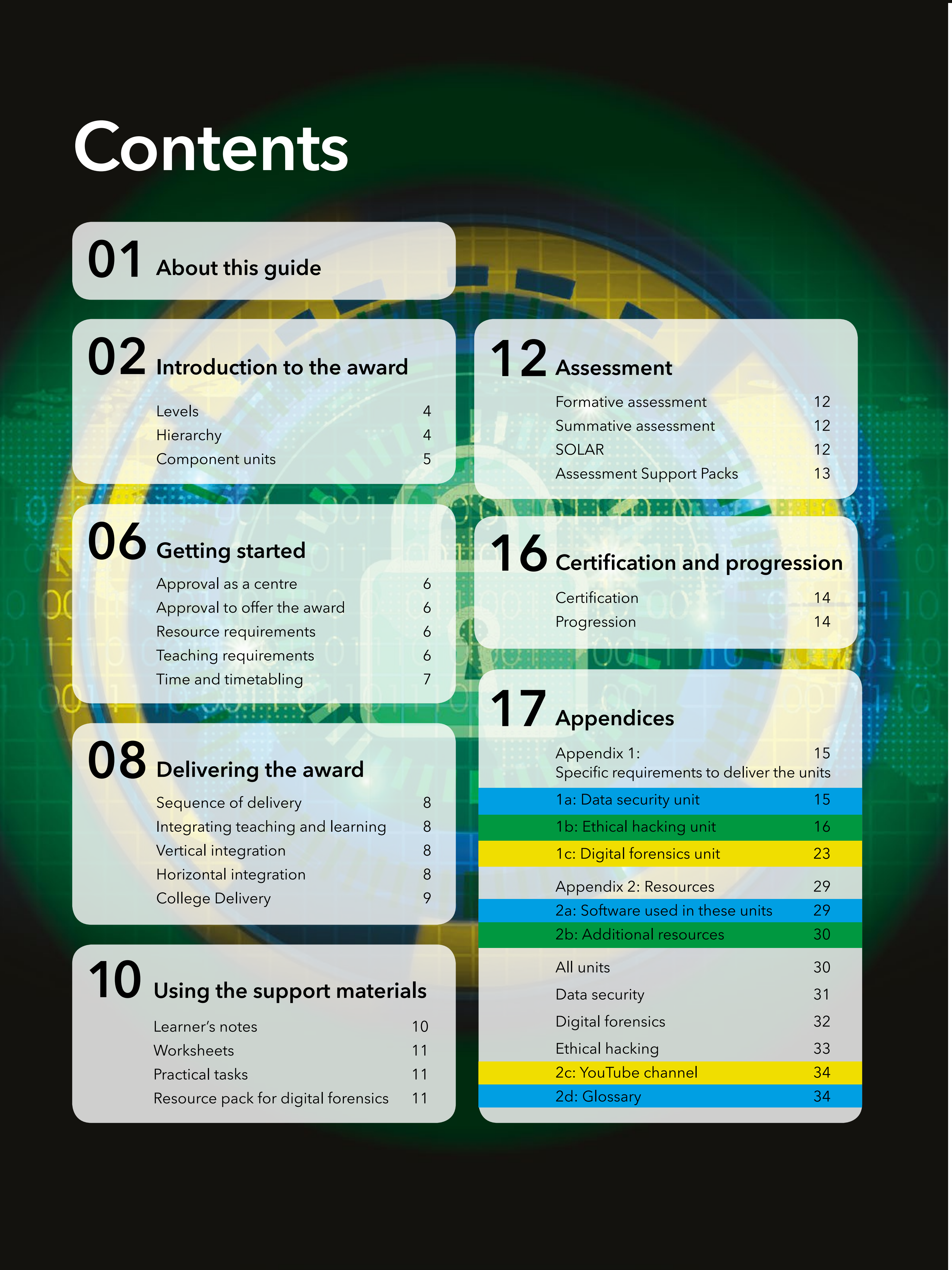
# NPA Cyber Security

## Educator's Guide

**Version 2.0** August 2019

Scottish Qualifications Authority
computing@sqa.org.uk
www.sqa.org.uk

SQA



# Contents

# About this guide

**This guide is intended for educators who are either considering the introduction of this qualification into their centres or who are currently delivering the award. For those considering the qualification, it provides information about its contents, details about resource requirements and advice about getting started. For those who already offer the award, it provides advice on teaching, learning and assessment, and information about support materials.**

The Educator's Guide is a key resource for educators and trainers who are about to, or currently, offer this qualification. It contains vital information about preparation, delivery, assessment and certification of the award.

**Please note: the materials referred to in this guide are not intended as a prescriptive 'content list' for the NPA Cyber Security course; they are intended to support learners and educators embarking on the qualification as a starting point and to support classroom learning and activities. It is expected that educators delivering the course make their own decisions about resources and teaching approaches that will best suit the needs of their learners.**

This document is a digital document, designed for reading on-screen. You can navigate the document using hyperlinks. The document includes links to external resources such as websites and PDFs.

The following diagram shows the process that should be followed when considering this qualification for the first time.

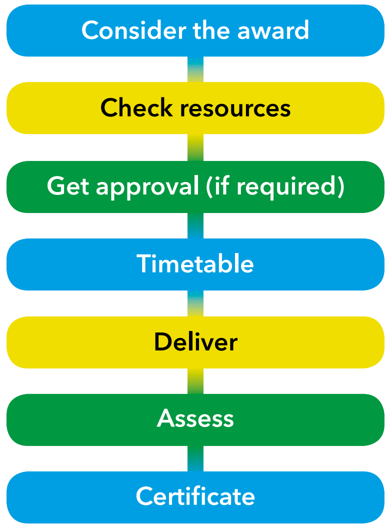

Consider the award
Check resources
Get approval (if required)
Timetable
Deliver
Assess
Certificate

FIGURE 1

This guide is structured to correspond to this process. There are sections corresponding to each sub-process. You can read this document sequentially or go directly to a specific section. For example, if you already deliver the award you may want to go straight to those sections relating to delivery and assessment.

A range of support materials are available to assist with the delivery of this qualification. This document explains what they are and how they can be used.

SQA wishes to thank the Scottish Government for its financial assistance in developing the materials.

# Introduction to the award

**National Progression Awards (NPAs) are vocational qualifications, designed to deliver knowledge and skills in a specific subject area. A wide variety of NPAs exist, with titles such as Digital Literacy, Computer Games Development and Digital Media. As the name implies, NPAs are nationally recognised qualifications that provide progression to further learning in a specific field. They differ from National Qualifications in a number of regards but mainly their focus on practical abilities and their method of assessment.**

The National Progression Award in Cyber Security was first introduced in 2015. The award is popular with learners, particularly at school level where hundreds of learners currently undertake the qualification. The NPA is used in a variety of ways within centres. Within schools, it is used to broaden the curriculum in the senior phase and encourage young people to consider careers in this field. In colleges, it is part of the National Certificate in Computing with Digital Media, which is designed for learners who wish to pursue careers in computing. In training centres, it is used to provide people with practical skills before they enter employment.

The NPA is an entry-level qualification in the field of cyber security, covering three main themes:

Data Security | Digital Forensics | Ethical Hacking

Each of the themes is represented within the qualification by separate units. There are National Units on Data Security, Digital Forensics and Ethical Hacking (see Table 1).

The qualification's subject page is available on the SQA website. This page contains important information about the award, including the group award specification (GAS). This document provides vital information about the qualification's aims, structure, contents and assessment. It should be read carefully.

## LEVELS

The qualification is available at three levels – SCQF levels 4, 5 and 6 (corresponding to National 4, National 5 and Higher). The following table illustrates the qualification structure at each level.

| SCQF level 4 (National 4) | | SCQF level 5 (National 5) | | SCQF level 6 (Higher) | |
|---|---|---|---|---|---|
| H9E2 44 | Data Security | H9E2 45 | Data Security | H9E2 46 | Data Security |
| H9HY 44 | Digital Forensics | H9HY 45 | Digital Forensics | H9HY 46 | Digital Forensics |
| H9J0 44 | Ethical Hacking | H9J0 45 | Ethical Hacking | H9J0 46 | Ethical Hacking |

TABLE 1

The qualification has the same structure at each level. It is awarded to learners who successfully complete all three units at the same level.

Technically, there are three awards – the NPA at level 4, level 5 and level 6. However, this guide will refer to them collectively (and singularly), unless the distinction is important.

## HIERARCHY

The units within the award have been placed into hierarchies (one for each theme). For example, the Data Security units are hierarchical, which means that a pass in the level 6 unit counts as a pass in level 5 and level 4 units. This permits learners to mix and match units across the levels and still gain the group award. For example, if a learner undertakes the level 5 (National 5) award but passes the Ethical Hacking unit at level 4 (National 4), they would gain the group award at level 4 (National 4). The qualification level awarded is the level of the lowest unit passed.

Hierarchies facilitate mixed ability teaching and permit learners to gain the level of award that they are capable of achieving. Decisions about levelling can be left until learners demonstrate their capabilities – when they can be entered for the appropriate level. Assessment has been designed to facilitate this.

## COMPONENT UNITS

There are nine units across the three levels. Each unit has three outcomes. The following table summarises the outcomes in each unit.

| Title | Code | Level | SQA credit value | SCQF credit points | Outcomes |
|---|---|---|---|---|---|
| Data Security | H9E2 44 | 4 | 1 | 6 | 1. Describe how personal data can be stored, used and shared by social media.<br>2. Identify the risks associated with storing and sharing personal data.<br>3. Apply basic practical methods of protecting personal data. |
| Data Security | H9E2 45 | 5 | 1 | 6 | 1. Describe the legal and ethical obligations around storing and sharing personal and business data.<br>2. Explain the causes and effects of data security breaches.<br>3. Protect data against security breaches. |
| Data Security | H9E2 46 | 6 | 1 | 6 | 1. Analyse the approach to data security made by organisations.<br>2. Investigate technologies and strategies used by businesses to protect customer data.<br>3. Create a security strategy for a small business. |
| Digital Forensics | H9J0 44 | 4 | 1 | 6 | 1. Describe the steps in the digital forensics process.<br>2. Apply basic techniques of data acquisition.<br>3. Examine digital evidence. |
| Digital Forensics | H9J0 45 | 5 | 1 | 6 | 1. Explain the digital forensics process.<br>2. Apply relevant techniques in acquiring data.<br>3. Examine digital evidence. |
| Digital Forensics | H9J0 46 | 6 | 1 | 6 | 1. Explain the digital forensics process and job roles.<br>2. Apply complex techniques in acquiring data.<br>3. Evaluate digital evidence. |
| Ethical Hacking | H9HY 44 | 4 | 1 | 6 | 1. Identify current legislation relating to computer crime.<br>2. Describe the basic methods that ethical and malicious hackers use to compromise computer systems.<br>3. Apply basic hacking methods to compromise computer systems in a controlled environment. |
| Ethical Hacking | H9HY 45 | 5 | 1 | 6 | 1. Describe current tools and techniques used by ethical and malicious hackers to compromise computer systems.<br>2. Explain current legislation relating to computer crime and hacking.<br>3. Perform a routine penetration test on a computer system within a controlled environment. |
| Ethical Hacking | H9HY 46 | 6 | 1 | 6 | 1. Analyse current trends in cybercrime.<br>2. Evaluate contemporary legislation relating to cybercrime.<br>3. Perform a complex penetration test on a computer system in a controlled environment. |

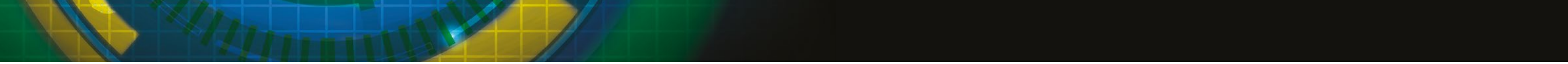
TABLE 2

The unit specification of each unit defines the purposes, outcomes, performance criteria and evidence requirements for each unit. The support notes within each specification provides information about teaching, learning and assessment. You should download the relevant specifications (via the hyperlinks above) and become familiar with their contents.

Table 2 illustrates the relationship between the units in each 'theme'. For example, Outcome 1 in each of the Digital Forensics units relates to the digital forensics process.

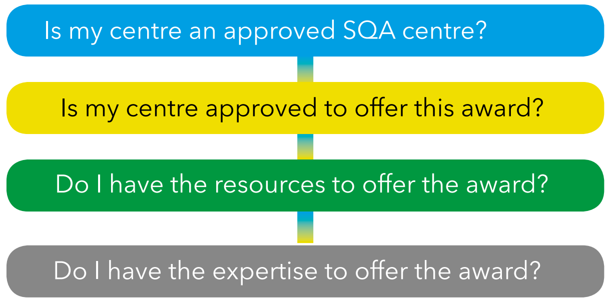
**Level 4:** Describe the steps in the digital forensics process.
**Level 5:** Explain the digital forensics process.
**Level 6:** Explain the digital forensics process and job roles.

This pattern in repeated in all of the units across all of the themes.



# Getting started

**Once you have decided that you would like to offer the award in your centre, you have to consider the following questions.**



Is my centre an approved SQA centre?

Is my centre approved to offer this award?

Do I have the resources to offer the award?

Do I have the expertise to offer the award?

There are two types of approval: (1) approval as a centre, and (2) approval to offer specific qualifications.

## APPROVAL AS A CENTRE

Before you can offer this award, your centre must be an approved SQA centre. Most schools and colleges, and many training organisations, are approved SQA centres. If you have never offered SQA qualifications before, you will require approval.

## APPROVAL TO OFFER THE AWARD

Approved centres require permission to offer specific awards. Schools and colleges in Scotland are automatically approved to offer this award and do not require to undergo any further approval. Other centres must seek approval.

*Further information about approval can be found on the SQA website.*

## RESOURCE REQUIREMENTS

Specialist hardware and software is required to deliver the practical outcomes for this NPA. Furthermore, some units require materials to be prepared in advance of the learners starting a unit. The specific requirements for each unit are detailed in the appendices that follow.  Please note that these preparations and materials are suggestions for centres and that the lists are not exhaustive.

## TEACHING REQUIREMENTS

In order to offer this award, a centre should be able to:

- assign an educator or instructor, who is qualified to teach Computing Science, to support learners through the material
- provide access to desktop or laptop computers capable of running the recommended specialist software
- allow enough class time to complete the course

The award can be delivered by qualified Computing Science educators. However, it would be prudent to investigate the course content and skills required in order to prepare for delivering the course. It is recommended that educators take advantage of related CPD opportunities/further reading to ensure that they are confident in their ability to deliver the award. Practitioners should familiarise themselves with the support materials and work through the practical tasks in preparation for delivery. It is also recommended to make contact with other educators, perhaps in your local learning community, who may be delivering the award in order to share ideas and good practice.

