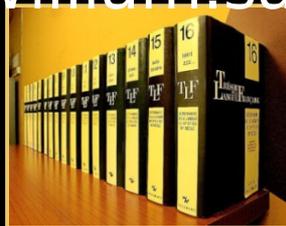


Analyse100010010100010011000110101010100011
 010011et010100110001110011010100101011
 1Traitement010100011000101011001101
 01001Informatique01010010110010C
 de0101la0100011101010001
 0101Langue01011100
 Française0101001
 0101010Analyse1
 10011000101010
 abcdefghijklmnopqrstuvwxyz
 abcdefghijklmnopqrstuvwxyz
 abcdefghijklmnopqrstuvwxyz
 abcdefghijklmnopqrstuvwxyz
 abcdefghijklmnopqrstuvwxyz
 abcdefghijklmnopqrstuvwxyz

PXE / WDS / ACRONIS

Journée 2RCE - 07 juin 2012 -
 Montbéliard
 William.sayer@atilf.fr



Sommaire

- Objectifs.
- Qu'est ce que PXE.
- Qu'est-ce que Windows Deployment Services.
- Architecture de déploiement de WDS.
- Avantages et Inconvénients.
- Fonctionnement de PXE et de WDS.
- Qu'est-ce que Acronis Backup & Recovery.



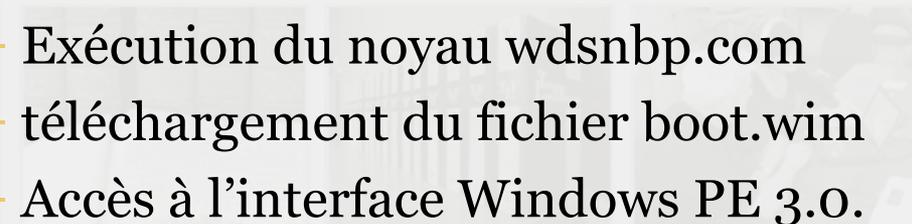
Objectifs

- Au sein de notre laboratoire :
 - Avec WDS :
 - déploiement de Windows 7 et bientôt Windows 8 sur les postes clients utilisant la technologie PXE.
 - Avec ACRONIS :
 - Sauvegarde et restauration des stations de travail spécifiques.
 - Sauvegarde serveur ou station en phase critique.
- Acronis et WDS, deux outils complémentaires.



Qu'est ce que PXE

- PXE (Preboot eXecution Environment) :
 - Norme créée par Intel.
 - Carte réseau compatible.
 - EEPROM : algorithme de recherche d'une adresse IP sur un serveur DHCP du réseau.
 - Activer fonction PXE dans le BIOS
 - Paramètre carte réseau.
 - Mode de démarrage en position 1.
 - WDSPXE/TFTP :
 - Exécution du noyau wdsnbp.com
 - téléchargement du fichier boot.wim
 - Accès à l'interface Windows PE 3.0.



Qu'est-ce que Windows Deployment Services

- C'est la version mise à jour de Remote Installation Services (RIS).
- C'est un rôle dans Windows server 2008 R2.
 - Serveur de déploiement (PXE – port 4011).
 - Serveur de transport (TFTP – port 69).
- Utilise le format d'image Windows pour traiter les images de démarrage, d'installation et de capture.
 - Métadonnées et fichiers sur partition.



Architecture de déploiement

■ Côté serveur :

- Windows serveur 2008 R2
- Serveur Active Directory
- Serveur DNS
- Serveur Windows Deployment Services
 - Serveur de déploiement PXE.
 - Serveur de transport TFTP.
 - Configurer l'option 60 : indiquer que ce serveur est serveur PXE.
 - Ne pas écouter le port 67.
- Serveur DHCP Microsoft
 - Option 60 → PXEClient.
 - Option 67 → Nom du fichier de démarrage : Boot\x86\wdsnbp.com

□ Côté client :

- Carte réseau ETHERNET compatible PXE
- BIOS configuré pour démarrer sur la carte réseau.
- Interface graphique Windows PE 3.0.

