.18]
- 0111 - String Encoding ^[p.23]
- 0112 - Date Time Stamps ^[p.24]

**Detailed Description**

The applicant should be able to:

1. **Understand** the fundamentals of exFAT and how it can affect digital forensics investigations
2. **Identify** the exFAT system files and **explain** their role
3. **Explain** the working of the \$Bitmap
4. **List** file records entries (active and inactive) and **extract** essential file metadata (file name, date-time values, file size, first cluster)
5. **Explain** the processes related to file move, renaming and deleting and the related impact on exFAT structures
6. **Exploit** techniques and tools for recovering deleted files on exFAT volumes
7. **Use** exFAT time stamps to allow the creation of timelines
8. **Extract** the cluster slack

**Related Forensic Process Stages**
 **Analysis**
6.1.22. 0302 - NTFS (L1)

The applicant is able to:

- **Understand** the role of NTFS in digital forensics
- **Use** open-source tools, **analyse**, **interpret**, and **investigate** digital evidence on NTFS file systems used in Windows environments



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	3 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- 0103 - Computer Data ^[p.18]
- 0111 - String Encoding ^[p.23]
- 0112 - Date Time Stamps ^[p.24]



Detailed Description

The applicant should be able to:

1. **Explain** the fundamentals of NTFS structures and how they can affect digital forensics investigations
2. **Explain** the core system file key features and their interaction with Windows OS features (OS, Applications, file system driver)
3. **Analyse** the Master File Table (MFT) for file recovery and timeline reconstruction
4. **Explain** the difference between residential and non-residential file record attributes
5. **Identify** NTFS file attributes, security descriptors, and access control lists for evidence gathering
6. **Recover** deleted files from an NTFS partition (without mounting)
7. **Extract** file metadata for allowing timeline analysis using NTFS-specific timestamps
8. **Export** the content from identified Alternate Data Streams (ADS)
9. **Extract** the history for a file, if available, from the USN Journal \$J file
10. **Export** MFT record slack and cluster slack content
11. **Demonstrate** awareness of the detection of anti-forensics



Related Forensic Process Stages

Analysis

6.1.23. 03A02 – NTFS (L2)

The applicant is able to:

- **Analyse** NTFS volumes at byte level



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	6 hours
Labs	6 hours
Total	12 hours



Prerequisites

The applicant should prove the knowledge of:

- 0103 - Computer Data ^[p.18]
- 0111 - String Encoding ^[p.23]
- 0112 - Date Time Stamps ^[p.24]
- 0202 - Carving - Level 1 ^[p.26]
- 02A01 - Carving - Level 2 ^[p.62]
- 0302 - NTFS (L1) ^[p.36]



Detailed Description

The applicant should be able to:

1. **Apply** best practices for mitigating challenges such as anti-forensic techniques and encrypted data
2. **Export** sparse and encrypted files
3. **Analyse** and **rebuild** data runs
4. **Repair** damaged \$boot
5. **Carve** MFT records and **rebuild** damaged MFT
6. **Mount** shadow copies



Related Forensic Process Stages

[Analysis](#)

6.1.24. 0303 – Windows Recycle Bin

The applicant is able to:

- **Explain** the Windows deletion process of deleted files stored in the recycle bin
- **Recover** the file and **provide** details about the deletion process



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	3 hours
Total	5 hours



Prerequisites

The applicant should prove the knowledge of:

- 0302 - NTFS (L1) [p.36]



Detailed Description

The applicant should be able to:

- **Explain** how recycled files are stored in the folder structure when examining a volume during the forensic process
- **Explain** the impact on the file renaming and \$I file in the MFT and **analyse** its content
- **Explain** the process of file recovery by the user and potential traces
- **Liaise** with the \$Journal history to **provide details** about the deletion process



Related Forensic Process Stages

[Analysis](#)

6.1.25. 0304 – Windows Event Logs

The applicant is able to:

- **Explain** the role of Windows Event Logs
- **Identify** most common Windows Channel and EventID and their usage
- **Be able to search** for specific logs in EventViewer or in .evtx files



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	2 hours
Total	4 hours



Prerequisites

The applicant should prove the knowledge of:

- 0206 - XML Parsing ^[p.67]



Detailed Description

The applicant should be able to:

- **Localise** Windows Event Logs
- **Explain** the role of Windows Event Logs
- **Identify** different Windows Provider / EventID (automatically generated by the system or generated by user activity)
- **Open** or **parse** the Event Logs with GUI or command line tools to **recover** and **export** in a human-readable form
- **Identify** the most important EventID for a forensic investigator (account manipulation, login, deletion, ...)
- **Search** for specific logs in EventViewer or in .evtx files
- **Understand** and **interpret** key/values in the most common Windows Event Logs



Related Forensic Process Stages

Analysis

Observations

The MC does not cover:

- Reconstruction of user or system activity or the anti-forensics methods detection

6.1.26. 0305 – Windows Prefetch

The applicant is able to:

- **Enable** the identification, extraction, interpretation, and correlation of Windows artifacts in forensic investigations, focusing mainly in prefetch and log analysis
- **Reconstruct** user activity (executions, open documents, external devices used)
- **Reconstruct** system activity (software installation, services, scheduled tasks, persistence)

Version

2026-06-03

Level

Basic



Estimated Workload

Lessons	2 hours
Labs	2 hours
Total	4 hours

Prerequisites

The applicant should prove the knowledge of:

-  0112 - Date Time Stamps ^[p.24]
-  0301 - exFAT ^[p.35]
-  0302 - NTFS (L1) ^[p.36]



Detailed Description

The applicant should be able to:

- **Interpret** key fields of prefetch (.pf), jump lists, and LNK to infer what was executed, when, and from where
- **Enumerate** and **analyse** scheduled tasks, their triggers, and their history (EVTX / XML on disk)
- **Detect** WMI persistence (event filters/consumers/bindings) and suspicious BITS jobs
- **Use** Windows Error Reporting (WER) artefacts and dumps to **pivot** to binaries/paths and moments of crash/execution



Related Forensic Process Stages

 **Analysis**

6.1.27. 0306 – Windows Registry Analysis

The applicant is able to:

- **Explain** the role of Windows Registry Hives
- **Extract** keys and values in a human-readable form with an explanation about the forensic interest and ways to cross-check the findings



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	4 hours
Total	7 hours



Prerequisites

The applicant should prove the knowledge of:

- Access to NTFS file systems using digital forensic software
- Installation of dedicated tools (regripper, RegExplorer, ...)
- Data types (strings, integer, ...)



Detailed Description

The applicant should be able to:

1. **Localise** and **recover** the registry hives
2. **Open** or **parse** the registry hives with GUI or command line tools to **recover and export** in a human-readable form
 - Registered users and related properties, including accesses and information related to the use of a Microsoft Account (SAM)
 - USBdevices (SYSTEM)
 - USBSTOR (SYSTEM)
 - Mounted devices (SYSTEM)

- Bluetooth devices (SYSTEM)
- Time zone (SYSTEM)
- Networks list (SOFTWARE)
- Uninstalled software (SOFTWARE)
- OneDrive (USER)
- Typed URLs (USER)
- Recent documents (USER)
- User assists (USER)
- Jump lists (USER)

3. **Explain** the forensic importance of each of the key/values exported and, if any, how it can be cross-checked with other information.



Related Forensic Process Stages

 **Analysis**



Observations

The MC does not cover:

- How to access the registry hives

Comments:

- Cross-check can be performed using FS metadata, \$J or event logs. The FiRST report is not considered a valid cross-check as it uses the registry to provide the information.

6.1.28. 0307 - Windows Process Analysis (L1)

The applicant is able to:

- **Understand** The Windows process concepts
- **Perform** Process enumeration and triage
- **Identify** unexpected behavior of a process.



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	10 hours
Total	12 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic Computer Architecture (TBC)
- 📄0102 - Reporting ^[p.17]
- 📄0306 - Windows Registry Analysis ^[p.40]
- 📄 ^[p.17] 📄0309 - Windows Portable Executable Analysis ^[p.82]
- 📄0314 - Windows Services ^[p.89]



Detailed Description

The applicant should be able to:

1. **Define** core terms: process, thread, handle, token, session, service, parent/child process, job object.
2. **Describe** the Windows process lifecycle (creation → execution → termination) at a high level.
3. **Identify** common user-mode vs kernel-mode boundaries relevant to process artefacts.
4. **Recognise** common legitimate Windows processes and their typical roles.
5. **Explain** why command-line arguments, environment, and parent process context matter in investigations.
6. **List** processes from a live system.
7. **Identify** and **Collect** basic process metadata.
8. **Classify** processes into "expected vs unexpected" based on host role and context.
9. **Prioritise** processes for deeper review using simple indicators.
10. **Interpret** command lines to **infer** basic intent (downloaders, LOLBins usage, script engines).
11. **Describe** the behavior of a process on a Windows machine in a dedicated report.



Related Forensic Process Stages

📄Analysis

📄Documentation

📄Presentation



Observations

TO BE REVIEWED BY THE TEAM.

6.1.29. 0308 – Windows Command Line and PowerShell

The applicant is able to:

- **Operate** with fluency (and safely) with the console.
- **Understand** the filesystem structure and be able to operate in (with) it.
- **Understand** and apply operations with processes (start, stop, list, query services, ...)
- **Understand** how to interface with the operating system (users, permissions, system info, networking...).
- **Apply** basic scripting to automate tasks (note to self: probably remove this)



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	4 hours
Labs	4 hours
Total	8 hours



Prerequisites

The applicant should prove the knowledge of:

- Windows Architecture foundations
- Basic Programming skills (if scripting section is not removed)



Detailed Description

The applicant should be able to:

- **Operate** the terminal fluently
 - Open and use **Command Prompt vs PowerShell** appropriately (and know when admin rights are needed).
 - Use **help** effectively (help, /?, Get-Help, Get-Command).
 - Work with **paths, quoting, wildcards**, and environment variables.
 - Redirect/pipe output and create readable logs (>, >>, |, Select-String, Out-File).
- **Interact** and **understand** the filesystem underneath
 - Deal with files and folders:
 - CMD: dir, copy, move, del, mkdir, rmdir

- PS: Get-ChildItem, Copy-Item, Move-Item, Remove-Item, New-Item
- Find files by a criteria and basic content searching:
 - CMD: where, findstr
 - PS: Get-ChildItem -Recurse, Select-String
- Basic archiving tasks: zip/unzip via PowerShell or built-in utilities.
- **Manage** processes and services
 - List and manage processes:
 - CMD: tasklist, taskkill
 - PS: Get-Process, Stop-Process
 - Start/stop/query services:
 - CMD: sc, net start/stop
 - PS: Get-Service, Start-Service, Stop-Service
 - Troubleshoot steps.
- **Implement** and automate tasks
 - System information gathering, networking and connectivity.
 - User management, groups,
 - Software management.
- **Logging** and system observability
 - PS: Get-WinEvent
 - CMD: wevtutil

6.1.30. 0309 – Windows Portable Executable Analysis

The applicant is able to:

Explain the Portable executable purpose and structure.

Perform the safe handling and acquisition of a PE sample.

Perform the static analysis of a PE Sample and interpret the possible capabilities.



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	10 hours
Total	13 hours



Prerequisites

The applicant should prove the knowledge of:

- 9902 - Hexadecimal Viewer ^[p.43]



Detailed Description

The applicant should be able to:

- **Define** what a PE file is and **differentiate** PE types (EXE, DLL, SYS, etc.).
- **Identify** the main PE components: DOS header, NT headers, optional header, section table, sections.
- **Manipulate** safely a Portable Executable and ensure chain of custody.
- **Describe** (at a high level) the Windows loader's role in mapping a PE into memory.
- **Extract** basic file metadata (size, timestamps when available, compilation timestamp caveats).
- **Extract** relevant information about the **potential** capabilities of a Portable Executable (static analysis).



Related Forensic Process Stages

Identification

Analysis

Documentation

Presentation

6.1.31. 0310 – Windows Critical Directories

The applicant is able to:

- **Identify** the security-relevant map of Windows 11 directories.
- **Identify** common per-user data locations. may be we can merge 1st and 2nd?
- **Interpret** temporary and cache paths (TEMP/TMP, common internet cache locations) ¿collide with browser mc?
- **Identify** where Windows stores key forensic logs and diagnostics on disk.
- **Identify** on-disk registry hive storage locations (system hives and user hives).
- **Interpret** high-level access/permissions differences between shared vs per-user directories.



Version

2026-06-03

**Level**

Basic



Estimated Workload

Lessons	2 hours
Labs	2 hours
Total	4 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic OS knowledge (Microsoft Windows)
- MC Filesystem?



Detailed Description

The applicant should be able to:

- **Identify** critical Windows directories and their purposes (e.g., C:\Windows\System32, SysWOW64, Temp, Program Files, ProgramData, user profile paths, Startup locations).
- **Describe** common file types found in each area (executables, drivers, configs, logs, scheduled task XML, shortcuts).
- **Explain** the 32-bit vs 64-bit layout basics (System32 vs SysWOW64) and why it matters during triage.
- **Use** built-in tools to navigate and query the filesystem safely (Explorer properties, dir, where, basic PowerShell listing).
- **Collect** directory listings and basic metadata (paths, sizes, timestamps, owners when accessible).
- **Extract** persistence-relevant artifacts from key locations (Startup folders, ProgramData, user temp drop locations, common “living-off-the-land” staging paths).
- **Compare** directory contents against expected baselines for a workstation/server role (what “belongs” vs what stands out).
- **Classify** findings into benign/admin vs suspicious (unexpected executables in user-writable dirs, masquerading names, odd nesting).
- **Detect** simple red flags (system binaries outside Windows directories, unsigned binaries in critical paths, hidden/system attribute abuse where visible).
- **Document** a concise map of “what was found where” including paths, hashes, and why each item matters.