# TIME AND TIMETABLING

**While the exact time allocated to each unit is at the discretion of the centre, the notional design length for each unit (at each level) is 40 hours. Therefore, to deliver all three units, we recommend approximately 120 hours of study.**

Period lengths and timetable structures will vary between centres, so it would be at the discretion of each centre how it timetables the qualification. Learner will require approximately 3 hours per week to complete the course, although this is at the discretion of the centre. It is anticipated that learners will devote some time outside of class to research their work.

Units can be delivered as 'stand-alone' or as part of the group award. It is anticipated that the majority of learners will be attempting the group award; in this scenario, it would be logical to attempt the Data Security unit first, as this contains principles that are relevant to the other units. The Ethical Hacking and Digital Forensics units can be delivered in any order.

Learners may be expected to undertake work outside of timetabled classes in order to develop their knowledge and skills. This will be especially important for levels 5 and 6; learners should be encouraged to learn independently as far as possible.

An alternative approach to unit delivery is to deliver the award holistically. Holistic delivery involves treating the qualification as a single 'course', with a single 'syllabus', which is timetabled, delivered and assessed as a single entity. This is explored further in the next section.

# Delivering the award

## SEQUENCE OF DELIVERY

**The units can be delivered in any order. However, the following sequence is, perhaps, the most logical and will allow learners to gradually gain the required knowledge and skills.**

Data Security → Ethical Hacking → Digital Forensics

Data Security contains knowledge that is required in the other two units. The knowledge and skills gained as part of the Ethical Hacking unit can be used within the Digital Forensics unit to better contextualise learning.

## INTEGRATING TEACHING AND LEARNING

An alternative to unit-by-unit delivery is integrated delivery. Integration of teaching and learning involves identifying and separating topics across units and levels so that the topic is taught once but applied several times. Integration of teaching and learning can be done in one of two ways: vertical integration and horizontal integration. Vertical integration involves combining units at the same level into one course. Horizontal integration involves combining units with the same theme across levels.

## VERTICAL INTEGRATION

Vertical integration involves delivery by level. In other words, the three units at one level are taught holistically. For example, the three units at SCQF level 5 (National 5) are combined into a single course. To facilitate this, the contents of the three units (at the one level) are combined into a single syllabus and educators deliver this syllabus (rather than three separate units).

## HORIZONTAL INTEGRATION

Horizontal integration involves delivery by topic. In other words, the three units relating to one topic are taught holistically. For example, the three units relating to data security are combined into one multi-level topic. To facilitate this, the contents of the three units (relating to the same theme) are considered one topic and educators teach by topic (rather than three separate units).

The approach taken with the learner's notes (see next section) uses horizontal integration. At the time of writing, vertical approaches have not been developed, but it is hoped that this will be done in a later version of the document.

## COLLEGE DELIVERY

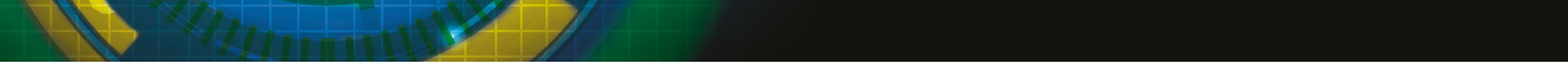
Colleges may have fewer restrictions than schools in terms of network access. The following advice relates to colleges but may be applicable to other centres that have fewer restrictions than those typically affecting schools. Improved network access will permit colleges to create more complex virtual machines to deliver the Ethical Hacking and Digital Forensics units. By doing this, learners can explore different exploits and weaknesses in systems and gain a better understanding of the key concepts.

Colleges may have the ability to have a standalone network set-up for the purposes of this award. This would reduce the impact of the practical tasks on the college's network. The required standalone network may be relatively modest, comprising a few PCs with a laptop as the penetration-testing machine.

**The Data Security** unit would be delivered in college as in any other centre, as the majority of this unit is theory-based, unlike the other units. There is one practical element in level 5, 'configuring a wireless router', but this is something that most centres should manage, provided they can get access to a router. This device does not need to connect to the centre's network in order to complete the task. From a college perspective, some issues may arise when it comes to researching topics due to the security set-up of the college IT department. For example, searching for 'hacking tools' may be blocked in colleges, as is likely in most other centres.

**Ethical Hacking** is the unit for which colleges may be able to provide a different standard of practical set-up to that of other centres, due to their potential flexibility and availability of equipment. An example of a college set-up for Ethical Hacking would be using VirtualBox™ with Kali Linux as the penetration tester machine. Alongside Kali Linux, there could be an operating system, such as Windows 7™ and a Domain Controller, such as Server 2008 (or newer versions). By running these virtual machines together from VirtualBox™, ensuring that they are all set-up on an internal network so as not to access the college network, a network can be emulated to allow the learners to find the weaknesses for different Operating Systems. The more virtual machines that are added to the VirtualBox™ network, the more scope for exploration the learners will have. This will allow them to consolidate the concepts further. Additional learning support could be in the form of SQL injection and WordPress scanning, by setting up a WordPress virtual machine.

**Digital Forensics** is likely to be delivered to the same level in all centres, as this is not as technically demanding as the Ethical Hacking unit is. There are specialised pieces of software that some centres may not have the authorisation or resources to run. Software, such as packet sniffers, may be restricted by the majority of IT departments, regardless of the type of centre. When delivering this unit, centres could potentially use virtual machines to keep the tools off the centre's network and this is where colleges may have more scope than other centres. As with the Ethical Hacking unit, a college could create a more complex set of virtual machines and provide more tools to allow learners to explore the concepts further, rather than potentially learning about tools that they may not be able to actually use.



# Using the support materials

The following support materials are available.

- Learner's notes
- Worksheets
- Practical tasks
- Resource pack for the Digital Forensics unit
- Resource list (included in this Guide as an appendix)
- YouTube channel (link provided in this Guide in the appendix)
- Glossary of terms (included in this guide as an appendix)
- Assessment Support Packs (see the separate section on Assessment)
- Formative assessment questions (see the separate section on Assessment)

These materials are available, on request, from SQA. These materials collectively provide a complete curricular package that permits centres to deliver the award without additional preparation or development of materials.

Items 1–4 are described below. Assessment is discussed in the next section and the Resources, YouTube Channel and Glossary are listed in an appendix at the end of this guide.

## LEARNER'S NOTES

Three sets of learners' notes are available.

Data Security

Ethical Hacking

Digital Forensics

Each set of notes spans all three levels of the award. For example, the Data Security notes cover the award at SCQF level 4, level 5 and level 6. The level within each set of notes is clearly sign-posted. The 'default' is level 4, with sections relating to other levels clearly designated 'level 5' or 'level 6'. Learners need only read those sections that relate up to the level they are attempting. So, for example, a learner attempting level 5 (National 5) would read the 'unlevelled' sections and those sections designated 'level 5'; they would not be required to read any section designated 'level 6'. Please note that those studying at level 6 should read all of the notes and where possible complete all of the worksheets and practical exercises.

The notes are self-contained. Learners are not required to undertake any further reading (although additional reading is recommended). Learners should be able to attempt formative and summative assessments (see next section) using these materials.

The notes follow the sequence of the outcomes and performance criteria in the units. It is anticipated that they will be used in a variety of ways within centres.

## WORKSHEETS

For each unit, a set of worksheets has been created to support the knowledge contained in the Learner's Notes. These are theory-based activities to help reinforce learners' understanding. The Learner's Notes refer to the worksheets, ensuring that learners know when to complete the task. Each worksheet is levelled; it is assumed that a level 6 learner should be completing all of the worksheets.

## PRACTICAL TASKS

The practical tasks are aimed towards Outcome 3 of the units, as this is the practical element. These practical exercises are support mechanisms to prepare the learner for the summative practical assessment.

These are offered as exercises that, if competed, will fulfil many of the course performance criteria, but they are not mandatory.

For the Ethical Hacking unit, practical, step-by-step instructions are included in the pack which will take learners through the process of 'hacking' a target machine.

The Digital Forensics unit **does require materials to be prepared in advance** of the learners starting the practical exercises. A Resource Pack (described below) is provided to help with this.

An appendix to this guide deals with the preparations needed to deliver the practical tasks and practical assessment for each of the units.

Needless to say, it would be beneficial for educators to familiarise themselves with these materials and adapt as appropriate.

Centres may choose to use any or all of the practical exercises provided for each unit. These practical exercises may be subject to capabilities of the centres in terms of hardware, software and flexibility. The concepts should still be delivered, even if the techniques cannot be fully put into practice.

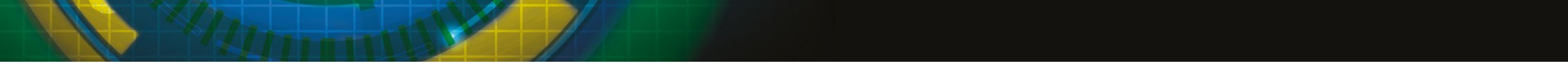
## RESOURCE PACK FOR DIGITAL FORENSICS

Some of the practical tasks in the Digital Forensics units require the learner to use prepared files. These are provided in the Resource Pack.

The Resource Pack is divided into two folders: **Learners and Educators.**

The Learners folder contains five files, (three '.jpg' image files and two '.docx' pro forms for learners to complete their reports for two of the tasks.) These files should be copied to each learner's documents space.

The Educators folder contains a large variety of folders and files that represent what might have been 'saved' from a hard drive at an alleged crime scene. These are used, as directed later in this Guide to create 'evidence' drives that the learners may examine, visually and then using forensic software to try to uncover potential evidence of a crime. These files should only be used to make up 'evidence' drives.



# Assessment

Assessment of National Progression Awards (NPAs) differs from National Qualifications. There is no final examination or coursework component. Summative assessment comprises a practical activity and a selected response (multiple-choice) test for each unit (see below).

The assessment materials comprise:

- Formative assessment
- Summative assessment

Formative assessment is optional and is undertaken at specific points in each unit. It is used to test knowledge and understanding and diagnose misunderstandings among learners so that an intervention can take place to rectify the problem(s). Summative assessment is mandatory (for certification) and is normally attempted when learning is complete.

## FORMATIVE ASSESSMENT

Sets of formative questions have been prepared for each unit. These multiple-choice and multiple-response questions are provided on SOLAR (please see the section on using SOLAR later in this guide). The Learner's Notes indicate when formative questions should be attempted.

## SUMMATIVE ASSESSMENT

Each unit has two assessment elements: (1) a practical task and (2) a multiple-choice theory test (accessed via SQA SOLAR). Learners are required to demonstrate that they have achieved all of the performance criteria for that unit by the successful completion of both of these elements.

Learners who are successful in all three units will be eligible for the group award at the level of their lowest achieved unit. This will be PASS/FAIL; learners are not graded.

Centres can devise their own assessments (based on the evidence requirements within each unit specification) or use Assessment Support Packs (ASPs). An ASP is available for each of the nine units. These can be downloaded from SQA Secure.

Learners who achieve different levels of success in the SOLAR assessment and practical assessments for a given unit will be awarded the unit at the lowest level achieved. For example, a learner who achieves a passing grade in the Ethical Hacking unit SOLAR assessment at level 6, but whose practical assessment only meets level 5 performance criteria, can be awarded the Ethical Hacking unit at level 5. There is no need for the learner to sit the level 5 SOLAR assessment.

## SOLAR

SOLAR is an online e-assessment platform that allows assessments to be delivered on various electronic platforms. It is self-marked with automatic feedback for the learners.

The SOLAR tests remain the principle means of summative assessment for the theory-based element of the units at each of the levels. SOLAR assessments will have to be set-up depending on the centre's process for this.

### How to get access

All SQA approved centres can get access to SOLAR for current assessments on subjects that they are delivering. Your centre may already have valid users who can create an account for you and request new subject access. If, however, your centre is new to SOLAR, you can request access to SOLAR via the 'Training and Access' section on their website https://www.sqasolar.org.uk, which is located under the Centres Tab.

### Basics of the system

In order to run SOLAR assessments, Adobe Flash PlayerTM and Adobe readerTM are required on your device (currently version 12 is advised as the minimum).

Once installed and you have been given access to the system, you would use your Centre Login to create other users, upload learner details and to schedule assessments. (The Centre Login can be found on the Home page.)

SOLAR is not linked to the SQA registration and certification systems, so learners have to be uploaded to the SOLAR system, as well as be registered, and certification details submitted to SQA.

Once learners are uploaded, assessments can be scheduled to be taken within a window of up to six months.

Learners will be given a secure 'Keycode' to access the system and run the assessment; once complete, they would then submit or 'Finish' the assessment to see their result and review a full breakdown of their assessment. (Educators can also access functionalities, such as results, learners' scripts and assessment breakdown by topic or outcomes, through their login.)

## ASSESSMENT SUPPORT PACKS

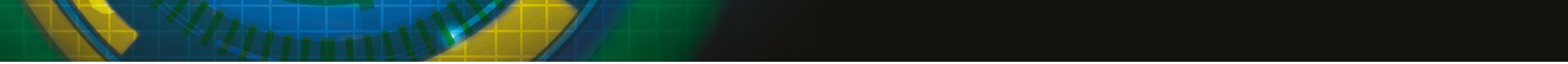
Assessment Support Packs are provided for each of the units at each of the levels. These outline the requirements for the assessment. The theory-based assessment questions are not in the Assessment Support Pack and you are pointed towards SOLAR for this part. The practical-based assessment is in the Assessment Support Pack along with sample answers.

All assessment support packs can be accessed via the SQA secure site (https://secure.sqa.org.uk/). Given the confidential nature of the documents on the secure site, only SQA Co-ordinators are provided with login details. Therefore, requests for ASPs should be processed through the SQA Co-ordinator in your centre.

