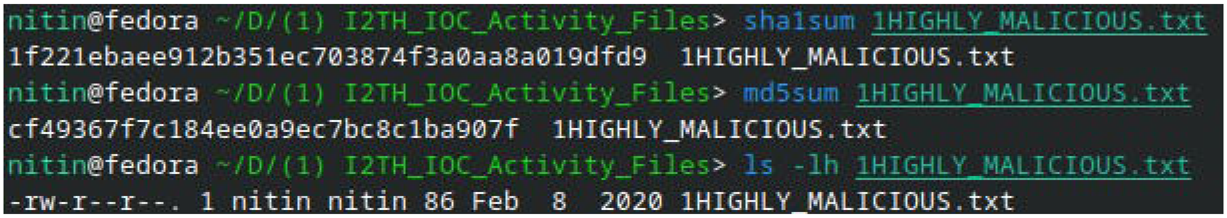
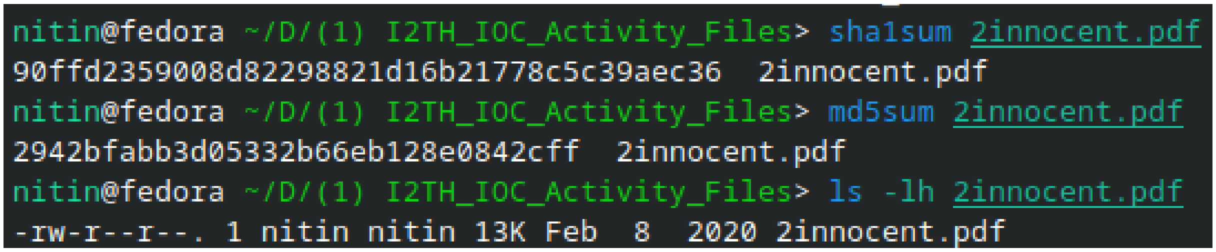
Generating Indicators [Activity]

File Beginning With “1”
1.What is the SHA1 hash value of this file?
1f221ebaee912b351ec703874f3a0aa8a019dfd9
2.What is the MD5 hash value of this file?
cf49367f7c184ee0a9ec7bc8c1ba907f
3.What is the file size (in bytes, with no separators such as “,”) of this file?
86
4.What is the full file name (and extension) of this file?
1HIGHLY_MALICIOUS.txt



```
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> sha1sum 1HIGHLY_MALICIOUS.txt
1f221ebaee912b351ec703874f3a0aa8a019dfd9  1HIGHLY_MALICIOUS.txt
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> md5sum 1HIGHLY_MALICIOUS.txt
cf49367f7c184ee0a9ec7bc8c1ba907f  1HIGHLY_MALICIOUS.txt
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> ls -lh 1HIGHLY_MALICIOUS.txt
-rw-r--r--. 1 nitin nitin 86 Feb  8  2020 1HIGHLY_MALICIOUS.txt
```

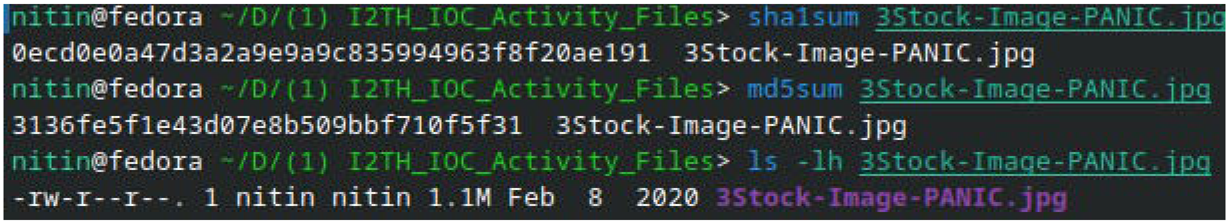
File Beginning With “2”
1.What is the SHA1 hash value of this file?
90ffd2359008d82298821d16b21778c5c39aec36
2.What is the MD5 hash value of this file?
2942bfabb3d05332b66eb128e0842cff
3.What is the file size (in bytes, with no separators such as “,”) of this file?
13,264
4.What is the full file name (and extension) of this file?
2innocent.pdf



```
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> sha1sum 2innocent.pdf
90ffd2359008d82298821d16b21778c5c39aec36  2innocent.pdf
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> md5sum 2innocent.pdf
2942bfabb3d05332b66eb128e0842cff  2innocent.pdf
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> ls -lh 2innocent.pdf
-rw-r--r--. 1 nitin nitin 13K Feb  8  2020 2innocent.pdf
```