Related Forensic Process Stages

**Identification****Extraction/Preservation****Analysis****Documentation****Presentation**

6.1.32. 0311 – Windows History

The applicant is able to:

- **Explain** the two major Windows lineages (DOS-based *Windows 9x* vs *Windows NT*).
- **Justify** why NT became the foundation for modern Windows.
- **Compare** core kernel design concepts across eras (stability, isolation, privilege separation)..
- **Identify** Windows execution primitives (processes vs threads).
- **Compare** 32-bit vs 64-bit address-space realities.
- **Interpret** how signing requirements affect IR triage.



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1 hours
Labs	0 hours
Total	1 hours



Prerequisites

The applicant should prove the knowledge of:

- Basic computer architecture.
- Basic DFIR.



Detailed Description

The applicant should be able to:

- Understand the difference between Windows lineages:
 - **Compare** core kernel design concepts across eras (stability, isolation, privilege separation)
 - **Map** these to operational consequences for defenders
 - **Identify** Windows execution primitives (processes vs threads)
- Core kernel design concepts:
 - **Explain** the user-mode vs kernel-mode boundary
 - **Interpret** why crossing that boundary changes risk and evidence value (drivers, core OS components)
 - **Map** these to operational consequences for defenders

- **Explain** how virtual memory and paging relate to system stability and forensic visibility, including what the page file contributes to “committed memory.”
- 16-32-bit vs 64-bit address-spaces
 - **Understand** 16bit booting of the system (real mode)
 - **Interpret** why larger virtual address spaces change both reliability and mitigation effectiveness
 - **Map** major mitigation milestones to Windows generations: **DEP/NX** (Windows XP/Server 2003+), **ASLR** (Windows Vista+), **CFG** (supported on modern Windows client/server)
 - **Interpret** what each is intended to prevent
 - **Explain** (conceptually) how these mitigations reduce common tampering and hooking opportunities.
- Identify the role of driver signing policies in kernel trust:
 - **Interpret** how signing requirements affect IR triage of suspicious drivers.



Related Forensic Process Stages

Identification

Extraction/Preservation

Analysis

Documentation

Presentation

6.1.33. 0312 – Windows Office Documents Analysis

The applicant is able to:

- **Identify** common Office file types and containers (DOC/DOCX, XLS/XLSX, PPT/PPTX, RTF, OLE/CFB vs OOXML/ZIP).
- **Describe** typical document components relevant to analysis (streams, relationships, embedded objects, macros, templates).
- **Explain** common attack surfaces: VBA macros, DDE, OLE embedded content, remote templates, ActiveX, exploit-style documents.
- **Use** safe-handling workflows (isolated VM, disable macros, no network, read-only extraction).
- **Extract** indicators from documents (URLs/domains, file paths, suspicious commands, template URIs, embedded executables).
- **Detect** basic obfuscation and evasion clues (encoded strings, split keywords, unusual metadata, high-entropy blobs, malformed structure warnings).



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	4 hours
Labs	2 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- 0310 - Sample Micro-Credential description ^[p.83]
- 0206 - XML Parsing ^[p.67]



Detailed Description

The applicant should be able to:

- **Interpret** what is the implication that an OOXML is a ZIP packet with parts and relationships. And **map** what parts are usually filled with content, metadata and external references.
- **Identify** macro-enabled extensions (i.e. .docm/.xlsm/.pptm) y **justify** why the ".m" suffix changes the risk level and the triage.
- **Explain** where are the relevant pieces of metadata stored in the OOXML (docProps/core.xml, docProps/app.xml) and interpret its forensic value, and its limitations.
- **Identify** typical risk signals in documents (not going into detail on how they are exploited): macros, embedded OLE objects, templates/external resources, obfuscated content, extension/structure incoherences, etc.
- **Explain** the role of **Mark of the Web (MoTW)** and the role of stream **Zone.Identifier** as an evidente, and **interpret** its impact in Office controls.
- **Interpret** the intention of the Protected View item and **justify** why it is a relevant control when doing evidences analysis.
- **Identify** which office controls can avoid opening/execution (file block settings) and **map** then on how they affect to the forensic analysis work flow (open vs statically extract,...).
- **Compare** internal structures in OOXML vs OLE/CFBF.
- **Report** the triage underlining risks and recommending next steps to follow.



Related Forensic Process Stages

Identification	Extraction/Preservation	Analysis	Documentation	Presentation
----------------	-------------------------	----------	---------------	--------------

6.1.34. 0313 – Windows Shadow Copies

The applicant is able to:

- **Understand** what is a snapshot vs set and interpret requester/writer/provider.
- **Understand** restore points.
- **Understand** and **Interpret** shadow storage.
- **Understand** Previous Versions local.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	2 hours
Labs	2 hours
Total	4 hours



Prerequisites

The applicant should prove the knowledge of:

- ...
- ...



Detailed Description

The applicant should be able to:

- **Explain** what is a shadow copy and differentiate individual shadow copies vs shadow copies sets (with IDs GUID).
- **Explain** the architecture of VSS (requester–writer–provider) and justify why it allows consistent “hot” captures (freeze/short thaw).
- **Identify** main sources for shadow copies in windows 11 (backup/restore points / recovery functions)
- **Identify** safely which shadow copies exist in the system under investigation. Map this information to triage decisions
- **Identify** where VSS storage context is at the system level (relationship with System Volume Information) and explain why it is a protected area.
- **Interpret** VSS writers state and justify its impact in relation to copy integrity.
- **Explain** how shadow copies are seized in a defense environmen

- **Identify** common risky patterns related to VSS (removal / absence of backups, configuration changes, VSS repeated errors) .
- **Produce** brief triage report.



Related Forensic Process Stages

 **Identification**
 **Extraction/Preservation**
 **Analysis**
 **Documentation**
 **Presentation**

6.1.35. 0314 – Windows Services

The applicant is able to:

- **Understand** what is SCM, SVCHOST and the grouping of services.
- **Explain** the architecture of the Service Control Manager (SCM).
- **Understand** types of start modes, trigger-start, services accounts permissions and DACL.
- **Understand** the services accountability, relation service-process and **identify** services properties (image path, account, dependencies, start type,...)
- **Identify** normal vs suspicious services.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	4 hours
Labs	2 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

-  0307 - Windows Process Analysis (L1) ^[p.79]
-  0310 - Microsoft Windows Critical Directories ^[p.83]

Detailed Description

The applicant should be able to:

- **Understand** when it boots, which its (SCM) role and why it is the orchestrator of the services.
- **Compare** services running within a process owned by the user vs services not in a process owned by the user. And **Interpret** the role of svchost.exe
- **Identify** the essential configuration elements of a service (name, binary/path, start, dependencies, account where it is running in) and **explain** where in the system they are reflected.
- **Interpret** the different types of starting (automatic, manual, disabled) and **explain** the concept of trigger-start (services started by events) and why they are relevant for the triage.
- **Compare** normal accounts where services are being (LocalSystem/LocalService/NetworkService) run and **justify** risks/evidences from the PoLP.
- **Identify** the permissions model (DACL/rights) on the service object and the SCM and **explain** why excessive permits are a defensive risk.
- **Explain** the concept of service hardening / isolation (SID) and **interpret** their intention: limit their lateral impact among services.
- **Identify** anomalous service alerts (binary in an unusual path, binary not signed, unusual privileged account, automatic start with no previous awareness).

Related Forensic Process Stages

 Identification	 Extraction/Preservation	 Analysis	 Documentation	 Presentation
--	---	--	---	--

6.1.36. 0315 – Windows Security Model

The applicant is able to:

- **Understand** tokens/SIDs/privileges; UAC; MIC; security descriptors; DACL/SACL; **explain** in a report the general authorization logic.
- **Interpret** read-only inspection of tokens/integrity level; high-level reading of ACLs (files/registry/services); basic reading of SDDL where applicable.
- **Explain** why something was allowed/denied; detect excessive permissions as a signal; prioritize what to validate and how to **document** it.

Version

2026-06-03

Level

Intermediate



Estimated Workload

Lessons	4 hours
Labs	2 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- 0306 - Windows Registry Analysis ^[p.40]
- 0310 - Microsoft Windows Critical Directories ^[p.83]
- 0314 - Windows Services ^[p.89]



Detailed Description

The applicant should be able to:

- **Explain** the Windows authorisation model (subject -> token -> object -> security descriptor) and **map** how an Allow/Deny decision is made.
- **Identify** the key components of an access token (SIDs, groups, privileges, restrictions) and **explain** why every process/thread carries a security context.
- **Compare** UAC and the concept of filtered vs elevated tokens, and **justify** why being an admin does not mean always running elevated.
- **Explain** Mandatory Integrity Control (MIC) and **interpret** why the integrity level is evaluated before the DACL in many access decisions.
- **Identify** what a security descriptor is (owner, DACL, SACL) and **explain** the difference.
- **Interpret** common "trap" rules in ACLs (total access / total access denial).
- **Identify** the role of SIDs (including well-known SIDs) and **map** who is who in real-world permissions (users, local/domain groups).
- **Explain** what privileges are and distinguish rights over objects (ACL) from system privileges (token), and **interpret** defensive implications.
- **Interpret** effective permissions in response scenarios.
- **Report** explaining the most likely cause of a permissions-related finding (normal vs misconfiguration vs suspicious activity) and **recommend** next verification steps.



Related Forensic Process Stages

Identification	Extraction/Preservation	Analysis	Documentation	Presentation
-----------------------	--------------------------------	-----------------	----------------------	---------------------

6.1.37. 0316 – Windows Credentials Protection

The applicant is able to:

- **Understand** Windows credential/secrets landscape and protection mechanisms (DPAPI, DPAPI-NG, Credential Manager/Locker, LSASS/LSA Protection, Credential Guard/VBS) and why they matter for intrusion and lateral movement.
- **Assess** an endpoint's identity security posture by interpreting on/off signals, **identifying** relevant evidence/telemetry, and prioritizing what to collect first in LEA triage.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	3 hours
Labs	3 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- 0315 - Windows Security Model ^[p.90]
- 0105 - Hashing (L1) ^[p.21]
- 0410 - Decryption Strategy ^[p.106]



Detailed Description

The applicant should be able to:

- **Explain** the map of secrets in Windows (hashes, tickets, keys, app-saved credentials) and **justify** why protecting them is critical in intrusion investigations and lateral movement.
- **Explain** the role of DPAPI as a user-/machine-level data protection mechanism and **interpret** its guarantees (typically same user and same machine).
- **Compare** classic DPAPI vs DPAPI-NG (CNG DPAPI) and **map** when each makes sense (protection for sets of principals vs local context).
- **Identify** what Credential Manager / Credential Locker are (may be from at a high level) and **interpret** what stored credentials means for triage (access persistence, reuse risk).
- **Explain** the role of LSASS/LSA in credential management and justify the goal of LSA Protection: reduce exposure to unauthorized injection/loading into the LSA process.

- **Explain** what Credential Guard is, interpret how it uses Virtualization-Based Security (VBS) to isolate secrets, and **justify** which attacks it aims to mitigate (conceptually).
- **Interpret** on/off signals of these protections on an endpoint (identity security posture) and **map** those signals to response decisions: which risks are plausible and which are reduced.
- **Identify** evidence sources and telemetry related to these protections (configuration, system state, and relevant events) and **justify** what to collect first in a LEA case.
- **Interpret** operational scenarios (suspected credential theft / remote session / posture change) and **produce** a cautious hypothesis based on the host posture and the type of credential involved.
- Draft a brief, reproducible **report** that describes: protection posture (DPAPI/Locker/LSA/Credential Guard), residual risks, and next defensive steps.



Related Forensic Process Stages

 Identification
  Extraction/Preservation
  Analysis
  Documentation
  Presentation

6.1.38. 0317 – Windows Bootchain Startup

The applicant is able to:

- **Understand** Secure Boot, Trusted Boot, Measured Boot (TPM), boot chain components, BCD and its purpose.
- **Interpret** Secure Boot/TPM status, safely inventory BCD.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	4 hours
Labs	4 hours
Total	8 hours



Prerequisites

The applicant should prove the knowledge of:

-  1101 - Computer Architecture ^[p.150]
-  0316 - Windows Credentials Protection ^[p.92]
-  0315 - Windows Security Model ^[p.90]

-  1104 - Bios Access ^[p.153]
-  1107 - TPM Chip ^[p.156]
-  0410 - Decryption Strategy ^[p.106]
-  0115 - Computer Memory ^[p.56]
- UEFI

Detailed Description

The applicant should be able to:

- **Explain** the modern boot chain in Windows 11 (from UEFI to Windows Boot Manager to loader to OS kernel).
- **Explain** what UEFI Secure Boot is and justify its objective: allow booting signed/trusted boot software (firmware, UEFI drivers, Option ROMs, EFI apps, OS).
- **Explain** trusted boot and interpret how protection continues after Secure Boot by verifying Windows boot components, reducing the load of corrupted/malicious components.
- **Explain** measured boot (TPM)
- **Understand** what BCD is and identify what type of information it stores and interpret a basic BCD inventory data to **respond** to IR questions like "which entry is used?", "are there multiple loaders?", "are there atypical parameters?".
- **Identify** relevant boot evidence sources : configuration (BCD), Secure Boot/Trusted Boot/TPM Status, and log channels linked to boot/servicing.
- **Interpret** defensive signals of possible manipulation or degraded postures (Secure Boot disabled, repeated boot component failures, anomalous configuration changes, ...)
- **Produce** a triage report

Related Forensic Process Stages

 Identification	 Extraction/Preservation	 Analysis	 Documentation	 Presentation
--	---	--	---	--

6.1.39. 0318 – Windows Virtualisation Subsystems

The applicant is able to:

- **Understand** VBS/VSM/HVCI; Hyper-V (root vs child partitions); WSL2 and ext4 VHD; typical paths/artifacts.
- **Verify** VBS/HVCI status (read-only); inventory Hyper-V VMs/artifacts; identify WSL distros and their VHD; **document** access via \wsl\$.
- **Infer** impact on scope/acquisition; prioritize evidence; **report** findings.