The following table summarises the assessment approach in the ASP for each unit.

| Unit | Level | Knowledge | Practical |
|---|---|---|---|
| **Data Security** | 4 | Multiple-choice assessment on SOLAR requiring 60% pass mark | Practical assignment involving selection of strong passwords, checking website security and protecting personal data in social media services. |
| **Digital Forensics** | 4 | Multiple-choice assessment on SOLAR requiring 60% pass mark | Select appropriate tools for examining digital evidence. Perform analysis of digital evidence and construct a timeline of events accordingly. |
| **Ethical Hacking** | 4 | Multiple-choice assessment on SOLAR requiring 60% pass mark | Select and apply basic features of software that could be used for hacking (with guidance). Use current methods to defend/ attack a computer system in a controlled environment. |
| **Data Security** | 5 | Multiple-choice assessment on SOLAR requiring 60% pass mark | Identify software and hardware that can be used to enhance security. Identify workplace rules that enhance security and apply methods of improving security to a specific solution. Learners to create a data security solution for a recent data security breach. |
| **Digital Forensics** | 5 | Multiple-choice assessment on SOLAR requiring 60% pass mark | Identify system specific information. Perform an analysis of evidence using software tools. Record findings of the process. |
| **Ethical Hacking** | 5 | Multiple-choice assessment on SOLAR requiring 60% pass mark | Identify the scope of a penetration test on a computer system. Perform reconnaissance of target's footprint. Perform scanning, enumeration and vulnerability scanning on a penetration test. Identify risks, threats and vulnerabilities exposed by penetration test and communicate the results of the test. |
| **Data Security** | 6 | Multiple-choice assessment on SOLAR requiring 60% pass mark | Define cyber security risks faced by small businesses. Explain potential solutions to these threats and create a security strategy for a small business. |
| **Digital Forensics** | 6 | Multiple-choice assessment on SOLAR requiring 60% pass mark | Identify system specific information. Perform hard disk and network analysis. Record the findings of the process. Evaluate the results of the digital forensic examination. Communicate the evaluation results of the forensic examination |
| **Ethical Hacking** | 6 | Multiple-choice assessment on SOLAR requiring 60% pass mark | Scope a system or web-based penetration test. Conduct target information gathering reconnaissance. Use a range of hacking tools and techniques to demonstrate system or web-based vulnerability testing. Conduct system or web-based vulnerability exploit attacks. Identify the risks, threats and vulnerabilities exposed by the test, and how an attacker might leverage them. Communicate the results of the test. |

TABLE 3



# Certification and progression

## CERTIFICATION

Registration of learners can be done via SQA Connect or your college MIS system. SQA Connect is the online portal for SQA approved schools, colleges, employers and training providers (centres), and other approved organisations, to access a range of services that provide delivery and operational support for our qualifications.

Likewise, learners can be resulted via SQA Connect or your college MIS system. Results are only required for the individual units, not the group award. Once all the contributing units have been achieved, a certificate will be issued.

You can find out more about how to register and certificate learners on the SQA website.

## PROGRESSION

The main means of progression is from level to level within the suite of qualifications. For example, a learner who completes the level 4 (equivalent to National 4) award may wish to attempt the level 5 (equivalent to National 5) or level 6 (equivalent to Higher) qualification. Due to the hierarchical nature of the NPAs, it should be possible for learners to progress to higher levels (within the suite) in a compressed amount of time and with reduced assessment.

The award also provides progression to other qualifications. For example, learners who completes the level 5 or level 6 award could progress to HNC Cyber Security. The award (together with additional qualifications) would also permit progression to degree courses in cyber security.

The NPA at level 6 gives **14 UCAS points** that can contribute towards further and higher education course entry.

**https://www.sqa.org.uk/sqa/74738.html**

# Appendices

## APPENDIX 1: SPECIFIC REQUIREMENTS TO DELIVER THE UNITS

### 1A: DATA SECURITY UNIT

### GENERAL HARDWARE REQUIREMENTS

Learners should have access to a modern, networked computer, desktop or laptop that is capable of running modern software. An operating system of Windows 7™ or higher is recommended along with 4GB RAM or higher.

### GENERAL SOFTWARE REQUIREMENTS

A standard office suite such as Microsoft Office™, OpenOffice™ or Pages™/Numbers™/Keynote™.
An up-to-date web browser such as Chrome™, Firefox™, Edge™ or Internet Explorer™.

### WORKSHEET SPECIFIC REQUIREMENTS

There are 31 Worksheets associated with this unit. Each has its level clearly signposted. Most of the Worksheets involve 'paper and pencil' exercises, Internet research tasks or group discussions. There are two exceptions to this:

**TASK 21** involves creating a 'Caesar Cipher Wheel' and gives instructions to the learners on how to do this. This involves printing a single sheet with the wheels on it and then cutting out the two wheels. Educators may find it helpful to have copies of this sheet printed in advance along with a supply of scissors and paper fasteners to join the two discs and just leave the learner to cut out and join the discs - particularly centres that have changed to centralised printing!

**TASK 24** involves creating a 'Pringles Enigma machine'. This involves some construction work by the learner for which they will need:

**Scissors**
Printouts of enigma wiring (Links to download the printouts are provided in the Task)
Glue (Prit-stick™ is fine) - One regular empty Pringles™ tube

Again, it is probably advisable to pre-print the enigma wiring sheets in advance and to collect sufficient empty Pringles cans for the class.

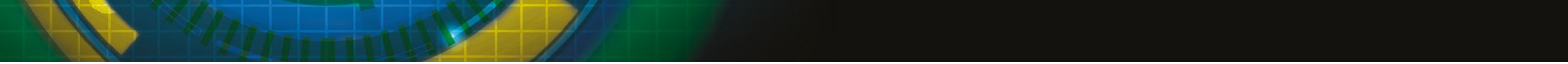
### ASSESSMENT SPECIFIC REQUIREMENTS

The 'practical assessments' for levels 4 and 6 both involve 'paper and pencil' exercises and no additional hardware or software requirements to those already listed.

However, the Level 5 assessment does involve a small practical exercise in which the candidate has to use a web browser to log on to an unprotected Wi-Fi router. They then have to locate the current security settings within the router setup and recommend how these settings could be improved. Make the settings and take a screen shot to show the new secure settings in place as evidence, before returning the router to its unprotected state ready for the next candidate.

The Wi-Fi router does not have to be modern – any redundant Wi-Fi router than can still be assessed through a web browser will do. You do have to know the IP address of the router – often it is something like 192.168.0.1, but there are variations, check the router's documentation. This IP address must be given to the candidate. This router should not be connected to the centre's network or to the Internet.

If the candidate's computer does not have Wi-Fi, then the browser software in a candidate's smartphone will work just as well.



## 1B: ETHICAL HACKING UNIT

In addition to the general hardware and software requirements set out for the Data Security unit, the Ethical Hacking unit does require specialist software.

First and foremost, all hacking exercises must be carried out within a **controlled environment** so that the activities remain firmly within the law!

The controlled environment can take many forms, depending on a centre's circumstances.

1. A university may allow a centre to access their 'hacking lab' remotely through a simple web browser. Which universities offer this? Unfortunately, no definitive answer can be given for this, centres must approach a university individually and ask – some will, some won't!

2. Colleges who deliver Cyber Security courses will have 'hacking labs' already set up for their students. If they have spare time on their timetable, centres may be able to arrange for their learners to visit the college and complete the practical exercises.

To accommodate the use of colleges and university facilities, the practical exercises for the Ethical Hacking unit are deliberately set at the end of the theory materials so that the practical exercises can be completed together within a short block.

3. Some centres may wish to set up a small private network, completely isolated from the centre's network using a collection of redundant computers or even Raspberry Pis. This does, however, require a level of technical knowledge and space within the centre to accommodate the extra equipment.

4. Most centres create a controlled environment on each of the learners' own computers using virtualisation. However, the network security protocols put in place by some councils prevent the use of virtualisation on a centre's computers. If this is the case with your centre, then you must try one of the first three options above.

Virtualisation is a technique that allows one computer (the host) to install and run other operating systems and networks on top of its own operating system. The additional operating systems and networks that are piggy-backing onto the computer are referred to a 'virtual machines'. The host and the virtual machines share the same processor, memory and storage, so the more powerful the host the better the virtual machines will run.

Fortunately, most modern computers have enough memory and have processors that are powerful enough to run virtualisation. Virtualisation allows each computer to be set up with its own independent 'hacking lab'. The 'hacking lab' typically consists of as a minimum, an 'attack' virtual machine and a 'victim' virtual machine connected through a 'virtual network'. Even though the host computer is attached to the centre's network, the virtualisation software is set up so that the 'hacking lab' is completely isolated from the centre's network. However, the virtualisation software must be set up properly for this to happen.

NOTE: While modern PCs and Macs will have no problem running virtualisation software, older PCs may need to have virtualisation switched 'on' at the BIOS level in order for it to run.

A common (and free) virtualisation software is called VirtualBox. It is available for both MacOS and Windows based computers.

- VirtualBox may be downloaded from here.

The most popular 'attack' virtual machine is called Kali. This is a specially developed version of the Linux operating system that comes packed with 'hacking' tools. It is also free.

- Kali may be downloaded from here.

The most popular 'victim' virtual machine that is suitable for beginners is called Metasploitable. Again, this is specially developed version of the Linux operating system that has many vulnerabilities built into it to practice the attacks.

- Metasploitable may be downloaded from here.

## CREATING A CONTROLLED ENVIRONMENT USING VIRTUALBOX

Setting up a virtual machine (VM) on a centre's host computer is subject to certain constrictions:

When running a VM, the host system's resources (processor, memory, backing storage etc.) need to be shared between the host OS and the VM. At the installation stage, decisions need to be made about how much use of these resources will be allocated to each machine. VirtualBox gives the user complete control of this, but there are recommended settings that should work well with the VMs used in these instructions. Generally speaking, most VMs won't require huge amounts of system resources.

The host computer system has a finite amount of backing storage – modern systems have huge amounts of backing storage, ranging from hundreds of Gigabytes to 1 or 2 Terabytes. When installing a Virtual Machine, some of this backing storage will be allocated to the VM. NB: this is not the same as the "minimum storage requirements" for the guest operating system; this is the total amount of backing storage that machine will be able to use. For example, when installing a VM for Windows XP, you may note that the backing storage requirement for XP is 1.5 Gigabytes; If, however, you specify this figure for your storage allocation, that means you will not be able to add any software or files to that machine, as there is only room for the Operating System itself and nothing else! So, it is advisable to allocate some extra storage so that files can be created, programs installed etc. to make the system actually usable.

The storage set aside for the VM will not be accessible from the host system automatically; for all intents and purposes, they are completely separate entities, they just happen to exist on the same computer.

The same applies for Memory and Processor use. When running a VM, the system will need to have the native OS, VirtualBox and the VM OS in memory simultaneously. As such, users decide how much of the host computer's memory to allocate to the VM. This memory is then "ring-fenced" for use by the VM when it is running and will not be accessible to the native system. Processor time is also divided in a similar way.

As a result of this sharing of resources, some users may experience a drop in performance when using VMs, particularly if running more than one. Modern systems with fast processors and large memories shouldn't have any trouble, but you may notice a slight lag. The systems should still be perfectly usable with a reasonable balance between performance and resource use. It should also be noted that there can be a detrimental effect to allocating too much of the system's resources to the VM, which can actually result in lower overall performance.

If you find that the computer has slowed to a snail's pace, then it is worth checking some basics, such as:

- Make sure the computer is not in 'economy / power-saving' mode; this setting will adjust your computers settings to low-power in order to conserve battery but, will 'limit' the speed of your machine. When using VMs, you should ensure your computer is in 'High Performance' mode.
- Check that the allocated memory / backing storage / processing power is enough for the VM. VirtualBox is normally very good at recommending the correct settings, but you may wish to double check.

## INSTALLING VIRTUALBOX

These instructions will act as a guide for installing VirtualBox and setting up a small ‘hacking lab’. Fortunately, this is a straightforward process.

The first step is to visit the VirtualBox Website.
Be sure to download the correct one for your host machine (you will notice different links for MacOS / Windows / Linux systems), then run the installation file and follow all instructions. The instructions in this guide are based on a Windows installation, however the process is very similar to that on MacOS.

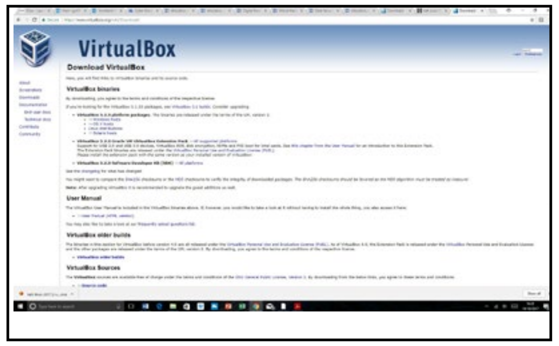
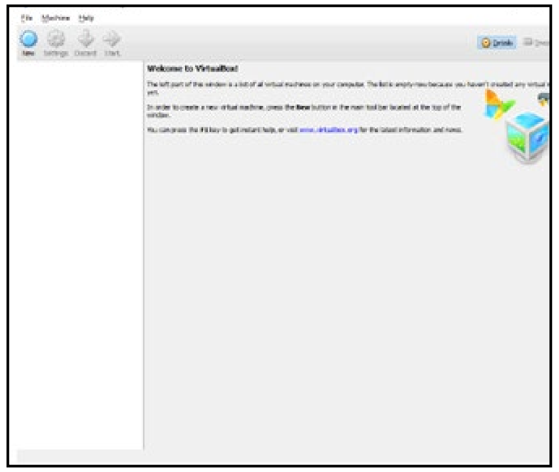


FIGURE 3: VIRTUALBOX WEBSITE

When VirtualBox is installed, click finish and it will launch. The main screen should look something like this (may not be identical, as VirtualBox is regularly updated).

Some useful extra features can be installed via the VirtualBox Extension pack - we will do this now:

1. Go back to the VirtualBox Downloads site and click on the link to download the Extension Pack.
2. From the VirtualBox main screen, go to file-preferences- extensions.
3. Click on the small down arrow on the right side of the window – navigate to the location of the extension pack and select it, then confirm and install.
4. Now that the extension pack is installed, extra features such as access to the host machine’s USB ports and improved performance. A reboot will be required before the changes take effect.



Welcome to VirtualBox!

FIGURE 4: VIRTUALBOX INTERFACE

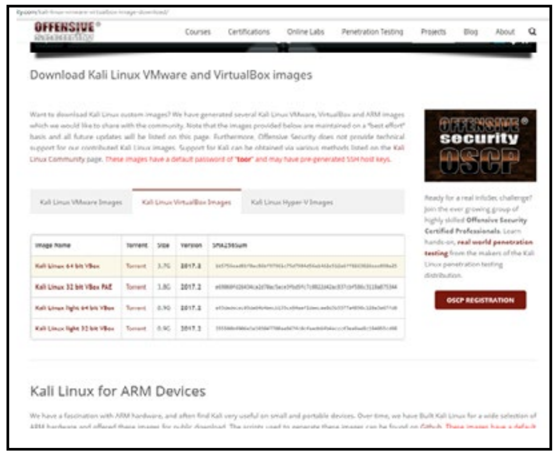
Once this is completed, we are ready to download our first  Virtual Machine – Kali Linux.

## KALI LINUX

Kali Linux is a distribution of Linux specifically produced for Penetration Testing. As such, it comes pre-loaded with lots of software tools that are useful for hacking computer systems.

Some may question the ethics of producing such a distribution, but Kali is merely the tool; like a hammer, it can be used for good, or for ill – that decision is left to the user.

Kali Linux will be the “attacker” machine that we will use to attempt to penetrate the security of other computer systems. A VirtualBox VM for Kali Linux can be downloaded from the Offensive Security website.