□ Côté gestion :

- Console mmc pour gérer le serveur, les images et les comptes d'ordinateurs clients.

Avantages et Inconvénients

■ Avantages :

- Natif sur Windows serveur 2008 R2.
- Rapidité de déploiement.
- Facilité de prise en main.
- Permet d'homogénéiser les configurations des postes de travail.
- Personnalisation des images déployées et installation de package via MDT.
- Intégration des drivers.

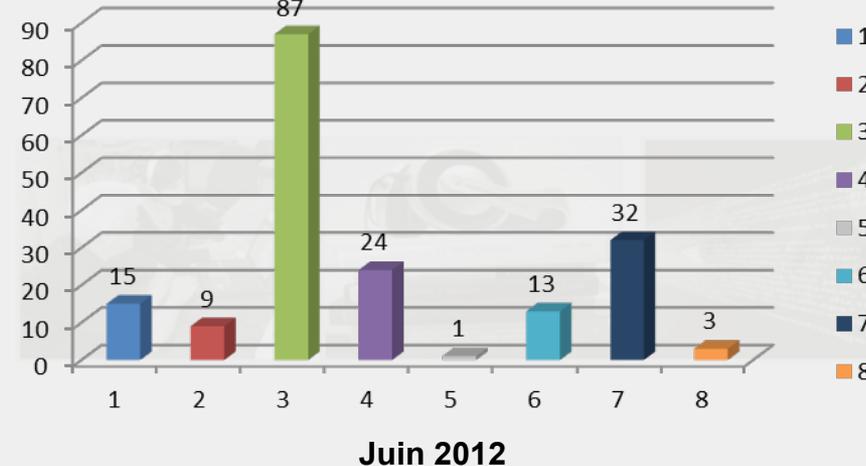
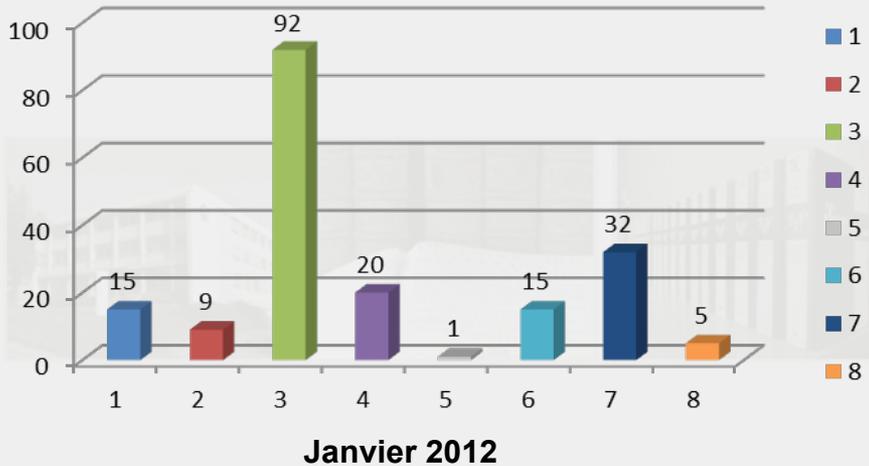
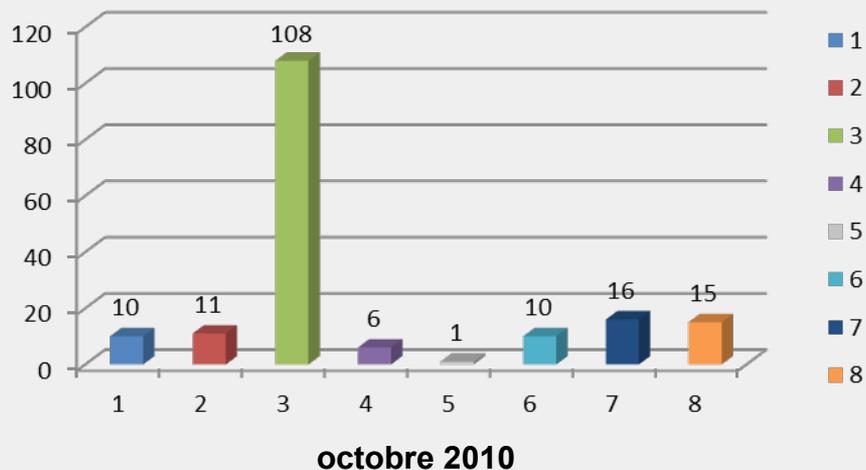
□ Inconvénient :

- Pas de déploiement pour Linux et MacOS X.
- Ne clone pas les disques.