Version

2026-06-03

**Level**

Intermediate

**Estimated Workload**

Lessons	4 hours
Labs	4 hours
Total	8 hours

**Prerequisites**

The applicant should prove the knowledge of:

-  FS:001 File Systems Information
-  0301 - exFAT ^[p.35]
-  0302 - NTFS (L1) ^[p.36]
-  0316 - Windows Credentials Protection ^[p.92]
-  0115 - Computer Memory ^[p.56]
-  1101 - Computer Architecture ^[p.150]
-  0314 - Windows Services ^[p.89]
-  0117 - Virtual Machines ^[p.58]
-  0501 - Network Structures ^[p.111]

**Detailed Description**

The applicant should be able to:

- **Explain** the virtualization landscape in Windows 11 and distinguish three layers: Hyper-V (VM virtualization), VBS/VSM (security isolation on top of the hypervisor), and WSL2 (Linux in a lightweight VM).
- **Explain** what VBS is and **justify** its defensive objective (create a hypervisor-based isolated environment that is as a root of trust, even assuming kernel compromised).
- **Interpret** the role of Virtual Secure Mode (VSM) as a hypervisor mechanism that enables new security boundaries (e.g., the foundation for Credential Guard and others).
- **Explain** what Memory Integrity / HVCI is and **justify** why it changes the kernel threat model (code-integrity validation in an isolated environment and restrictions on executable pages).
- **Compare** classic vs virtualized artifacts and evidence surfaces (e.g., host processes/services vs vmmem/WSL/Hyper-V components) and **map** which forensic questions each can answer.
- **Identify** key Hyper-V artifacts (virtual disks, checkpoints/configuration) and **explain** why they are relevant for acquisition and incident scoping.

- **Identify** that WSL2 stores each distribution in an ext4 VHD (ext4.vhdx) and **justify** the implications: potential evidence “inside” the VHD, and different permission semantics/use cases.
- **Explain** how Linux files are accessed from Windows (e.g., \wsl\$) and **interpret** permission implications (access under the distro’s default user) and dependencies (the 9P service).
- **Identify** relevant WSL configuration files (wsl.conf and .wslconfig) and **explain** why they affect posture/environment when interpreting evidence.



Related Forensic Process Stages

Identification

Extraction/Preservation

Analysis

Documentation

Presentation

6.1.40. 0319 – Windows Memory Structure And Management

The applicant is able to explain Windows memory management concepts and identify the Windows memory artefacts needed for acquisition planning and forensic analysis.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	3 hours
Labs	2 hours
Total	5 hours



Prerequisites

The applicant should prove the knowledge of:

- 0115 - Computer Memory ^[p.56]
- 0207 - Memory Management Fundamentals ^[p.157]
- 0308 - Windows Command Line and PowerShell ^[p.81]
- 0315 - Windows Security Model ^[p.90]



Detailed Description

The applicant should be able to:

- **Explain** Windows virtual memory concepts, process address spaces, kernel memory, handles, threads, modules, VADs, pools, and sessions.

- **Identify** major Windows memory-backed artifacts: processes, DLLs, drivers, services, registry hives in memory, network objects, clipboard remnants, credentials-related structures, and command-line artifacts.
- **Explain** the role of `pagefile.sys`, `swapfile.sys`, `hiberfil.sys`, crash dumps, and memory compression.
- Describe the forensic relevance of Windows security features such as LSASS protection, Credential Guard, VBS/HVCI, BitLocker, Secure Boot, and TPM use at a conceptual level.
- **Explain** how Windows version, build, symbols, architecture, and security configuration affect memory analysis.
- **Document** OS build, architecture, boot mode, security state, and memory-related files before analysis.



Related Forensic Process Stages

 **Identification**

 **Analysis**

 **Documentation**



Observations

N.A

6.1.41. 0320 – Windows Memory Analysis

The applicant is able to analyse Windows memory images to identify and extract processes, network activity, loaded modules, user activity, credential-related traces, in memory files, suspicious behaviors, and understand the analysis limitations.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	3 hours
Labs	4 hours
Total	7 hours



Prerequisites

The applicant should prove the knowledge of:

-  0319 - Windows Memory Structure And Management ^[p.96]
-  0321 - Windows Memory Acquisition Techniques ^[p.98]

-  0306 - Windows Registry Analysis ^[p.40]
-  0102 - Reporting ^[p.17]
-  0307 - Windows Process Analysis (L1) ^[p.79]
-  0203 - Regular Expressions - Level 1 ^[p.27]

Detailed Description

The applicant should be able to:

- **Prepare** a Windows memory image for analysis by identifying OS build, architecture, symbol/profile requirements, and image quality.
- **Use** memory-analysis tools such as Volatility 3, MemProcFS, Tools4LEA tools, strings, YARA, and timeline helpers.
- Reconstruct process, thread, parent-child, handle, DLL, driver, and service relationships.
- **Identify** network connections, sockets, command lines, registry artifacts, loaded modules, injected code indicators, and persistence clues.
- **Distinguish** normal Windows activity from suspicious anomalies using corroborating artifacts.
- **Extract** and preserve relevant artefacts with a clear explanation of tool limitations and confidence level.
- **Produce** findings suitable for a forensic report.

Related Forensic Process Stages

 **Analysis**

 **Documentation**

 **Presentation**

Observations

TO BE COMPLETED

6.1.42. 0321 – Windows Memory Acquisition Techniques

The applicant is able to acquire Windows memory and related memory-backed artefacts using appropriate forensic procedures, and document acquisition quality, limitations, and risks.

Version

2026-06-03

Level

Intermediate



Estimated Workload

Lessons	2 hours
Labs	4 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- 0801 - Memory Acquisition - Level 1 [p.142]
- 0319 - Windows Memory Structure And Management [p.96]
- 0105 - Hashing (L1) [p.21]
- 0315 - Windows Security Model [p.90]



Detailed Description

The applicant should be able to:

- **Select** an acquisition path for a live Windows system, hibernated system, crashed system, or Windows VM.
- **Use** one or more Windows memory acquisition tools in a controlled lab and record repeatable acquisition metadata.
- **Preserve** and hash memory images, hibernation files, pagefiles, crash dumps, and VM saved-state memory where available.
- **Explain** how BitLocker, TPM, Credential Guard, VBS, EDR/AV, administrative privilege, and system uptime affect acquisition choices.
- **Identify** signs of incomplete or unreliable acquisition, including tool failure, unsupported OS build, insufficient privileges, truncation, and write-target problems.
- **Produce** a defensible acquisition log for court or internal audit.



Related Forensic Process Stages

Identification

Extraction/Preservation

Documentation



Observations

TO BE COMPLETED

6.1.43. 0401 – Cryptography Basics (L1)

The applicant is able to:

- **Understand** the main idea about cryptography
- **Interpret** the differences between symmetric and asymmetric cryptography

- **Plan** strategic approaches related with software that uses cryptography



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	4 hours
Labs	2 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- 0103 - Computer Data ^[p.18]
- 0105 - Hashing (L1) ^[p.21]



Detailed Description

The applicant should be able to:

- **Explain** the Confidentiality, Integrity, Availability, Authentication and Non-Repudiation (CIAAN) model
- **Recognize** the differences between symmetric and asymmetric cryptography
- **Understand** the Message Authentication Code (MAC) concept
- **Understand** digital signatures
- **Describe** Key Derivation Functions (KDF)
- **Explain** the salt and the implications of it



Related Forensic Process Stages

Identification

Extraction/Preservation

Analysis

Documentation

Presentation

6.1.44. 0402 - Use of Masks

The applicant is able to:

- **Understand** the need of masks and maskfiles
- **Use** masks and maskfiles
- **Use** special characters in masks

- **Create** masks and maskfiles



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	2 hours
Total	4 hours



Prerequisites

The applicant should prove the knowledge of:

- ...
- ...



Detailed Description

The applicant should be able to:

- **Understand** when they need to use masks or maskfiles
- **Use** masks and maskfiles
- **Justify** when to choose between masks or maskfiles
- **Use** the increment mode
- **Design** and **use** custom charsets
- **Recall** the existence of the default maskfile
- **Summarize** maskfile syntax
- **Summarize** command like masks syntax
- **Use** special characters in masks
- **Create** masks and maskfiles
- **Understand** how Markov Chains can affect the output of masks

6.1.45. 0403 – Wordlists

The applicant is able to:

- Understand what a wordlist is
- Create a wordlist

- Use wordlists for decryption approaches



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1 hour
Labs	1 hours
Total	2 hour



Prerequisites

The applicant should prove the knowledge of:

- None



Detailed Description

The applicant should be able to:

- **Recognize** wordlists
- **Understand** wordlists' limitations
- **Use** wordlists in decryption challenges
- **Create** wordlists from different themed topics and corpuses

6.1.46. 0404 - Rules

The applicant is able to:

- **Understand** the need of rules
- **Use** rules for decryption tools such as Hashcat and John the Ripper
- **Design** and **optimize** rules in the aforementioned tools



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	2 hours
Labs	3 hours
Total	5 hours



Prerequisites

The applicant should prove the knowledge of:

- 0403 - Wordlists ^[p.101]



Detailed Description

The applicant should be able to:

- **Understand** how rules work
- **Decide** when to **use** rules
- **Interpret** and **use** rules
- **Understand** how rule stacking works
- **Recognize** impact of rules
- **Understand** the --loopback option in tools such as Hashcat

6.1.47. 0405 – Hash Extraction

The applicant is able to:

- **Describe** the importance of hash extraction
- **Identify** encryption parameters.
- **Distinguish** protector types that support password recovery.
- **Identify, retrieve** and **operate** on hashes from different sources.
- **Prepare** extracted hash for password recovery.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	2 hours
Labs	1 hours
Total	3 hours



Prerequisites

The applicant should prove the knowledge of:

- 0105 - Hashing (L1) ^[p.21]



Detailed Description

The applicant should be able to:

- **Identify** the encryption parameters required for password hash extraction (hash function, cipher, key derivation settings) and locate where they are stored within an encrypted volume.
- **Distinguish** protector types that support password recovery from those that require alternative recovery approaches.
- **Collect** authentication hashes from network traffic and packet capture files.
- **Explain** the conditions under which a network authentication flow provides a hash suitable for password recovery.
- **Explain** the challenges of hash extraction from mobile devices.
- **Retrieve** a password hash from an encrypted storage volume.
- **Prepare** extracted hash data in the correct format for use with password recovery tools.



Related Forensic Process Stages

Identification

Extraction/Preservation

6.1.48. 0407 – Password Analysis

The applicant is able to:

- **Understand** the importance of analyzing previously collected passwords
- **Analyze** the structure and logic of passwords and **formulate** smarter approaches to guess them



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1 hours
Labs	2 hours
Total	3 hours



Prerequisites

The applicant should prove the knowledge of:

- 0402 - Use of Masks ^[p.100]
- 0403 - Wordlists ^[p.101]
- 0404 - Rules ^[p.102]



Detailed Description

The applicant should be able to:

- **Identify** patterns and **interpret** logic of previous collected passwords
- **Analyse** passwords manually
- **Analyse** passwords using tools
- Reduce the space search by **formulating** efficient candidates post-analysis



Related Forensic Process Stages

 **Identification**

 **Analysis**

6.1.49. 0408 – Preprocessing

The applicant is able to:

- **Explain** the purpose of wordlist preprocessing.
- **Separate** noise and duplicate entries from a wordlist.
- **Explain** how a preprocessor generates candidates.
- **Develop** a probabilistic model from known passwords.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	3 hours
Labs	3 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- 0403 - Wordlists ^[p.101]
- 0404 - Rules ^[p.102]



Detailed Description

The applicant should be able to:

- **Explain** the purpose of preprocessing in password recovery and why it improves candidate quality compared to using raw wordlists directly.
- **Identify** types of unwanted content in a wordlist that reduce recovery effectiveness.
- **Describe** the effect of candidate ordering on recovery efficiency (dictionary-like candidates first, exhaustive combinations last).
- **Explain** how a preprocessor generates candidates by chaining unmodified elements from a wordlist.
- **Apply** cleaning operations to remove unwanted content and produce a deduplicated wordlist.
- **Separate** entries already present in other wordlists to avoid redundant candidate generation.
- **Develop** a probabilistic model from a password dataset and generate candidates from it.
- **Combine** rule sets derived from multiple password datasets to produce a merged candidate set.



