Digital Forensics report

Q1: As a forensic examiner, you are required to analyze the given capture file using Wireshark and answer the following questions in your report:
https://drive.google.com/file/d/16GR5hpLa-Jlo7HcJiN2BFAIMLO0I3IG5/view?usp=sharing

1) Is this an Attack? Justify your answer.
Distributed Denial of service (DDOS) attack , because I see multiple IP Addresses sending requests to this IP 10.0.64.129 in order to to overwhelm the server

2) Discover the source geo IP country? (do your own research)
source geo IP used to map ip address to country ,city and ASN they are public available for every one
source geo IP countries are
1-Argentina in city of Buenos Aires
2-Belgium in city of Brussels
3-Canada
4-China in both cities Wenzhou Tianjin and others
5- Colombia
6- Croatia in city of Split and others
7- Germany in cities of Dusseldorf ,Bonn ,Frechen ,Noerten-Hardenberg ,Nassenfels,Berlin,Cologne,Wesseling,Remagen,Stuttgart,Berlin,Bad Freienwalde ,Golzow,Bad Oeynhausen,Bergisch Gladbach,Rhede,Karlsruhe,Düsseldorf, Dortmund,Werl,Frankfurt am Main,Erlangen,Ludwigshafen am Rhein,Gaggenau and others
8-India
9-Israel in cites of Tel Aviv,Ramat Gan , Ness Ziona and others
10- Jaban in city Tokyo and others
11- Mexico in cites Campeche and Solidaridad
12- Russia
13- Slovenia
14-Sweden in city of Degerfors
15- Switzerland in city of Adliswil
16- The Netherlands
17-Turkey in cities of Guzelbahce , Ankara and others
18-United Kingdom in cities of London ,Acton ,Willenhall ,Barnet and others
19-United States in cities of Chandler,Baton Rouge,San Antonio,Ashburn,Baton Rouge,Charlottesville,Vinita,Omaha,Muncie,Oakland,Indianapolis,Southborough, Tappahannock,Walla Walla,Benton City,Austin,Dallas

3) How many countries are involved?
19 countries involved in this attack

4) Choose any of the identified locations in Question 2, how many packets come from the location you choose? Mention the location and the number of packets.
Israel came from it 23 packets and from each city
Ness Ziona came from it 2 packets
Ramat Gan came from it 14 packets
Tel Aviv came from it 7 packets

5) Are these packets made by a bot or normal devices?

bot , because we observed a large number of requests coming from a limited set of IP addresses. This indicates a coordinated attack from a botnet.

6) Extract the TTL of the packets and show how it can be used in discovering attacks?

all packet have TTL value 254

Normal TTL Behavior: Every packet has a TTL value, which represents the maximum number of hops it can traverse. As the packet moves through routers, the TTL decreases by one at each hop.

Baseline Establishment:Create a baseline or normal range of TTL values for your network under regular conditions. This baseline reflects the typical number of hops between different parts of your network.

Anomaly Detection: Monitor TTL values in real-time. Sudden deviations from the established baseline could indicate a problem.

TTL Exhaustion: In a DoS attack, attackers may flood the network with packets, deliberately setting TTL values to very low numbers. This causes routers to quickly discard the packets, generating a large number of ICMP Time Exceeded messages.

Detection of Unusual Patterns: Look for unusual patterns, such as a flood of packets with TTL values outside the normal range. This could suggest an attack.

Thresholds and Rate Limiting: Implement thresholds for acceptable TTL values and consider rate limiting. If incoming packets exceed expected limits or if TTL values fall outside predefined thresholds, it may indicate a DoS attack.

Q2: As a forensic examiner, you received a storage image file with its SHA256 hash code.

1) Forensically speaking, what should be done before attempting to the storage image file?

Calculate hash values of the acquired storage image file. Compare these hash values with the hash values of the original device to ensure the integrity of the forensic image. This verification process helps establish that the acquired image is an identical copy of the original.

