General marking criteria

1. There are two questions. Answer both questions. Note that the two questions are related and both deal with the scenario given below.
2. In all questions, the marks are awarded for addressing the problems set, the quality of your discussion and justification of your assumptions/choices/conclusions etc.
3. You are expected to research your answers and to cite appropriate academic and/or other sources in an appropriate format for the type of report you have been asked to write. It is probably not sufficient to use only the module notes.
4. You may need to make assumptions about the systems involved in order to propose solutions; this is acceptable provided any such assumptions are realistic, clearly stated and do not conflict with any information provided to you.
5. Present your answers on A4 pages, with a minimum 11pt font, minimum 120% line spacing (what Word calls "Multiple 1.08"), and minimum 2cm margins either side.

Each question has an indicated number of pages in which to answer it. Cover page and reference lists or bibliographies do not count towards these limits. Excess pages will not be marked.

Scenario

During the pandemic, the offices of the University of Grand Fenwick's Computer Science dept. had been largely unoccupied, with only essential admin. and support staff on duty. Academic staff have been permitted to access their offices occasionally, in order to pick up essential books, papers and equipment, or between face to face teaching sessions.

Because of this, the IT manager has taken the opportunity to conduct an audit and maintenance exercise to identify all equipment present in dept. and perform essential updates.

During this process, a device was found plugged into a USB docking station in one of the staff offices. The member of staff whose office it is denies all knowledge of this device and reports that it they do not believe it was present when they last checked their office on 4th November 2020. The device was found on 25th January 2021.

The IT manages is concerned that this device may be evidence of a breach, or attempted breach, of security and has requested that you carry out an examination of it and provide further advice (see below).

A suitably qualified technician has imaged the device and will provide you with the image and a record of the examination of the physical device, which includes photographs, any serial numbers etc.

Background - the department runs a mixture of Debian Linux and Windows desktop machines in staff offices, with some staff also using Macintosh, Chrome, Android and iOS devices on the wireless network. It has its own Windows servers for data storage (accessible from Windows and Linux desktops) and a contract with Google for email, cloud data storage and other services (accessible by anyone with a departmental user account).. Access to central University services is available via the dept. network which is connected to the main University network through a managed switch.

Task

1. [40 marks] Examine the device image, and related information, and produce your report, for senior management (some of whom are not IT specialists), giving as much information as possible about the device's involvement, or potential to be involved, in a security breach. Your report is not intended to be used for court proceedings at this stage, but should highlight anything which may be significant should a prosecution be required. *Maximum length: 5 pages.*

2. [60 marks] Produce a plan for how you would conduct an investigation to determine which systems had been affected by an incident involving a device of this type, including details of the nature of any evidence you would hope to recover from affected systems, how/where you would find this evidence, and what it would mean. Your plan should include consideration of any legal as well as technical issues which affect the ability to present any of the relevant evidence in court in this case.

NOTE: This should be a plan which will work for **FUTURE** investigations, and should not necessarily be specific to this incident. It should be possible for a competent IT technician to follow the plan and recover evidence without having to further interpret the plan. The plan must include sufficient information for the IT team to prepare, in advance, for an investigation to be carried out as soon as an incident has been detected. *Maximum length: 10 pages.*

Mark allocation - for guidance only.

In Question 1, marks will be allocated for clarity & usability of your report (10), application of sound forensic methods (10) and use of appropriate analytical & interpretive methods (20).

In Question 2, marks will be given for identification of potential evidence sources (25), consideration of evidential issues (10), evidence of structured planning (15) and overall usability & clarity of the plan (10).