Related Forensic Process Stages

Identification

Extraction/Preservation

Analysis

6.1.50. 0410 – Decryption Strategy

The applicant is able to:

- **Understand** the concept of weakest link
- **Implementing** contextual information from previous investigations to password decryption
- **Leverage** the existence of biometrics and password policies
- **Integrating** the existence of cloud forensics



Version

2026-06-03

**Level**

Basic

**Estimated Workload**

Lessons	2 hours
Labs	1 hours
Total	3 hours

**Prerequisites**

The applicant should prove the knowledge of:

- 0405 - Hash Extraction ^[p.103]
- 0407 - Password analysis ^[p.104]

**Detailed Description**

The applicant should be able to:

- **Understand** the concept of weakest link
- **Implementing** contextual information from previous investigations to password decryption
- **Leverage** the existence of biometrics and password policies
- **Integrating** the existence of cloud forensics

**Related Forensic Process Stages** **Identification** **Analysis**

6.1.51. 0411 – Decryption Hardware Strategy

The applicant is able to:

- **Estimate** the importance of hardware access
- **Search** for new techniques and technologies for hardware access
- **Implement** lawful hardware access on encryption devices

**Version**

2026-06-03

**Level**

Advanced



Estimated Workload

Lessons	2 hours ¹
Labs	1 hours
Total	2 hours



Prerequisites

The applicant should prove the knowledge of:

- ^[p.103] 0401 - Cryptography Basics (L1) ^[p.99]
- 0405 - Hash Extraction ^[p.103]
- 0408 - Preprocessing ^[p.105]
- 0410 - Decryption Strategy ^[p.106]



Detailed Description

The applicant should be able to:

- **Estimate** the importance of lawful hardware access
- **Search** for new techniques and technologies for lawful hardware access
- **Implement** lawful hardware access on encryption devices
 - **Understand** the importance of DMA



Related Forensic Process Stages

Identification

Extraction/Preservation

Analysis



Observations

6.1.52. 0412 – Decryption Performance Limits

The applicant is able to:

- **Analyze** the use and impact of the CPU and GPU in usage of decryption tools such as Hashcat or John the Ripper
- **Interpret** how slow hash functions and anti-GPU functions interact with CPU and GPU
- **Organizing** strategies for performance optimizations in decryption tools
- **Choosing** the most efficient hardware specifications for the task
- **Recognize** how Markov Chains can be of use when encountering performance limits



Version

2026-06-03

**Level**

Advanced

**Estimated Workload**

Lessons	2 hours
Labs	1 hours
Total	3 hours

**Prerequisites**

The applicant should prove the knowledge of:

- 1101 - Computer Architecture ^[p.150]
- 0105 - Hashing (L1) ^[p.21]
- 0401 - Cryptography Basics (L1) ^[p.99]
- 0402 - Use of Masks ^[p.100]
- 0404 - Rules ^[p.102]
- ^[p.102] 0410 - Decryption Strategy ^[p.106]

**Detailed Description**

The applicant should be able to:

- Be aware and analyze the use and impact of CPU and GPU in usage of decryption tools
 - Management of spacesearch
 - Feasability of certain cases
 - Difference in using CPU vs GPU for decryption, such as memory size difference, number of cores for parallelization
 - **Improve** performance bottlenecks in Decryption problems by fine-tuning certain parameters for parallelization
- **Comparing** slow hash functions and anti-GPU functions and how they affect decryption
- **Perform** efficient approaches on decryption when using tools due to this knowledge
- **Understand** which hardware components may be more suitable for the job

6.1.53. 0413 – Decentralised Decryption

The applicant is able to:

- **Explain** the password recovery framework across network.
- **Describe** how the candidate set is divided and sent to each node.
- **Configure** a shared server to track already-tested candidates.

- **Configure** a distributed password recovery framework across multiple computers.



Version

2026-06-03



Level

Advanced



Estimated Workload

Lessons	2 hours
Labs	2 hours
Total	4 hours



Prerequisites

The applicant should prove the knowledge of:

-  0410 - Decryption Strategy ^[p.106]
-  0412 - Decryption Performance Limits ^[p.108]



Detailed Description

The applicant should be able to:

- **Explain** how password recovery can be split across multiple computers and speeds up the overall process.
- **Identify** what a password recovery framework needs to do to manage a distributed password recovery attempt:
 - Measure each computer's speed and assign an appropriate portion of work
 - Send the necessary files to each computer
 - Collect results and track overall progress
 - Control which users and computers can access which tasks
- **Configure** a duplicate tracking server to skip already-tested candidates.
- **Configure** a distributed password recovery framework to assign and **run** a password recovery task across multiple computers.



Related Forensic Process Stages

 **Analysis**

6.1.54. 0501 – Network Fundamentals

The applicant is able to:

- **Understand** the definitions of various network types
- **Recognise** different network architectures



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	5 hours
Labs	1 hours
Total	6 hours



Detailed Description

The applicant should be able to:

- **Identify** network types (LAN, WAN, WLAN)
- **Recognise** network topologies
- **Distinguish** between local devices and remote infrastructure
- **Draft** a schematic representation of the network and its main components



Related Forensic Process Stages

 **Identification**

 **Documentation**

 **Presentation**



Observations

This MC doesn't cover network mapping using tools

6.1.55. 0502 – Network Hardware

The applicant is able to:

- **Identify** essential network hardware and transmission media
- **Understand** how each device manages data transmission (broadcasting vs. switching).

**Version**

2026-06-03

**Level**

Basic / Intermediate / Advanced

**Estimated Workload**

Lessons	X hours
Labs	X hours
Total	X hours

**Prerequisites**

The applicant should prove the knowledge of:

- ...
- ...

**Detailed Description**

The applicant should be able to:

- Identify the specific equipment that holds potential evidence
- Understand the physical layout of a suspect's network
- Conduct effective seizures without disrupting unrelated systems

**Related Forensic Process Stages**

Identification
Extraction/Preservation
Analysis
Documentation
Presentation

**Observations**

6.1.56. 0503 – Network Models

The applicant is able to:

- **Master** the layered structure of data transmission, specifically the 7 layers of the OSI model
- **Master** the 4 layers of the TCP/IP model, to
- **Understand** how data is encapsulated and moved from application to physical media
- **Explain** the process of encapsulation and decapsulation of data as it travels down and up the protocol stack

**Version**

2026-06-03

**Level**

Basic / Intermediate / Advanced

**Estimated Workload**

Lessons	X hours
Labs	X hours
Total	X hours

**Prerequisites**

The applicant should prove the knowledge of:

- ...
- ...

**Detailed Description**

The applicant should be able to:

- Deconstruct complex cyber incidents by pinpointing exactly which layer was exploited
- Facilitate precise communication with technical analysts or forensic experts
- Analyse captured traffic to determine if headers have been manipulated during encapsulation to hide data

**Related Forensic Process Stages**

Identification	Extraction/Preservation	Analysis	Documentation	Presentation
----------------	-------------------------	----------	---------------	--------------

**Observations**

6.1.57. 0504 – Network Protocols

The applicant is able to:

- **Understand** the difference between TCP and UDP
- **Explain** the most common protocols (DNS, HTTP/HTTPS, SMTP, POP, SSH) roles and key specificities using simple examples

**Version**

2026-06-03

**Level**

Basic

**Estimated Workload**

Lessons	X hours
Labs	X hours
Total	X hours

**Prerequisites**

The applicant should prove the knowledge of:

- ...
- ...

**Detailed Description**

The applicant should be able to:

- Know exactly which service providers to target and which specific logs to request to trace a user's actions
- Recognize when a suspect is using standard communication channels abnormally to hide data or malicious tools
- Categorize what the suspect was doing to narrow the scope of the investigation

**Related Forensic Process Stages**
Identification
Extraction/Preservation
Analysis
Documentation
Presentation
**Observations**

6.1.58. 0601 – Linux Memory Structure And Management

The applicant is able to explain Linux memory management concepts and identify the Linux memory artefacts needed for acquisition planning and forensic analysis.

**Version**

2026-06-03

**Level**

Intermediate



Estimated Workload

Lessons	3 hours
Labs	2 hours
Total	5 hours



Prerequisites

The applicant should prove the knowledge of:

- 0115 - Computer Memory ^[p.56]
- 0207 - Memory Management Fundamentals ^[p.157]



Detailed Description

The applicant should be able to:

- **Explain** Linux process address spaces, kernel memory, virtual memory areas, page tables, file-backed mappings, anonymous mappings, and shared memory.
- **Describe** Linux memory-related artifacts: `/proc`, `/sys`, loaded modules, kernel logs, swap, core dumps, crash dumps, and process memory maps.
- **Explain** the role of kernel version, distribution, architecture, KASLR, kernel symbols, modules, containers, and namespaces in memory analysis.
- **Identify** evidence commonly found in Linux memory: processes, shell activity, network sockets, loaded modules, files, credentials/tokens, malware/rootkit traces, and container context.
- **Document** Linux system context needed for analysis: distro, kernel version, architecture, uptime, loaded modules, swap configuration, containerisation, and acquisition method.



Related Forensic Process Stages

Identification

Analysis

Documentation



Observations

TO BE DONE.

6.1.59. 0602 – Linux Memory Acquisition Techniques

The applicant is able to acquire Linux memory and related artefacts using appropriate methods, preserve acquisition metadata, and document limitations caused by kernel configuration, privilege, modules, containers, or cloud hosting.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	2 hours
Labs	4 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

- 0801 - Memory Acquisition (L1) ^[p.142]
- 0601 - Linux Memory Structure And Management ^[p.114]
- 9901 - Linux CLI ^[p.42]
- 0105 - Hashing (L1) ^[p.21]



Detailed Description

The applicant should be able to:

- **Select** an acquisition method for a Linux physical system, VM, server, container host, or cloud instance where authorised.
- **Use** Linux acquisition tools in controlled conditions, such as LiME, AVML, fmem, crash/kdump workflows, VM memory extraction, or approved platform tooling.
- **Collect** supporting live context before acquisition when appropriate: kernel version, loaded modules, processes, network state, uptime, swap status, and container context.
- **Preserve** memory images, swap files/partitions, crash dumps, and VM memory artefacts with hashes and logs.
- **Explain** risks from kernel module loading, acquisition footprint, kernel mismatch, secure boot, lockdown mode, EDR, and insufficient privilege.
- **Produce** a defensible Linux memory acquisition record.



Related Forensic Process Stages

Identification

Extraction/Preservation

Documentation



Observations

TO BE DONE.

6.1.60. 0603 – Linux Memory Analysis

The applicant is able to:

- **Do** ...
- **Do** ...



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	3 hours
Labs	4 hours
Total	7 hours



Prerequisites

The applicant should prove the knowledge of:

- 0601 - Linux Memory Structure And Management ^[p.114]
- 0602 - Linux Memory Acquisition Techniques. ^[p.115]
- 0203 - Regular Expressions (L1) ^[p.27]
- 9901 - Linux CLI ^[p.42]



Detailed Description

The applicant should be able to:

- **Prepare** a Linux memory image for analysis by identifying kernel version, architecture, symbol requirements, and acquisition quality.
- **Use** memory-analysis tools such as Volatility 3, strings, YARA, MemProcFS where supported, and Linux command-line analysis helpers.
- **Reconstruct** processes, parent-child relationships, command lines, environment variables, open files, sockets, loaded modules, and namespace/container context.
- **Identify** and **Extract** suspicious kernel modules, hidden processes, unusual network activity, credential or token traces, and rootkit indicators.
- **Interpret** memory findings alongside Linux artefacts such as `/proc`, logs, shell history, systemd/journal output, auth logs, and container metadata where available.

- **Document** commands, plugin outputs, confidence level, and limitations caused by symbols, kernel mismatch, incomplete acquisition, or anti-forensics.

Related Forensic Process Stages

 **Analysis**

 **Documentation**

 **Presentation**

Observations

TO BE DONE.

6.1.61. 0701 – macOS Architecture

The applicant is able to:

- **Understand** the macOS architecture
- **Understand** the role of System Integrity Protection (SIP) and its impact on forensic access
- **Identify** where forensic artefacts reside within each OS layer
- **Distinguish** between Apple Silicon and Intel Mac boot and security models

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	0.5 hours
Labs	1.5 hours
Total	2 hours

Prerequisites

The applicant should prove the knowledge of:

- General operating system concepts (processes, memory, file systems, user space)

Detailed Description

The applicant should be able to:

- **Understand** Core components of macOS architecture (Darwin, XNU kernel)
- **Understand** the filesystem structure and directory hierarchy
- **Explain** the user profile structure and forensic artifacts

- **Understand** Security mechanisms (Code Signing, Gatekeeper, Sandboxing, TCC)
- **Understand** System Integrity Protection, SSV, and cryptex integration
- **Understand** Significant Locations and the Core Location framework

 Related Forensic Process Stages

 Identification	
---	--

6.1.62. 0702 – macOS GUI and Boot Options

The applicant is able to:

- **Understand** macOS Graphical User Interface (GUI)
- **Explore** Mac boot options and system initialisation processes

 **Version**
2026-06-03

 **Level**
Basic

 Estimated Workload

Lessons	1.0 hours
Labs	1.0 hours
Total	2 hours

 Prerequisites

- The applicant should prove the knowledge of:
-  0701 - macOS Architecture^[p.118]

 Detailed Description

- The applicant should be able to:
- **Identify** the macOS desktop components: Application Menu, Apple Menu, Status Bar, Dock, Finder, Mission Control, and Launchpad
 - **Demonstrate** navigation of Finder: hidden files toggle, path bar, view options, Tags, and search functionality
 - **Locate** forensically significant areas via System Preferences / System Settings: Internet Accounts, Passwords, Users & Groups, Screen Time, Security & Privacy, Network, and Time Machine
 - **Recall** keyboard shortcuts for screenshots

- **Describe** Intel Mac and Silicon Mac boot options
- **Understand** Firmware password and Activation Lock on acquisition access



Related Forensic Process Stages

Identification

Analysis

6.1.63. 0703 – macOS as a Forensic Lab

The applicant is able to:

- **Explain** the advantages of using a Mac as a forensic workstation
- **Install** forensic tools using Homebrew and MacPorts package managers