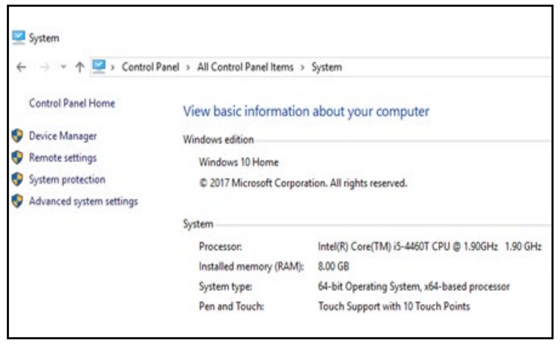
Download Kali Linux VMware and VirtualBox images

Kali Linux for ARM Devices

FIGURE 5: OFFENSIVE SECURITY WEBSITE

As we are using VirtualBox, you will need to make sure you download the correct version; make certain that you choose the “Kali Linux VirtualBox Images” tab before downloading. You will notice there are also Kali VMs available for VMWare; this is another software application that can be used for running Virtual Machines, and essentially does the same job as VirtualBox.

The next thing you will need to make sure of is whether to download the 32-bit or 64-bit version. This will depend on your native computer system. If you aren’t sure which one you have, you can check this in control panel-system:



View basic information about your computer

Windows edition

Windows 10 Home
© 2017 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Core(TM) i5-4460T CPU @ 1.90GHz 1.90 GHz
Installed memory (RAM): 8.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: Touch Support with 10 Touch Points

FIGURE 6: CHECKING FOR 64 OR 32 BIT OS

Here, you can view basic information about your computer. In this example, it clearly states we are using a 64-bit OS, so we should go ahead and download the 64-bit version of Kali Linux.

Once the download is complete, you should have a file called something like “Kali-version-XXX.ova”: This is the Virtual Machine file.

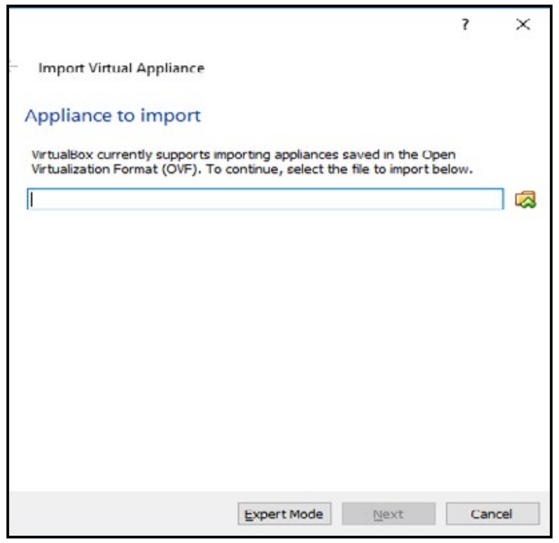
The next thing we have to do is import this VM into VirtualBox.

Launch VirtualBox if it isn’t already running.

Go to file-import appliance.

On the pop-up window, select the small folder icon on the right hand side, and navigate to the “.ova” file you downloaded earlier, then click next.

Follow the wizard to complete the installation, then you should see Kali Linux appear on your VM list in the left-hand pane of VirtualBox.



Import Virtual Appliance

Appliance to import

VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

FIGURE 7: CHOOSING THE VIRTUAL MACHINE FILE

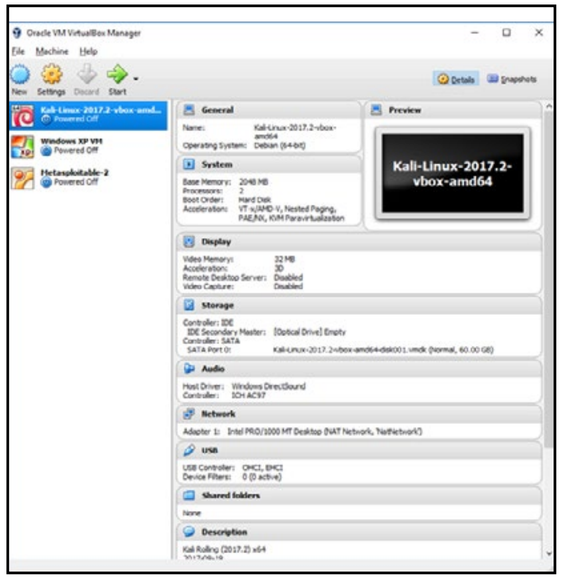
## CONFIGURING THE SETTINGS OF THE VIRTUAL MACHINE

Before Kali Linux is launched for the first time, you must check some of the settings to make sure that the makeshift “hacking lab” is going to work properly.

The network settings are particularly important, as the VMs have to be on the same network so that they can interact with each other. But also isolated from the centre’s network.

In VirtualBox, select the Kali machine. On the right-hand side, under Network, you should see Adapter 1: followed by the name of the network adapter with “NAT Network, ‘NatNetwork’” at the end. Don’t worry if this is not the case; we will fix this over the next couple of steps.

Click on Network



Kali-Linux-2017.2-vbox-amd... Powered Off
Windows XP VM Powered Off
Metasploitable-2 Powered Off

General
Name: Kali-Linux-2017.2-vbox-amd64
Operating System: Debian (64-bit)

System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display
Video Memory: 32 MB
Acceleration: 3D
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali-Linux-2017.2-vbox-amd64-disk001.vmdk (Normal, 60.00 GB)

Audio
Host Driver: Windows DirectSound
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'NatNetwork')

USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

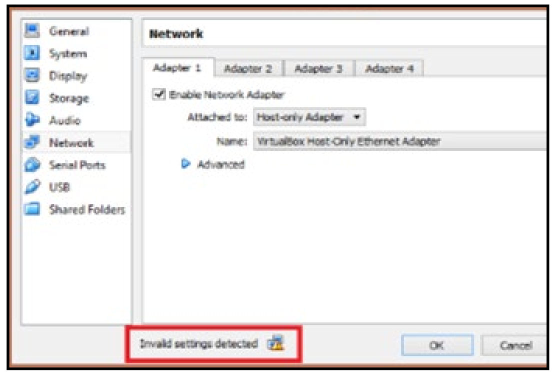
Shared folders
None

Description
Kali Rolling (2017.2) x64

FIGURE 7: CHOOSING THE VIRTUAL MACHINE FILE

If there is a problem, you will see 'invalid settings detected' as below. This means that VirtualBox does not already have a NAT network created; this is easily resolved.

First, cancel out of the Kali settings window, and go to "File – preferences".
Now, click on the Network tab on the left. Leave the tab at the top on NAT Networks, and click the green plus on the right-hand side.
You should see a new item appear called NatNetwork



☑ Enable Network Adapter
Attached to: Host-only Adapter
Name: VirtualBox Host-Only Ethernet Adapter
Invalid settings detected

FIGURE 9: INVALID SETTINGS

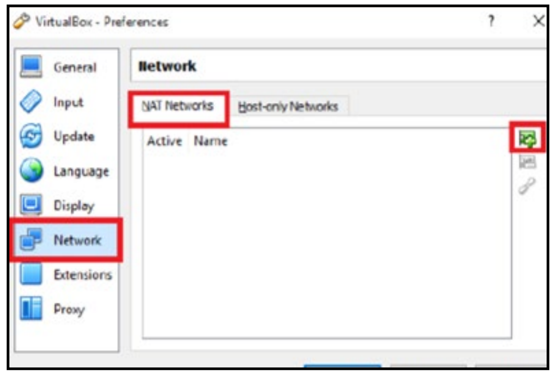
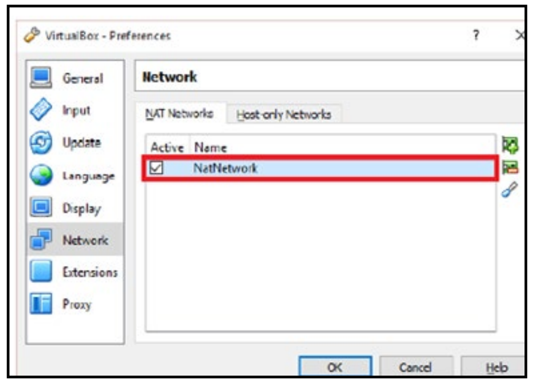


FIGURE 10: CREATING A NATNETWORK

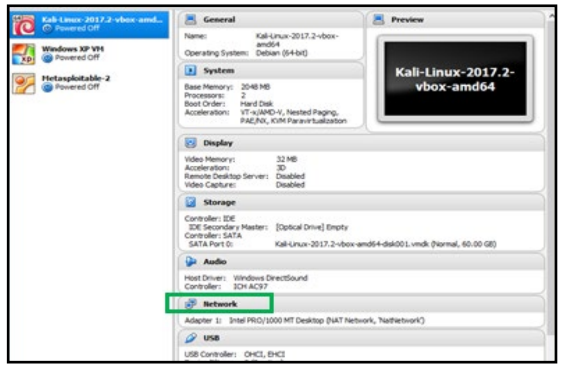
Click OK.

Now that the NatNetwork exists, we need to configure some of the settings for it.
On the main VirtualBox window, select the Network tab again.
You should see that NatNetwork is now selected in the 'name' drop-down box



☑ NatNetwork

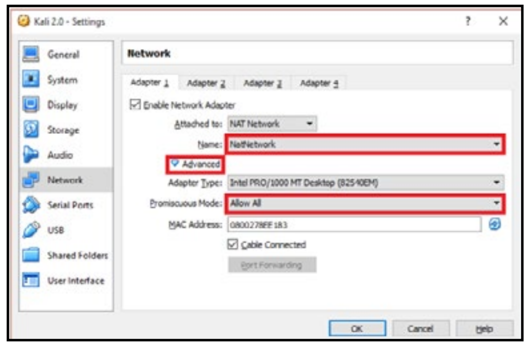
FIGURE 11: NATNETWORK CREATED



Name: Kali-Linux-2017.2-vbox-amd64
Operating System: Debian (64-bit)
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Video Memory: 32 MB
Acceleration: Disabled
Remote Desktop Server: Disabled
Video Capture: Disabled
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali-Linux-2017.2-vbox-amd64-disk001.vmdk (Normal, 80.00 GB)
Host Driver: Windows DirectSound
Controller: ICH AC97
Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'NatNetwork')
USB Controller: OHCI, EHCI

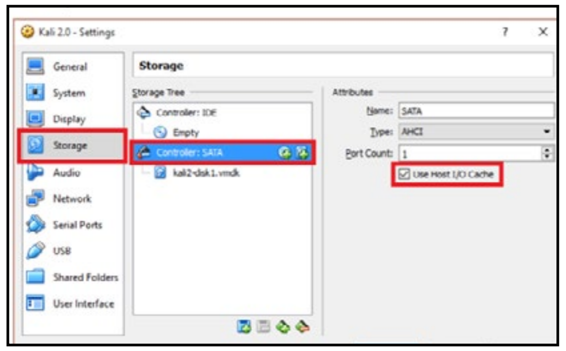
FIGURE 11: NATNETWORK CREATED

Click on 'Advanced' to reveal some more settings, and ensure allow all is selected in the Promiscuous Mode drop down box.
Our network configuration is now complete. There are some more settings that need to be tweaked.
While we have the settings menu open, click on Storage on the left-hand side, then click on Controller: Sata.
Also, make sure that the Use Host I/O Cache is checked



☑ Enable Network Adapter
Attached to: NAT Network
Name: NatNetwork
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Allow All
MAC Address: 080027BFE183
☑ Cable Connected

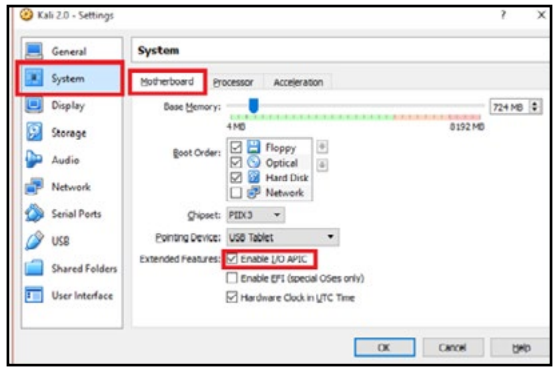
FIGURE 13: DETAILED NETWORK SETTINGS



Name: SATA
Type: AHCI
Port Count: 1
☑ Use Host I/O Cache

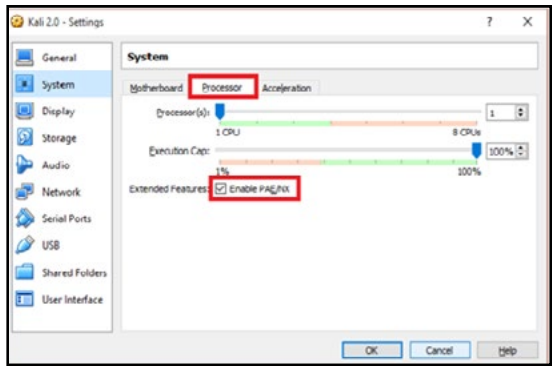
FIGURE 14: STORAGE SETTINGS

Next, click on System on the left-hand side. In the Motherboard tab, check that Enable I/O APIC is checked.
Next, go to the Processor tab and check that Enable PAE/NX is checked.



Base Memory: 724 MB
Boot Order: ☑ Floppy ☑ Optical ☑ Hard Disk ☐ Network
Chipset: PIIX3
Pointing Device: USB Tablet
Extended Features: ☑ Enable I/O APIC
☐ Enable EFI (special OSes only)
☑ Hardware Clock in UTC Time

FIGURE 15: MOTHERBOARD SETTINGS



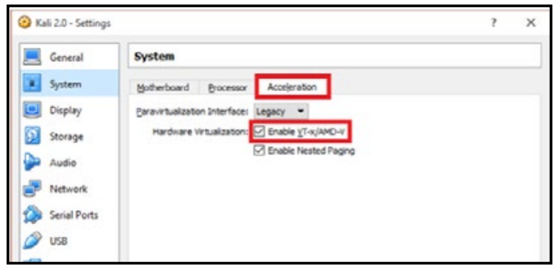
Processor(s): 1
Execution Cap: 100%
Extended Features: ☑ Enable PAE/NX

FIGURE 16: PROCESSOR SETTINGS

Finally, on the Acceleration tab, make sure that Enable VT-x/AMD-V is checked.

Click OK to save these settings. Our Kali Linux machine is now installed and configured.

**NB: You must also check all of these settings for the Metasploitable VM after you install it (later in this guide).**



Paravirtualization Interface: Legacy
Hardware Virtualization: ☑ Enable VT-x/AMD-V
☑ Enable Nested Paging

FIGURE 17: ACCELERATION SETTINGS

## STARTING KALI LINUX

Now that Kali is installed, it can be launched to test the installation.

From the VirtualBox main screen, select Kali, then click "Start" at the top. This will start the virtual machine.

