CS 393 Mid-term Answer Key

1. What is a “protected computer”? What amount of monetary damage to a protected computer system is necessary to violate the Computer Fraud and Abuse Act (18 USC 1030)? What factors can be included in this cost?

A computer used by the federal government or a financial institution, or one that affects interstate or foreign commerce (an Assistant US Attorney in Idaho said this could be any computer attached to the internet!). You only need $5000 (raised from $1000 in 1996) in one year for any computers affected in your organization. You can include anything that is a direct result of the attack(s) – the cost to investigate, the cost to determine damage to system(s), the cost to restore data, programs, files, etc., the cost to reload and/or reconfigure damaged software, and the cost to patch and re-secure systems.

2. What is a cryptographic checksum and how is it used?

A cryptographic checksum (aka message digest or fingerprint) is created by applying an algorithm to a file resulting in a string of bits called a hash value. While not unique (it is a fixed length string), it is commonly used as a “trip wire” to detect changes to critical system files.

3. How would you go about creating two **different** files with the same MD5 signature?

This is something you might want to do to counter an “expert witness” claim that MD5 signatures are like human fingerprints and no two are identical. It is a 128-bit checksum, so there are “only” 2^128 (or 3.4x10^38) possible values. Using ASCI (with say 127 characters) gives 9.3x10^39 possible 19 character files. Therefore, some of these files must have the same MD5 signature. So, it is *possible*. But once you start throwing around math like this, a jury might not understand it. If you can produce two files and have the “expert witness” say they have the same MD5 sig, it would completely discredit his/her testimony.

MD5 claims to be one-way (and nobody in the class found any claim otherwise) so it is extremely unlikely that we can create 2 different files from a given MD5 sig. That leaves us with two methods: create different files until any two have the same MD5 sig or start with a file and created different ones until the sigs match. More details about the pros/cons of each sounds like a homework problem …

4. Compare and contrast these methods for system logging: logging to a remote host, logging to a write-once media and logging to a line printer.

All three of these techniques put a copy of the logs in another location, while also writing to the normal place on the host. This results in an attacker needing to compromise another host or physical access to the resource.

	Remote logging	**Write-once media**	**Line printer**
Can combine logs of multiple hosts	**Trivial**	**N/A**	**N/A**
Unauthorized modifications	**Must compromise logging host**	**Requires physical access ***	**Requires physical access**
Detection of modifications	**Hard**	**Easier**	**Easiest**
Searching logs	**Most flexible**	**Less flexible**	**Cumbersome**
Maintenance	**Rotate logs and/or backup**	**Buy, replace and store CD-Rs**	**Buy, replace and store LOTs of paper**
Evidence for court	**Usual electronic file problems**	**Better – since you can't modify**	**Best – it is not electronic**
Reliability	**Usual computer issues + network**	**+ CD writer and media problems**	**+ Printer and toner/ ribbon problems**

5. What are the danger(s) involved in doing a live system review before making a forensic copy of the system disk drive(s)?

By conducting a live system review you WILL change some data on the disk. The evidence from this disk WILL NOT be as credible as if you pulled the plug and imaged the disk. This does not mean (as a few people said) that it will be thrown out of court or can't be used. ANYTHING can be evidence. It is the responsibility of the jury to determine the quality of the evidence (see also #9 answer). The things that you have to protect against (since the defense should point these out) are:

- **You could have changed something accidentally**
- **You could have planted evidence**
- **You could have deleted something that would exonerate the defendant**

You also have the problem that the owner of the system may have planted bombs that destroy data and/or changed some system utilities so what you are gathering during a live review are meaningless.

6. Describe in detail how you can hide data in the slack space. What do you need to do to keep it from being overwritten? From being discovered?

The easiest way is to find a utility such as bmap (Linux) that will do it for you. Or you can create a file equal to the size of a cluster, delete it and create a 1 byte file in the same cluster. How? In C, fopen(), write(secret), fflush(), rewind(), write(byte), fclose(). You can also find ways to access specific blocks/clusters on the disk. To keep from being overwritten, you can make the 1 byte file read-only. You can also mark the disk blocks as bad using a disk utility, but then you have to create or find utilities to read bad blocks. Yet another method is to write data and then re-partition your drive so these blocks are not part of an active file system. We need to assume that an investigator has access to software such as EnCase, so they will find the bits. We can either encrypt them so they can't determine the contents or hide the data in images stenography (or the like). All of this is very system-dependent.