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	1.5 hours
Total	2.5 hours



Prerequisites

The applicant should prove the knowledge of:

- 0701 - macOS Architecture ^[p.118]



Detailed Description

The applicant should be able to:

- **Describe** the advantages of a Mac as a forensic station
- **Explain** why no single tool covers all macOS artefacts
- **Execute** the SIP deactivation procedure
- **Understand** Gatekeeper activation and deactivation reasons
- **Perform** installation of forensics tools



Related Forensic Process Stages

[Identification](#)
[Analysis](#)

6.1.64. 0704 – macOS Mount Images

The applicant is able to:

- **Explain** the macOS challenge with EWF/E01 images
- **Use** xmount to convert an E01 image on-the-fly to a virtual DMG and mount it read-only mode
- **Verify** the mounted volume using diskutil list and by browsing via Finder and Terminal
- **Detach** a mounted forensic image



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	2.0 hours
Total	3.0 hours



Prerequisites

The applicant should prove the knowledge of:

- 0701 - macOS as a Forensic Lab ^[p.120]



Detailed Description

The applicant should be able to:

- **Classify** forensic image formats: raw/DD, EWF/E01, AFF4, and DMG
- **Describe** xmount: purpose, installation via Homebrew
- **Execute** xmount
- **Use** hdiutil to attach images
- **Interpret** hdiutil output
- **Execute** diskutil list and interpret the output for a mounted forensic image
- **Verify** read-only status
- **Demonstrate** browsing the mounted volume in Finder and via Terminal

- **Unmount** the image
- **Describe** virtual write support options: xmount --cache and hdiutil -shadow and assess their use for Spotlight index reconstruction
- **Perform** the complete mount workflow on an E01 image

Related Forensic Process Stages

 Identification

 Extraction/Preservation

6.1.65. 0705 – macOS APFS

The applicant is able to:

- **Explain** APFS fundamentals
- **Describe** the APFS major structural components: checkpoint area, space manager, object map
- **Identify** volume layout and explain the forensic role of each volume
- **Understand** macOS Boot Disk Structure in different macOS versions
- **Understand** forensics value of System Volume
- **Understand** forensics value of Data Volume
- **Use** Sleuth Kit to examine APFS structures and extract file metadata

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	1.5 hours
Labs	2.0 hours
Total	3.5 hours

Prerequisites

The applicant should prove the knowledge of:

-  0701 - macOS Architecture ^[p.118]
-  0702 - macOS GUI and Boot Options ^[p.119]
-  0703 - macOS as a Forensic Lab ^[p.120]
-  0704 - macOS as a Forensic Lab ^[p.121]

Detailed Description

The applicant should be able to:

- **Recall** HFS+ limitations
- **Describe** the APFS container model
- **Explain** copy-on-write (CoW) mechanics and assess how they differ from HFS+ and affect file recovery potential
- **Describe** atomic safe-save: crash-safe file replacement and evaluate its implications for forensic artefact creation
- **Understand** instant file clones
- **Understand** space sharing between volumes
- **Explain** sparse files
- **Identify** the APFS major structural components: checkpoint area, space manager, object map B-tree, file system tree B-tree, and extent reference tree
- **Recall** the macOS boot disk volume roles: System (read-only sealed), Data (user/app data), Preboot, Recovery, VM (swap), and Update
- **Analyse** APFS container and volume details using GUI Disk Utility
- **Use** Sleuth Kit to retrieve volume statistics

Related Forensic Process Stages

 **Extraction/Preservation**  **Analysis**

6.1.66. 0706 – macOS Acquisition

The applicant is able to:

- **Identify** the Mac model and chipset type
- **Determine** the correct acquisition approach
- **Acquire** an Intel Mac
- **Explain** the hardware-based encryption on T2 Macs
- **Acquire** an Apple Silicon Mac

Version

2026-06-03

Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	3.0 hours
Total	4.0 hours



Prerequisites

The applicant should prove the knowledge of:

- 0701 - macOS Architecture ^[p.118]
- 0702 - macOS GUI and Boot Options ^[p.119]
- 0703 - macOS as a Forensic Lab ^[p.120]



Detailed Description

The applicant should be able to:

- **Classify** Mac models by chipset generation (Intel, Intel+T2, Apple Silicon)
- **Identify** the acquisition method
- **Describe** Target Disk Mode acquisition for Intel Macs
- **Demonstrate** Intel Mac acquisition
- **Demonstrate** the bootable live OS approach
- **Assess** the forensic implications of Open Firmware password protection
- **Execute** acquisition commands using Terminal
- **Understand** Secure Boot settings on T2 Macs
- **Describe** the T2 Secure Enclave hardware encryption model
- **Assess** the challenge of FileVault 2 on T2 hardware
- **Execute** T2 Mac acquisition
- **Demonstrate** Silicon Mac acquisition



Related Forensic Process Stages

Identification

Extraction/Preservation

6.1.67. 0707 – macOS File Types

The applicant is able to:

- **Identify** different file types
- **Explain** the purpose of plist files
- **Parse** plist files

- **Identify** forensically significant plist files within a forensic image



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	1.5 hours
Total	2.5 hours



Prerequisites

The applicant should prove the knowledge of:

-  0701 - macOS Architecture ^[p.118]
-  0702 - macOS GUI and Boot Options ^[p.119]
-  0703 - macOS as a Forensic Lab ^[p.120]
-  0704 - macOS Mount Images ^[p.121]
-  0706 - macOS Acquisition ^[p.123]  ^[p.120]



Detailed Description

The applicant should be able to:

- **Describe** file types in macOS
- **Describe** plist files
- **Distinguish** between XML plist and binary plist formats
- **Analyze** plist and db files
- **Identify** forensically significant plist files
- **Extract** forensically relevant values from plist and db files using the appropriate tool



Related Forensic Process Stages

 **Extraction/Preservation**  **Analysis**

6.1.68. 0708 – macOS Disk Images

The applicant is able to:

- **Describe** Mac disk image format types
- **Create** disk images
- **Verify** disk image integrity
- **Locate** disk images found within a forensic case image
- **Analyse** disk images found within a forensic case image



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	1.5hours
Total	2.5 hours



Prerequisites

The applicant should prove the knowledge of:

- 0703 - macOS as a Forensic Lab ^[p.120]
- 0704 - macOS Mount Images ^[p.121]
- 0706 - macOS Acquisition ^[p.123] 0708 ^[p.120]



Detailed Description

The applicant should be able to:

- **Understand** different types of disk images
- **Classify** Mac disk image types
- **Identify** which forensic tools support which disk image formats
- **Execute** hduutil for creation, verification and protection images
- **Use** find and file commands to locate disk images within a forensic image
- **Examine** disk image



Related Forensic Process Stages

[Extraction/Preservation](#)
[Analysis](#)

6.1.69. 0709 – macOS User Accounts

The applicant is able to:

- **Identify** system version
- **Identify** User account
- **Analyse** User home folder



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	1.5hours
Total	2.5 hours



Prerequisites

The applicant should prove the knowledge of:

- [0704 - macOS Mount Images](#) ^[p.121]
- [0707 - macOS File Types](#) ^[p.124]
- [0708 - macOS Disk Images](#) ^[p.126] [\[p.123\] \[\\[p.120\\]\]\(#\)](#)



Detailed Description

The applicant should be able to:

- **Identify** system version and build number artefacts
- **Analyse** boot history and system update records
- **Establish** a system timeline
- **Identify** user accounts
- **Verify** user accounts
- **Examining** home folder structure

- **Analyse** login configuration



Related Forensic Process Stages

 **Analysis**

6.1.70. 0710 – macOS Artifacts Keychain

The applicant is able to:

- **Identify** keychain types
- **Analyse** keychain's data



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	2.0 hours
Total	3.0 hours



Prerequisites

The applicant should prove the knowledge of:

-  0704 - macOS Mount Images ^[p.121]
-  0707 - macOS File Types ^[p.124]
-  0708 - macOS Disk Images ^[p.126]  ^[p.123]  ^[p.120]



Detailed Description

The applicant should be able to:

- **Describe** keychains role as encrypted credential and certificate storage
- **Identify** keychain types: Login Keychain, Local Items Keychain, System Keychain, and System Roots
- **Examine** keychain
- **Understand** critical limitations



Related Forensic Process Stages

[Analysis](#)

6.1.71. 0711 – macOS Artifacts Browser

The applicant is able to:

- **Locate** File Quarantine artefacts
- **Interpret** File Quarantine artefacts
- **Identify** different browsers artefacts
- **Examine** different browsers artefacts
- **Reconstruct** browsers activity



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	2.0 hours
Total	3.0 hours



Prerequisites

The applicant should prove the knowledge of:

- 0704 - macOS Mount Images ^[p.121]
- 0707 - macOS File Types ^[p.124]
- 0708 - macOS Disk Images ^[p.126]
- ^[p.123] 0709 - macOS User Accounts ^[p.127] ^[p.120]



Detailed Description

The applicant should be able to:

- **Describe** File Quarantine and the structure of the quarantine extended attribute
- **Examine** quarantine extended attributes on a live system
- **Identify** browser data storage paths

- **Describe** Safari's WebKit engine
- **Evaluate** the implications of iCloud sync for local artefact completeness
- **Locate** Safari artefacts
- **Examine** Safari settings and data
- **Locate** Chrome artefacts
- **Examine** Chrome settings and data
- **Locate** Firefox artefacts
- **Examine** Firefox settings and data
- **Execute** SQL queries against Safari History.db to extract visits with human-readable timestamps
- **Assess** recovery of deleted Safari artefacts
- **Correlate** browser artefacts from multiple browsers to produce a unified browsing activity timeline



Related Forensic Process Stages

 **Analysis**

6.1.72. 0712 – macOS Artifacts Communication

The applicant is able to:

- **Locate** Address Book database
- **Extract** contacts and their associated metadata
- **Analyse** Mail.app artefacts
- **Extract** iMessage and SMS records
- **Interpret** iMessage and SMS records from the Messages chat.db database
- **Reconstruct** a communication timeline from Address Book, Mail, and Messages artefacts



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	1.5 hours
Total	2.5 hours



Prerequisites

The applicant should prove the knowledge of:

-  0704 - macOS Mount Images ^[p.121]
-  0707 - macOS File Types ^[p.124]
-  0708 - macOS Disk Images ^[p.126]
-  ^[p.123]  0709 - macOS User Accounts ^[p.127]  ^[p.120]



Detailed Description

The applicant should be able to:

- **Identify** the macOS communication applications: iMessage, SMS relay, Mail, FaceTime, and common third-party apps and list their artefact locations
- **Locate** the Address Book database
- **Describe** the Mail application storage model: IMAP/POP3/Exchange support, iCloud Mail, and local folder structure
- **Locate** Mail data
- **Extract** Mail account information
- **Examine** .emlx files
- **Locate** Mail attachments
- **Distinguish** iMessage from SMS/MMS
- **Examine** communication apps
- **Assess** deleted iMessage record recovery



Related Forensic Process Stages

 **Analysis**

6.1.73. 0713 – macOS Artifacts Recently Used

The applicant is able to:

- **Explain** the purpose of the Recently Used Items artefacts and their format evolution
- **Analyse** recent item data



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	1.5 hours
Total	2.5 hours



Prerequisites

The applicant should prove the knowledge of:

- 0704 - macOS Mount Images ^[p.121]
- 0707 - macOS File Types ^[p.124]
- 0708 - macOS Disk Images ^[p.126]
- ^[p.123] 0709 - macOS User Accounts ^[p.127] ^[p.120]



Detailed Description

The applicant should be able to:

- **Explain** the purpose of the Recently Used Items artefacts and their format evolution
- **Locate** the SharedFileList directory
- **Identify** the relevant SFL4 files for recent documents, applications, and volumes
- **Export** recent item data
- **Examine** recent item data
- **Reconstruct** a forensic timeline using recently used item findings



Related Forensic Process Stages

Analysis

6.1.74. 0714 – macOS Artifacts Deleted Files

The applicant is able to:

- **Locate** Trash artefacts
- **Examine** Trash artefacts



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	2.0 hours
Total	3.0 hours



Prerequisites

The applicant should prove the knowledge of:

- 0704 - macOS Mount Images ^[p.121]
- 0707 - macOS File Types ^[p.124]
- 0708 - macOS Disk Images ^[p.126]
- ^[p.123] 0709 - macOS User Accounts ^[p.127] ^[p.120]



Detailed Description

The applicant should be able to:

- **Locate** Trash artefacts
- **Examine** Trash artefacts
- **Explain** APFS deletion mechanics, allocation blocks, and the effect of TRIM on file recovery from SSDs
- **Perform** live and post-mortem FSEvents analysis
- **Establish** file deletion intent and timeline



Related Forensic Process Stages

Analysis

6.1.75. 0715 - macOS Artifacts Snapshots

The applicant is able to:

- **Explain** Time Machine scheme
- **Identify** local snapshots
- **Analyse** snapshots



Version

2026-06-03

**Level**

Basic

**Estimated Workload**

Lessons	1.0 hours
Labs	1.5 hours
Total	2.5 hours

**Prerequisites**

The applicant should prove the knowledge of:

- 0704 - macOS Mount Images ^[p.121]
- 0705 - macOS APFS ^[p.122]
- 0707 - macOS File Types ^[p.124]
- 0708 - macOS Disk Images ^[p.126]
- ^[p.123] 0709 - macOS User Accounts ^[p.127] ^[p.120]

**Detailed Description**

The applicant should be able to:

- **Explain** Time Machine's backup scheme, local snapshot creation schedule,
- **Differ** snapshots and full backups
- **Identify** local snapshots
- **List** the types of data recoverable from the snapshots
- **Identify** available snapshots on a volume
- **Mount** a specific snapshot
- **Analyse** snapshots