When prompted, the default username for Kali is root, and the password is toor. (in case you don't notice – the password 'toor' is 'root' spelt backwards!) If all goes well, you should see the Kali desktop shortly after entering the credentials; it should look something like the following:

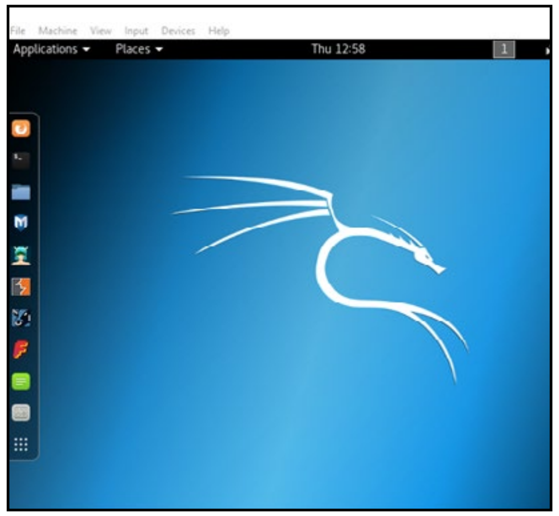


FIGURE 18: KALI LINUX DESKTOP

Now that Kali is up and running, you should take a few moments to familiarise yourself with the interface and have a look around. You should see that this is a complete, self-contained computer within a computer! At the top right, you have access to power and network settings; on the left, you will see the 'dock' which, amongst other things contains shortcuts to an internet browser, a terminal window and the file explorer.

For this course, we will mainly be using the terminal in Kali, the file explorer and a few applications.

If you click on the folder icon on the dock, this will take you to the file explorer. You should see that it isn't all that different to computers that you normally use, storing files and folders in a hierarchical manner.

After you have taken some time to familiarise yourself with the Kali interface, we will leave it be for now so that we can install another Virtual Machine.

## METASPLOITABLE

### What is Metasploitable?

Metasploitable is a Linux based operating system which is designed to be intentionally vulnerable in order to allow people to learn practical hacking skills. It is an ideal "victim" machine on which to begin to practice hacking skills!

### Installing Metasploitable

The first thing to do is download and install the Metasploitable VM. The necessary files can be downloaded from SourceForge.

Go ahead and download Metasploitable. Take a note of where you are saving the download (likely will default to your "downloads" folder) but check to be sure.

Once the files are on your computer (and extracted), they will be imported into VirtualBox.

Installing Metasploitable is exactly the same process we followed to install Kali, so this section will be briefer as you can refer to the Kali installation instructions earlier in this guide.

Click on File – Import Appliance

Click on the folder button with the green arrow to browse your computer and locate the file "Metasploitable 2.ova" (yours may have a slightly different name, but it should be an ".ova" file)

Leave the default settings as they are, then click import.

You should now see Metasploitable alongside Kali in the VirtualBox main screen.

At this point, you should check the settings for the Metasploitable machine, particularly the Network settings, to ensure it is using the same NatNetwork as Kali; if this is not done, the Virtual Machines will not be able to communicate with each other.

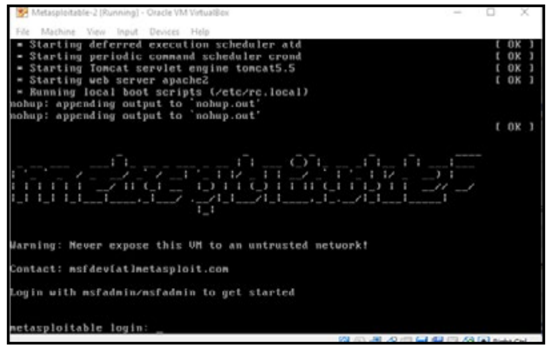
**You must check through each of the settings we configured for the Kali machine and do the same for Metasploitable.**

You can now launch Metasploitable. After a few moments, it will ask you for a username and password; both are "msfadmin".

After logging in, you will be met with the command prompt. Metasploitable does not have a Graphical User Interface like Windows or Kali; it is entirely command driven. It is still a fully operational computer, but you can only use it by typing in the commands. There is no mouse pointer, no windows, no icons etc.

For this course, however, and for anyone who wants to learn about ethical hacking and penetration testing, it is absolutely vital to learn how to use the command line.

When learner's gain access to their "victim" machine, they won't be able to control it with the mouse, or even see the GUI; everything they do will involve using the command line. They can easily access the command prompt on a Linux machine by opening a terminal window.



Metasploitable-2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
 * Starting deferred execution scheduler atd                         [ OK ]
 * Starting periodic command scheduler crond                         [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                          [ OK ]
 * Starting web server apache2                                       [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                     [ OK ]