Qu'est-ce que ACRONIS Backup & Recovery

- C'est une solution de reprise d'activité après sinistre.
 - Serveur de déploiement PXE.
 - Sauvegarde à chaud :
 - Les serveurs physique et virtuel sous Windows et Linux.
 - Sauvegarde et restauration
 - Des stations de travail Windows et Linux.
 - Gestion centralisée des postes de travail et des serveurs distribués.
 - Permet de traverser une image TIB.
 - Récupération fichiers ou dossiers.
 - Conversion d'une sauvegarde en machine virtuelle :
 - Vmware, Microsoft, Parallels ou KVM.
- C'est une solution robuste mais payante :
 - Au alentour de 700 € pour protéger un serveur.
 - Mise à jour du ou des serveurs Acronis.

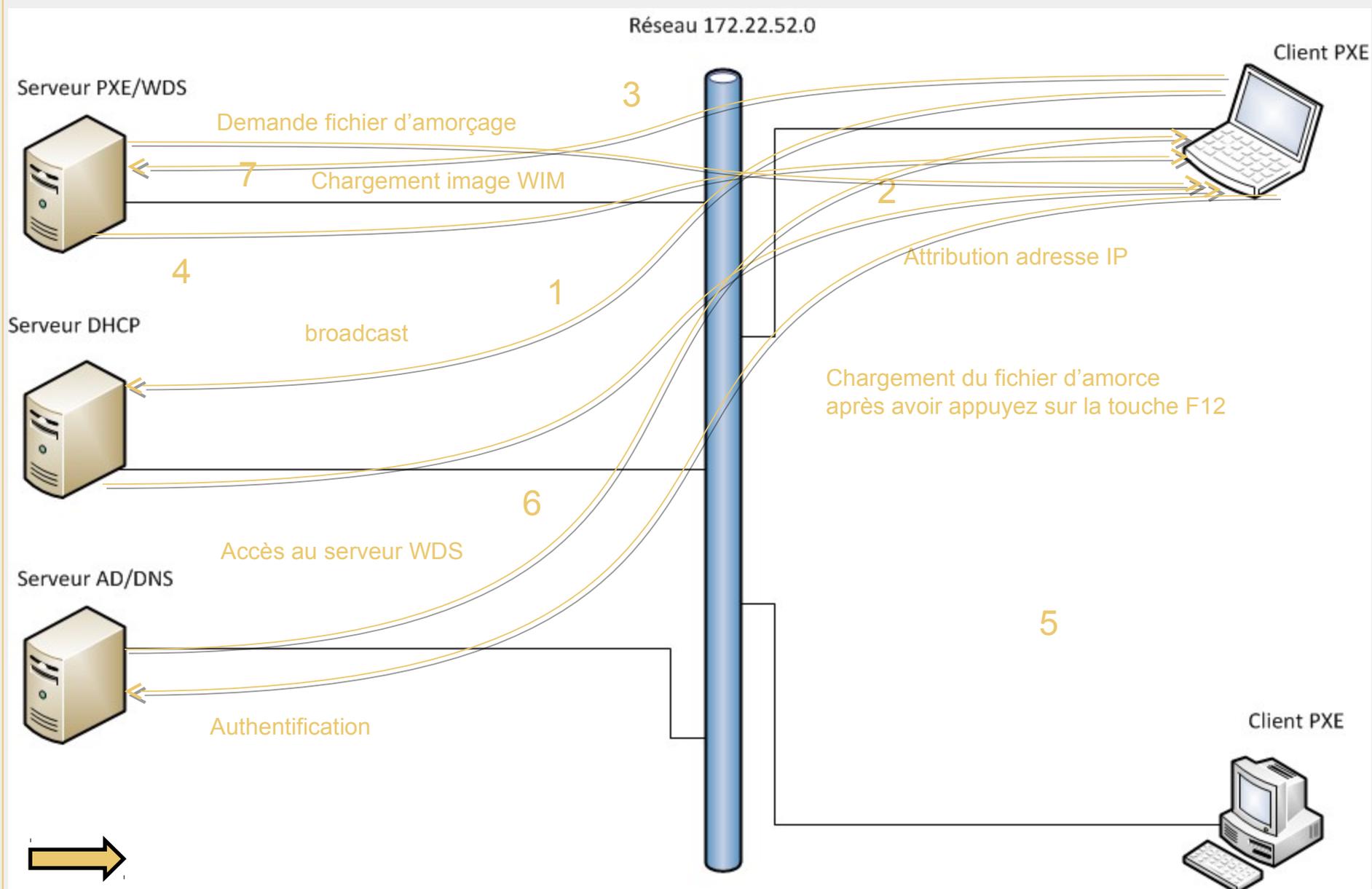
Conclusions



Des Questions ?



Fonctionnement de PXE et WDS



Trame ETHERNET connexion serveur PXE

Etape 1

14	8.809605	Intel_80:d2:92	Broadcast	ARP	60 who has 172.22.52.207? Tell 172.22.52.222
15	8.809621	Hewlett-_04:77:0d	Intel_80:d2:92	ARP	42 172.22.52.207 is at 00:1f:29:04:77:0d
16	8.809795	172.22.52.222	172.22.52.207	DHCP	590 DHCP Request - Transaction ID 0x1280d292
17	8.828833	Hewlett-_04:77:0d	Broadcast	ARP	42 who has 172.22.52.222? Tell 172.22.52.207
18	8.828981	Intel_80:d2:92	Hewlett-_04:77:0d	ARP	60 172.22.52.222 is at 00:11:11:80:d2:92
19	8.828994	172.22.52.207	172.22.52.222	DHCP	1066 DHCP ACK - Transaction ID 0x1280d292
20	8.829807	172.22.52.222	172.22.52.207	TFTP	78 Read Request, File: boot\x86\wdsnbp.com, Transfer type: octet, tsize\000=0\000
21	8.830322	172.22.52.207	172.22.52.222	TFTP	56 Option Acknowledgement, tsize\000=31124\000
22	8.830479	172.22.52.222	172.22.52.207	TFTP	60 Error Code, Code: Not defined, Message: TFTP Aborted
23	8.830700	172.22.52.222	172.22.52.207	TFTP	83 Read Request, File: boot\x86\wdsnbp.com, Transfer type: octet, blksize\000=1456\000
24	8.831142	172.22.52.207	172.22.52.222	TFTP	57 Option Acknowledgement, blksize\000=1456\000
25	8.831293	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 0
26	8.831561	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 1
27	8.831898	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 1
28	8.831953	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 2
29	8.832281	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 2
30	8.832328	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 3
31	8.832653	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 3
32	8.832708	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 4
33	8.833013	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 4
34	8.833123	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 5
35	8.833430	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 5
36	8.833513	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 6
37	8.833796	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 6
38	8.833842	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 7
39	8.834134	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 7
40	8.834177	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 8
41	8.834454	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 8