**Related Forensic Process Stages**
Analysis

6.1.76. 0716 – macOS Extended Attributes and Spotlight

The applicant is able to:

- **Identify** the purposes of extended attributes
- **Analyse** extended attributes
- **Identify** Spotlight components

- **Analyse** metadata



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.5 hours
Labs	2.0 hours
Total	3.5 hours



Prerequisites

The applicant should prove the knowledge of:

- 0704 - macOS Mount Images ^[p.121]
- 0705 - macOS APFS ^[p.122]
- 0707 - macOS File Types ^[p.124]
- 0708 - macOS Disk Images ^[p.126]
- ^[p.123] 0709 - macOS User Accounts ^[p.127] ^[p.120]
- 0713 - macOS Artifacts Recently Used ^[p.131]



Detailed Description

The applicant should be able to:

- **Explain** the origin of extended attributes
- **Identify** the purposes of extended attributes
- **Distinguish** between inline xattr storage (small values in inode) and separate xattr B-tree node storage (large values)
- **List** the forensically significant xattr types
- **Identify** metadata subtypes
- **Analyse** extended attributes
- **Describe** the Spotlight architecture
- **Identify** Spotlight components
- **Locate** the Spotlight file structure
- **List** metadata attributes for a specific file
- **Analyse** metadata



Related Forensic Process Stages

 **Analysis**

6.1.77. 0717 – macOS Log Files

The applicant is able to:

- **Describe** the evolution of macOS logging
- **Identify** log files
- **Analyse** log files



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.5 hours
Labs	2.0 hours
Total	3.5 hours



Prerequisites

The applicant should prove the knowledge of:

-  0704 - macOS Mount Images ^[p.121]
-  0705 - macOS APFS ^[p.122]
-  0707 - macOS File Types ^[p.124]
-  0708 - macOS Disk Images ^[p.126]
-  ^[p.123]  0709 - macOS User Accounts ^[p.127]  ^[p.120]



Detailed Description

The applicant should be able to:

- **Describe** the evolution of macOS logging
- **Identify** log storage paths
- **Distinguish** between live log collection and dead-box log collection
- **Recall** which log paths are included in Time Machine backups

- **Identify** log file formats
- **Describe** the Apple Unified Logging architecture
- **Identify** the Unified Log file structure
- **Analyse** log files
- **Correlate** log events across subsystems to reconstruct a complete user session or system event sequence



Related Forensic Process Stages

 **Analysis**

6.1.78. 0718 – macOS Network Connections

The applicant is able to:

- **Identify** Wi-Fi artefact types
- **Locate** Wi-Fi artefacts
- **Examine** Wi-Fi artefacts



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	2.0 hours
Total	3.0 hours



Prerequisites

The applicant should prove the knowledge of:

-  0704 - macOS Mount Images ^[p.121]
-  0705 - macOS APFS ^[p.122]
-  0707 - macOS File Types ^[p.124]
-  0708 - macOS Disk Images ^[p.126]
-  ^[p.123]  0709 - macOS User Accounts ^[p.127]  ^[p.120]

Detailed Description

The applicant should be able to:

- **Identify** Wi-Fi artefact types
- **Locate** Wi-Fi artefacts
- **Locate** the location cache
- **Describe** location cache structure
- **Describe** Significant Locations
- **Summarise** location artefact priorities
- **Extract** MAC addresses and interface names from the forensic image
- **Correlate** Wi-Fi artifacts and location artefacts to reconstruct a chronological travel and connectivity timeline
- **Examine** Wi-Fi artefacts

Related Forensic Process Stages

 **Analysis**

6.1.79. 0719 - macOS iOS Backups

The applicant is able to:

- **Describe** the iOS backup concept
- **Locate** iOS backup
- **Examine** iOS backup

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	1.0 hours
Labs	2.0 hours
Total	3.0 hours



Prerequisites

The applicant should prove the knowledge of:

-  0704 - macOS Mount Images ^[p.121]
-  0705 - macOS APFS ^[p.122]
-  0707 - macOS File Types ^[p.124]
-  0708 - macOS Disk Images ^[p.126]
-  ^[p.123]  0709 - macOS User Accounts ^[p.127]  ^[p.120]



Detailed Description

The applicant should be able to:

- **Describe** the iOS backup concept
- **Locate** iOS backup
- **Explain** iOS backup directory naming
- **Describe** the iOS backup snapshot structure
- **Identify** the key backup files
- **Examine** iOS backup



Related Forensic Process Stages

 **Analysis**

6.1.80. 0720 – macOS iOS iCloud

The applicant is able to:

- **Identify** iCloud services available on macOS
- **Locate** iCloud artifacts
- **Examine** iCloud artifacts



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.0 hours
Labs	1.5 hours
Total	2.5 hours



Prerequisites

The applicant should prove the knowledge of:

- 0704 - macOS Mount Images ^[p.121]
- 0705 - macOS APFS ^[p.122]
- 0707 - macOS File Types ^[p.124]
- 0708 - macOS Disk Images ^[p.126]
- ^[p.123] 0709 - macOS User Accounts ^[p.127] ^[p.120]



Detailed Description

The applicant should be able to:

- **List** iCloud services available on macOS
- **Locate** iCloud settings
- **Describe** iCloud encryption
- **Explain** two-factor authentication and trusted devices
- **Identify** iCloud token storage in the keychain
- **Compare** live vs dead acquisition for iCloud data
- **Locate** iCloud account information
- **Examine** iCloud Drive artifacts
- **Execute** iCloud database analysis
- **Locate** Safari iCloud Tabs database
- **Parse** the Safari iCloud Tabs database
- **Examine** the Photos library for iCloud sync



Related Forensic Process Stages

Analysis

6.1.81. 0721 – macOS App Activities and Device State

The applicant is able to:

- **Describe** Screen Time

- **Identify** Screen Time screenshot artefacts
- **Examine** Screen Time
- **Describe** PowerLog
- **Locate** the PowerLog database
- **Examine** PowerLog



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1.5 hours
Labs	2.0 hours
Total	3.0 hours



Prerequisites

The applicant should prove the knowledge of:

- 0704 - macOS Mount Images ^[p.121]
- 0705 - macOS APFS ^[p.122]
- 0707 - macOS File Types ^[p.124]
- 0708 - macOS Disk Images ^[p.126]
- ^[p.123] 0709 - macOS User Accounts ^[p.127] ^[p.120]
- ^[p.136] 0717 - macOS Log Files ^[p.136]
- ^[p.136] 0718 - macOS Network Connections ^[p.137]
- 0719 - macOS iOS Backups ^[p.138]
- 0720 - macOS iOS iCloud ^[p.139]



Detailed Description

The applicant should be able to:

- **Describe** Screen Time
- **Identify** Screen Time screenshot artefacts
- **Examine** Screen Time
- **Describe** PowerLog

- **Locate** the PowerLog database
- **Examine** PowerLog
- **Synthesise** Screen Time, PowerLog, Unified Logs, network connections, browser history, communication records, and iCloud artefacts into a unified chronological activity timeline

Related Forensic Process Stages

 **Analysis**

6.1.82. 0801 – Memory Acquisition (L1)

The applicant is able to acquire memory from common physical and virtual systems using standard tools, preserve acquisition metadata, and defend acquisition decisions in a forensic context.

Version

2026-06-03

Level

Intermediate

Estimated Workload

Lessons	2 hours
Labs	3 hours
Total	5 hours

Prerequisites

The applicant should prove the knowledge of:

-  1101 - Computer Architecture ^[p.150]
-  0115 - Computer Memory ^[p.56]  ^[p.58]
-  0117 - Virtual Machines ^[p.58]
-  0207 - Memory Management Fundamentals ^[p.157]

Detailed Description

The applicant should be able to:

- **List** common memory sources and formats: RAM dump, crash dump, hibernation file, pagefile, swap file, VM memory file, saved state, and cloud snapshot where available.
- **Select** an acquisition approach based on system state, volatility, legal authority, encryption risk, and operational constraints.

- **Use** basic memory acquisition tools in controlled scenarios, such as winpmem, FTK Imager, Magnet RAM Capture, DumpIt, LiME, AVML, or equivalent local tooling.
- **Record** acquisition metadata: tool name/version, command line, date/time, timezone, system state, user/session context, storage target, hashes, and observed errors.
- **Explain** the forensic impact of live acquisition, including possible memory modification by the acquisition tool.
- **Verify** acquisition output and preserve the original image for analysis.



Related Forensic Process Stages

 **Identification**

 **Extraction/Preservation**



Observations

This credential should focus on safe, standard acquisition methods. Advanced encryption, anti-forensic, and hostile-system cases belong in  0802 - Memory Acquisition (L2) ^[p.143].

6.1.83. 0802 – Memory Acquisition (L2)

The applicant is able to plan and perform advanced memory acquisition in constrained forensic scenarios, including encrypted, virtualised, protected, unstable, or high-value systems, while documenting legal authority, operational risk, evidence quality, and limitations.



Version

2026-06-03



Level

Advanced



Estimated Workload

Lessons	3 hours
Labs	5 hours
Total	8 hours



Prerequisites

The applicant should prove the knowledge of:

-  0801 - Memory Acquisition (L1) ^[p.142]
-  0319 - Windows Memory Structure And Management ^[p.96]
-  0321 - Windows Memory Acquisition Techniques ^[p.98]

- 📄0601 - Linux Memory Structure And Management ^[p.114]
- 📄0602 - Linux Memory Acquisition Techniques ^[p.115]
- 📄0401 - Cryptography Basics (L1) ^[p.99]

📄 Detailed Description

The applicant should be able to:

- **Build** an acquisition strategy for systems where shutdown, reboot, login, encryption, endpoint protection, or business continuity creates risk.
- **Explain**, at a high level, how full-disk encryption, TPM-backed key release, hibernation, suspend state, and memory-resident secrets influence acquisition timing.
- **Compare** acquisition options for physical systems, VMs, suspended systems, crash dumps, hibernation files, cloud workloads, and enterprise-managed endpoints.
- **Evaluate** acquisition quality and risk when using live tools, hypervisor-level capture, crash dump generation, or artifact-based memory reconstruction.
- **Identify** when advanced specialist support is required rather than attempting unsafe or destructive procedures.
- **Produce** a defensible acquisition plan with alternatives, assumptions, legal constraints, expected artifacts, validation steps, and residual risk.

📄 Related Forensic Process Stages

📄 Identification

📄 Extraction/Preservation

📄 Documentation

6.1.84. 0803 – Memory Analysis and Reporting

The applicant is able to conduct end-to-end memory analysis, extract and validate relevant findings, identify limitations, and produce a clear forensic report that supports technical and non-technical review.



Version

2026-06-03



Level

Intermediate / Advanced



Estimated Workload

Lessons	2 hours
Labs	6 hours
Total	8 hours



Prerequisites

The applicant should prove the knowledge of:

- 0801 - Memory Acquisition (L1) ^[p.142]
- 0320 - Windows Memory Analysis ^[p.97]
- ^[p.30] 0603 - Linux Memory Analysis ^[p.117]
- 0102 - Reporting ^[p.17]



Detailed Description

The applicant should be able to:

- **Describe** a repeatable methodology for memory analysis: intake, image triage, tool selection, artefact extraction, validation, interpretation, and reporting.
- **Use** specialised memory-analysis tools such as Volatility 3, MemProcFS, strings, YARA, carving tools, and timeline helpers where appropriate.
- **Extract** and interpret artefacts related to processes, network activity, files, registry or configuration data, user activity, malware, encryption, and memory-resident secrets where lawful.
- **Identify** anti-forensic indicators and analysis limitations, including missing pages, wrong symbols/profile, acquisition corruption, memory encryption, injected code, or hidden processes.
- **Corroborate** memory findings with disk, log, registry, file, browser, or network artefacts when available.
- **Produce** a defensible report that separates facts, inferences, limitations, confidence, and recommendations.



Related Forensic Process Stages

Identification	Extraction/Preservation	Analysis	Documentation	Presentation
----------------	-------------------------	----------	---------------	--------------

6.1.85. 0901 – Windows Malware Analysis Foundations and Lab Safety

The applicant is able to:

- **Prepare** and document an isolated Windows malware-analysis environment for authorised forensic work.
- **Handle** suspected malware samples safely while preserving evidence integrity and chain of custody.
- **Select** an appropriate static or dynamic analysis workflow based on case context and risk.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	2 hours
Labs	3 hours
Total	5 hours



Prerequisites

The applicant should prove the knowledge of:

- 0101 - Electronic Evidence Admissibility ^[p.16]
- 0102 - Reporting ^[p.17]
- ^[p.44] 0103 - Computer Data ^[p.18]
- 0105 - Hashing (L1) ^[p.21]
- 0117 - Virtual Machines ^[p.58]
- 9903 - GUI Forensic Software ^[p.44]



Detailed Description

The applicant should be able to:

1. **Explain** the legal, ethical, and operational constraints for malware handling in a forensic or training environment.
2. **Prepare** an isolated Windows analysis lab using documented containment controls, snapshots, evidence storage, and rollback procedures.
3. **Preserve** suspected malware samples with hashes, source information, timestamps, storage location, and chain-of-custody notes.
4. **Differentiate** static analysis, dynamic analysis, memory analysis, and reverse engineering at a high level.
5. **Define** analysis stop conditions, escalation points, and safety limitations before execution of any sample.
6. **Document** lab configuration, tool versions, network isolation, sample identity, and analysis assumptions.