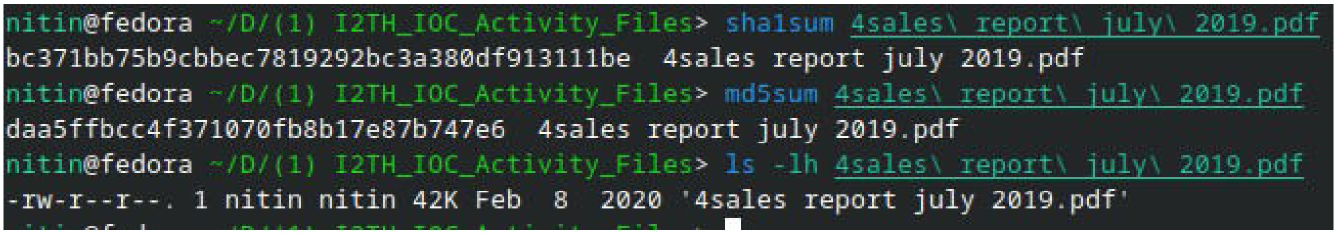
File Beginning With “3”
1.What is the SHA1 hash value of this file?
0ecd0e0a47d3a2a9e9a9c835994963f8f20ae191
2.What is the MD5 hash value of this file?
3136fe5f1e43d07e8b509bbf710f5f31
3.What is the file size (in bytes, with no separators such as “,”) of this file?
10,66,208

4.What is the full file name (and extension) of this file?
3Stock-Image-PANIC.jpg



```
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> sha1sum 3Stock-Image-PANIC.jpg
0ecd0e0a47d3a2a9e9a9c835994963f8f20ae191  3Stock-Image-PANIC.jpg
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> md5sum 3Stock-Image-PANIC.jpg
3136fe5f1e43d07e8b509bbf710f5f31  3Stock-Image-PANIC.jpg
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> ls -lh 3Stock-Image-PANIC.jpg
-rw-r--r--. 1 nitin nitin 1.1M Feb  8  2020 3Stock-Image-PANIC.jpg
```

File Beginning With “4”
1.What is the SHA1 hash value of this file?
bc371bb75b9cbbec7819292bc3a380df913111be
2.What is the MD5 hash value of this file?
daa5ffbcc4f371070fb8b17e87b747e6
3.What is the file size (in bytes, with no separators such as “,”) of this file?
43,002
4.What is the full file name (and extension) of this file?
4sales report july 2019.pdf



```
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> sha1sum 4sales\ report\ july\ 2019.pdf
bc371bb75b9cbbec7819292bc3a380df913111be  4sales report july 2019.pdf
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> md5sum 4sales\ report\ july\ 2019.pdf
daa5ffbcc4f371070fb8b17e87b747e6  4sales report july 2019.pdf
nitin@fedora ~/D/(1) I2TH_IOC_Activity_Files> ls -lh 4sales\ report\ july\ 2019.pdf
-rw-r--r--. 1 nitin nitin 42K Feb  8  2020 '4sales report july 2019.pdf'
```

Additional Questions
1.In IOCe, when trying to add new IOC values, what is the first property available under the Network heading? (Similar to how we selected FileItem properties)
Network DNS
2.In IOCe, there are option to add values from email, Snort, and Task Items, true or false?
True
3.What does IOC stand for?
Indicators of Compromise
4.Which of the following are examples of IOCs? (Choose any that apply)
Email Sending Address, File Name, File Hash, String