2) Is this file considered intact? Justify your answer.

file is intact because ,I used Get-FileHash command to get the value of image file is AD2F61D34627D5687583A22A410721F2B2B5B52A753905D474F08E1747225598 and it is algorithm is **SHA256** , which they are the same value hash and algorithm of original data.

3) Load the image file with Autopsy and analyze the output of the extraction. (show screenshots of the configuration)

Autopsy_configueiation
Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name: charlie-2009-11-12
Base Directory: D:\Viruse project do not open\semester 5 new\A) Projects\DF_projrct\
Browse
Case Type: Single-User Multi-User
Case data will be stored in the following directory:
:\Viruse project do not open\semester 5 new\A) Projects\DF_projrct\charlie-2009-11-12
< Back
Next >
Finish
Cancel
Help
Search
ENG
11:27:21 AM
12/6/2023

Autopsy_configueiation
Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: 1
Examiner
Name: mohamed
Phone: 01096616978
Email:
Notes:
Organization
Organization analysis is being done for: Not Specified
Manage Organizations
< Back
Next >
Finish
Cancel
Help
Search
ENG
11:28:03 AM
12/6/2023

Autopsy_configueiation
Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Solr Keyword Search Service Opening Case Resources
Opening text index. For large cases this may take several minutes.
Cancel
3 items
Search
ENG
11:28:37 AM
12/6/2023

Autopsy_configueiation
charlie-2009-11-12 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help
4 items
Search
ENG
11:29:04 AM
12/6/2023

Autopsy_configueiation
charlie-2009-11-12 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help
5 items
Search
ENG
11:29:29 AM
12/6/2023

Autopsy_configueiation
charlie-2009-11-12 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
D:\Viruse project do not open\semester 5 new\A) Projects\DF_projrct\charlie-2009-11-12.E01
Browse
Ignore orphan files in FAT file systems
Time zone:
(GMT+2:00) Africa/Cairo
Sector size:
Auto Detect
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
NOTE: These values will not be validated when the data source is added.
< Back
Next >
Finish
Cancel
Help
7 items
Search
ENG
11:31:13 AM
12/6/2023

Autopsy_configueiation
charlie-2009-11-12 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, rec..
Global Settings
< Back
Next >
Finish
Cancel
Help
7 items
Search
ENG
11:32:00 AM
12/6/2023

Autopsy_configueiation
charlie-2009-11-12 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
Processing data source and adding it to a local database. File analysis will start when this finishes.
Status
*This process may take some time for large data sources.
< Back
Next >
Finish
Cancel
Help
No known hash set.
Known file search will not be executed.
8 items
Search
ENG
11:32:43 AM
12/6/2023

charlie-2009-11-12 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Data Sources
1 Results
Save Table as CSV
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help
Analyzing files from charlie-2009-11-12.E01
0%
(3 more...)
9 items

charlie-2009-11-12 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Data Sources
1 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
charlie-2009-11-12.E01_1 Host
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Metadata (1)
Shell Bags (22)
USB Device Attached (7)
Analysis Results
Encryption Detected (1)
Extension Mismatch Detected (7)
OS Accounts
Tags
Score
Reports
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
12/06/23 11:33:29 EET Encrypted files in archive detected.
Some files in archive: internalList.zip are encrypted. Embedded File Extractor extractor was unable to extract all files from this archive.
Analyzing files from charlie-2009-11-12.E01
1%
(3 more...)
10 items

4) You are asked to write a report about the disk image describing all the details of the extracted data.