Related Forensic Process Stages

Identification	Extraction/Preservation	Analysis	Documentation
----------------	-------------------------	----------	---------------

Observations

This micro-credential is a safety and workflow prerequisite for Windows static and dynamic malware analysis. It does not cover exploit development, evasion, or malware authoring.

6.1.86. 0902 – Windows Static Malware Analysis

The applicant is able to:

- **Analyse** a Windows executable without running it and extract technical indicators, metadata, and likely capabilities.
- **Use** PE structure, strings, imports, resources, signatures, entropy, and other static evidence to form defensible analysis hypotheses.
- **Document** static findings, limitations, confidence, and recommended next analysis steps.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	3 hours
Labs	9 hours
Total	12 hours



Prerequisites

The applicant should prove the knowledge of:

-  0901 - Windows Malware Analysis Foundations and Lab Safety ^[p.145]
-  0102 - Reporting ^[p.17]
-  0105 - Hashing (L1) ^[p.21]
-  0111 - String Encoding ^[p.23]
-  9902 - Hexadecimal Viewer ^[p.43]
-  0308 - Windows Command Line and PowerShell ^[p.81]
-  9903 - GUI Forensic Software ^[p.44]

Detailed Description

The applicant should be able to:

1. **Preserve** a suspected Windows malware sample without executing it and record hashes, file metadata, source, and handling notes.
2. **Identify** file type, PE architecture, compilation metadata caveats, section layout, entropy, imports, exports, resources, overlays, and digital signatures.
3. **Extract** strings, URLs, paths, registry keys, mutex names, API names, configuration-like data, and other candidate indicators.
4. **Recognise** common signs of packing, obfuscation, embedded payloads, suspicious resources, and anti-analysis indicators.
5. **Infer** likely capabilities from static evidence, such as persistence, credential access, discovery, command execution, network communication, or payload staging.
6. **Correlate** static findings with known-good Windows behavior and clearly separate evidence from hypotheses.
7. **Report** static indicators, likely behaviors, confidence level, limitations, and recommended dynamic-analysis questions.

Related Forensic Process Stages

 Identification

 Analysis

 Documentation

 Presentation

Observations

This micro-credential does not require executing the sample. Low-level reverse engineering and code patching are outside this level unless added as a future advanced credential.

6.1.87. 0903 – Windows Dynamic Malware Analysis

The applicant is able to:

- Execute suspected Windows malware in an authorized isolated lab and monitor host, process, registry, file-system, memory, and network behavior.
- Correlate dynamic observations with static findings to describe behavior, impact, and indicators of compromise.
- Preserve analysis artifacts and produce a defensible dynamic-analysis report with limitations and containment notes.

Version

2026-06-03

Level

Advanced



Estimated Workload

Lessons	3 hours
Labs	12 hours
Total	15 hours



Prerequisites

The applicant should prove the knowledge of:

- 0901 - Windows Malware Analysis Foundations and Lab Safety ^[p.145] ^[p.145]
- 0902 - Windows Static Malware Analysis ^[p.147]
- ^[p.113] 0304 - Windows Event Logs ^[p.38]
- 0306 - Windows Registry Analysis ^[p.40]
- 0307 - Windows Process Analysis (L1) ^[p.79]
- 0308 - Windows Command Line and PowerShell ^[p.81]
- ^[p.89] 0314 - Windows Services ^[p.89]
- 0318 - Windows Virtualisation Subsystems ^[p.94]
- 0500 - Network Fundamentals
- 0503 - Network Protocols ^[p.113]



Detailed Description

The applicant should be able to:

- **Prepare** an isolated Windows dynamic-analysis lab, record its baseline state, and verify rollback before sample execution.
- **Execute** a suspected malware sample only in an authorised lab and monitor process, file-system, registry, service, scheduled task, network, and memory-related behavior.
- **Capture** before-and-after evidence, including screenshots, command outputs, logs, exported monitor traces, network captures, and sample-generated artifacts.
- **Correlate** dynamic behavior with static-analysis hypotheses and distinguish observed behavior from inferred intent.
- **Identify** persistence attempts, privilege or defense-related behavior, command execution, lateral movement hints, network callbacks, payload drops, and cleanup behavior when visible.
- **Preserve** dynamic-analysis artifacts, rollback the lab, and document containment status after execution.
- **Report** observed behavior, indicators, confidence, tool limitations, environmental limitations, and recommended follow-up analysis.

Related Forensic Process Stages

 Identification
  Extraction/Preservation
  Analysis
  Documentation
  Presentation

Observations

This micro-credential covers controlled observation and evidence collection. It does not cover bypassing detection, evasion development, exploit development, or malware authoring.

6.1.88. 1101 – Computer Architecture

The applicant is able to identify the main hardware and firmware components of a computer system, explain their role in storage and volatile data handling, and assess their relevance during digital forensic triage, acquisition, and reporting.

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	4 hours
Labs	2 hours
Total	6 hours

Prerequisites

The applicant should prove the knowledge of:

- Computer hardware
- Operating systems

Detailed Description

The applicant should be able to:

- **Identify** CPU, RAM, storage, motherboard, firmware, TPM, expansion cards, and peripheral interfaces.
- **Explain** how CPU architecture, buses, memory channels, storage interfaces, and firmware affect acquisition choices.
- **Recognise** RAM form factors, storage interfaces, PCIe lanes, removable media, and external ports relevant to evidence handling.
- **Explain** the role of BIOS/UEFI, boot order, secure boot, TPM, and hardware virtualisation features at a conceptual level.

- **Distinguish** volatile and non-volatile components and explain what evidence may be lost when power state changes.
- **Document** hardware observations in a way that supports later acquisition and analysis decisions.



Related Forensic Process Stages



Observations

Keep this credential broad enough to serve **storage**, **decryption**, and **memory forensics** and other futur microcreds.

6.1.89. 1102 – Disk Interface

The applicant is able to:

- **Identify** disk drive SATA, NVMe/PCIe, SAS
- **Identify** disk drive interfaces
- **Select** the correct hardware adapter for forensic acquisition
- **Choose** the appropriate write-blocker



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	1 hours
Labs	1 hours
Total	2 hours



Prerequisites

The applicant should prove the knowledge of:

- ...
- ...

Detailed Description

The applicant should be able to:

- Physically **distinguish** between various storage interface standards (M.2 Key M vs. Key B, U.2, mSATA, IDE, SATA, SCSI)
- **Choose** the correct hardware adapter and appropriate write-blocker for forensic acquisition to ensure data integrity

Related Forensic Process Stages

 Identification
  Extraction/Preservation
  Analysis
  Documentation
  Presentation

6.1.90. 1103 – Deletion Mechanism

The applicant is able to:

- **Assess** the likelihood of data recovery based on the drive type (HDD vs. SSD/NVMe)
- **Understand** the impact of TRIM and Garbage Collection on data persistence and forensic recovery

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	2 hours
Labs	2 hours
Total	4 hours

Prerequisites

The applicant should prove the knowledge of:

-  1102 - Disk Interface ^[p.151]

Detailed Description

The applicant should be able to:

- **Explain** to a legal stakeholder why evidence may have spontaneously disappeared from a seized laptop due to TRIM and Garbage Collection features.
- **Contrast** the persistence of deleted data on traditional magnetic platters versus NAND Flash memory.

- **Understand** the active data destruction processes inherent in modern SSD optimisation.

 Related Forensic Process Stages

 Identification	 Extraction/Preservation	 Analysis	 Documentation	 Presentation
---	--	---	---	---

6.1.91. 1104 – Bios Access

The applicant is able to:

- **Do** this thing
- **Do** this other thing
- ...

 Version

2026-06-03

 Level

Basic / Intermediate / Advanced

 Estimated Workload

Lessons	X hours
Labs	X hours
Total	X hours

 Prerequisites

The applicant should prove the knowledge of:

- ...
- ...

 Detailed Description

The applicant should be able to:

- ...
- ...

 Related Forensic Process Stages

 Identification	 Extraction/Preservation	 Analysis	 Documentation	 Presentation
---	--	---	---	---

Observations

6.1.92. 1105 – Bios Type

The applicant is able to:

- **Know** where to navigate in the BIOS
- **Know** if the BIOS is Legacy or UEFI
- ...



Version

2026-06-03



Level

Basic / Intermediate / Advanced



Estimated Workload

Lessons	X hours
Labs	X hours
Total	X hours



Prerequisites

The applicant should prove the knowledge of:

- ...
- ...



Detailed Description

The applicant should be able to:

- **Navigate** a UEFI interface to identify the boot order, disable "Fast Boot" (to allow access to BIOS), and identify the presence of Secure Boot signatures
- **Understand** how the boot mode determines partition interpretation and OS launch procedures
- **Recognise** the impact of UEFI security features on the forensic process
- **Configure** system settings to facilitate forensic access without compromising evidence integrity.



Related Forensic Process Stages

 Identification

 Extraction/Preservation

 Analysis

 Documentation

 Presentation

+ Observations

6.1.93. 1106 – Bios Virtualisation

The applicant is able to:

- **Check** BIOS/UEFI settings or CPU flags to see if hardware virtualisation is enabled (VT-x / AMD-V)
- **Understand** the implications of virtualisation as a method for obfuscating user activity.

 **Version**
2026-06-03

 **Level**
Basic / Intermediate / Advanced

 **Estimated Workload**

Lessons	X hours
Labs	X hours
Total	X hours

 **Prerequisites**
The applicant should prove the knowledge of:

- ...
- ...

 **Detailed Description**
The applicant should be able to:

- **Navigate** low-level system settings to detect active virtualisation features
- **Interpret** hardware flags that indicate a host's capability to run isolated environments

 **Related Forensic Process Stages**

 **Identification**  **Extraction/Preservation**  **Analysis**  **Documentation**  **Presentation**

+ Observations

6.1.94. 1107 – TPM Chip

The applicant is able to:

- **Identify** the physical TPM chip on a motherboard.
- **Understand** the role of the TPM in Full Disk Encryption (FDE) solutions like BitLocker or LUKS.
- **Explain** why moving an encrypted hard drive to a different computer will render the data inaccessible without the recovery key



Version

2026-06-03



Level

Basic / Intermediate / Advanced



Estimated Workload

Lessons	X hours
Labs	X hours
Total	X hours



Prerequisites

The applicant should prove the knowledge of:

- ...
- ...



Detailed Description

The applicant should be able to:

- **Locate** the hardware security module on various motherboard types
- **Explain** the cryptographic binding between the TPM chip and the encrypted storage media
- **Perform hardware-based BitLocker key extraction** via TPM bus sniffing using logic analysers (if no PIN code required on Windows)



Related Forensic Process Stages

Identification

Extraction/Preservation

Analysis

Documentation

Presentation



Observations

6.1.95. 1108 – Memory Management Fundamentals

The applicant is able to explain how operating systems manage physical and virtual memory, and use that understanding to reason about memory acquisition quality and memory analysis results.



Version

2026-06-03



Level

Intermediate



Estimated Workload

Lessons	3 hours
Labs	3 hours
Total	6 hours



Prerequisites

The applicant should prove the knowledge of:

-  1101 - Computer Architecture ^[p.150]
-  0115 - Computer Memory ^[p.56]
-  0103 - Computer Data ^[p.18]



Detailed Description

The applicant should be able to:

- **Explain** virtual memory, paging, page tables, address translation, and memory protection at a practical level
- **Distinguish** process address spaces, kernel address space, shared memory, memory-mapped files, and device memory.
- **Explain** how swap/pagefiles, hibernation, crash dumps, and compressed memory relate to RAM contents.
- **Describe** common memory allocation concepts: heap, stack, pools, slabs, caches, and object reuse.
- **Explain** why memory analysis depends on OS version, kernel symbols, profiles, type information, and acquisition format.
- **Identify** common causes of incomplete or misleading memory findings: acquisition race conditions, missing pages, encrypted/compressed pages, stale structures, overwritten memory, and symbol mismatch.



Related Forensic Process Stages

Identification

Analysis

Documentation

Observations

This credential is the conceptual bridge between Computer Memory and OS-specific memory micro-credentials.

6.1.96. 9901 – Linux Command Line Interface

The applicant is able to:

- **Understand** basic commands in Linux, for managing users, navigating the file system, managing permissions, upgrading the operating system, installing tools, using tools to gather basic session information, creating, analysing and modifying text files, using the output of one tool as the input to another, managing compressed archives, analysing raw data and metadata, manipulating files and conducting basic file system searches.