Trame ETHERNET Authentication sur le Domaine du serveur WDS

Etape 2

14	16.499810	Intel_80:d2:92	Broadcast	ARP	60	who has 172.22.52.207? Tell 172.22.52.222
15	16.499829	Hewlett-_04:77:0d	Intel_80:d2:92	ARP	42	172.22.52.207 is at 00:1f:29:04:77:0d
16	16.500089	172.22.52.222	172.22.52.207	TCP	66	49164 > microsoft-ds [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	16.500200	Hewlett-_04:77:0d	Broadcast	ARP	42	who has 172.22.52.222? Tell 172.22.52.207
18	16.500378	Intel_80:d2:92	Hewlett-_04:77:0d	ARP	60	172.22.52.222 is at 00:11:11:80:d2:92
19	16.500392	172.22.52.207	172.22.52.222	TCP	66	microsoft-ds > 49164 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
20	16.500755	172.22.52.222	172.22.52.207	TCP	60	49164 > microsoft-ds [ACK] Seq=1 Ack=1 win=65536 Len=0
21	16.501400	172.22.52.222	172.22.52.207	SMB	213	Negotiate Protocol Request
22	16.502028	172.22.52.207	172.22.52.222	SMB2	306	NegotiateProtocol Response
23	16.502613	172.22.52.222	172.22.52.207	SMB2	162	NegotiateProtocol Request
24	16.503104	172.22.52.207	172.22.52.222	SMB2	306	NegotiateProtocol Response
25	16.510991	172.22.52.222	172.22.52.207	SMB2	220	SessionSetup Request, NTLMSSP_NEGOTIATE
26	16.511341	172.22.52.207	172.22.52.222	SMB2	395	SessionSetup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
27	16.512511	172.22.52.222	172.22.52.207	SMB2	707	SessionSetup Request, NTLMSSP_AUTH, User: SYSTEM\administrateur, Unknown message type
28	16.513977	172.22.52.207	172.22.52.222	SMB2	159	SessionSetup Response, Unknown message type
29	16.514786	172.22.52.222	172.22.52.207	SMB2	170	TreeConnect Request Tree: \\172.22.52.207\IPC\$
30	16.514907	172.22.52.207	172.22.52.222	SMB2	138	TreeConnect Response
31	16.515491	172.22.52.222	172.22.52.207	SMB2	226	Ioctl Request DFS Function:0x0065
32	16.520606	172.22.52.222	172.22.52.207	ISAKMP	414	Unknown 243
33	16.521098	172.22.52.207	172.22.52.222	SMB2	131	Ioctl Response, Error: STATUS_NOT_FOUND
34	16.523711	172.22.52.222	172.22.52.207	SMB2	176	TreeConnect Request Tree: \\172.22.52.207\RemInst
35	16.523816	172.22.52.207	172.22.52.222	SMB2	138	TreeConnect Response
36	16.531881	172.22.52.222	172.22.52.207	DCERPC	210	Request: call_id: 3 Fragment: Single opnum: 3 ctx_id: 0
37	16.531999	172.22.52.207	172.22.52.222	DCERPC	206	Response: call_id: 3 Fragment: Single ctx_id: 0
38	16.534107	172.22.52.222	172.22.52.207	DCERPC	174	Alter_context: call_id: 4 Fragment: Single 1a927394-352e-4553-ae3f-7cf4aafca620 v1.0, NTLMSSP_NEGOTIATE
39	16.534889	172.22.52.207	172.22.52.222	DCERPC	350	Alter_context_resp: call_id: 4 Fragment: Single, NTLMSSP_CHALLENGE accept max_xmit: 5840 max_recv: 5840
40	16.536001	172.22.52.222	172.22.52.207	DCERPC	628	AUTH3: call_id: 4 Fragment: Single, NTLMSSP_AUTH, User: SYSTEM\administrateur
41	16.536026	172.22.52.222	172.22.52.207	DCERPC	390	Request: call_id: 4 Fragment: Single opnum: 0 ctx_id: 0 1a927394-352e-4553-ae3f-7cf4aafca620 v1
42	16.536077	172.22.52.207	172.22.52.222	TCP	54	5040 > 49163 [ACK] Seq=297 Ack=1031 win=256 Len=0