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: _
```

FIGURE 19: METASPLOITABLE COMMAND LINE INTERFACE

This unit won't be going into learning the command line in this guide, but an excellent starting point is an online course on Codeacademy which will take learners through the basics:

It is strongly recommended that learners (and educators) sign up for a free account and complete this course. It is billed as a '3 hour' course, and it will be time well spent! Knowledge of the command line will allow them to exert more control over computers and accomplish a wider variety of tasks.

An alternative source on using the Linux Command Line is the free book from the Raspberry Pi team that can be downloaded from here.

A virtual machine must be installed and setup on each of the learner's machines. However, this should only need to be completed for the first time the Ethical Hacking course will be run.

## ASSESSMENT SPECIFIC REQUIREMENTS

The 'practical assessments' do not require any additional hardware or software set up.

### 1c: Digital Forensics unit

In addition to the general hardware and software requirements set out for the Data Security unit, the Digital Forensics unit does require specialist software and additional hardware to complete the Practical Tasks and the practical assessments.

### Additional hardware requirements

For all levels of study, each learner will need at least **2 USB Flash drives** for personal use – plus one set up as a potential source of evidence of a crime – plus a similar one set up for the assessment. These later two may be shared between candidates and used in successive years.

One of these USB Flash drives will be used to hold a suite of Digital Forensics applications. It should be at least 16GB capacity. Once created as described later in this appendix, it can be used with learners in successive years.

Some of the practical tasks in this unit require the learner to 'image' a drive or to analyse a drive. This can take hours even with, for example, a 16GB drive! These tasks should be carried out on much lower capacity (250MB – 500MB) drives only. If such low capacity drives are not readily available, then the capacities of larger drives may be reduced. Instructions for reducing the capacity of a USB Flash drive are included later.

Level 6 candidates only will require access to a **computer with Administration** access connected to a **Wi-Fi router**. This may be a redundant laptop or desktop computer. It does not need to have Wi-Fi, as long as it can be connected by an Ethernet cable to the Wi-Fi router. **This computer must not be connected to the centre's network.** The Wi-Fi router may be same as the one used for the level 5 practical assessment in Data Security.

**Task 3** requires the use of some basic Lego blocks to build mini crime scenes.

In addition, learners will be expected to use their own smartphones to record 'crime scenes'.

### Additional software requirements

**Tasks 1** and **2** require access to a basic Paint type program that allows images to be imported and annotated. This will normally be part of the installed software on a centre's computer.

**Task 2** requires two images named Task_2a.jpg and Task_2b.jpg. These are provided in the Learners' folder of the Resources Pack that makes up one of the elements for this unit.

**Task 5** requires the learner to make a 'clone' of recovered files. The files to make up the 'clone' are provided in the Educators folder of the Resources Pack.

**Tasks 8** and **11** requires the learner to examine a 'clone' of recovered files (from **Task 5**) to try to identify potential evidence relating to a crime.

**Task 10** also requires an image named Task_10.jpg which is also included in the Resources Pack.

**Task 14** uses a set of files that were used to train Law Enforcement Officers in Digital Forensic in New Orleans, USA. A link to download the set of files is provided.

**Tasks 11** and **14** are used as 'rehearsals' for the practical assessments at levels 5 and 6. To help the learner complete the tasks, Pro Forma files are provided in the Learners folder of the Resources Pack – DF Task 11 Pro Forma.docx and DF Task 14 Pro Forma.docx. These follow the same pattern as the ones supplied as part of the ASPs for these levels.

There is no one Digital Forensics application that can carry out all of the Tasks required in the Performance Outcomes. Instead a variety of separate applications must be used. Fortunately, these are all portable applications and can be installed on a single USB Flash Drive to create Digital Forensics field kit.

The applications that are required (in the order in which they will be used in the Practical Tasks are as follows:

**FTK Imager** is used to create forensic quality memory and disk images. It may be downloaded from here.

**NOTE:** The software is free, but you have to register with the company and supply a working email address. Once registered you will receive an email with a link to the download. You will also receive a follow-up email asking if you would like pricing for their full software suite – just politely point out that it is for educational purposes only and you won't be buying the suite and they won't annoy you again.

Once downloaded choose to install to a folder called 'Utilities'. The software is portable and can be copied later onto multiple USB Flash Drives.

**Speccy** is used to gather detailed information about a computer's system. Normally this is easily available, but access to it is blocked by restrictions imposed at most centres, so this does the job instead. It may be downloaded from here.

**NOTE:** DO NOT click on the big Install button! Instead click on the 'customize' link just below the button and then on the 'more' link on the next page – this will let you choose where to install the application – choose to install it in the 'Utilities' folder. Again, the application is portable.

**Autopsy** is free Digital Analysis software capable of reading everything on a storage media or an image of storage media – this means it can not only read and extract information from all of the files that are visible, but also from files that have been hidden, disguised, deleted and even from ones that have been partially overwritten. It may be downloaded from here.

This is also portable and should also be installed in the 'Utilities' folder.

**jphswin** is a free basic steganography application. Its download site is found here. (Choose the option on the web page that reads 'Download from here: JPHS for WINDOWS')

This will actually download a 'zip' file that once expanded contains three steganography programs – two of which only run under the Command Line interface, but the third called jphswin.exe will run happily with a GUI on Windows 10 (though it was written for Windows 2005!)

Once downloaded and expanded, copy the jphswin application to the 'Utilities' folder.

**USBDeview** is a free utility that will detail all of the USB devices that have been connected to a Windows based computer since it was first switched on. It may be downloaded from here.

Once downloaded, install it in the 'Utilities' folder.

**NetworkMiner** is used to analyse wired and wireless networks. This application is only required for level 6 learners and candidates. It may be downloaded from here.

**NOTE:** This free software application is capable of capturing all plain text traffic on a network! Under no circumstances should it be installed on a computer attached to the centre's main network.

Once downloaded, again choose to install it into the 'Utilities' folder.

Once all of the above applications have been downloaded and installed in the Utilities folder, the contents of this folder can be simply copied to a USB Flash drive (the 16GB one) for each learner.

Preparing USB Flash Drives for use by the learners.

USB Flash Drives are used throughout the Unit in place of the computer Hard Drives.

Modern Hard drives have very large capacities, which means that it will take a very long time to image or analyse their contents. Even the capacity of readily available USB Flash Drives is too big for training purposes – however, their capacity can be reduced to more a manageable size if you follow these instructions (exactly!)

**Reducing the capacity of a USB Flash Drive**

Since Windows 7, Microsoft has included a utility called Disk Management.

1 First, insert the USB Flash Drive into a spare USB Socket.

2 To access Disk Management, right-click on the Windows 'Start' button in the bottom left corner of the screen.

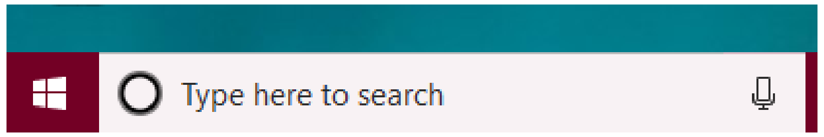


FIGURE 20: METASPLOITABLE COMMAND LINE INTERFACE

This will open up the 'Management' menu

3 Click on Disk Management

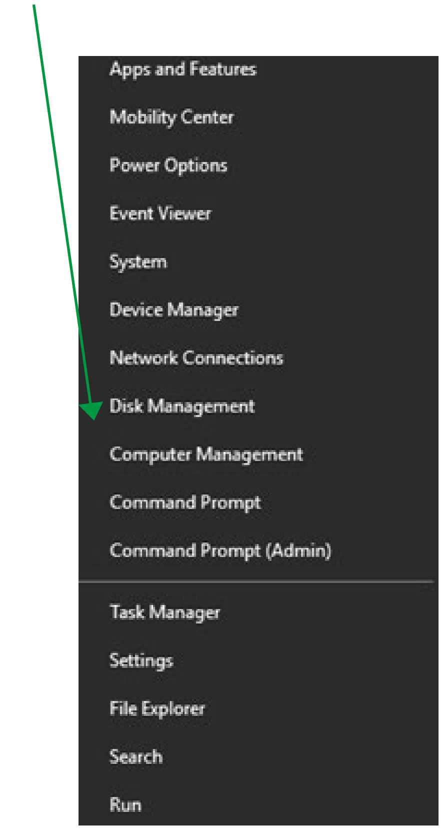
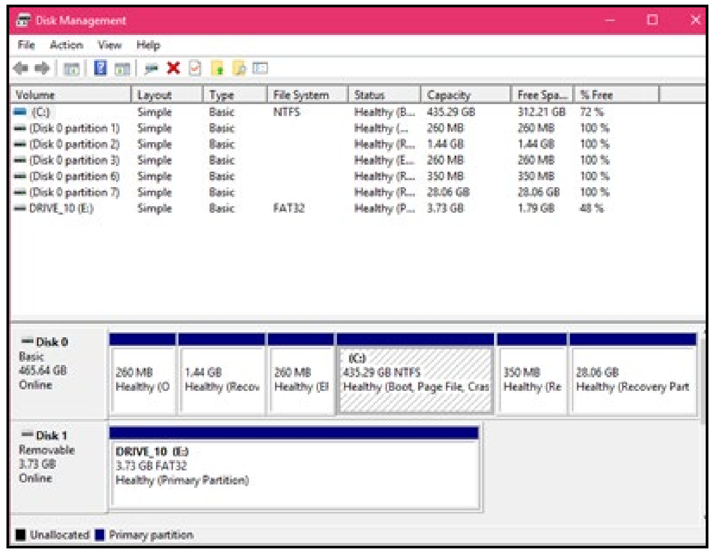


FIGURE 21: WINDOWS MANAGEMENT POPUP



| Volume | Layout | Type | File System | Status | Capacity | Free Spa... | % Free |
|---|---|---|---|---|---|---|---|
| (C:) | Simple | Basic | NTFS | Healthy (B... | 435.29 GB | 312.21 GB | 72 % |
| (Disk 0 partition 1) | Simple | Basic | | Healthy (... | 260 MB | 260 MB | 100 % |
| (Disk 0 partition 2) | Simple | Basic | | Healthy (R... | 1.44 GB | 1.44 GB | 100 % |
| (Disk 0 partition 3) | Simple | Basic | | Healthy (E... | 260 MB | 260 MB | 100 % |
| (Disk 0 partition 6) | Simple | Basic | | Healthy (R... | 350 MB | 350 MB | 100 % |
| (Disk 0 partition 7) | Simple | Basic | | Healthy (R... | 28.06 GB | 28.06 GB | 100 % |
| DRIVE_10 (E:) | Simple | Basic | FAT32 | Healthy (P... | 3.73 GB | 1.79 GB | 48 % |

| | | | | | | |
|---|---|---|---|---|---|---|
| Disk 0<br>Basic<br>465.64 GB<br>Online | 260 MB<br>Healthy (O | 1.44 GB<br>Healthy (Recov | 260 MB<br>Healthy (El | (C:)<br>435.29 GB NTFS<br>Healthy (Boot, Page File, Cras | 350 MB<br>Healthy (Re | 28.06 GB<br>Healthy (Recovery Part |
| Disk 1<br>Removable<br>3.73 GB<br>Online | DRIVE_10 (E:)<br>3.73 GB FAT32<br>Healthy (Primary Partition) | | | | | |

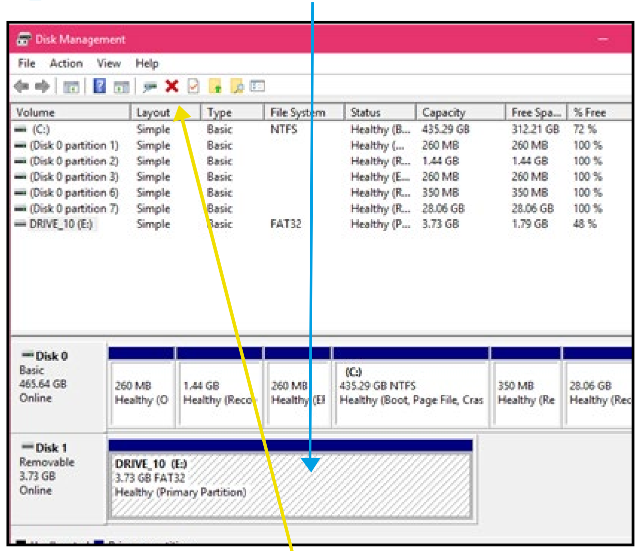
■ Unallocated ■ Primary partition

FIGURE 22: WINDOWS DISK MANAGEMENT UTILITY

In this example a 4GB (3.73GB) drive labelled 'DRIVE_10' is being used, but the instructions are the same for all sizes.

First the drive must be erased – as implied, this wipes all data from the drive so make sure it doesn't contain anything you need!

4 To erase a disk, first click on it to select it:



Disk Management

| Volume | Layout | Type | File System | Status | Capacity | Free Spa... | % Free |
|---|---|---|---|---|---|---|---|
| (C:) | Simple | Basic | NTFS | Healthy (B... | 435.29 GB | 312.21 GB | 72 % |
| (Disk 0 partition 1) | Simple | Basic | | Healthy (... | 260 MB | 260 MB | 100 % |
| (Disk 0 partition 2) | Simple | Basic | | Healthy (R... | 1.44 GB | 1.44 GB | 100 % |
| (Disk 0 partition 3) | Simple | Basic | | Healthy (E... | 260 MB | 260 MB | 100 % |
| (Disk 0 partition 6) | Simple | Basic | | Healthy (R... | 350 MB | 350 MB | 100 % |
| (Disk 0 partition 7) | Simple | Basic | | Healthy (R... | 28.06 GB | 28.06 GB | 100 % |
| DRIVE_10 (E:) | Simple | Basic | FAT32 | Healthy (P... | 3.73 GB | 1.79 GB | 48 % |

Disk 0
Basic
465.64 GB
Online

260 MB Healthy (O | 1.44 GB Healthy (Reco | 260 MB Healthy (EI | (C:) 435.29 GB NTFS Healthy (Boot, Page File, Cras | 350 MB Healthy (Re | 28.06 GB Healthy (Rec

Disk 1
Removable
3.73 GB
Online

DRIVE_10 (E:)
3.73 GB FAT32
Healthy (Primary Partition)

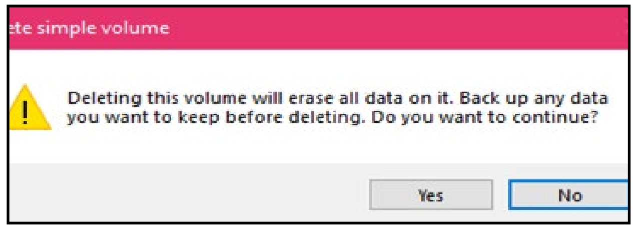
FIGURE 23: ERASING A VOLUME

5 Now click on the red X icon in the command ribbon at the top.

You will see this warning and before you commit yourself to wiping the contents from the disk:

6 If you are happy to continue, click the Yes button.

Once erased it will be labelled 'Unallocated' – at this point you can now reduce the available capacity of the drive.

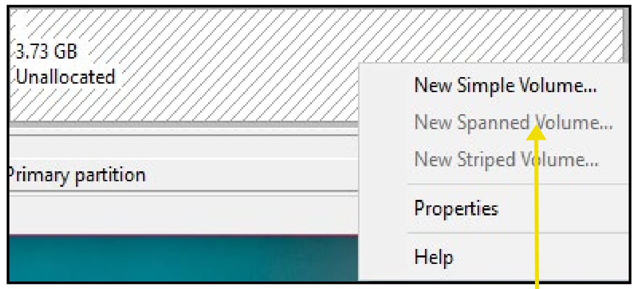


ete simple volume

Deleting this volume will erase all data on it. Back up any data you want to keep before deleting. Do you want to continue?

FIGURE 24: DELETE ALERT

7 Right-click on the drive to see this pop-up menu:



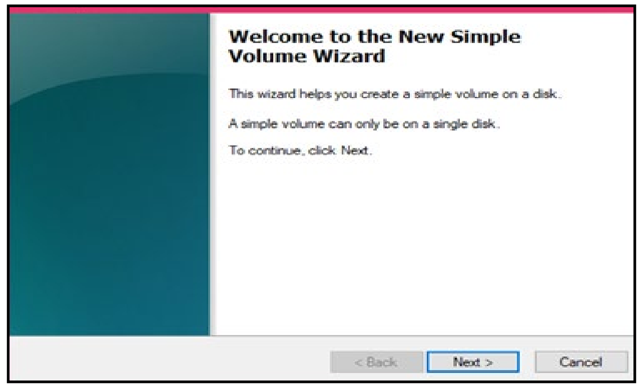
3.73 GB
Unallocated

rimary partition

FIGURE 25: NEW VOLUME POPUP MENU

8 Select the option **New Simple Volume...**

9 Click Next to continue
On the next screen you can set the usable size of the disk.



Welcome to the New Simple Volume Wizard

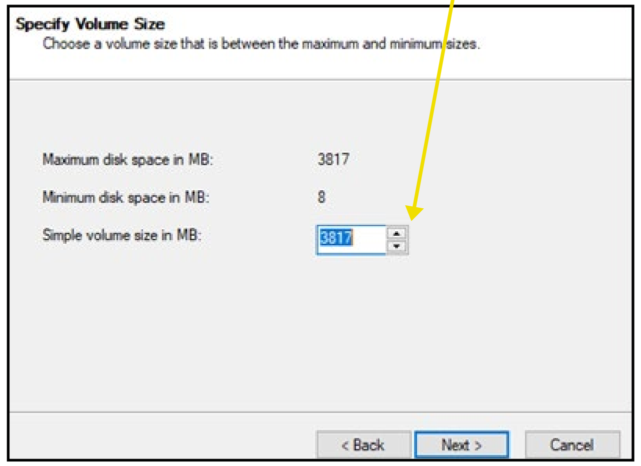
This wizard helps you create a simple volume on a disk.

A simple volume can only be on a single disk.

To continue, click Next.

FIGURE 26: NEW SIMPLE VOLUME WIZARD

10 Change the size to about 200 and then click Next



Specify Volume Size
Choose a volume size that is between the maximum and minimum sizes.

Maximum disk space in MB: 3817

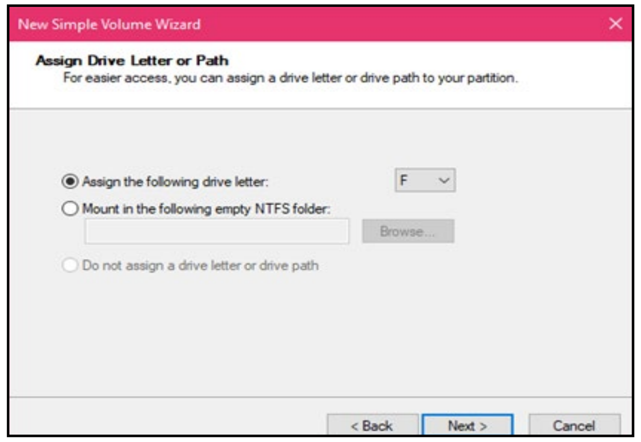
Minimum disk space in MB: 8

Simple volume size in MB: 3817

FIGURE 27: SET THE SIZE OF THE NEW VOLUME

11 Don't need to change anything on this screen so just click Next again.

On the next screen you can choose how you want the new volume formatted.



New Simple Volume Wizard

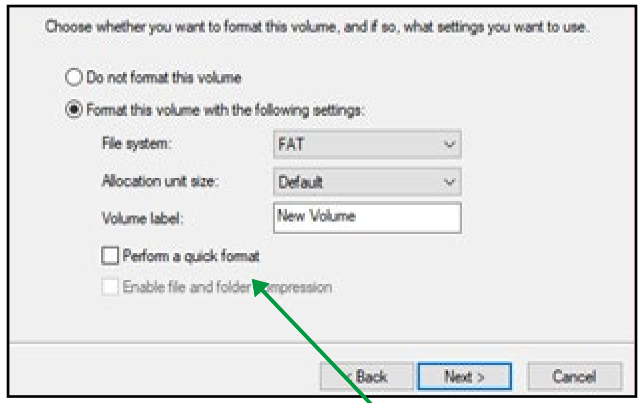
Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.

● Assign the following drive letter: F

○ Mount in the following empty NTFS folder:

○ Do not assign a drive letter or drive path

FIGURE 28: DRIVE LETTER



Choose whether you want to format this volume, and if so, what settings you want to use.

○ Do not format this volume

● Format this volume with the following settings:

File system: FAT

Allocation unit size: Default

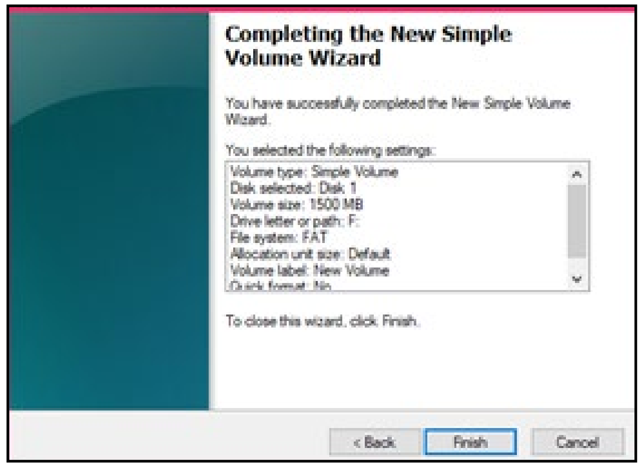
Volume label: New Volume

□ Perform a quick format

□ Enable file and folder compression

FIGURE 29: FORMATTING OPTIONS

12 Make sure **'Perform a quick format' is unchecked!** Give the new volume a meaningful name and click **Next** to show a summary of your decisions up to this point – this is your last chance to change your mind! So, check it carefully!



Completing the New Simple Volume Wizard

You have successfully completed the New Simple Volume Wizard.

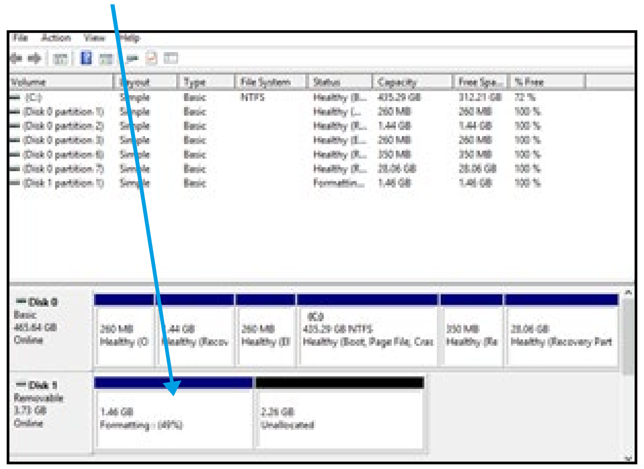
You selected the following settings:

Volume type: Simple Volume
Disk selected: Disk 1
Volume size: 1500 MB
Drive letter or path: F:
File system: FAT
Allocation unit size: Default
Volume label: New Volume
Quick format: No

To close this wizard, click Finish.

FIGURE 30: NEW VOLUME SUMMARY

13 Only when you are satisfied that the settings are correct, click **Finish** to start the process. Depending on the size of the drive, formatting will take a few minutes and you can see the progress in % completed in the main window.



| Volume | Layout | Type | File System | Status | Capacity | Free Spa... | % Free |
|---|---|---|---|---|---|---|---|
| (C:) | Simple | Basic | NTFS | Healthy (B... | 435.29 GB | 312.21 GB | 72 % |
| (Disk 0 partition 1) | Simple | Basic | | Healthy (... | 260 MB | 260 MB | 100 % |
| (Disk 0 partition 2) | Simple | Basic | | Healthy (R... | 1.44 GB | 1.44 GB | 100 % |
| (Disk 0 partition 3) | Simple | Basic | | Healthy (E... | 260 MB | 260 MB | 100 % |
| (Disk 0 partition 6) | Simple | Basic | | Healthy (R... | 350 MB | 350 MB | 100 % |
| (Disk 0 partition 7) | Simple | Basic | | Healthy (R... | 28.06 GB | 28.06 GB | 100 % |
| (Disk 1 partition 1) | Simple | Basic | | Formattin... | 1.46 GB | 1.46 GB | 100 % |

Disk 0
Basic
465.64 GB
Online

260 MB Healthy (O | 1.44 GB Healthy (Recov | 260 MB Healthy (EI | (C:) 435.29 GB NTFS Healthy (Boot, Page File, Cras | 350 MB Healthy (Re | 28.06 GB Healthy (Recovery Part

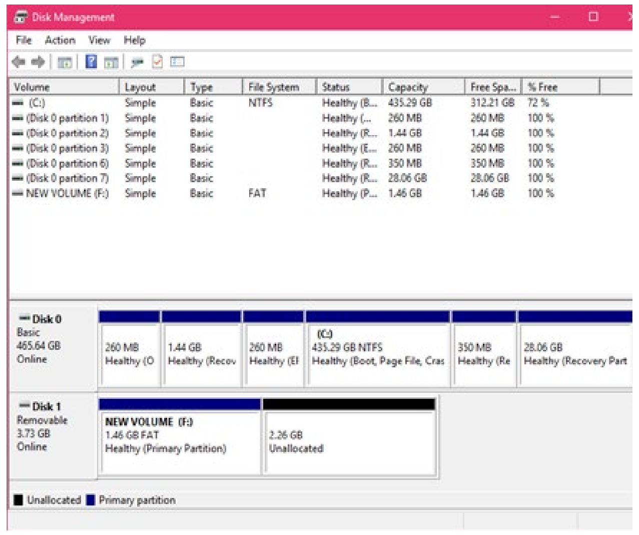
Disk 1
Removable
3.73 GB
Online

1.46 GB
Formatting : (49%)

2.26 GB
Unallocated

FIGURE 31: NEW VOLUME FORMATTING

14 When it is finished you will see the drive with new volume and next to it a section of unallocated storage space. Unfortunately, with the Windows Operating System you cannot access or use this 'unallocated' space on a USB Flash Drive – Windows only recognizes the first volume.



Disk Management

| Volume | Layout | Type | File System | Status | Capacity | Free Spa... | % Free |
|---|---|---|---|---|---|---|---|
| (C:) | Simple | Basic | NTFS | Healthy (B... | 435.29 GB | 312.21 GB | 72 % |