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	6 hours
Total	9 hours



Detailed Description

The applicant should be able to:

1. **Access** the terminal (command prompt) to **use** CLI commands
2. **Use** the manual pages and help files to **understand** how to use commands
3. **List** the purpose of special Linux directories (/bin, /etc, /var, /dev, /mnt)
4. **Navigate** the Linux file system (ls, cd, pwd, ~)
5. **List, modify** and **create** system users and groups
6. **Differentiate** between super users and standard users
7. **Create** files (touch) and **edit** permissions and owners
8. **Update** and **upgrade** the Linux kernel and **install** or **remove** tools

9. **Utilise** useful informational commands (date, who, whoami)
10. **Create** and **modify** files using redirection (echo) and built-in editors (e.g., nano)
11. **Chain** commands together using piping
12. **List** and **describe** the contents of text files (cat, less, more, head, tail, wc, diff)
13. **Compress** and **extract** archives (tar, gzip, zip, 7z)
14. **View** and **parse** raw data (xxd, strings)
15. **Analyse** file metadata (file, stat)
16. **Copy, move** and **delete** files and folders
17. **Utilise** basic file search with the locate and updatedb commands



Related Forensic Process Stages

 **Extraction/Preservation**

 **Analysis**

 **Documentation**

 **Presentation**

6.1.97. 9902 – Hexadecimal Viewer

The applicant is able to:

- **Open** a file or a forensic image using an hexadecimal viewer (CLI or GUI) to **navigate** in the content using absolute and relative offsets and to **search for, select, interpret** and **export** selected content for further forensic processing



Version

2026-06-03



Level

Basic



Estimated Workload

Lessons	3 hours
Labs	4 hours
Total	7 hours



Prerequisites

The applicant should prove the knowledge of:

-  0101 - Electronic Evidence Admissibility ^[p.16]
-  0103 - Computer Data ^[p.18]
-  0111 - String Encoding ^[p.23]

- 0112 - Date Time Stamps ^[p.24]

Detailed Description

The applicant should be able to:

1. **Open** a file in a hexadecimal editor or viewer and **secure** the content (so it can not be tampered with)
2. **Navigate** in the file using absolute and relative offsets in bytes, sectors and multiples of it expressed in decimal and hexadecimal
3. **Select** a group of bytes
4. Using installed features, **interpret** unsigned and signed integer values, strings and date-time in different formats and endianness
5. **Export** a group of bytes to a raw file

Related Forensic Process Stages

 **Analysis**

 **Presentation**

6.1.98. 9903 – GUI Forensic Software

The applicant is able to:

- **Locate, recover**, and **report** digital evidence using GUI forensic software

Version

2026-06-03

Level

Basic

Estimated Workload

Lessons	5 hours
Labs	9 hours
Total	14 hours

Prerequisites

The applicant should prove the knowledge of:

- 0103 - Computer Data ^[p.18]
- 0105 - Hashing (L1) ^[p.21]
- ^[p.21] 0111 - String Encoding ^[p.23]

-  0112 - Date Time Stamps [p.24]
-  0203 - Regular Expressions (L1) [p.27]
-  0301 - exFAT [p.35]
-  0302 - NTFS (L1) [p.36]

Detailed Description

The applicant should be able to:

1. **Install** and **configure** a GUI forensic tool (e.g., Autopsy)
2. **Navigate** the User Interface to **accomplish** the desired task
3. **Create** a new case and **set** its settings
4. **Add** data sources and **verify** their integrity
5. **Select** and **execute** modules or plugins, and **select** the required ones to **retrieve** the information that is being looked for
6. **Fine-tune** the keyword search module (string extraction options, lists of keywords, sub-string matches and regex)
7. **Use** the image gallery to **browse** the media files
8. **Create** timelines, including filtering based on the type of artefacts
9. **Tag, comment** and **report** artefacts

Related Forensic Process Stages

 **Extraction/Preservation**

 **Analysis**

 **Documentation**

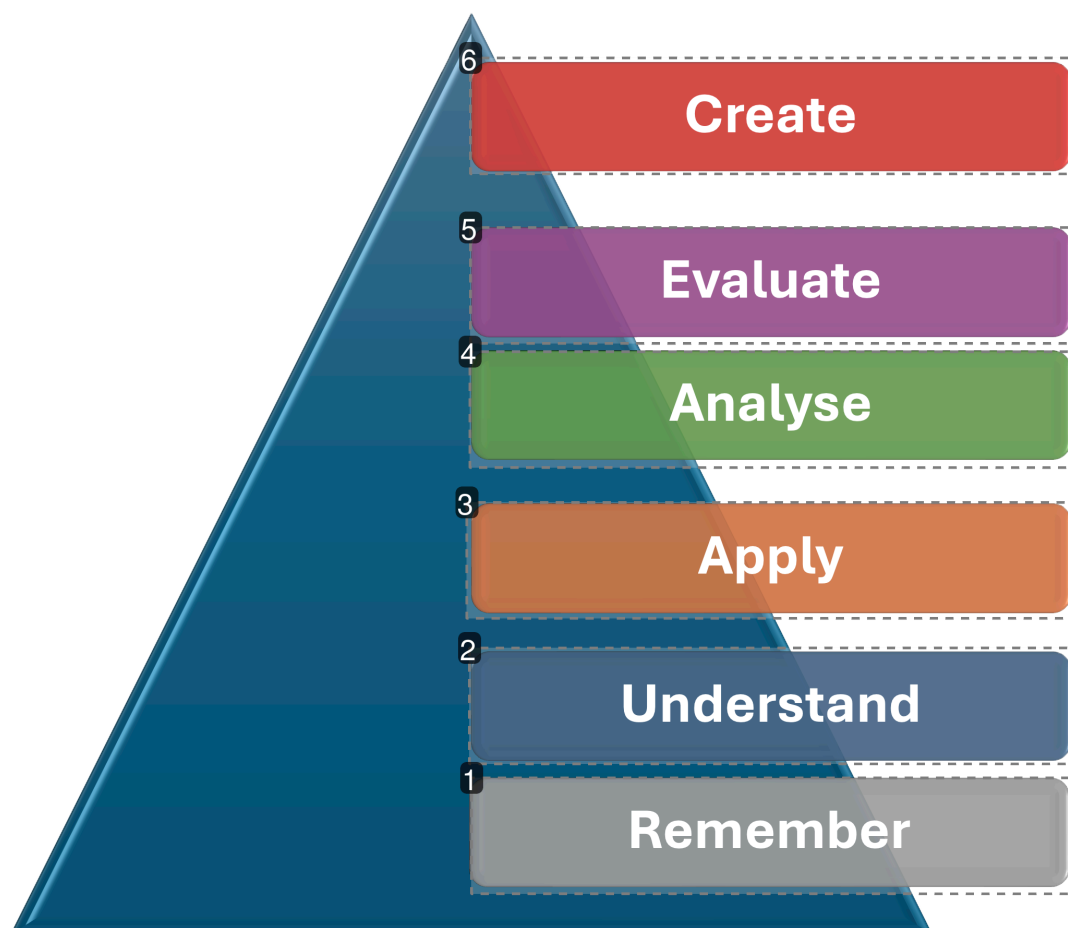
 **Presentation**

6.2. Taxonomy

MCs validate a certain level of knowledge or practice. The levels are described within a taxonomy.

The chosen one is **Bloom's taxonomy**, which is widely used in literature and education strategies.

The taxonomy level defines the styles and complexity of the questions required to assess that an MC is fully addressed by the practitioner.



1. Remember

Remember

Recognise and recall facts and concepts



Operational Verbs

Define, Duplicate, Cite, List, Memorise, Repeat, State, Select, Identify



Example

At the end of the lesson, the attendee will be able to *list* all steps of the digital forensic process in the correct sequence.

2. Understand

Understand

Explain ideas and concepts

Grasp the meaning behind the information and explain it in their own words



Operational Verbs

Classify, Describe, Discuss, Explain, Identify, Locate, Recognise, Report, Report, Select, Translate, Illustrate, Translate



Example

At the end of the lesson, the attendee will be able to *explain with their own words* the importance of the electronic evidence principles and how it may impact the admissibility in front of Court.

3. Apply

Apply

Use information in new situations, use the knowledge in real-life situations to solve problems or perform tasks



Operational Verbs

Execute, Implement, Solve, Use, Demonstrate, Interpret, Operate, Schedule, Sketch, Adapt, Solve, Use, Employ



Example

At the end of the lesson, the attendee will be able to *execute the forensic acquisition* of a whole USB thumb drive using the **dd** tool and *mount* the first exFAT partition in read-only on a Linux forensic box.

4. Analyse

Analyse

Draw connections between ideas

Breaking down information into components or parts and seeing how they relate and work together



Operational Verbs

Differentiate, Organise, Relate, Compare, Contrast, Distinguish, Examine, Experiment, Question, Test, Categorise, Prioritise, Simplify, Inspect



Example

At the end of the lesson, the attendee will be able to *distinguish* which of two identical files recovered from two different devices was downloaded from the Internet by *comparing* the date/time metadata and *examining* the potential alternate data stream.

5. Evaluate

Evaluate

Justify a stand or a decision.

Assess data, make judgments and back up decisions with clear reasoning



Operational Verbs

Appraise, Argue, Defend, Judge, Select, Support, Value, Critique, Weigh, Verify, Validate, Recommend



Example

At the end of the lesson, the attendee will be able to *write a report arguing* that a file was downloaded from the Internet using the available file properties and metadata. They will *defend* their argument by explaining the role of the computer's internal clock and how they *validated* that the time server was not disconnected.

6. Create

Create

Produce new or original work

Combine ideas in new ways to develop original work or innovative solutions



Operational Verbs

Design, Assemble, Construct, Conjecture, Develop, Formulate, Investigate, Author, Integrate, Invent, Plan



Example

At the end of the course, the attendee will be able to *modify an existing* Python script to automatically check the existence of an alternate data stream for all files on an NTFS volume.

6.3. Digital Forensics Stages

Digital Forensics stages

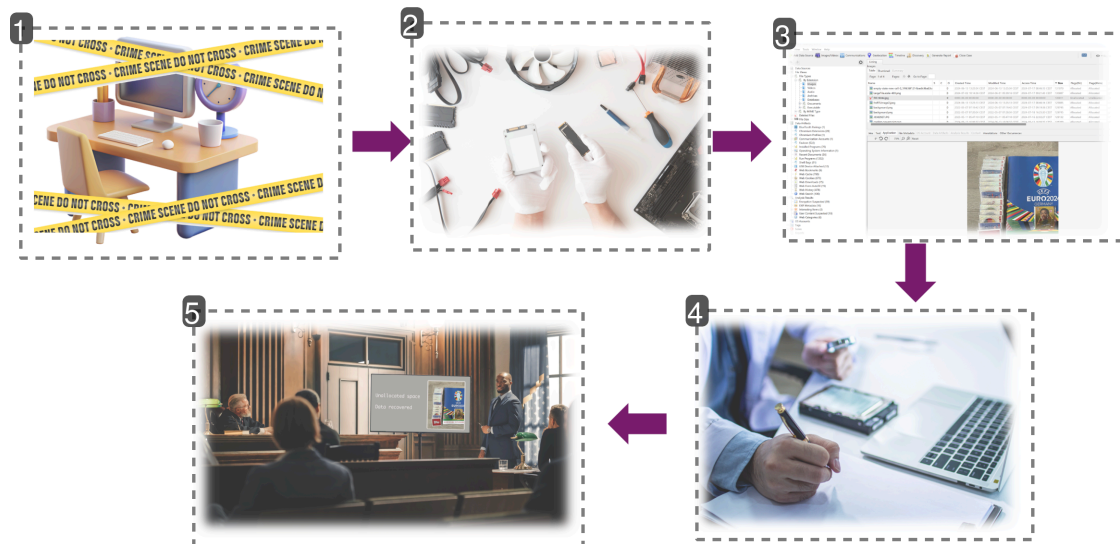
What are the 5 stages of a Digital Forensics Investigation?

Digital forensics involves the recovery, investigation, and analysis of electronic data to uncover evidence for litigation, criminal cases, internal investigations, and data breaches.

Forensic investigators use advanced tools to unearth critical evidence, build timelines of illicit activities, and preserve  evidence in a manner that is admissible in civil and criminal courts.

To properly handle these high-stakes cases, computer forensic investigators conduct a structured and process-driven investigation to ensure the integrity of the data and its admissibility in a Court of Law.

Procedure



1. Identification

The first step in all digital investigations involves identifying all devices and resources that might hold relevant data.

This includes organisational devices such as desktops, laptops, servers, and network systems, as well as personal devices including smartphones, tablets, and external storage media. Each identified device is then carefully seized and isolated to prevent data tampering.

In cases where data resides on servers or in cloud storage, strict access controls are implemented to ensure that only the authorised investigative team can access the data, thereby maintaining its integrity and security.

2. Extraction and Preservation

Once the devices involved in the investigation have been secured, the digital forensics investigator uses specialised forensic techniques to extract all potentially relevant data. This process involves creating a "forensic image", which is an exact bit-by-bit digital copy of the original data.

The forensic image is then used for in-depth analysis, ensuring the original data remains untouched and stored securely in a safe location.

This meticulous approach safeguards the integrity of the evidence, even if the investigation encounters unforeseen issues, preventing any tampering or data loss.

3. Analysis

After securing and duplicating the data, digital forensic investigators employ various advanced techniques to meticulously analyse the extracted data for evidence of wrongdoing.

This process includes:

- **Reverse Steganography:** Extracting hidden data by examining the underlying hash or character string of an image or other data items.
- **File or Data Carving:** Identifying and recovering deleted files by locating and reconstructing file fragments.
- **Keyword Searches:** Using specific keywords to locate and analyse relevant information, including deleted data.

Investigators also use other sophisticated methods to uncover, piece together, and interpret evidence, ensuring a thorough examination of all potential digital clues.

This comprehensive analysis helps build a clear and detailed understanding of the activities in question.

4. Documentation

After completing the analysis, computer forensics investigators meticulously document their findings to provide a clear and comprehensive overview of the whole investigative process and its results.

This documentation includes detailed reports, logs, and visual aids such as charts and timelines, highlighting critical activities involved in the wrongdoing.

Proper documentation ensures that each investigation step is recorded accurately, facilitating the reconstruction of events and the presentation of evidence in legal proceedings. This thorough approach significantly enhances the credibility and reliability of the investigation.

5. Presentation

Upon completing the investigation, the findings are compiled and presented to the appropriate Court, board, or group responsible for deciding the outcome of an allegation.

Digital forensic investigators frequently function as expert witnesses, summarising the uncovered evidence and explaining their analysis and conclusions.

They prepare comprehensive reports and visual aids to illustrate the findings clearly and effectively, ensuring that all relevant evidence is communicated in an understandable and persuasive manner, thereby supporting the judicial or administrative decision-making process.