**GROUP 10**

**Submitted to:**

**Asst. Professor Waseem Iqbal**

**Submitted by:**

**Abdul Wahid**

**Muhammad Hamad**

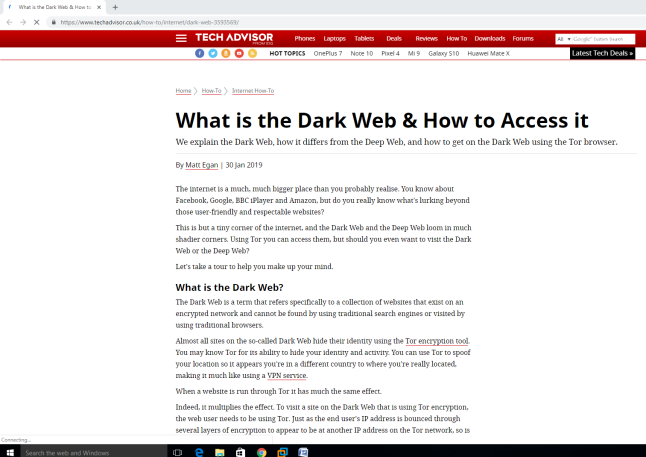
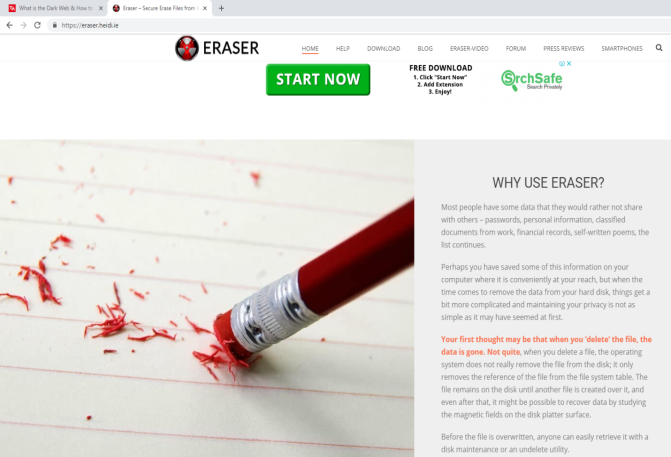
**Crime Investigation scene**

Group-10 working on a crime investigation scene trying to decrypt file using passwords. There are two evidences, one is digital in the system and second one in the crime enviornment.

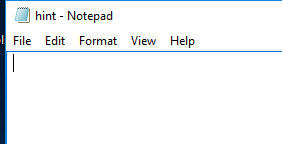
**Crime scene**

* One computer system found
* Two links opened in the chrome browser
* <https://www.techadvisor.co.uk/how-to/internet/dark-web-3593569/>
* <https://eraser.heidi.ie/>
* One empty notepad file named “hint.txt” opened

**Snapshots of open links**



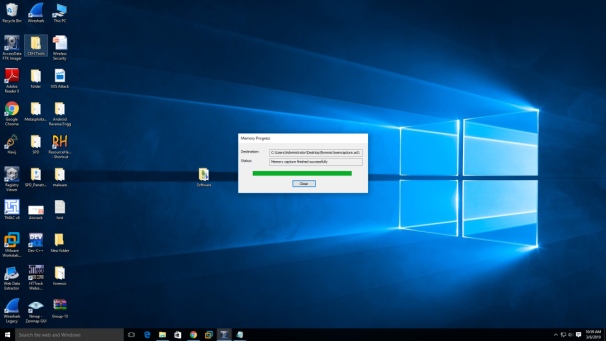
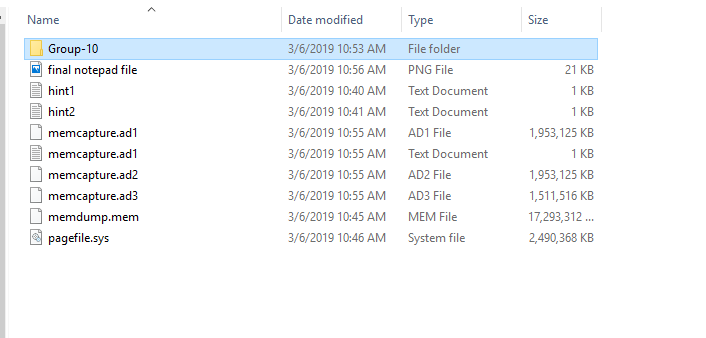
**Snapshots of open notepad file**



**Steps as a first responder**

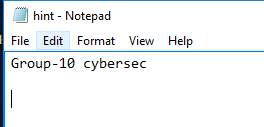
1. We did not want to contaminate the evidences so we acquire the image of volatile memory and page file.

**Snapshots of acquired memory image**



1. We save as “hint.txt” with different file name
2. Then we undo this new notepad file and extract the information.

**Snapshot of extracted information**

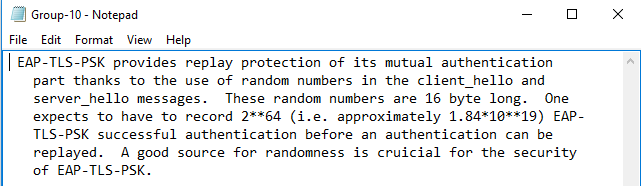


1. Then we tried extracted information as password on this file and successfully extract the file.



1. After successfully extracting contents of zip file, we came to know that there is an encrypted file within a file.
2. After that we try some random password related to existing environment but unable to crack.
3. Then we started looking for physical environment evidence
4. At last we finally found a slip on which password was written through which we decrypt file within a file.
5. We found the following contents shown in the snapshot

**Snapshot of extracted contents of file within a file**



**Conclusion**

1. Attacker trying to replay the session
2. Attacker reading articles about dark web and tor to spoof location

THE END