| (Disk 0 partition 1) | Simple | Basic | | Healthy (... | 260 MB | 260 MB | 100 % |
| (Disk 0 partition 2) | Simple | Basic | | Healthy (R... | 1.44 GB | 1.44 GB | 100 % |
| (Disk 0 partition 3) | Simple | Basic | | Healthy (E... | 260 MB | 260 MB | 100 % |
| (Disk 0 partition 6) | Simple | Basic | | Healthy (R... | 350 MB | 350 MB | 100 % |
| (Disk 0 partition 7) | Simple | Basic | | Healthy (R... | 28.06 GB | 28.06 GB | 100 % |
| NEW VOLUME (F:) | Simple | Basic | FAT | Healthy (P... | 1.46 GB | 1.46 GB | 100 % |

Disk 0
Basic
465.64 GB
Online

260 MB Healthy (O | 1.44 GB Healthy (Recov | 260 MB Healthy (EI | (C:) 435.29 GB NTFS Healthy (Boot, Page File, Cras | 350 MB Healthy (Re | 28.06 GB Healthy (Recovery Part

Disk 1
Removable
3.73 GB
Online

NEW VOLUME (F:)
1.46 GB FAT
Healthy (Primary Partition)

2.26 GB
Unallocated

■ Unallocated ■ Primary partition

FIGURE 32: USB WITH REDUCED CAPACITY READY

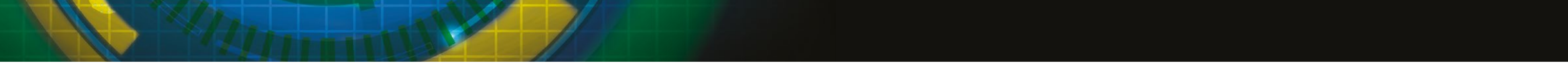
15 The reduced capacity drive is now ready for use.

16 For Task 5, you will add some files to it according to the instructions that follow.

17 You will also need another reduced capacity drive like this, with no files on it, for Task 9.

18 Exit the Disk Management application and safely remove the disk.

19 Repeat the process for as many reduced capacity drives as you require.



## PREPARING A USB FLASH DRIVE FOR USE WITH TASK 5, 8 AND 11.

The **DF Practical Resources Pack** is divided into two folders: **Educator** and **Learner.**

The contents of the Learner folder may be copied onto the shared area of a centre's network so that each learner can have their own copy of each of the files.

The Educator folder must not be copied to the learners' shared area on a centre's network! The contents of this folder are used to create a source of potential evidence of a (fictitious) crime.

This contains the files and folders 'recovered' from a suspect's laptop to match a scenario.

1 Copy all of the folders and files onto a reduced capacity disk (200MB)

This contains all of the files in plain sight, so before the learners can use the drive, some must be deleted:

2 In the **Pictures** folder, delete the 14 files named '**Porcelain 1.jpg**' to '**Porcelain 14.jpg**'

3 In the Documents folder, delete the files named '**Unsuccessful bid EDS.pdf**' and '**Unsuccessful bid EDS 2.pdf**'

4 This must be repeated for each drive. **NOTE**: do not make the deletions first and then copy the folders to the drive – deletions must only be made on the drive to be analysed after the files have been copied!

## PREPARATIONS FOR THE LEVEL 6 TASKS 13 AND 14

**Tasks 13** and **14** involve performing a network analysis using the **NetworkMiner** application.

As stated earlier, this must not be used on the centre's main network!

Instead, set up an old computer (a laptop with Wi-Fi is best) connecting to an old Wi-Fi router (such as the one needed for the practical assessment at Level 5 Data Security unit). The router should not be connected to the Internet.

The computer should be operating with the logged-on user with 'Administrator' privileges and therefore have no restrictions applied to it as NetworkMiner must be '**Run as administrator**' for it operate.

**Task 4** makes use of materials that are used in the training of Digital Forensic Examiners for US Police Forces. The materials should be downloaded as a 'zipped' file from here.

The 'zipped' file contains three network log files and a small image of a suspect's storage medium. All four should be made available to the learners for the task. (They do not need to be on one of the reduced capacity drives.

(NOTE: The answers to this task are also available from this URL)

## ASSESSMENT SPECIFIC REQUIREMENTS

The 'practical assessments' for levels 4, 5 and 6 all involve creating 'evidence' drives to be examined that match a different crime scenario for each level. The instructions for making up the 'evidence' drives from Task 5 should give the assessor a start when making up their own evidence drives. Once made they can be used in successive years each time the course is run.

It is anticipated that the 'evidence' will be localised so that the candidates can relate to the crime scenario. This does require some work by the assessor to make up the evidence drives.

Currently, the SQA does not supply them – the ASP just outlines the crime scenario and leaves it to each centre to make up their own assessment drives. So, the first time the Cyber Skills course runs, the assessor should make sure they start to prepare these 'evidence' drives in advance rather than trying to do them at the last minute when a learner tells them that they are ready for the practical assessment!

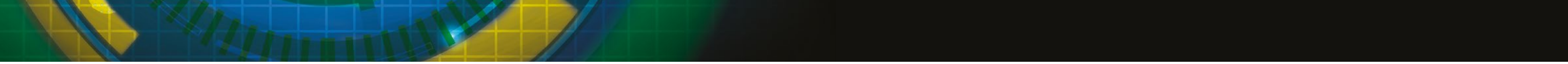
## APPENDIX 2: RESOURCES

Below is a list of resources that have been collated to provide the educator with further information. These are not expected to be given to learners, unless the educator deems that suitable for the cohort. Some of the resources are specific to a unit and some are general that have many useful elements within them for any of the three units. Whilst it is likely that some of the websites included below may be blocked in certain local authority computer systems due to the nature of their content, learners could use them for research outside of class. Alternatively, educators may wish to download resources in order to make them available to learners.

### 2a: Software used in these units

| Item | Description | Use |
|---|---|---|
| **VirtualBox™** | A virtualiser for Intel x86 hardware. | Allows virtual machines to be set-up to create a 'hacking lab'. |
| **Kali Linux** | A Linux distribution containing forensic and hacking tools | Operating system equipped with a wide range of tools for penetration testing and digital forensics. |
| **Metasploitable** | An intentionally vulnerable Ubuntu distribution that can be used to practice intrusion and forensic techniques. | Can be used as 'target' machine in a penetration test |
| **FTK Imager** | Creates disk images. | Used to create forensic image files from drives; may be useful for set-up of Digital Forensics practical work. |
| **Speccy** | Derives system specifications. | Inspects the hardware of a computer system in detail, providing a summary of specifications. |
| **Windows Disk Management** | Disk management tool. Native to Windows OS. | Provides basic information about selected drives, partitions, file system, etc. Allows the available memory of a USB drive to be reduced to a more manageable size. |
| **Autopsy™** | Digital forensics tool. | Performs forensic analysis of storage devices/image files. Able to recover deleted files, display raw hex and perform file signature analysis. |
| **jphswin** | Steganography software | Basic application that allows one JPEG image to be conceal inside another JPEG image. The application also allows the concealed image to be recovered. |
| **USBDeview** | Utility program that documents USB devices | This small application will provide details of all USB devices that have been connected to a computer. |
| NetworkMiner | Tracks all network traffic. | Used for 'packet-sniffing'/network analysis. |

TABLE 4



## 2b: Additional resources

### All units

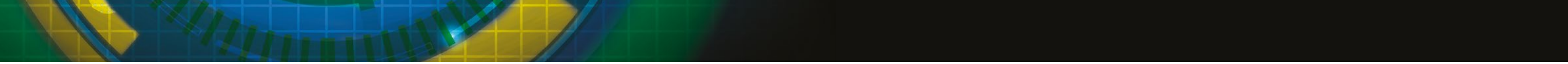
| Resources | Description |
|---|---|
| **Cyber First Courses** | Cyber Security courses available across the UK, which may be of interest to pupils |
| **Threatsaurus** | Downloadable PDF with definitions and descriptions of various cyber threats |
| **Wired News Website** | Tech news website for articles on contemporary cyber security issues |
| **Computer Weekly News Website** | Tech news website for articles on contemporary cyber security issues |
| **Hacker News Website** | Tech news website for articles on contemporary cyber security issues |
| **Info Security News Website** | Tech news website for articles on contemporary cyber security issues |
| **Cybrary Cyber Security Courses** | Collection of free online courses on cyber security/ penetration testing, etc |
| **Tech Partnership** | Collection of IT resources including a Cyber Security simulation game |
| **Cyber Security Text Book** | Cyber Security a Practitioner's Guide, David Sutton, BCS, ISBN 978-1-78017-340-5 |
| **Novalabs Cyber Game** | Online game teaching basic cyber security |
| **Cyber Security Challenge** | Website detailing various Cyber Security challenges and competitions |
| **Introduction to Cyber Security** | Online introductory course on Cyber Security by FutureLearn |
| **CyberSkillsLesson** | A set of simulations covering many aspects of Cyber Security. Although not written to support the NPA, educators may find them a very useful resource for use with the general education Computing courses in S1 – 3 and as introductory lessons for the NPA. |

TABLE 5

## Data Security

| Resources | Description |
|---|---|
| **Women of Influence** | Article on women in Cyber Security |
| **Information Commissioner Office** | Home page for ICO |
| **Book: The Art of Deception** | The Art of Deception, Kevin Mitnick and William Simon, Wiley, ISBN 978-0-7645-4280-0 |
| **8 Simple Rules for Securing your Network** | Article on best practice/advice for securing your own network |
| **Get Safe Online** | Government website giving basic cyber advice and guidance |
| **Cyber Aware** | Government website giving basic cyber advice and guidance |
| **Live Threat Map** | Live map showing cyber-attacks as they occur |
| **Small Business Cyber Guide** | PDF file with government advice for small businesses on Cyber Security |
| **Security Threats for Small and Medium Businesses** | Website with advice on cyber awareness for businesses |
| **Security Checklist for Businesses** | Website with advice on cyber awareness for businesses |
| **National Cyber Security Centre** | Home page of NCSC |
| **10 steps to Cyber Security** | Government strategy/advice for businesses to protect against cyber-attack |
| **Cyber Security Breaches Survey** | Government breakdown of cyber attacks |

TABLE 6



## Digital Forensics

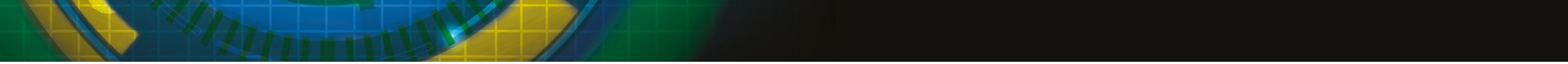
| Resources | Source |
|---|---|
| **Contemporaneous Notes** | Definition and discussion of contemporaneous notes in the context of Digital Forensics |
| **The Basics of Digital Forensics Text book** | The Basics of Digital Forensics (2nd Edition), by John Sammons, Syngress, ISBN 978-0-120801635-0 |
| **Linux Text book** | Linux User & Developer, Issue 182, ISSN 2041-3270 |
| **Good Practice Guide for Computer Based Electronic Evidence** | https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelinescomputer_evidence%5B1%5D.pdf |
| **Introduction to Digital Forensics** | Introductory information to Digital Forensics by Forensic Control |
| **Digital Forensics and Crime** | Government article on Digital Forensics |
| **Forensic Images** | Website offering digital image files for practice |
| **Introduction to Steganography** | Web article introducing digital steganography/data transformation |
| **Online Hex Editor** | Free online hex editor for file analysis |
| **Steganography examples** | Website with some examples of steganographic image files |

TABLE 7

## Ethical Hacking

| Resources | Source |
|---|---|
| **Process of Legislation** | Government website detailing the legislative process |
| **How laws are made** | Government website explaining how a bill becomes law |
| **Data Protection Act** | BBC website explaining the Data Protection Act (About to become out of date, but may be useful for comparison of changes made) |
| **Computer Misuse Act** | BBC Bitesize website explaining the Computer Misuse Act |
| **RIPA** | Description and discussion of RIPA from Justice Website |
| **RIPA 2016** | Government website detailing RIPA |
| **Articles on the misuse of RIPA**<br>**BBC / The Guardian / The Guardian (2)** | Various articles on the misuse of RIPA |
| **Police and Justice Act** | Open Rights Group summary of Police and Justice Act |
| **Cyber Crime news site** | Guardian section on Cyber Crime for contemporary developments |
| **Sony Hack** | BBC news article on Sony Pictures hack |
| **Confidentiality agreement** | Example of confidentiality agreement |
| **RBS Phishing** | Examples of phishing from RBS |
| **Code Academy: Command Line** | Online Linux Command Line course from CodeAcademy |
| **Hack Me: Hack vulnerable sites** | Website offering facilities to attack deliberately vulnerable websites |
| **MD5 hash: encrypt and decrypt password** | Website with functionality for calculating hash numbers |
| **Basics of Hacking Text book** | The Basics of Hacking and Penetration Testing (2nd Edition), by Patrick Engebretson, Syngress, ISBN 978-0-12-411644-3 |
| **Hacking Exposed Text book** | Hacking Exposed (7th Edition), Stuart McClure, Joel Scanbray, George Kurtz, McGrawHill, ISBN 978-0-07-178028-5 |
| **Penetration Testing with Raspberry Pi** | Penetration Testing with Raspberry Pi, Joseph Muniz and Aamir Lakhani, Packt, ISBN 978-1-78439-643-5 |

TABLE 8



## 2c: YouTube channel

A YouTube channel has been created and populated with videos that are relevant to the three units. There are sub-categories for Cyber Security, Data Security, Digital Forensics and Ethical Hacking. These videos have not been sub-divided into levels, as some of them may be appropriate for more than one level. Therefore, it is suggested that these are watched prior to being delivered to a class to ensure suitability for the learners. Educators may wish to show certain videos in order to trigger discussion on certain aspects of cyber security that may inform their work.

## 2d: Glossary

The glossary provides definitions of some of the most commonly used words within the units. These definitions are used throughout the learners' notes, worksheets and practical tasks. The glossary is provided as a support document for learners to ensure that they have an understanding of the common terms used within cyber security. It is recommended that it be provided to learners when they commence the award.

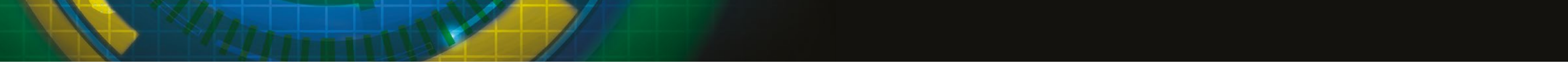
# GLOSSARY OF TERMS

| WORD | DEFINITION |
|---|---|
| **A-B** | |
| Access control | Controlling who has access to a computer, database or online service and the information it stores. |
| Acquisition | The collection and examination of forensic evidence. |
| Analysis | Making sense of data. |
| Asset | Something of value to a person, business or organisation. |
| Authentication | The process, usually through a Username and password, that is used to verify that someone is who they claim to be when they try to access a computer or online service. |
| Autopsy | Public Domain storage analysis software. |
| Back up | A copy of files or data stored on a computer disk or server as a safeguard against loss or corruption of data. Should be on a separate disk in a separate location from the original. |
| Backing Storage | Any non-volatile data storage that will retain a computer's data even after the computer is powered off. |
| Backing up | The process of doing the above. |
| Best evidence | An exact image of memory or storage medium. |
| Biometric Data | Biometric data is a general term used to refer to any computer data that is created during a biometric process. |
| Black Hat Hacker | A person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons. |
| Bring your own device (BYOD) | Where individuals are allowed to use their own digital devices on the corporate setting. |
| Broadband | High-speed data transmission system. |

| WORD | DEFINITION |
|---|---|
| **C-D** | |
| Certificate | Web certificates attest to the genuineness of a website. |
| Certification body | An independent organization that provides certification services, for example Verisign. |
| Chain of Custody | The documentation that records the sequence of custody, control, transfer, analysis, and location of physical or electronic evidence. |
| Checksum | A digit representing the sum of the correct digits in a piece of stored or transmitted digital data, against which later comparisons can be made to detect errors in the data. |
