Errata for Sec+ CG 2nd edition (from ProCert comments)

Chapter 3, Pg. 73. Section: Service Packs (add to note at top of page): Another tool you can use to find out the SP level besides msinfo32.exe is the winver command. This can be run in the Run prompt, in the search box, or in the Command Prompt. Either way, it will bring up the "About Windows" window. You can also discern SP levels directly in the Command Prompt. For example, if you open the Command Prompt in Windows 7 and see on the top line "Microsoft Windows [Version 6.1.7600]" then no SP is installed. But if you do this on Windows 7 with SP1 you will see "Microsoft Windows [Version 6.1.7601]". Note the difference in the last number. You can also see this by simply typing ver. You can also find out the OS name, version, and SP level with the following syntax:

systeminfo|findstr /B /C:"OS Name" /C:"OS Version"

Note the pipe symbol between systeminfo and findstr. Also, the text within the quotes is case sensitive.

In this example, the resulting output on a Windows 7 Ultimate OS with SP1 installed would be:

OS Name: Microsoft Windows 7 Ultimate

OS Version: 6.1.7601 Service Pack 1 Build 7601

For the Version/SP level only, omit the following: /C:"OS Name"

Chapter 7, Pg. 250. Section: Wireless Transmission Vulnerabilities (insert as note after third paragraph): Warchalking: Warchalking is the act of physically drawing symbols in public places that denote open, closed, or protected wireless networks. This is done by attackers to let other attackers know about open wireless networks. However, some organizations use the symbols as well to let people know that they have an open wireless network available to the public. In this case, the symbols will be professionally presented. Various symbols are used including the open node (two half circles back to back), closed node (a closed circle), and a circle with a W which stands for a WEP or WPA-encrypted network.

Chapter 12 Pg 425. Section: Encryption Algorithms (Insert as note after RC topic): Blowfish and Twofish are two ciphers designed by Bruce Schneier. The original Blowfish is a block cipher designed as an alternative to DES (the name also pertains to a suite of products). It has a 64-bit block size and variable key size between 1 and 448 bits. Bruce Schneier recommends the newer Twofish cipher which has a block size of 128 bits and a key size up to 256 bits. These symmetrical ciphers have not been compromised as of 2011.

Chapter 12 Pg 432. Section: Cryptographic Hash Functions (Insert as new topic after SHA topic): RIPEMD and HMAC: RIPEMD stands for the RACE Integrity Primitives

Evaluation Message Digest. As of 2011, the latest version (RIPEMD-160) is a 160-bit message digest algorithm used in cryptographic hashing. It is used less than SHA-1 and was designed as an open source hashing algorithm. HMAC stands for Hash-based Message Authentication Code. It is a calculation of MACs through the use of a cryptographic hash function such as MD5 or SHA-1. If for example SHA-1 is used, the corresponding MAC would be known as HMAC-SHA1.

Chapter 15 Pg 532. Section: Incident Response Procedures (insert directly after the seven steps of incident response):

There are many basic forensic procedures that can be utilized within the incident response process. Most commonly, these are applied during steps 3, 4 and 7. Some of these include:

> **Capturing and hashing of system images:** We have already discussed how to capture the image of a computer as well as how to hash files and images but it is important to review these. If a computer's data is to be used as evidence, the entire drive should be imaged (copied) before it is investigated. The imaging process should be secured and logged, and the image itself should be hashed; the hashing process should take place before and after the image is created. This will protect the image from tampering and prove the integrity of the image. Generally, imaging is done to the hard drive of the computer, but if the computer is on, memory and other components/media can also be imaged. It is important to consider OOV when imaging any media, as we will discuss below. (See Chapter 2 and Chapter 11 for more information on capturing images and Chapter 12 for more information on hashing.)
>
> **Capture Video:** Any video surveillance equipment that recorded an incident will need to be analyzed. Before doing so, recorded video should be captured to a computer or to an external media device. Once again, the process should be secured and logged so that a person cannot claim that the evidence has been tampered with. Different municipalities, governments, and organizations will have varying policies on how this is to be accomplished. A forensic analyst should be well versed on these policies before responding to an incident. Keep in mind that the time stamp for video might be incorrect. When this happens, the investigator should establish what "real" time is, using a legitimate time server. The "real" time should be compared to the time stamp of the video. The difference between the two is known as the record time offset.
>
> **Capture Screenshots:** A computer that is being investigated might be compromised. Therefore, it is usually not wise to use screen capturing software that is installed on the affected computer. Instead, take actual photos of the various screens you wish to capture using a camera.
>
> **Network Traffic Captures and Logs:** As part of an investigation, an analyst will review network captures made with network sniffing programs such as Wireshark

or Network Monitor: these are covered in depth in Chapters 10 and 11. Logs should also be preserved, hashed, and stored including firewall logs, server logs, and router/switch logs. Various network device logs are discussed in Chapters 5-7.

Order of Volatility (OOV): OOV can be summarized as the life expectancy of various types of captured data during forensic analysis. For example, CD-ROM discs can be preserved for tens of years, and floppy disks and tape backup can usually be preserved for years. However, information stored in memory, and running processes only last for seconds (or even milliseconds or nanoseconds). The OOV of media and captured data should be considered when gathering evidence that will be used in a court of law.

Witnesses: Witnesses are people who were present during an event and were cognizant of what happened during the event. They are used during court cases and investigations to describe what they saw, heard, smelled, felt, and so on. A witness can corroborate evidence that was gathered from video, computer logs, captures, and other technical evidence.

Track Man Hours and Expenses: Every action that is taken by the investigators of an incident response team should be logged and documented so as to act as a proper audit trail. Investigators normally need to sign in before being allowed access to an affected area or computer. The total man hours, sign in and sign out times, as well as any expenses incurred should be thoroughly documented. Man hours might be tracked through a computer system. For more information on the log in of users, and policies governing how and when they can log in see Chapter 9.