in Data artifacts , firstly analyzing communication accounts in emails in msg_43.txt, we found a spamed mail blocked by spam Firewall was send to webmaster@python.org it has attached file with named auto__mail.python.bat as you see in text part in bellow photo

charlie-2009-11-12 - Autopsy 4.21.0
Listing
Table Thumbnail Summary
3 Results
Save Table as CSV
Source Name S C O Account Type ID Data Source
msg_25.txt 0 EMAIL mailer-daemon@zinfandel.lacita.com charlie-2009-11-12.E01
msg_25.txt 0 EMAIL linuxuser-admin@www.linux.org.uk charlie-2009-11-12.E01
msg_43.txt 0 EMAIL webmaster@python.org charlie-2009-11-12.E01
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Extracted Text Translation
Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text
BANNED FILENAME ALERT
Your message to: xxxxxxx@dot.ca.gov, xxxxxxxxxxxx@dot.ca.gov, xxxxxxxxx@dot.ca.gov, xxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxx@dot.ca.gov, xxxxxx@dot.ca.gov, xxxxxxxxxxxxxxx@dot.ca.gov, xxxxxxxxxxxxxxx@dot.ca.gov, xxxxxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxxxxxxxxxxx@dot.ca.gov, xxxxxxxxxxxxxxx@dot.ca.gov, xxxxxx

secondly analyzing communication accounts in emails in msg_25.txt we found mail returned due to Too many hops 19 and we have max 17 mail was send from linuxuser-admin@www.linux.org.uk to scoffman@wellpartner.com

in below pictures we see installed program on this hard drive we see java ,python windows security updates ,firefox , thunderbird and many more

charlie-2009-11-12 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Installed Programs
96 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Program Name Date/Time Data Source
software 1 Hotfix for Windows XP (KB970653-v3) v.3 2009-11-09 02:07:56 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB971657) v.1 2009-11-09 02:07:51 EET charlie-2009-11-12.E01
software 1 Update for Windows XP (KB973815) v.1 2009-11-09 02:07:45 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB960859) v.1 2009-11-09 02:07:39 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB973507) v.1 2009-11-09 02:07:32 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB973354) v.1 2009-11-09 02:07:26 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB956744) v.1 2009-11-09 02:07:20 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB973869) v.1 2009-11-09 02:07:13 EET charlie-2009-11-12.E01
software 1 Security Update for Windows Media Player (KB973540) 2009-11-09 02:07:06 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB971557) v.1 2009-11-09 02:07:00 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB971633) v.1 2009-11-09 02:06:55 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB970238) v.1 2009-11-09 02:06:48 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB968537) v.1 2009-11-09 02:06:42 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB961501) v.1 2009-11-09 02:06:36 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB959426) v.1 2009-11-09 02:06:29 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB960803) v.1 2009-11-09 02:06:23 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB952004) v.1 2009-11-09 02:06:17 EET charlie-2009-11-12.E01
software 1 Security Update for Windows XP (KB956572) v.1 2009-11-09 02:06:07 EET charlie-2009-11-12.E01
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
$$$PROTO.HIV
Avg
C07ft5Y
Classes
Clients
Gemplus
Google
InstalledOptions
Intel
Search
ENG
3:22:25 PM
12/11/2023

charlie-2009-11-12 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Installed Programs
96 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Program Name Date/Time Data Source
software 1 Intel(R) PRO Network Adapters and Drivers 2009-11-09 01:30:08 EET charlie-2009-11-12.E01
software 1 DXM_Runtime 2009-11-09 01:22:58 EET charlie-2009-11-12.E01
software 1 Branding 2009-11-09 01:22:36 EET charlie-2009-11-12.E01
software 1 PCHealth 2009-11-09 01:21:06 EET charlie-2009-11-12.E01
software 1 DirectAnimation 2009-11-09 01:20:57 EET charlie-2009-11-12.E01
software 1 NetMeeting 2009-11-09 01:20:57 EET charlie-2009-11-12.E01
software 1 AddressBook 2009-11-09 01:20:56 EET charlie-2009-11-12.E01
software 1 ICW 2009-11-09 01:20:56 EET charlie-2009-11-12.E01
software 1 OutlookExpress 2009-11-09 01:20:56 EET charlie-2009-11-12.E01
software 1 DirectDrawEx 2009-11-09 01:20:51 EET charlie-2009-11-12.E01
software 1 Fontcore 2009-11-09 01:20:51 EET charlie-2009-11-12.E01
software 1 IE40 2009-11-09 01:20:51 EET charlie-2009-11-12.E01
software 1 IE4Data 2009-11-09 01:20:51 EET charlie-2009-11-12.E01
software 1 IE5BAKEX 2009-11-09 01:20:51 EET charlie-2009-11-12.E01
software 1 IEData 2009-11-09 01:20:51 EET charlie-2009-11-12.E01
software 1 MobileOptionPack 2009-11-09 01:20:51 EET charlie-2009-11-12.E01
software 1 SchedulingAgent 2009-11-09 01:20:51 EET charlie-2009-11-12.E01
software 1 Connection Manager 2009-11-09 01:16:54 EET charlie-2009-11-12.E01
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
$$$PROTO.HIV
Avg
C07ft5Y
Classes
Clients
Gemplus
Google
InstalledOptions
Intel
Search
ENG
3:23:47 PM
12/11/2023