7. What is the US Computer Assistance Law Enforcement Act? Does a department computer lab manager need to worry about it?

This question was not graded. There was a proposed Computer Assistance act in addition to a Communications Assistance act (commonly known as CALEA). In the future, don't use "no results in google" as an argument that is doesn't exist. ☺

8. Give the steps to seize a disk drive from a PC in a way that will stand up in court.

Detailed note taking is an absolute requirement. You have to be prepared to (under oath) recreate everything that happened during the seizure. In addition, videotaping the process when possible is highly recommended. These steps assume you have the legal right to seize the disk:

- **take pictures (plus video if possible) of the overall scene**
- **photograph the system configuration (peripherals, cables, S/Ns, …)**
- **document and label all connections**
- **pull the plug (if system is currently on)**
- **remove the hard drive (noting the model number, S/N, settings, etc)**
- **make two images of the drive using software (e.g. EnCase) on a portable forensics workstation**
- **verify both images**
- **put drive in evidence bag, seal and sign to start the chain-of-custody**
- **complete an inventory list of all items that will be removed from the scene**

9. A forensic copy was made before sealing the original disk drive in an evidence bag. The copy has been damaged and another one needs to be created. What should you do?

The choice is to not use the evidence or open the bag and re-image the disk (with the associated risks). (Also note that this is the situation where the defense wants the disk imaged by a third-party lab to verify things.) The first point is to document everything – we should be able to (under oath) reconstruct all of the events that took place. It would also be a good idea to videotape this process and invite the defense to observe (if possible). Break the seal and remove the disk. Run a checksum (the same process we did when originally seizing it) and compare to our writtern notes/printed checksums. If something doesn't match – STOP before making things worse. If they match, then the drive hasn't been tampered with and we can make new images. Once finished and verified, we place the disk and old evidence bag into a new evidence bag and seal. The old evidence bag contains the chain-of-custody to this point, so we need to keep it. Note that this is not an ideal situation, but it is better to re-image and let the jury decide than to just not use the evidence.

10. What actions are made illegal in the UA BOR Regulations on Information Resources?

Nothing is made illegal by the regulations. Some activities discussed might be illegal, but this is because there are state and federal laws against these activities.

11. How many different combinations are possible for 10 character passwords (without salt) where the characters are limited to [a-zA-Z0-9]? How many attempts per second are needed to brute-force this in 1 week? Is there a system out there that can do it?

Possible characters = 26+26+10 = 62
Possible 10 character passwords = 62^10 = 839,299,365,868,340,224 = 8.4x10^17
Seconds in one week = 7 days * 24 hours * 60 minutes * 60 seconds = 604,800
62^10 / 604,800 = 1,387,730,432,983 attempts per second in a week (worst-case)

Possible systems. The fastest system on www.top500.org is the Earth Simulator at 35.86 teraflops. Each attempt would have to be less than 26 floating-point operations. Very unlikely – especially since this machine was designed for a different problem and the performance is not likely to be 36 teraflops on this problem. On the desktop, the fastest speed I found was about 1 millions tries/sec, which would require about 1300 PC/workstations.

12. A case example on page 61 in Casey describes how the Melissa virus author was discovered via an Ethernet address hidden in a MS Word document. Give the pros/cons of this from the viewpoint of a forensics investigator. Should all documents contain this information (i.e. do the pros outweigh the cons)?

The question asked for pros/cons from the forensics investigator's viewpoint. This makes any privacy/big brother/etc points moot. (They are important and we have/will discuss in class, but that is not what the question here.)

Just about everyone agreed that this is more evidence available for the investigator. A crucial part of this is *how reliable* is this evidence. If I have a file with your MAC address, that *does not* mean that you created the file. It means that the file was created on your system OR somebody changed that to your MAC address using a hex/text editor. In other words, it would have about the same level of credibility as the return address on an envelope or e-mail message. As an investigator, you should follow this to the MAC address and look for corroborative evidence. This also provides the "smart" criminal with a way to create spurious "leads" and anyone to cause a "friend" to be harassed by law enforcement.

If I was on a jury and the only evidence you presented was this file has the defendant's MAC address in it, I wouldn't convict. I would also have strong words for the media during my 15 minutes of fame. Now, what if there was a mechanism to ensure that every file on a system was tagged with an ID and there was no way to change it? Look up Palladium. We'll talk about that after the presentations.