Trame ETHERNET sélection d'une image d'installation

Etape 3

70	23.243473	172.22.52.222	172.22.52.207	SMB2	362 Create Request File: Images\windows 7 Pro\win7proSoftATILF(x86).wim
71	23.243700	172.22.52.207	172.22.52.222	SMB2	298 Create Response File: Images\windows 7 Pro\win7proSoftATILF(x86).wim
72	23.244392	172.22.52.222	172.22.52.207	SMB2	146 Close Request File: Images\windows 7 Pro\win7proSoftATILF(x86).wim
73	23.244526	172.22.52.207	172.22.52.222	SMB2	182 Close Response
74	23.248535	172.22.52.222	172.22.52.207	SMB2	418 Create Request File: Images\windows 7 Pro\win7proSoftATILF(x86).wim
75	23.248752	172.22.52.207	172.22.52.222	SMB2	386 Create Response File: Images\windows 7 Pro\win7proSoftATILF(x86).wim
76	23.254111	172.22.52.222	172.22.52.207	SMB2	171 Read Request Len:4096 off:0 File: Images\windows 7 Pro\win7proSoftATILF(x86).wim
77	23.266736	172.22.52.207	172.22.52.222	SMB2	4234 Read Response
78	23.267494	172.22.52.222	172.22.52.207	TCP	60 49164 > microsoft-ds [ACK] Seq=3126 Ack=5051 win=65536 Len=0
79	23.267927	172.22.52.222	172.22.52.207	SMB2	171 Read Request Len:4616 off:4431872 File: Images\windows 7 Pro\win7proSoftATILF(x86).wim
80	23.268136	172.22.52.207	172.22.52.222	SMB2	4754 Read Response
81	23.268912	172.22.52.222	172.22.52.207	TCP	60 49164 > microsoft-ds [ACK] Seq=3243 Ack=9231 win=65536 Len=0
82	23.269117	172.22.52.222	172.22.52.207	TCP	60 49164 > microsoft-ds [ACK] Seq=3243 Ack=11011 win=65536 Len=0
83	23.270768	172.22.52.222	172.22.52.207	SMB2	322 Create Request File: Images\windows 7 Pro\res.rwm
84	23.270939	172.22.52.207	172.22.52.222	SMB2	298 Create Response File: Images\windows 7 Pro\res.rwm
85	23.271593	172.22.52.222	172.22.52.207	SMB2	146 Close Request File: Images\windows 7 Pro\res.rwm
86	23.271727	172.22.52.207	172.22.52.222	SMB2	182 Close Response
87	23.278092	172.22.52.222	172.22.52.207	SMB2	354 Create Request File: Images\windows 7 Pro\win7proSoftATILF(x86)
88	23.278233	172.22.52.207	172.22.52.222	SMB2	131 Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
89	23.278803	172.22.52.222	172.22.52.207	SMB2	394 Create Request File: Images\windows 7 Pro\win7proSoftATILF(x86).wim
90	23.278976	172.22.52.207	172.22.52.222	SMB2	330 Create Response File: Images\windows 7 Pro\win7proSoftATILF(x86).wim
91	23.280640	172.22.52.222	172.22.52.207	SMB2	378 Create Request File: Images\windows 7 Pro\Res.rwm
92	23.280834	172.22.52.207	172.22.52.222	SMB2	386 Create Response File: Images\windows 7 Pro\Res.rwm
93	23.281888	172.22.52.222	172.22.52.207	SMB2	171 Read Request Len:4096 Off:0 File: Images\windows 7 Pro\Res.rwm
94	23.282700	172.22.52.207	172.22.52.222	SMB2	4234 Read Response
95	23.283479	172.22.52.222	172.22.52.207	TCP	60 49164 > microsoft-ds [ACK] Seq=4684 Ack=14988 win=65536 Len=0
96	23.283909	172.22.52.222	172.22.52.207	SMB2	171 Read Request Len:2550 Off:8193339392 File: Images\windows 7 Pro\Res.rwm
97	23.284083	172.22.52.207	172.22.52.222	SMB2	2688 Read Response
98	23.284887	172.22.52.222	172.22.52.207	TCP	60 49164 > microsoft-ds [ACK] Seq=4801 Ack=18882 win=65536 Len=0



Fonctionnement plateforme WDS