charlie-2009-11-12 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Installed Programs
96 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Program Name Date/Time Data Source
software 1 Security Update for Windows XP (KB923789) 2009-11-09 02:03:35 EET charlie-2009-11-12.E01
software 1 Update for Windows XP (KB898461) v.1 2009-11-09 01:51:27 EET charlie-2009-11-12.E01
software 1 Windows Genuine Advantage Validation Tool (KB892130 2009-11-09 01:51:22 EET charlie-2009-11-12.E01
software 1 Windows Genuine Advantage Validation Tool (KB892130 2009-11-09 01:51:21 EET charlie-2009-11-12.E01
software 1 AVG 9.0 2009-11-09 01:44:32 EET charlie-2009-11-12.E01
software 1 Microsoft Visual C++ 2005 Redistributable v.8.0.59193 2009-11-09 01:44:29 EET charlie-2009-11-12.E01
software 1 Intel(R) Extreme Graphics 2 Driver 2009-11-09 01:33:44 EET charlie-2009-11-12.E01
software 1 Intel(R) PRO Network Adapters and Drivers 2009-11-09 01:30:08 EET charlie-2009-11-12.E01
software 1 DXM_Runtime 2009-11-09 01:22:58 EET charlie-2009-11-12.E01
software 1 Branding 2009-11-09 01:22:36 EET charlie-2009-11-12.E01
software 1 PCHealth 2009-11-09 01:21:06 EET charlie-2009-11-12.E01
software 1 DirectAnimation 2009-11-09 01:20:57 EET charlie-2009-11-12.E01
software 1 NetMeeting 2009-11-09 01:20:57 EET charlie-2009-11-12.E01
software 1 AddressBook 2009-11-09 01:20:56 EET charlie-2009-11-12.E01
software 1 ICW 2009-11-09 01:20:56 EET charlie-2009-11-12.E01
software 1 OutlookExpress 2009-11-09 01:20:56 EET charlie-2009-11-12.E01
software 1 DirectDrawEx 2009-11-09 01:20:51 EET charlie-2009-11-12.E01
software 1 Fontcore 2009-11-09 01:20:51 EET charlie-2009-11-12.E01
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
$$$PROTO.HIV
Avg
C07ft5Y
Classes
Clients
Gemplus
Google
InstalledOptions
Intel
Search
ENG
3:23:08 PM
12/11/2023

we see on this drive windows xp is installed on this drive

we see in the below picture the previously connected devices which they are
5 different USB ROOT HUB , mouse and DELL keyboard

we see in the below pictures the stored web bookmarks

we see in below picture the downloads history

we see in below pictures some encrypted and suspected encrypted files so it is better if you collect this data before turning off computer if it was turned on

we see bad files caught by antivirus and trapped in quarantine

we see in prefs.js.moztmp file a evidence that user is attempting to send spam mails

here is a list of all users on the system and their roles

<u>For group 8: Charlie 2009-11-12 Disk</u>
https://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/drives-redacted/
<u>the SHA256 hash is:</u>
AD2F61D34627D5687583A22A410721F2B2B5B52A753905D474F08E1747225598