| Cloud | Very large digital storage facilities, situated around the world, that allow users to store their data for them. |
| Cloud computing | Where data or software services are hosted on a remote server instead of on site. |
| Computer Network | A telecommunications network that allows computers to exchange data. In computer networks, networked computing devices exchange data with each other using a data link. |
| Contemporaneous notes | A record of what actions were carried out made at the time they were carried out. |
| Crime | An activity that has been declared as being illegal. |
| Cyber Resilience | Refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events. Cyber Resilience is an evolving perspective that is rapidly gaining recognition. |
| Cyber Security | Cyber security consists of technologies, processes and measures that are designed to protect systems, networks and data from cybercrimes. |
| Data | Facts and statistics collected together for reference or analysis. |
| Data Breach | A security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so. |
| Data Controller | The Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. |
| Data server | Where a server hosts data for common access by a variety of users. |
| Decryption | The process of using a decryption key to make encrypted data readable. |
| Digital Device | Any electronic device that stores digital data. |
| Digital Forensic Examiner/Analyst | The person who will examine and analyse digital evidence. |
| Digital Forensic Technician | The person who will attend the scene of a crime to collect digital evidence. |
| Digital Forensics | Computer Scientific tests or techniques to help solve a crime. |
| Disclosure | The legal requirement for the prosecution to tell the defence what evidence they have on a case. |

| WORD | DEFINITION |
|---|---|
| **E–F** | |
| EnCase | Professional storage analysis software. |
| Encryption | The transformation of data to prevent its information content from being read by users that do not have the correct decryption key. |
| Ethernet | Communications architecture for wired local area networks based upon IEEE 802.3 standards. |
| Ethical Hacker | A person who hacks into a network in order to test or evaluate its security, rather than with malicious or criminal intent. |
| Ethics | Moral principles that govern a person's behaviour or the conducting of an activity. |
| Faraday Bag | A container that prevents its contents from receiving or sending any wireless signals. |
| File carving | A process of reconstructing a file from the different parts stored on storage media such as magnetic hard drives or SD cards. |
| Filter | The technique of reducing the amount of information by concentrating on just a few characteristics. |
| Firewall | Hardware or software designed to prevent unauthorised access to a computer or network from another computer or network by establishing a set of rules that determines what information is allowed pass into and out of a computer. |
| Flash Memory | Read and write memory that retains its contents when power is removed. |
| Forensic Readiness | The ability to collect, preserve and analyse potential digital evidence from computers. |
| Forensics | Scientific tests or techniques used in connection with the detection of crime. |
| **G–H** | |
| Geotag | A digital tag that assigns a geographical location to a photograph or video, a posting on a social media website, etc. |
| Geotagging | Geotagging is the process of adding geographical identification metadata to various media such as a geotagged photograph or video. |
| Hacker | Someone who violates computer security for malicious reasons, kudos or personal gain. |
| Hacking | To gain unauthorised access to data in a system or computer. |
| Hacktivist | A person who gains unauthorized access to computer files or networks in order to further social or political ends. |
| Hard disk | The permanent storage medium within a computer used to store programs and data. |
| Hashing | A process of calculating mathematical 'fingerprint' of computer memory or storage medium that uniquely identifies its contents. |
| Heuristic detection | Heuristic analysis is a method employed by many computer antivirus programs designed to detect previously unknown computer viruses, as well as new variants of viruses already in the 'wild'. |
| Hexadecimal | A shorthand way of representing binary numbers. The digital 0 to 9 and the letters A to F are used to identify groups of 4 binary digits. |
| High Court | The next highest court in Scotland that deals with serious cases that may require long jail sentences. |
| HTTP | Hypertext Transport (or Transfer) Protocol, the data transfer protocol used on the World Wide Web. |
| HTTPS | Hypertext Transport (or Transfer) Protocol Secure is a protocol for secure communication over a computer network which is widely used on the internet. |

| WORD | DEFINITION |
|---|---|
| **I–J** | |
| Identification | The process of recognising a particular user of a computer or online service. |
| IDS | Intrusion Detection System is a device or software application that monitors a network or systems for malicious activity or policy violations. |
| Instant messaging | Chat conversations between two or more people via typing on computers or portable devices. |
| Internet Service Provider (ISP) | Company that provides access to the internet and related services. |
| Intrusion Detection System (IDS) | Program, or device, used to detect that an attacker is attempting or has attempted unauthorised access to a computer system. |
| Intrusion Prevention System (IPS) | As above but also blocks unauthorised access when detected. |
| IP Address | A unique string of numbers separated by full stops that identifies each computer using the Internet Protocol to communicate over a network. |
| ISP | Internet Service Provider – the company the supplies and maintains a user's connection to the internet. |
| Judge | The person appointed to be in charge of how a case is tried in the High Court. |
| **K–L** | |
| Key | A method of scrambling data to keep its contents secret. |
| Keylogger | Malware or physical device that records every keystroke on a computer to secretly capture private information such as usernames and passwords or other sensitive data. |
| Law Enforcement Agencies | Any group or organisation charged by the government to uphold UK law. This includes: Police; Security Services; Military; HM Customs and Excise; etc. |
| Lead Investigator | The person appointed to oversee an investigation. |
| Legal Framework | A set of rules that defines what an examiner can and cannot do in the course of their examination. |
| Legislation | The process of making or enacting laws. |
| Local Area Network (LAN) | Communications network linking multiple computers within a defined geographical location such as an office building, school or college. |
| Lord Advocate | The legal officer in Scotland who is responsible for presenting cases in the High Court. |
| **M–N** | |
| Macro virus | Malware that uses macro scripting through VBA to gain access to data via MS Office files. |
| Malware | Abbreviation of Malicious software. Software designed for malicious purposes such as stealing data or hijacking web links. It includes viruses, worms, Trojans, keyloggers and more. |
| Management system | A set of processes used by an organisation to meet policies and objectives for that organisation. |
| Mass Surveillance | The gathering of large amounts of personal data. |
| MD5 | A type of hashing code used to verify that a copy is identical to the original. |
| Media formatting | The process of preparing storage media to accept files. It creates a new empty directory, ready for the first entry. |
| Memory | In the context of the Digital Forensic notes this refers to Random Access Memory or RAM. |
| Metadata | Data about data that is stored with the data, eg for a photograph, this may include the camera used, the exposure, the lens and the location. |
| Morals | Standards of behaviour; principles of right and wrong. |
| Network firewall | Software device that controls traffic to and from a network. |
| NetworkMiner | Public Domain network analysis software for Windows. |
| nmap | Public Domain network analysis software for Linux. |
| Node | The term given to a digital device connected to a network. |



| WORD | DEFINITION |
|---|---|
| **O–P** | |
| Password | A secret series of characters used to authenticate a person's identity. |
| pcap | The file format used by Network Analysis software to save e its results (Short for 'packet capture'). |
| Penetration test | A software attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data. |
| Personal Data | Any information relating to an identified or identifiable natural person. |
| Personal firewall | Software running on a PC that controls network traffic to and from that computer. |
| Personal information | Personal data relating to an identifiable living individual. |
| Phishing | Method used by criminals to try to obtain financial or other confidential information (including user names and passwords) from internet users, usually by sending an email that looks as though it has been sent by a legitimate organisation (often a bank). The e-mail usually contains a link to a fake website that looks authentic. |
| Phone Service Provider | Companies that provide the structure for us to operate mobile communications devices. |
| Portable device | A small, easily transportable computing device such as a smartphone, laptop or tablet computer. |
| Prime copy | An exact image of memory or storage medium that is kept in case the working copy becomes altered. |
| Private Data | Data that is not made available to the general public, such as passwords and financial account details. |
| Procurator Fiscal | The legal officer in Scotland who is responsible for deciding if a case should go to court for trial or not. |
| Promiscuous mode | The setting of a computer connected to a network that allows it to accept all traffic on the network instead of just traffic addressed to it. |
| Property Register | The form used to record each exhibit that may hold potential evidence in a case. |
| Proxy server | Server that acts as an intermediary between users and others servers, validating user requests. |
| PsTools | A suite of programs that can be downloaded from the Microsoft website for examining the current activity of a computer. |
| **Q–R** | |
| Report | Presenting the relevant facts that occurred in a manner that can be understood by non-experts. |
| Resilience | Preparing for and maintaining continued business operations following disruption or crisis. Cyber resilience means making sure that your system can be restored as quickly as possible. |
| Restore | The recovery of data following computer failure or loss. |
| Risk | Something that could cause an organisation not to meet one of its objectives. |
| Risk assessment | The process of identifying, analysing and evaluating risk. |
| Router | Device that directs messages within or between networks. |
| **S–T** | |
| Screen scraper | A virus or physical device that logs information sent to a visual display to capture private or personal information. |
| Security control | Something that modifies or reduces one or more security risks. |
| Security information and event management (SIEM) | Process in which network information is aggregated, sorted and correlated to detect suspicious activities. |
| Security perimeter | A well-defined boundary within which security controls are enforced. |
| Sensitive Data | Sensitive personal data is defined in Section 2 of DPA and an individual's racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health; sexual life; or criminal offences, sentences, proceedings or allegations. |
| Server | Computer that provides data or services to other computers over a network. |
| SFA1 and 2 | A type of hashing code used to verify that a copy is identical to the original. |
| Sheriff | The person appointed to be in charge of how a case is tried in the Sheriff Court. |
| Sheriff Court | The second lowest court in Scotland that can try cases by jury. |
| Smart | In the context of devices, this means that the device connects to and communicates through the internet |
| Smartphone | A mobile phone built on a mobile computing platform that offers more advanced computing ability and connectivity than a standard mobile phone. |

| WORD | DEFINITION |
|---|---|
| **S–T** | |
| Spyware | Malware that passes information about a computer user's activities to an external party. |
| SQL injection | A computer attack in which malicious code is embedded in a poorly-designed application and then passed to the backend database. The malicious data then produces database query results or actions that should never have been executed. |
| Station | The term given to a computer connected to a network. |
| Steganography | The technique of concealing a file inside another file (detecting them is called steganalysis). |
| Storage medium | The means used to store data – this could be on an SD card, USB Flash Drive, Optical Disk (such as a CD) or a Magnetic Hard Disk. |
| Tablet | An ultra-portable, touch screen computer that shares much of the functionality and operating system of smartphones, but generally has greater computing power. |
| The Cloud | Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the internet, or 'The cloud.' |
| Threat | Something that could cause harm to a system or organisation. |
| Threat actor | A person who performs a cyber-attack or causes an accident. |
| Timeline | A list of events presented in the order in which they occurred. |
| TOR | The 'Onion Ring' A way of routing communications over the internet that makes it very difficult to trace their origins or destinations. |
| Two-factor authentication | Obtaining evidence of identity by two independent means, such as knowing a password and successfully completing a smartcard transaction. |
| **U–V** | |
| USBDeview | Software Application that identifies all USB devices that are currently, or have been in the past, connected to a particular computer. |
| User account | The record of a user kept by a computer to control their access to files and programs. |
| Username | The short name, usually meaningful in some way, associated with a particular computer user. |
| Virtual Private Network (VPN) | Link(s) between computers or local area networks across different locations using a wide area network that cannot access or be accessed by other users of the wide area network. |
| Virus | A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data. |
| Vulnerability | A flaw or weakness that can be used to attack a system or organisation. |
| **W–X** | |
| Wardriving | Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a laptop or smartphone. Software for wardriving is freely available on the internet. |
| Warrant | A legal document provided by a court that gives permission for defined actions to be taken. |
| Warwalking | Same as wardriving, but on foot instead of in a vehicle. |
| White Hat Hacker | Security specialists employed to use hacking methods to find security flaws that black hat hackers may exploit. |
| Wide Area Network (WAN) | Communications network linking computers or local area networks across different locations. |
| Wi-Fi | A means of connecting two or more computers within a localised area (Wireless LAN) using radio technology. |
| Windows Registry | A log kept by computers running the Windows Operating System that holds information about what is happening as the computer is running. |
| Wiretapping | The practice of connecting a listening device to a telephone line to monitor conversations secretly. |
| Working copy | The image of memory or storage medium that will be examined and analysed. |
| Worm | Malware that replicates itself without further user action so it can spread to infiltrate other computers. |
| Write Blocker | A device that can be used to make an exact copy of the memory of digital devices and the contents of storage devices. |

Scottish Qualifications Authority
computing@sqa.org.uk

www.sqa.org.uk