CS-480—Senior Seminar
Study questions for *Computer Forensics*
Fall '02

Chip Yeakey

"Computer Forensics: High-Tech Law Enforcement". Garber, Lee. *IEEE Computer*. January 2001. pg.22-27.

"Forensic Methodologies: A computer Forensic Professional's Compass". Kuchta, Kelly J. *Information Systems Security* January/February 2002

"EPIC analysis of New Justice Department Guidelines on Searching and Seizing Computers". `http://www.cpsr.org/cpsr/privacy/epic/guidelines_analysis.txt`

1. How might computer forensics make it easier for law enforcement to do their job? How does it change the balance between police powers and personal rights?

2. Is having to obtain a warrant sufficient to protect personal privacy in this new field? Is it possible to have a warrant that is pointed enough to limit searching to a subset of information on a drive? What does the EPIC analysis of the federal guidelines have to say about this?

3. In the side note "Nerd with a gun" in the *Computer* article how does the last sentence make you feel about this field? Does it seem that a single individual is getting too much power without a sufficient check system? What mechanisms are there to prevent abuse in a case like this?

4. Is publishing this info about how data is found even after "deletion" dangerous since it can inform criminals how to better avoid leaving evidence? Were you a "perpitrator" how would this article influence your choice of operating systems?

5. Garber mentions the difficulty of finding, on MSWindows systems, files that do not have standard file extensions. How do unix systems typically determine file types? What is the standard unix utility that does what he was trying to do?

6. How are modifications to a paper document detected? Is it possible to detect modifications to magnetic media in the same way? How is it that the integrity of data on magnetic media can be assured? Are the procedures outlined in the Information Systems Security article and the EPIC analysis of the Justice Department guidelines sufficient to assure the integrity of data on magnetic media? In light of its mutability, how is it that data from confiscated magnetic media can be admitted as evidence?

7. What do you think about useing a Linux cluster to break encrypted files? What does this plan have to say about the degree of expertise of the investigators.

8. How do the step by step recomendations from the Justice Department affect the investigators in this article? Do they seem to be following them and is it a problem that they are not required to do so? Do the guidelines have any power at all without requiring investigators to follow them?

9. Knowing all we do, is it realistic for this type of data to hold up in court?