

Hand in a stapled, printed copy with your answers.

Homework: /SI110/Cyber Operations/Forensics

1) Read the following article carefully. Read it carefully, don't just skim! You should see a lot of references to things we've covered in this course.

<http://www.wired.com/threatlevel/2011/12/manning-assange-laptop/>

a. What poor password practices did Manning follow that allowed digital forensics experts to recover more information than would otherwise have been possible?

b. What information did the forensics analysis find by examining the SSH logs on Manning's computer?

2) Suppose some mysterious hacker steals rona's password file and posts it on the infamous hacker website wookieleaks.org and, furthermore, posts a link to that wookieleaks posting on Dr. Stahl's SI110 messageboard: rona.cs.usna.edu/~stahl/www/msg/mb.html. This scenario involves Midn Bad (m159999) and Midn Sap (m158888).

Midn Bad does the following:

- 1) pulls up Dr. Stahl's message board
- 2) follows the link to the wookieleaks page copy&pasting Midn Sap's username and password hash into a file on his laptop
- 3) goes to passwordcrack.com, enters Midn Sap's password in a form field, submits (the site then returns a page displaying the cracked password)
- 4) ssh's to his own rona account
- 5) gives the command `su - m158888` which allows him to "switch user" to Midn Sap, since he now knows Sap's password.
- 6) Finally ... he deletes all of Midn Sap's files.

Describe at least four different pieces of forensic evidence that should exist after this scenario plays out. For each: describe what it is, where it exists, and why it is there!

what it is	where it exists	why it is there